马耳他 Malta（MiCA）加密资产服务提供商（CASP）牌照

申请注册指南

Malta (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 提供专业讲解

✅ 点击这里可以下载 PDF 文件：关于仁港永胜

1）牌照名称 + 服务商署名 + 文档说明（PDF/附件索取提示）

牌照名称（MiCA）： Crypto-Asset Service Provider（CASP）授权/牌照（欧盟《MiCA》框架下）马耳他 Malta（MiCA）CASP 加密交易所牌照｜本文由仁港永胜唐生拟定讲解
主管机关（马耳他）： Malta Financial Services Authority（MFSA）
递交方式： MFSA Licence Holder Portal（LH Portal）线上递交（MFSA 已在 Crypto-Assets 专页集中发布 Rulebook、Forms、Returns、Outsourcing Notification 等）
交付说明（仁港永胜交付包可索取）：

- ✅《马耳他 MiCA-CASP 申请注册指南》（本文件）
- ✅《CASP Master Checklist（A–I）》
- ✅《Business Plan + Programme of Operations 模板包》
- ✅《AML/CFT 制度包 + STR 机制 + 风险评估》
- ✅《ICT/DORA 外包治理包 + 钱包安全/冷热钱包/多签/BCP/DR》
- ✅《RFI 补件应答包 + 面谈题库》

注：上述模板、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）。

2）牌照介绍与申请优势（MiCA 统一框架 + 马耳他优势）

2.1 MiCA 统一框架价值（"一张牌照，全欧盟护照"）

MiCA（Regulation (EU) 2023/1114）建立 CASP 的**统一授权、统一行为规则、统一持续监管框架**，并允许获授权后通过 **passporting（跨境通报）**向其他欧盟成员国提供服务（自由提供服务/设立分支）。

2.2 马耳他申请优势（适合"合规+机构合作+欧盟扩张"路线）

- **规则与表格"集中化、可下载、可递交"**：MFSA 在 Crypto-Assets 专页集中发布 MiCA Rulebook、CASP Return、Outsourcing Notification、Authorisation Application Forms 等材料，利于把申请包做成"可审查闭环"。
- **从 VFA 向 MiCA 迁移的制度衔接**：马耳他通过《Markets in Crypto-Assets Act》（Chapter 647）把 MiCA 落地到国内法体系，并推动 VFA 体系逐步退场；对既有主体设有过渡/转换路径。
- **持续监管"报表化"趋势明确**：MFSA 已推出 CASP Return 及其编制指引（含审计包、提交时限等），对"获牌后持续合规"要求更清晰。

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

- **MFSA**：马耳他金融服务监管机关，负责 MiCA 框架下的 CASP 授权、持续监管、报表与外包通知等。

3.2 核心法源与配套

- **欧盟主法：MiCA（EU 2023/1114）**：CASP 授权、治理、资本/保障、客户保护、外包与信息披露、跨境护照等。
- **马耳他实施法：Markets in Crypto-Assets Act（Chapter 647 / Act XXXVI of 2024）**：马耳他把 MiCA 体系落地并形成国内法衔接。
- **MFSA MiCA Rulebook / Guidance / Returns & Forms**：MFSA 对申请、持续义务、报表、外包通知等执行层要求的规则化文件与表格集合。
- **DORA（EU 2022/2554）**：金融实体 ICT 风险、第三方外包、韧性测试等要求（建议 CASP ICT 体系"直接按 DORA 标准建"以降低后期整改成本）。

4）申请条件概览（公司实体/实质经营/资本与保障/治理/技术/客户保护/护照/第三国招揽）

> 监管审查逻辑一句话：**"业务定性清楚 + 人与股东适任 + AML 可运行 + ICT 可审计 + 客户保护可验证 + 资本/保障可覆盖 + 外包可控"**。

4.1 公司实体与实质经营（Substance）

- 需在欧盟内设立法人实体并满足"有效管理地/关键管理与控制可被监管触达"。
- 建议在马耳他落地：办公地址、核心岗位（至少合规/MLRO/ICT 风险责任人）、董事会会议留痕与授权矩阵、可审计 IT 运维安排。

4.2 资本/审慎保障（Prudential Safeguards）

- 按 MiCA 的服务类型与风险确定最低资本与持续保障；通常还需要配套：三年财务预测、压力测试、运营风险覆盖说明、（如适用）保险或等效保障安排。

4.3 治理与三道防线

- 董事会/高管职责清晰；合规、风险、内审、ICT 风险等控制职能形成闭环；利益冲突、投诉、信息披露、营销审批等可留痕。

4.4 业务模型与"Programme of Operations"

- 必须明确拟提供的 CAS 服务类型、提供方式（平台/经纪/执行/托管/转账/投顾等）、客户类型（零售/专业）、收费与资金流/资产流路径、外包与关键供应商依赖。

4.5 技术安全与外包可控（对齐 DORA）

- 钱包（冷热分离、多签、密钥管理/HSM、权限分层、对账、审计轨迹）
- 安全测试（渗透测试、漏洞管理、变更管理）
- BCP/DR（RTO/RPO、演练证据）
- 外包治理（尽调、合同/SLA、审计权、退出/迁移方案）
  MFSA 已发布 **MiCA Outsourcing Notification Form**（外包通知表）作为监管抓手之一。

4.6 客户保护与第三国招揽边界

- 客户资产隔离、费用与风险披露、投诉机制、利益冲突、适当性/适配性（如涉及投顾/组合管理/复杂产品）。
- 对第三国客户：需控制跨境招揽、制裁与高风险辖区、数据跨境与营销表述风险（避免"未获授权"或"申请中等同持牌"的误导性表述）。

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）

> 马耳他实操建议：**Pre-application 先把"服务范围+系统蓝图+外包清单+人员与股东包"定稿**，否则后面补件会被"反复打回"。

Stage 0｜项目立项与差距评估（Week 1–2）

- MiCA 服务清单映射（决定资本/岗位/系统深度）
- 差距评估：资本、人、制度、系统、外包、数据治理
- 输出：差距清单 + 里程碑计划 + 预算表

Stage 1｜Pre-Application 沟通（Week 2–4）

- 与 MFSA 预沟通：拟申请服务、关键外包、治理与资源配置口径
- 同步准备 LH Portal 递交结构与索引（按 MFSA Rulebook/Forms 逻辑）

Stage 2｜正式递交（Week 6–10）

- 通过 LH Portal 递交申请表与附件（Programme of Operations + BP + AML + ICT + Fit&Proper + 股东/UBO 包等）

Stage 3｜完整性审查（Completeness Check）

- 核对：材料齐全、结构与索引、声明与证明可核验
- 常见卡点：UBO 穿透/SoF/SoW 不闭环、关键岗位资历不足、ICT/外包描述不可审计

Stage 4｜实质审查与补件（RFI）/面谈（如有）

- 重点问答：
  1. 服务定性与客户旅程是否与授权一致
  2. AML 可运行（规则、报警、STR 决策留痕）
  3. 钱包/密钥/权限/对账/审计轨迹
  4. 外包治理与退出机制（DORA 视角）
  5. 客户保护与营销合规

Stage 5｜批准（含原则性批准/条件）→ 上线（Go-live）

- 满足资本到位、关键岗位正式任命、系统验收、培训与演练证据、外包合同与审计权落地
- 获批后再走 MiCA 护照通报（Article 65 等）与跨境营销合规审核。

6）所需材料清单（Master Checklist）A–I 分类（交付版）

说明：MFSA 已在其官网栏目提供与金融机构/规则簿相关的入口与表格资源（包括 **Returns and Forms**、以及**外包通知表（Outsourcing Notification Form）等），并在其 MiCA 规则文件中明确了外包通知的递交渠道与提前期要求**（例如通过 LH Portal 提交、关键/重要外包需提前通知等）。

本清单以 **MiCA（EU 2023/1114）+ ESMA/EBA Level 2/3 RTS/ITS + DORA（EU 2022/2554）** 的监管审查逻辑为主线，结合 **MFSA 的本地化落地口径（Rulebook/Forms/Portal）**做"提交级"颗粒度整理。

A｜公司设立与法定文件（Corporate & Legal Pack）

目标：证明 EU 实体合规存在 + 有效管理地 + 实质经营（substance）+ 监管可触达。

A1. 公司注册证书、商业登记摘录、公司章程（Memorandum & Articles）
A2. 注册地址证明（租约/业主同意书/办公室照片与平面图建议）
A3. 股东名册、董事名册、公司秘书资料、签字授权人清单
A4. 组织架构图（Org Chart）+ Headcount Plan（3 年人员编制）
A5. 有效管理地证据：董事会章程（Board Charter）、会议频率计划、会议纪要模板、决策留痕机制
A6. 业务范围与牌照服务映射：拟申请 CAS 服务类型清单（逐项对齐 MiCA）
A7. 关联公司/集团结构说明（如适用）+ 集团治理与支持说明（Shared Services/IT/Compliance）
A8. 税号/VAT（如适用）申请进度表；数据保护负责人（DPO）或责任人安排（如适用）
A9. 内部政策库索引（Policy Library Index）+ 文档控制/版本管理规则
A10. 监管沟通授权文件（PoA/Authorisation Letter）、项目联系人清单与沟通机制

B｜股东/UBO/重大持股包（Shareholding / Qualifying Holdings / UBO Pack）

目标：穿透清晰 + 资金来源闭环（SoF/SoW）+ 声誉/适当人选（Fit & Proper）+ 持续通知机制。

B1. 股权结构穿透图（至自然人 UBO）+ 控制权说明信（投票权/协议控制/可转债/期权等）
B2. "重大持股/重要影响"门槛清单：≥10%/逐级控制链条/实际控制人认定说明
B3. 股东/UBO 身份与住址证明（有效期管理：近 3 个月等）
B4. 资金来源（SoF）声明 + 资金路径图（Money Trail Map：从哪里来→如何到公司→是否持续可用）
B5. 财富来源（SoW）声明 + 佐证（审计报表/分红/股权出售/资产处置/薪酬税单等）
B6. 声誉与合规记录：无犯罪/无破产/无重大诉讼/无监管处罚声明（+ 不利媒体检索与澄清备忘录）

B7. 制裁/PEP 自查与筛查结果留档（含供应商报告或截图）
B8. 关联方披露与关联交易政策（含转让定价/费用分摊逻辑）
B9. 持股变更与持续通知制度：股权变动预警、董事会审批、监管报备流程
B10. 投资者/募资路径说明（如涉及外部融资）+ 投资者适格性筛选政策（如适用）

C｜董事/高管 Fit & Proper（Management Body & Senior Management Pack）

目标：证明"能管、愿管、可问责、可投入、可被监管核验"。

C1. 董事/高管清单（含职责分工、任命文件）
C2. 每位董事/高管监管版 CV（可核验：项目、规模、职责、合规成果、技术/风险治理经验）
C3. 学历/资格证书、推荐信/任职证明、监管面谈可核验材料
C4. 诚信/声誉声明：刑事/金融犯罪/洗钱相关、破产、监管处罚、诉讼披露
C5. 时间投入声明（Time Commitment）+ 兼职/外部董事席位清单
C6. 利益冲突声明（COI）+ 关联方任职披露 + 回避机制
C7. 董事会技能矩阵（Skill Matrix）+ 治理培训计划
C8. 管理层问责框架（Accountability）+ 重大事项上会机制（AML/ICT/客户资产/外包）
C9. 新产品审批流程（NPC）、定价/费用治理机制（含返佣/做市利益冲突控制）
C10. 面谈题库（Board/CEO/COO/CTO/CCO/MLRO）+ 标准答题稿（RFI/Interview pack）

D｜控制职能与关键岗位（Compliance/MLRO/Risk/Internal Audit/ICT Governance）

目标：三道防线清晰 + 独立性 + 资源充足 + 汇报线直达董事会。

D1. 合规负责人（CCO）任命函 + JD + 汇报线说明（独立性）
D2. MLRO 任命函 + JD + STR 决策权限与升级路径
D3. 风险负责人任命 + 企业风险管理框架（ERM）+ 风险偏好（Risk Appetite）
D4. 内部审计安排（内部/外包）+ 年度内审计划（IAP）+ 独立性声明
D5. ICT 安全负责人 / ICT Risk Owner / CISO（或等效）任命 + 职责边界
D6. 合规监控计划（CMP）+ 抽查策略 + 整改跟踪（Issue Tracking）
D7. 年度合规/AML/ICT 培训计划 + 材料清单 + 考核记录模板
D8. 记录保存政策（Records Retention）+ 调阅与监管检查应对流程
D9. 投诉处理政策、利益冲突政策、广告与营销合规政策（含审批日志）
D10. 外包治理政策（对齐 DORA/第三方风险）+ 外包登记册（Outsourcing Register）

E｜Programme of Operations + Business Plan（运营方案与商业计划）

目标：监管最看重的"业务闭环"：服务类型—客户旅程—资金/资产流—风险与控制—系统与外包—持续报告。

E1. Programme of Operations 正文（服务类型、提供地点、提供方式：线上/分支/外包/代理）
E2. 客户旅程流程图（开户→交易/托管→充值/提现→风控→投诉→关户）
E3. 产品清单与收费表（交易费/点差/托管费/提现费/第三方费用/返佣披露）
E4. 客户分类（零售/专业）政策 + 专业客户证明文件清单
E5. 市场进入与护照策略：目标国家清单 + 通报路径 + 当地营销合规边界
E6. 资金与资产流路径图：法币/加密分离、对账机制、客户资产隔离说明
E7. 交易执行/撮合规则（平台类）、市场监控（刷量/操纵）与异常处置
E8. 三年财务预测（P/L、BS、CF）+ 成本结构（合规/系统/审计/人员/保险/法律）
E9. 审慎保障方案（资本/保险/等效保障）+ 压力测试/情景分析
E10. 退出与关停计划（Wind-down Plan）：客户资产安全退出、通知、数据留存、供应商切换

F｜AML/CFT/CPF 制度包（可运行+可审计）

目标：不是"文件合规"，而是"制度+系统+证据链"。（并对齐欧盟 AML 演进：AMLA、Travel Rule、制裁、链上风险）

F1. AML 总政策（AML Policy）+ MLRO 职责与汇报线
F2. AML 风险评估方法论（客户/产品/地域/渠道/交易行为/链上风险）
F3. CDD/EDD 程序（自然人/法人/UBO 识别、控制权核验、面签/远程核验）
F4. 制裁/PEP 筛查流程（频率、命中处置、冻结/拒绝/上报）
F5. 交易监控规则库（场景、阈值、报警、误报管理、模型版本管理）
F6. 链上分析策略与工具说明（地址风险评分、混币/暗网暴露、跨链风险）
F7. STR/SAR 决策树 + 提交流程 + "未报送原因"留痕模板

F8. 高风险国家策略、第三方付款/现金策略（如适用）
F9. 记录保存年限与可检索归档（含审计轨迹）
F10. 独立 AML 审查机制（内审或外部独立评估）+ 年度 AML 报告模板

G｜ICT / 钱包 / 安全（对齐 DORA 的"可审计"体系）

目标：把 ICT 当作"监管资产"。尤其托管/平台/兑换：冷热钱包、多签、权限、日志、韧性演练必须可核验。

G1. 系统架构图（应用/数据/网络）+ 数据流图（含敏感数据分级）
G2. 访问控制（RBAC/最小权限）、MFA、权限变更留痕与四眼原则
G3. 密钥管理政策（HSM/分片/备份/轮换/签名仪式）
G4. 冷/热钱包策略、阈值/限额、隔离与对账机制（链上链下对账）
G5. 日志策略（不可篡改、留存期、检索、审计导出）+ SIEM/监控告警
G6. 漏洞管理与补丁管理、代码审计/发布管理、供应链安全（开源依赖）
G7. 渗透测试计划与报告 + 整改闭环
G8. 事件响应计划（IRP）+ 取证与证据保全 + 通报模板（含重大事件分级）
G9. BCP/DR：RTO/RPO、灾备架构、演练计划与记录
G10. 外包/云服务 ICT 风险：合同审计权、数据驻留、退出与迁移（Exit Plan）

H｜客户条款/披露/投诉（Consumer & Client Protection Pack）

目标：客户保护要"写得清楚、做得到、留得下证据"。

H1. 客户协议（T&C）模板（服务描述、责任边界、关户/终止、争议解决）
H2. 风险披露声明（波动、技术风险、托管风险、第三方风险、不可逆交易等）
H3. 费用披露清单（透明到每个收费项与触发条件）
H4. 客户资产隔离说明 + 客户资金/资产流说明 + 对账频率与差异处理
H5. 投诉处理政策：渠道、时限、分级、复核、记录保存与复盘改进
H6. 利益冲突政策（做市/返佣/自营或关联方交易等）+ 披露文本
H7. 适当性/适配性制度（如涉及投顾/组合管理/复杂产品）+ 问卷与记录模板
H8. 广告与营销合规政策 + 营销材料审批日志（Marketing Approval Log）
H9. GDPR：隐私政策、DPA、数据主体权利流程、跨境传输评估（如适用）

I｜申报声明/费用/项目管理（Submission, Declarations, Fees & PMO）

目标：把申请做成"监管可读的项目包"，补件（RFI）有战情室机制，文件可追溯。

I1. 申请表与附件目录（按监管 RTS/ITS 逻辑编号）
I2. 逐项对照表（Requirements Mapping）：法规条款 → 文件证据 → 位置/编号
I3. 董事会决议（提交申请/任命关键岗位/批准外包/批准政策库）
I4. 监管沟通记录表（Q&A Log）、补件应答模板（RFI Cover Letter）
I5. 文件公证/认证/翻译清单 + 有效期管理表
I6. 费用预算表（政府/监管年费/审计/法律/技术/保险/人员）
I7. 上线前验收清单（Go-Live Checklist）+ 条件落实清单（capital/insurance/system readiness）
I8. 重大变更报备流程（股权/董事/关键岗位/服务范围/外包/核心系统）
I9. 持续合规日历（年度报告、审计、培训、演练、外包复评）
I10. 数据字典（Data Dictionary）：客户/交易/钱包/风控/制裁/投诉字段来源与口径

仁港永胜唐生提示｜如何把 A–I 变成"监管友好"的递交件

1. **先做索引再写正文**：先搭 A–I 文件夹树、编号规则、对照表（条款→证据），再填充内容。
2. **所有关键结论都要"证据链"**：人（CV/声明/任命/汇报线）+ 制度（政策/流程）+ 系统（日志/截图/报告）三件套。
3. **外包按 DORA 思路一次做对**：外包登记册、尽调、合同审计权、退出计划、持续监控，避免后期反复整改。（MFSA 也在其规则文件中明确外包通知与表格机制；如涉及关键/重要外包，务必按其要求通过 portal 提交通知并满足提前期。）

仁港永胜建议

如贵司以马耳他作为 MiCA CASP 申请地，我们建议把材料按本 A–I 结构直接做成：

- **《Master Checklist + 索引号 + 版本管理表》**（可递交）

- **《RFI 补件战情室包》**（可补件：问答库、证据链清单、责任矩阵）
- **《DORA 化 ICT/外包治理包》**（可审计：日志、测试、演练、外包合同条款库）

为何选择仁港永胜（服务优势）

- **一体化交付**：MiCA/CASP 申请文件 + AML/CFT 制度 + ICT/DORA 外包治理 + 客户条款披露，一次性成体系，避免多团队碎片化。
- **强模板库**：BP/Programme of Operations 模板、Risk Register、STR 决策树、外包尽调清单、面谈题库、RFI 应答包、护照通报包等可直接落地。
- **实操导向**：以"可审计、可证据化、可解释"为标准组织材料，提高通过率与审查效率。
- 注：本文所涉 **Master Checklist（可编辑版）/索引号规则/对照表模板/RFI 应答包/面谈题库/外包合同条款库（DORA）** 等电子档，可向仁港永胜唐生有偿索取。

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 10% / 重大持股与控制权（核心逻辑）

- 对达到或可能构成"重大影响力"的股东/UBO：必须提供**穿透结构图（到自然人）+ 控制权说明信**（投票权、协议控制、可转债/期权等潜在控制工具）。
- **资金来源（SoF）/财富来源（SoW）**要形成闭环：钱从哪里来 → 怎么到申请实体 → 是否足以覆盖 12–36 个月经营与资本要求。

7.2 声誉与不利信息（媒体/诉讼/处罚）

- 背景调查与不利信息解释备忘录（Negative News Memo）
- 诉讼/破产/监管处罚声明 + 佐证
- 制裁与 PEP 自查与筛查结果留档

7.3 持续通知（ongoing change）

- 重大股权变动、控制权变化、UBO 变化、资金结构变化、关联交易变化，均需建立"变更评估→监管沟通→实施→留档"闭环（获牌后更关键）。

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 必配关键岗位（建议最低配置）

- **Compliance Officer（合规负责人）**：建立合规监控计划、营销合规审查、投诉机制监督、监管报送协调
- **MLRO（反洗钱报告官）**：风险评估、CDD/EDD、交易监控、制裁筛查、STR 决策与报送、培训与独立审查
- **ICT Risk Owner / 信息安全负责人（CISO 或等效责任人）**：DORA 体系落地、事件响应、外包与韧性
- **Risk Management（风险负责人）**：风险偏好、KRI/KPI、压力测试、客户资产风险控制
- **Internal Audit（内审）**：可外包，但需独立性、审计计划与整改闭环

8.2 独立性与汇报线（监管非常看重）

- 合规/MLRO 应具备**直达董事会/合规委员会**的汇报线
- 资源充足：工具、预算、人手、访问权限
- 证据链：培训、抽查、STR 记录、模型调参、监控工单、投诉工单均可审计

8.3 外包边界

- 外包不免除责任；敏感职能不宜"完全空心化"
- MFSA 提供 **MiCA Outsourcing Notification Form**，意味着外包治理会成为检查与报备重点。

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）

9.1 钱包与密钥管理（托管/平台/转账类必做）

- 冷热分离、热钱包限额、冷钱包签名仪式留痕
- 多签门限（M-of-N）、关键人分离、HSM/分片/离线备份
- 地址白名单/黑名单、链上/链下对账、资产证明与审计轨迹

9.2 安全与可审计（DORA 化写法）

- RBAC 权限矩阵、MFA、日志不可篡改、变更管理
- 渗透测试 + 漏洞整改闭环
- 事件响应（分级、隔离、取证、通报、复盘）
- BCP/DR：RTO/RPO、演练计划与记录、灾备架构

9.3 外包与第三方（云/KYC/链上分析/托管/撮合引擎）

- 供应商尽调、SLA/KPI、审计权、数据所在地、退出/迁移计划
- 关键外包登记册（Outsourcing Register）+ 定期评估报告
- 重大外包变化：通知/报备机制（配合 MFSA 外包通知表）。

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）

- **资产隔离**：客户资产与自有资产隔离、钱包隔离、对账频率、差异处理与补偿政策
- **费用披露**：交易费、点差、提现费、托管费、第三方费用、返佣/做市利益冲突披露
- **投诉机制**：专岗/渠道/时限/升级/复盘（投诉台账可审计）
- **利益冲突**：关联交易、做市/自营边界、员工交易、礼品招待
- **适当性/适配性**：涉及投顾/组合管理/复杂产品时必须强化；零售/专业客户分类与证明文件清单化

11）官方收费与预算（政府费/年费/审计/法律/技术/保险/人员成本）

11.1 MFSA/马耳他"申请费"（按 CASP 类别）

马耳他《Markets in Crypto-Assets Act (Fees) Regulations》对 CASP 申请费设置为：

- **Class 1：€10,000**
- **Class 2：€20,000**
- **Class 3：€25,000**
  （如申请多项服务，通常按最高适用类别计费）

11.2 年度监管费（年费结构）

法规信息显示：年度监管费由固定部分与（如适用）与规模相关部分构成，固定部分示例：

- Class 1：€10,000；Class 2：€25,000；Class 3：€50,000（并可能叠加与规模相关的计算项，需按法规文本口径测算）

11.3 典型"全周期预算科目"（做 BP/预算表可直接用）

- 政府/监管：申请费、年费、变更费（如服务范围调整等）
- 审计与会计：年度审计、AML 独立审查、（如适用）SOC/安全审计
- 法律与牌照顾问：申请文件、合同条款、外包协议、数据保护/GDPR
- AML 工具：制裁/PEP、交易监控、链上分析、Travel Rule（如适用）
- ICT：渗透测试、SIEM/SOC、安全运营、密钥管理/HSM、BCP/DR 演练
- 人员：合规/MLRO/风控/IT 安全/内审/客服与运营
- 保险/等效保障：依据服务与风险（尤其托管/平台）配置

12）后续维护与续牌/持续合规（报告、审计、变更报备、培训、演练）

关键：马耳他已把"持续监管"做成 **CASP Return + 审计包 + 提交时限** 的报表化体系。

12.1 监管报告与报表（MFSA CASP Return）

MFSA 已发布 **CASP Return**及其编制指引，且明确：

- **Audited Annual CASP Return（AACR）**须在会计参考日后 **6 个月内提交**，并附 **Audit Pack**；
- 指引亦提到其他阶段性报送节奏与提交方式（通过 LH Portal）。

仁港永胜建议：把报表字段、数据字典、日志留存、对账机制在"申请阶段就设计进系统"，避免获牌后再补。

12.2 年度审计与独立审查（推荐"3 条线"）

- 年度财务审计（法定）
- AML 独立审查/内审（覆盖 CDD/EDD、制裁、STR、监控模型）
- ICT 安全与韧性审查（渗透测试、DR 演练复盘、外包审计）

12.3 重大变更报备（Change Management）

建立统一流程：**变更识别→影响评估（合规/AML/ICT/客户）→董事会审批→监管沟通/报备→实施→留档**
常见需报备/通知情形：

- 股权与控制权变化、UBO 变化
- 董事/关键岗位变更（合规/MLRO/ICT 风险责任人）
- 新增/减少服务范围、目标市场/护照策略变化
- 关键外包变化：云、托管、KYC、链上分析等（MFSA 有外包通知表，意味着外包变更很敏感）

12.4 培训与演练（监管看"证据链"）

- AML 年度培训（入职+岗位专项+案例复盘）
- 安全事件响应演练（桌面推演+实战演练）
- BCP/DR 演练（RTO/RPO 验证、恢复记录、改进闭环）
- 投诉处理与客户沟通演练（话术库+升级机制）

12.5 续牌/持续有效（实务口径）

MiCA 下通常不是"到期续牌"那种一次性换证逻辑，而是**持续满足条件 + 持续报告 + 重大变更报备**；若持续义务不满足，会触发监管措施（整改、限制业务、处罚等）。

13）办理时间预估（公司设立、文件编制、审查窗口、缓冲）

下表为"项目管理口径"的可执行预估（实际取决于服务范围、股东结构复杂度、系统与外包数量、RFI 轮次）。

13.1 典型时间轴（建议倒排）

1. **公司设立与基础实质**：2–6 周

- 注册、银行/资金安排、办公室、核心岗位到位、董事会治理框架

2. **文件编制与系统证据链**：6–12 周

- Programme of Operations + BP
- AML/CFT 手册 + 风险评估 + STR 机制
- ICT/DORA：架构图、权限矩阵、钱包方案、渗透测试计划、BCP/DR
- 股东/UBO SoF/SoW 闭环包 + Fit&Proper 包

3. **递交与完整性审查**：约 4–8 周（视监管排队与材料质量）
4. **实质审查与 RFI/面谈**：8–20+ 周（高不确定区间）
5. **批准后条件落实与上线**：4–12 周

- 注资/保障到位、关键岗位任命、系统验收、培训演练证据、外包合同与审计权落地

13.2 "缓冲期"怎么留才稳

- 至少预留 **2–3 轮 RFI** 的应答窗口
- 股东/UBO 如涉及多层 SPV、跨境资金路径，需额外缓冲（通常是最大变量）
- 托管/平台类系统复杂，需预留渗透测试与整改周期

14）《马耳他 Malta（MiCA）CASP 牌照常见问题（FAQ 大全）Q1–Q300》

马耳他MiCA常见问题（FAQ）题库

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。

A｜监管框架与牌照定位（Q1–Q30）

Q1：什么是 MiCA 下的 CASP?
A：CASP（Crypto-Asset Service Provider）是指在欧盟《MiCA》框架下，向客户提供加密资产服务（如托管与管理、运营交易平台、兑换、执行/传递订单、转移服务、投资建议、组合管理等）的机构。若在欧盟境内向客户提供这些服务，一般需要获得授权并接受持续监管。

Q2：MiCA 监管什么、不监管什么?
A：MiCA 主要监管三块：
1）加密资产发行（尤其 ART/EMT 稳定币与其他 crypto-assets 的白皮书披露与义务）；
2）CASP 的授权与行为规则（客户保护、治理、资本/保障、外包与 ICT 风险等）；
3）市场滥用相关要求（适用于加密资产市场）。
MiCA 不替代传统证券法体系：若代币构成金融工具/证券，仍可能落入 MiFID/Prospectus 等框架；也不取代 AML 法（AML 通常在各国 AML 法及欧盟 AML 套件下执行）。

Q3：哪些业务最容易被认定为需要 CASP 授权?
A：典型包括：

- 托管钱包/托管私钥、代客户持有或控制加密资产
- 经营 CEX/交易撮合平台（订单簿、撮合、做市/流动性提供）
- 法币↔加密资产、加密资产↔加密资产兑换
- 经纪/代理下单、传递订单、执行订单
- 为客户提供加密资产转移服务（转账/划转）
- 投资建议、组合管理（尤其涉及零售客户）

Q4：我只做"软件"或"技术服务"，也要牌照吗?
A：看你是否"向客户提供受监管的加密资产服务"。纯技术供应商（不接触客户资产、不对客户提供受监管服务、不对客户作出服务承诺）通常不以 CASP 身份被授权；但若你以自己品牌向客户提供托管/交易/转移等，即使外包了系统，也可能被认定为 CASP。

Q5：DeFi、DEX 是否完全不受监管?
A：不等同。若存在可识别的运营主体、前端由某实体运营、对客户提供服务、或存在关键控制点（如托管、订单路由、费用收取），仍可能触及监管边界。此外，国家监管机构会结合"实质控制"和"客户关系"判断。

Q6：MiCA 是否有"护照"机制?
A：是。CASP 在一国获授权后，可通过 MiCA 的跨境通报机制在其他成员国提供服务（自由提供服务或设立分支）。实务上仍需要：目标国营销合规、语言披露、投诉与客户沟通机制、本地税务与雇佣安排等配套。

Q7：护照=不用理其他国家监管?
A：不是。护照意味着"授权层面通用"，但**消费者保护、广告营销、语言披露、税务、数据保护、民商事责任**等仍需要满足当地规则；一些成员国对营销、投诉、语言、费用披露会更严格。

Q8：MiCA 与 DORA 的关系是什么?
A：MiCA 提出 CASP 的治理、外包与 ICT 风险管理要求；DORA 则是金融实体 ICT 韧性"硬法"，强调：ICT 风险治理、事件管理、韧性测试、第三方风险、信息共享等。实操建议：CASP 的 ICT 体系应直接按 DORA 标准构建，减少后续整改与审查风险。

Q9：MiCA 与 AML 法的关系是什么?
A：MiCA 不取代 AML。CASP 仍需遵守本国 AML/CFT 法与监管要求（CDD/EDD、制裁筛查、交易监控、STR 报送、记录保存、培训、独立审查等）。欧盟层面也在推进 AMLA 与新 AML 规则（趋势是更统一、更数据化）。

Q10：MiCA 下 CASP 服务类型有哪些?
A：常见包括：

- 托管与管理加密资产（custody）
- 运营交易平台（trading platform）

- 兑换（crypto-crypto / fiat-crypto）
- 执行订单、传递订单
- 为客户提供转移服务（transfer）
- 投资建议（advice）
- 组合管理（portfolio management）
  （具体分类以 MiCA 服务清单为准；申请必须明确你拟提供的服务组合）

Q11：我想同时做交易所+托管+法币出入金，能一张牌搞定吗？
A：可以申请覆盖多项服务，但监管审查强度会显著提高：资本/保障、治理、系统安全、客户保护、利益冲突、做市/自营边界、外包控制、清结算与对账等都要更完整。

Q12：我只做 OTC（柜台）兑换也需要吗？
A：若你对客户提供兑换服务（尤其法币↔加密资产），通常会触及受监管服务。若你只是撮合信息且不参与交易执行、不收取费用、不控制资金与资产，可能不同；但多数商业 OTC 模式会构成受监管活动。

Q13：我只做"经纪介绍"收介绍费呢？
A：关键看你是否"参与订单传递/执行""代表客户交易""提供投资建议"。单纯广告导流也要注意营销合规与误导风险；若你对客户提供个性化建议或实际撮合交易路径，风险上升。

Q14：MiCA 下 CASP 是否允许向零售客户提供服务？
A：允许，但对披露、适当性/风险提示、投诉机制、客户协议、费用透明度、市场滥用防控等要求更高；你需要明确零售/专业客户分层与相应保护措施。

Q15：MiCA 是否要求本地董事或本地人员？
A：MiCA 强调有效管理与监管可触达（substance）。各国 NCA 通常要求关键管理与控制在本国/欧盟真实存在：董事会运作、关键岗位（合规/MLRO/ICT 风险责任人）具备履职能力并能接受监管问询。

Q16：申请前是否建议做 Pre-application meeting？
A：强烈建议。可在正式递交前把：服务范围、客户类型、资产/资金路径、外包清单、关键岗位与股东结构，先与监管口径对齐，减少"定性错位"导致的补件与延误。

Q17：什么是"监管定性备忘录（Perimeter Memo）"？
A：是将你的业务模式与 MiCA 服务类型逐项映射，回答：你到底提供什么服务、边界在哪里、是否涉及托管/平台/投顾等高风险服务，从而决定资本、制度、系统与人员配置。

Q18：MiCA 对"申请中"宣传有什么限制？
A：严禁误导。常见合规做法是：明确披露"正在申请/未获授权"，不得使用会让客户误认为已受监管或已获牌的表述；营销材料需经过合规审批留痕。

Q19：CASP 能否提供衍生品交易？
A：MiCA 主要针对加密资产服务，不等同于衍生品监管。若涉及期货/差价合约/证券型代币衍生品，可能落入 MiFID/MiFIR 等框架及国家监管许可，需另行评估。

Q20：CASP 是否可以发币？
A：可以，但发行行为可能触及 MiCA 的发行/白皮书义务（尤其 ART/EMT）。如果既发币又做平台/托管，利益冲突与市场滥用风险管理会被重点审查。

Q21：什么是 ART/EMT？
A：MiCA 将稳定币分为资产参考代币（ART）与电子货币代币（EMT）。两者在发行主体资质、储备资产、赎回权、信息披露、审慎要求等方面更严格。

Q22：CASP 可以上架 ART/EMT 吗？
A：可以，但通常需要确保：发行与白皮书合规、持续信息披露、赎回与风险提示机制、市场滥用监控等，并且平台应建立上币审查与持续监控机制。

Q23：MiCA 对"市场滥用"有何要求？
A：包括对内幕信息、操纵市场、非法披露等的控制；平台需要监控异常交易、洗售、拉盘砸盘、虚假流动性等，并建立可审计的调查与处置流程。

Q24：MiCA 下 CASP 的核心监管关注点是什么？
A：通常是：

- 股东/UBO 与管理层适任性（fit & proper）
- AML 可运行（不是文件合规）
- ICT/钱包安全与外包可控（DORA 视角）
- 客户资产保护与披露
- 利益冲突与治理（尤其平台+做市+自营）
- 报表与持续合规能力（可审计证据链）

Q25：申请材料最容易被打回的原因？
A：服务定性不清、UBO/资金来源不闭环、关键岗位资历不足或"空心化"、ICT/外包描述不可审计、AML 没有可运行流程/证据链、客户条款与系统实际不一致。

Q26：监管会看我是否"真的能运营"吗？
A：会。除文件外，监管会通过问答、系统演示、日志与流程证据判断你是否具备实质运营能力：开户、KYC、监控、风控、提现审批、事故响应、投诉处理等。

Q27：MiCA 是否规定最低资本？
A：MiCA 对 CASP 有最低资本/自有资金及持续审慎保障要求（与服务类型与风险相关）。实操上需提交资本计划、财务预测、压力测试与风险覆盖说明。

Q28：资本可以是股东借款吗？
A：一般不建议以"可撤回"的形式替代法定资本/审慎保障；监管通常偏好：实缴股本、不可随意抽回的资金、明确的资金来源证明与持续经营能力。

Q29：能否用保险替代部分审慎保障？
A：部分框架允许以保险或等效保障工具覆盖某些风险，但是否可接受、覆盖范围与条款强度（免赔额、赔付条件、除外责任）会被审查。需提交保单摘要、覆盖说明与差距分析。

Q30：申请主体必须是欧盟公司吗？
A：通常需要在欧盟设立实体并获得授权。非欧盟公司可通过设立欧盟子公司/分支（取决于 NCA 规则）来申请，但核心管理与控制必须可被监管触达。

B｜公司设立与实质经营（Substance）（Q31–Q60）

Q31：申请前公司需要先设立好吗？
A：通常需要。监管会要求：公司注册文件、章程、董事任命、办公地址、组织架构、关键岗位安排等。

Q32：实质经营（substance）具体要做什么？
A：至少包括：

- 本地办公地址与可被监管检查的记录保存
- 董事会与治理机制真实运作（会议纪要、决议、授权）
- 关键岗位可履职（合规/MLRO/风控/ICT）
- 关键系统与外包安排可审计（合同、SLA、审计权、退出方案）
- 本地或欧盟内核心管理与控制

Q33：可以完全远程团队运营吗？
A：不建议。即便允许部分远程，监管仍会要求关键管理与控制在欧盟可触达，且需要明确谁在何处履职、如何管理风险与外包、如何保存记录与配合检查。

Q34：是否需要本地董事？
A：各国实务不同，但普遍要求董事会具备足够时间投入与本地/欧盟监管沟通能力。建议配置至少一名熟悉本地监管与合规的董事或高管，且能面谈应答。

Q35：是否需要设立分支机构？
A：不一定。若以自由提供服务（cross-border services）方式护照进入其他国家，可不设分支；但某些情况下（营销/客户服务/税务/语言）设分支更稳。

Q36：公司治理结构需要哪些委员会？
A：常见配置：董事会、风险与合规委员会、审计委员会（或等效安排）。小型机构可合并，但要证明独立性与有效监督。

Q37：三道防线怎么设计？
A：

- 第一线：业务与运营（开户、交易、客服、资金/资产操作）
- 第二线：合规与风险（政策、监控、审批、培训、报告）
- 第三线：内部审计（独立评估与整改跟踪，可外包但需独立）

Q38：内部审计一定要自建吗？
A：通常允许外包，但需：独立性、审计计划、覆盖 AML/ICT/运营关键流程、整改闭环、董事会监督。

Q39：需要指定合规负责人吗？
A：需要。合规负责人负责合规计划、监管沟通、营销审批、投诉监督、政策更新与报告协调。

Q40：MLRO 与合规负责人可以同一人吗？
A：视规模与风险而定，小型机构可能允许兼任，但监管会看：独立性、资源、是否能实际履职、是否存在利益冲突与工作量不可承受。

Q41：关键岗位是否必须全职?
A：不一定，但高风险服务（托管/平台）通常更倾向全职与本地/欧盟常驻。若兼职/外包，需要证明：可用性、响应速度、权限与独立性、替补安排。

Q42：如何证明"时间投入足够"?
A：提供：职务说明、时间分配声明、会议安排、值勤/值班制度、替补机制、过往履历与同类业务经验。

Q43：公司章程和股东协议会被审查吗?
A：会。监管关心：控制权、投票权、重大事项否决权、关联交易、利润分配与资金抽回机制是否影响审慎稳健。

Q44：需要制定授权矩阵（Delegation of Authority）吗?
A：强烈建议。列明：开户审批、EDD 审批、提现审批、上币审批、外包签署、事故响应、投诉升级、营销发布等的授权链条与双人复核机制。

Q45：记录保存要保存在哪里?
A：通常要求在欧盟可获得、可检查。若云存储或跨境存储，需满足数据保护、审计权与取证要求，并有灾备与不可篡改日志策略。

Q46：使用集团共享服务中心可以吗?
A：可以，但必须清晰：服务边界、SLA、费用分摊、控制权归属、数据访问与安全、审计权、退出与替代计划。

Q47：我可以用"白标交易所系统"快速上线吗?
A：可以，但监管会重点审查：供应商尽调、合同审计权、数据归属、关键控制（密钥/钱包/交易核心）是否在你方掌控、退出可行性与迁移计划。

Q48：监管会要求我先做系统验收吗?
A：很多情况下会要求你证明系统具备上线能力：权限矩阵、日志、风控规则、KYC 工作流、钱包安全、BCP/DR 等。

Q49：运营流程图必须画吗?
A：必须。至少要画：客户旅程（开户→交易→充提→投诉）、资金流/资产流、权限与审批流、异常处理流、外包与数据流。

Q50：如何证明"客户资产隔离"?
A：通过：钱包架构、账户结构、链上地址隔离策略、对账机制、资金/资产台账、差异处理政策、运营人员权限隔离与审计日志。

Q51：是否必须有本地银行账户?
A：不一定，但若涉及法币出入金与运营成本支付，需要可持续的资金安排。监管会关注：资金路径、反洗钱控制、银行合作与备选方案。

Q52：开银行账户困难会影响申请吗?
A：会影响可运营性证明，但不是绝对。可以用：EMI/支付机构合作、分层资金路径、托管账户方案等；但必须说明如何控制 AML 与客户资金安全。

Q53：董事会会议频率建议?
A：至少季度一次；高风险或早期阶段建议每月一次并保留会议纪要，形成"治理证据链"。

Q54：是否需要制定业务连续性计划（BCP）?
A：必须，且要有演练记录。包括：关键系统故障、供应商宕机、网络攻击、关键人不可用等情景。

Q55：灾难恢复（DR）必须有异地吗?
A：通常需要满足可接受的 RTO/RPO。对平台/托管类，建议异地灾备与定期演练，并提供恢复测试报告。

Q56：是否需要设立客服与投诉渠道?
A：需要。监管会看：响应 SLA、升级路径、记录保存、复盘与改进机制。

Q57：营销材料需要合规审批吗?
A：必须。要建立 Marketing Approval Log：谁审核、何时发布、风险披露是否完整、是否面向目标国家客户、是否误导。

Q58：是否需要设置"产品委员会/上币委员会"?
A：强烈建议。上币评估机制必须覆盖：法律定性、技术安全、发行背景、市场操纵风险、制裁/犯罪风险、披露与持续信息要求。

Q59：能否只写制度不落地?
A：不可。监管越来越强调"可验证的执行证据"。仅文档合规、无系统日志/工单/演练记录，会被视为高风险。

Q60：申请期间可以先试运营吗?
A：一般不应向公众提供受监管服务。可以进行内部测试、沙盒/试点（如本国提供），但需确保不构成未经授权的公众经营，并保留测试边界声明与记录。

C｜服务范围与业务模型（Programme of Operations）（Q61–Q100）

Q61：Programme of Operations 必须包含什么?
A：至少包括：

- 拟提供的 CAS 服务类型与边界
- 客户类型（零售/专业/机构）与目标市场
- 收费模式（手续费、点差、托管费、会员费等）
- 资金流/资产流与对账
- 钱包/托管与密钥管理（如适用）

- 风控与市场监控
- 外包与第三方依赖
- 投诉与客户保护
- 重大风险与缓释措施

Q62：交易平台必须说明哪些功能？
A：订单类型、撮合逻辑、做市/流动性机制、风控（限价/限额/熔断）、异常交易监控、交易暂停/下架机制、行情数据与披露、日志留存。

Q63：兑换服务（swap）必须说明什么？
A：定价来源、报价机制、点差与费用披露、对手方风险、流动性来源、冲击成本、订单执行方式、客户确认机制。

Q64：经纪/执行订单需说明什么？
A：最佳执行策略（best execution 的等效机制）、订单路由、潜在利益冲突、返佣/回扣披露、订单记录与可追溯性。

Q65：转移服务（transfer）需说明什么？
A：转账审批、地址风险评估、制裁筛查、链上监控、异常冻结与复核、误转处理、对账与入账规则。

Q66：托管服务需说明什么？
A：冷/热钱包架构、多签门限、密钥生成与备份仪式、权限矩阵、提现审批双人复核、资产隔离与对账、事故响应与赔付政策。

Q67：投顾/组合管理需说明什么？
A：客户适当性/适配性、风险承受能力评估、投资目标与限制、再平衡策略、费用与利益冲突披露、报告频率、止损/风控机制。

Q68：是否允许自营交易或做市？
A：可能允许，但属于高敏感点。必须建立：自营与客户交易隔离、信息隔离墙、利益冲突管理、做市规则透明度、异常交易监控与审计。

Q69：可否提供杠杆/融资？
A：通常涉及更高风险与可能触及其他金融监管许可。需要额外法律定性与可能的其他牌照/限制。

Q70：能否接入第三方流动性提供商？
A：可以，但需要外包/第三方风险管理：尽调、合同审计权、数据与日志、持续监控、退出方案与替代供应商。

Q71：客户资金/法币出入金如何设计？
A：常见方案：银行账户、EMI/PI 合作、托管账户、分层资金路径。必须说明：资金隔离、对账、退款、冻结与止付、异常处理与 AML 控制。

Q72：交易结算如何实现？
A：平台内账本+链上转移。必须说明：何时记账、何时链上确认、失败重试、对账频率、差异处理与客户通知。

Q73：如何处理链上拥堵/失败交易？
A：定义：超时阈值、手续费策略、重发机制、客户告知、退款/补发政策、事故记录与复盘。

Q74：是否需要披露"风险提示"？
A：必须。应覆盖：价格波动、流动性风险、技术风险、监管风险、托管与私钥风险、对手方风险、稳定币脱锚风险等。

Q75：如何界定零售客户与专业客户？
A：按本国法规与 MiCA 实务进行分类，并明确所需证明文件（资产证明、收入证明、机构证明、专业经验等）及升级/降级流程。

Q76：可以拒绝客户吗？
A：可以且应当。必须建立：拒绝/终止客户政策、黑名单与高风险名单、冻结资产与退款处理、记录保存与（如适用）STR 评估。

Q77：是否需要限制高风险国家/地区？
A：通常需要。建立：高风险辖区名单（FATF/EU 列表 + 本国名单）、额外 EDD、业务限制或拒绝政策。

Q78：如何处理 PEP 客户？
A：需 EDD：高级管理层批准、加强资金来源核查、持续监控、定期复核与更频繁的交易监控。

Q79：是否需要 Travel Rule？
A：欧盟 Travel Rule 已适用于加密资产转账信息随附要求（独立于 MiCA）。若你提供转移服务/提币等，需要实现发送方/接收方信息收集与传递、以及无信息转账的拦截与处置。

Q80：如何做链上分析？
A：使用链上分析工具（自建或外包），设置：地址风险评分、制裁地址识别、混币/暗网关联识别、异常路径报警，并建立人工复核与处置工单。

Q81：是否需要设置交易限额？
A：建议设置分层限额：未完成增强验证客户、零售客户、专业客户、机构客户；并结合风险评分动态调整。

Q82：如何管理手续费与点差披露？
A：必须透明：向客户披露所有费用组成（固定费、点差、网络费、第三方费用），并确保系统实际收费与条款一致，避免误导。

Q83：如何处理负余额或系统错误记账？
A：需有：差异处理 SOP、客户通知、补偿政策、事件记录、原因分析与防再发措施。

Q84：是否需要"上币后持续监控"？
A：必须。包括：项目重大事件、白皮书更新、合规状态、市场操纵风险、链上风险、制裁与犯罪风险、流动性与异常波动。

Q85：是否需要设置"下架机制"?
A：需要。下架触发条件：合规风险、技术漏洞、市场操纵、流动性枯竭、制裁/犯罪关联、信息披露严重不足等；并规定客户资产处置与公告机制。

Q86：是否允许匿名币?
A：高度敏感。多数监管与 AML 实务对隐私币采取限制或禁止上架/交易；若要支持必须有极强的 AML 控制并准备被监管质疑。

Q87：是否可以提供质押（staking）服务?
A：需要评估是否构成额外服务、是否涉及托管、收益分配与风险披露，且可能触及证券/集体投资计划等定性问题。建议单独做法律定性备忘录。

Q88：是否可以提供借贷/理财产品?
A：可能触及其他金融监管许可或消费者信贷规则，且风险更高。一般不建议在申请初期引入复杂产品。

Q89：能否面向全世界客户?
A：需遵守：目标市场法律、制裁与 AML、跨境营销规则、数据保护与税务合规。实操上建议分阶段：先欧盟，再扩展第三国合规接入策略。

Q90：是否需要本地语言支持?
A：多数国家对面向零售客户的披露、条款、投诉渠道会要求当地语言或可理解语言，尤其涉及营销与消费者保护。

Q91：是否必须提供客户对账单?
A：建议提供。包括：资产余额、交易记录、费用扣除、入金/出金记录、估值方法与风险提示。

Q92：如何处理硬分叉/空投?
A：需制定政策：是否支持、支持条件、风险披露、技术验收、客户通知、资产归属与税务提示。

Q93：如何处理链上回滚或共识攻击?
A：需定义：确认数策略、暂停充提机制、风险评估与公告流程、客户补偿与争议处理机制。

Q94：如何处理稳定币脱锚?
A：需：风控阈值（价格偏离、流动性下降）、交易限制或暂停、风险提示与公告、客户资产保护与对冲策略（如适用）。

Q95：如何处理极端行情与系统过载?
A：需要：限流、熔断、分级降级、订单风控、扩容策略、事件响应与沟通模板。

Q96：是否需要建立"客户资产证明/储备证明"?
A：不是所有国家都硬性要求，但趋势上监管与市场都要求更透明。建议建立：客户资产隔离证明、定期对账与第三方审计/证明机制。

Q97：如何处理客户争议（例如误转地址）?
A：明确责任边界与救济方式：地址验证提示、二次确认、人工复核机制（大额）、误转协助流程（但不保证可追回）、记录保存与投诉处理。

Q98：是否可以同时经营多品牌/多平台?
A：可以，但需统一治理、风险控制与合规审批；避免利用多品牌规避监管或误导客户，且要统一记录保存与报表口径。

Q99：是否可以接入代理商/渠道?
A：可以，但需：渠道尽调、佣金披露、营销合规审查、客户资料真实性责任划分、反洗钱协同与违规处置条款。

Q100：业务模型写得越"宏大"越好?
A：不是。申请阶段建议采取"可交付、可验证、可持续合规"的业务范围。过度扩张会引起：资本与资源不足、系统不匹配、补件增多、周期拉长。

D｜资本与审慎保障（Q101–Q130）

Q101：MiCA 下 CASP 的资本要求如何确定?
A：与拟提供的服务类型、风险暴露与规模相关。你需要提交：最低资本满足说明、持续自有资金维持机制、财务预测与压力测试。

Q102：资本要在申请时就实缴吗?
A：许多 NCA 会在授权前要求证明资本已到位或具备到位安排（例如原则性批准后注资）。最佳实践：准备银行证明、资金路径、董事会决议与验资/会计证明。

Q103：资本来源需要证明吗?
A：需要。提供：SoF/SoW、资金路径图（money trail map）、相关合同/分红记录/出售资产证明/银行流水等，形成可核验闭环。

Q104：集团注资可以吗?
A：可以，但需要穿透到最终 UBO 的资金来源，且要解释集团资金调拨机制、是否存在抽回风险、是否影响持续经营。

Q105：是否可以用可转换债/股东借款作为资本?
A：通常不建议替代法定资本。若作为补充资金，需要明确：次级性、不可随意撤回、期限、利息安排与对审慎稳健的影响。

Q106：监管会要求保险吗?
A：对部分风险（如托管责任、网络安全责任）可能更偏好有保险或等效保障。需要提供：保单范围、限额、免赔、除外责任与赔付触发条件。

Q107：是否需要准备压力测试?
A：建议准备。场景包括：市场暴跌、交易量激增、稳定币脱锚、供应商宕机、黑客攻击、银行/支付通道中断、集中客户挤兑等。

Q108：如何证明"持续经营能力"?
A：三年财务预测（损益/现金流/资产负债）、关键假设说明、敏感性分析、成本结构（人员/技术/审计/合规），以及融资计划与备选资金来源。

Q109：客户资产与自有资金如何隔离?
A：建立：账务隔离、钱包隔离、权限隔离、对账机制、银行/支付通道隔离（如适用），并在客户条款中明确资产归属与风险。

Q110：能否收取客户预付款或会员费?
A：可以，但需披露、退款规则、是否构成客户资金、以及如何在会计与资产隔离中体现，避免挪用或不透明。

Q111：如何处理客户资产短缺事件?
A：建立应急预案：立即冻结相关操作、内部调查、监管通知、客户沟通、补足机制、保险理赔（如有）、第三方审计与整改。

Q112：可否把客户资产用于质押/再投资?
A：高度敏感且通常不被允许或需要明确授权与极强披露（且可能触及其他监管）。申请初期建议坚决避免此类安排。

Q113：平台是否需要准备赔付政策?
A：若涉及托管与客户资产控制，建议准备：责任边界、赔付触发条件、上限、争议处理与保险覆盖说明。

Q114：是否需要准备资本监控指标（KRI）?
A：建议。包括：资本充足率、现金覆盖月数、运营成本覆盖、重大风险暴露、客户资产规模与集中度等。

Q115：资本是否可以分阶段到位?
A：可能可行，但需要与监管沟通并提供清晰计划与条件（例如：原则性批准后 X 天内注资到位）。

Q116：监管会查我是否"空壳"吗?
A：会。资本只是最低门槛，监管更看"资源是否匹配风险"。托管/平台若资本薄弱、人员不足、系统外包不可控，风险很高。

Q117：是否需要准备财务政策（会计政策）?
A：建议准备。特别是：加密资产计量、手续费确认、客户资产与公司资产的会计处理、收入确认与坏账政策。

Q118：能否使用稳定币作为资本?
A：通常不建议。监管倾向以法币/银行存款等稳定形式满足资本要求。若涉及加密资产，需评估波动与可用性。

Q119：资本存放在银行还是托管机构?
A：通常在银行更易被接受。若放在其他机构，需证明安全性、可用性与监管可核验性。

Q120：是否需要准备资本退出限制政策?
A：建议在董事会层面设定：资本分红/抽回限制、重大支出审批、关联交易审批，确保持续满足审慎要求。

Q121：如何处理关联交易与费用分摊?
A：必须透明：定价公允、合同化、可审计。关联交易是监管重点（尤其集团共享 IT/客服/流动性）。

Q122：是否需要制定反舞弊与反腐败政策?
A：建议。包括：礼品招待、利益冲突申报、员工交易政策、举报机制（whistleblowing）。

Q123：是否需要制定薪酬政策?
A：建议。强调：不激励过度冒险；关键岗位独立性；与合规/风险表现挂钩。

Q124：监管会看我的股东是否有监管历史吗?
A：会。股东/UBO 的合规记录、处罚、诉讼、破产、负面新闻都要披露并解释。

Q125：股东结构复杂会影响周期吗?
A：显著影响。层级多、跨境多、资金路径复杂，补件概率高。建议尽早做穿透图与 SoF/SoW 打包。

Q126：是否需要准备"集团支持函"?
A：若集团为申请实体提供资金/系统/人员支持，建议准备：支持承诺函、SLA、资源分配说明与长期承诺。

Q127：需要准备"退出计划（wind-down plan）"吗?
A：建议准备。包括：停止接客、平仓、客户资产返还、数据保存、供应商终止、员工安排与监管沟通。

Q128：如果业务失败，客户资产如何保障?
A：通过：资产隔离、对账、托管安排、退出计划、清算流程、客户通知与申诉机制。

Q129：是否需要准备恢复计划（recovery plan）?
A：视规模与风险而定。平台/托管类建议准备：资金补充路径、系统恢复、风险事件应对、客户沟通与监管通报。

Q130：资本与 AML 有关系吗?
A：有。AML 系统、合规人员、独立审查、培训、链上分析工具都是持续成本。资本与预算必须覆盖"合规可运行"，否则被认为不可持续。

E｜股东/UBO/适任性（Fit & Proper）（Q131–Q170）

Q131：什么是 Fit & Proper?
A：监管对董事、高管、关键岗位、重大股东/UBO 的适任性评估：诚信、能力、经验、财务稳健、时间投入与声誉。

Q132：哪些人需要做适任性审查?
A：通常包括：董事会成员、CEO/COO/CFO、合规负责人、MLRO、风控负责人、ICT 安全负责人、重大股东及 UBO。

Q133：需要提交哪些适任性材料?
A：一般包括：

- CV（含关键经验与职责）
- 无犯罪记录/诚信声明
- 破产/诉讼/监管处罚披露
- 教育与资格证书
- 推荐信或工作证明
- 时间投入声明与兼职披露
- 利益冲突声明

Q134：监管会做背景调查吗?
A：会。可能包括公开信息检索、监管数据库、媒体负面新闻筛查、制裁/PEP 检索等。建议准备 Negative News Memo（不利信息解释备忘录）。

Q135：曾经有行政处罚还能申请吗?
A：不一定绝对禁止，但需要：披露、解释、整改证明、持续控制措施，且最终取决于处罚性质、时间、严重性及监管判断。

Q136：关键岗位经验不足怎么办?
A：两条路：
1）更换或增配经验更强的人；
2）引入外部专家支持，但不能"外包掉责任"。监管更看"你机构内部是否有足够能力"。

Q137：可以用集团人员兼任关键岗位吗?
A：可以，但要证明：独立性、时间投入、汇报线、权限与可用性；以及不会被集团商业目标干扰。

Q138：董事会需要多少人?
A：取决于规模与风险。平台/托管类通常建议至少 2–3 名董事，且最好包含具备合规/风险/IT 经验的成员。

Q139：董事会是否需要独立董事?
A：不一定硬性，但越高风险业务越建议引入独立性，帮助监督利益冲突与风险治理。

Q140：UBO 不愿提供资料怎么办?
A：不可行。UBO 资料是核心。若无法提供穿透与 SoW/SoF，申请基本会卡死。

Q141：什么是 SoW 与 SoF?
A：SoW（Source of Wealth）：财富如何累积（行业、资产、投资等）；SoF（Source of Funds）：用于注资/运营资金的具体来源与路径（从哪个账户到哪个账户）。

Q142：资金路径证明需要到什么程度?
A：建议做到"可追溯到自然人或可核验实体收入"。提供：合同、分红决议、工资/股权出售证明、银行流水、纳税证明等。

Q143：股东层级太多怎么办?
A：建议简化。层级过多会导致：穿透、控制权、资金路径与关联交易难以解释，监管审查会更严。

Q144：是否需要披露股东协议中的否决权?
A：需要。监管关心"实际控制权"，任何否决权、表决权安排、可转债/期权都可能影响控制权认定。

Q145：股东是否需要提供财务报表?
A：重大股东/集团股东通常需要提供财务信息证明财务稳健与持续支持能力；UBO 则重点 SoW/SoF 与净资产证明。

Q146：关键岗位可以外包给咨询公司吗?
A：可外包部分支持工作，但关键职能责任必须在持牌实体内部承担。外包也需外包治理、审计权与退出机制。

Q147：如何证明"独立性"?
A：通过：汇报线直达董事会、薪酬不与交易量直接绑定、具备否决权、合规审批留痕、可独立调查与报告。

Q148：一个人兼任太多角色会怎样?
A：监管会质疑：是否能履职、是否存在利益冲突、是否导致控制薄弱。高风险业务建议职能分离。

Q149：关键岗位离职怎么办?
A：必须有替补计划（succession plan）：临时任命、外部候选、过渡期控制措施、监管通知流程。

Q150：股东变更是否需要监管批准?
A：重大股权/控制权变更通常需要事先通知或批准，具体取决于本国实施口径。你需要建立"变更评估→监管沟通→实施→留档"的流程。

Q151：董事变更需要报备吗?
A：通常需要。尤其关键岗位/董事变更是重大事项，需提交新任人选适任性材料并等待监管确认。

Q152：高管曾在加密平台工作但平台出过事，会影响吗?
A：可能。需要准备：事件说明、个人职责边界、整改与经验总结、证明个人诚信与能力。

Q153：是否需要进行员工背景调查?
A：建议对敏感岗位（钱包操作、资金、风控、合规）进行背景调查与诚信声明，减少内部舞弊风险。

Q154：员工交易政策必须有吗？
A：必须。包括：申报、禁止内幕交易、限制交易窗口、禁止操纵与与客户交易冲突、违规处分。

Q155：如何管理利益冲突？
A：制定政策与流程：识别→披露→缓释→记录；场景包括：自营/做市、关联方交易、返佣、员工持仓、上币利益等。

Q156：是否需要举报机制（whistleblowing）？
A：建议建立，尤其是金融实体。包括匿名渠道、保护举报人、调查与整改闭环。

Q157：是否需要合规年度计划？
A：需要。包括：监控主题、抽查频率、培训计划、制度更新、内审协作、监管报告节点。

Q158：关键岗位绩效如何设定才合规？
A：避免只看业务增长。合规岗位可用：整改完成率、监控覆盖、培训完成率、事件响应质量、审计发现关闭等指标。

Q159：董事会是否需要定期评估自身？
A：建议。包括：技能矩阵、培训、会议效率、监督有效性，形成治理证据。

Q160：监管会问什么适任性问题？
A：常见：你对业务风险理解？如何管理利益冲突？AML 如何运行？ICT/外包如何可控？重大事件怎么响应？你每周投入多少时间？谁对什么决策负责？

Q161：适任性材料怎么写更容易过？
A：核心是：与岗位职责对应（不是堆履历），突出：监管经验、风险管理、系统与流程落地经验、重大事件处理经验，并用证据支撑。

Q162：是否需要准备"面谈答题稿"？
A：强烈建议。按角色：董事/CEO、合规负责人、MLRO、CTO/安全负责人分别准备 50–100 问标准答案。

Q163：如果 UBO 是海外高净值人士，资料怎么准备？
A：准备：身份证明、住址证明、税务居民声明、资产证明、收入来源证明、银行推荐信（如有）、资金路径与解释备忘录、制裁/PEP 筛查记录。

Q164：如果 UBO 是公司/基金，怎么办？
A：必须穿透到最终自然人；若是上市公司需提供上市信息与控股结构；基金需提供基金文件、管理人信息、投资者穿透要求按本国口径执行。

Q165：若涉及信托结构？
A：需披露：委托人、受托人、受益人、保护人等，并解释控制权与资金来源。信托结构在申请中往往会被更严格审查。

Q166：负面新闻如何处理？
A：不要躲。做 Negative News Memo：事件事实、时间线、影响、整改、当前控制措施、第三方证明，形成"可接受解释"。

Q167：适任性材料是否需要公证/认证？
A：视本国要求。常见需要：公证、海牙认证、翻译。建议一开始就按"可递交标准"准备，减少补件。

Q168：适任性材料更新频率？
A：获牌后也要持续更新：岗位变动、负面事件、利益冲突更新、年度声明等。

Q169：适任性与 AML 有什么交叉？
A：若股东/高管有洗钱、欺诈、制裁风险或高风险背景，会直接影响 AML 风险评级与监管信任度。

Q170：适任性审查失败怎么办？
A：通常只能更换人选或补充更强的治理与控制措施并重新评估，但是否接受取决于监管态度。最佳策略是申请前先做内部适任性"自检"。

F｜AML/KYC/制裁/交易监控/STR（Q171–Q230）

Q171：CASP 必须执行 KYC 吗？
A：必须。开户前完成 CDD，识别客户与（如适用）UBO，评估风险并实施持续监控。

Q172：CDD 的最低要素是什么？
A：身份识别与验证、受益所有人识别、业务关系目的与性质、风险评估、制裁/PEP 筛查、持续监控与定期复核。

Q173：什么情况要做 EDD？
A：高风险客户/交易/国家、PEP、复杂结构、异常资金来源、混币/暗网关联、可疑行为等。EDD 包括更强的 SoW/SoF、管理层批准、更频繁复核。

Q174：制裁筛查要覆盖哪些对象？
A：客户、UBO、授权人、受益人、交易对手方（如可得）、链上地址（尤其与制裁相关实体/地址）、供应商与关键外包方。

Q175：链上地址也要筛查吗？
A：强烈建议。尤其提供提币/转账/托管服务时，地址风险筛查与链上监控是监管重点。

Q176：交易监控怎么做？
A：设置规则+模型：大额、频繁、结构化分拆、短进短出、与高风险地址交互、混币器、跨链桥异常、稳定币异常等，并形成报警工单→人工复核→处置/STR 决策→留痕。

Q177：什么是 STR？
A：可疑交易报告（Suspicious Transaction Report），当怀疑与洗钱/恐怖融资相关时，需要向本国 FIU 报告。必须保存决策记录与支持证据。

Q178：STR 是否必须在确定犯罪后才报？
A：不需要"确证犯罪"。达到"怀疑"阈值即可报。延迟或不报会带来严重监管风险。

Q179：报 STR 会通知客户吗？
A：通常禁止"tipping-off"（泄密通知）。你需建立内部保密与权限控制，避免告知客户导致调查受阻。

Q180：如何做客户风险评级？
A：基于客户类型、地域、产品、渠道、交易行为、链上风险、制裁/PEP 等维度打分，形成风险等级并驱动：限额、EDD、复核频率、监控强度。

Q181：如何处理高风险国家客户？
A：可采取：拒绝、限制服务、强化 EDD、降低限额、更高频监控、管理层批准。需在政策中写明并留痕。

Q182：如何处理混币器相关交易？
A：通常视为高风险：触发报警→加强尽调→要求解释与证明→必要时拒绝/冻结→评估 STR。

Q183：如何处理暗网关联地址？
A：高风险：冻结/限制、加强尽调、报告义务评估、持续监控、必要时 STR。

Q184：是否需要保存 KYC 资料多久？
A：依本国 AML 法（通常 5 年或更长）要求。必须确保可检索、可审计、数据保护合规。

Q185：如何处理资料过期？
A：建立定期复核：低风险年度/两年，高风险更频繁；触发事件（异常交易、负面新闻、地址风险上升）可提前复核。

Q186：能否接受"仅邮件/简化 KYC"？
A：不建议。监管倾向要求可靠验证与反欺诈机制（活体检测、证件真伪、地址证明、设备指纹等）。

Q187：如何防止冒名开户？
A：引入：活体检测、证件 OCR/防伪、黑名单、设备指纹、IP/地理位置异常检测、行为分析、二次验证与人工复核。

Q188：企业客户 KYC 的重点是什么？
A：公司注册与存续证明、股权结构与 UBO 穿透、董事与授权人、业务性质与资金来源、财务信息、交易目的、制裁/PEP 筛查。

Q189：如何验证企业 UBO？
A：穿透至自然人：股东名册、公司注册处文件、章程、股东协议、控制权解释、必要时公证/认证文件。

Q190：如果企业客户拒绝披露 UBO？
A：一般应拒绝建立业务关系或限制服务，且记录原因并评估 STR。

Q191：如何管理代理商带来的客户？
A：代理商不是挡箭牌。最终责任在 CASP。需对代理商尽调、协议约束、资料质量抽查、营销合规监督与违规处分条款。

Q192：如何做交易限额与 AML 联动？
A：按风险等级设置：充值、交易、提现、单日/单月限额；风险升高自动降额或触发 EDD。

Q193：如何处理异常大额提现？
A：触发：二次验证、地址风险评估、资金来源核查、管理层批准、必要时延迟或拒绝并评估 STR（注意合法性与合同条款）。

Q194：如何管理"可疑但未报 STR"的情形？
A：必须留痕：为何未达到怀疑阈值、采取了哪些缓释措施、是否加强监控、复核计划、负责人与审批链条。

Q195：是否需要 AML 培训？
A：必须。入职培训 + 年度培训 + 岗位专项培训；保留签到、材料、测试成绩与复盘记录。

Q196：是否需要 AML 独立审查？
A：强烈建议。第三线或外部独立审查覆盖：政策、执行、系统、STR 决策、记录保存与整改闭环。

Q197：如何处理制裁命中？
A：立即冻结/停止交易、内部升级、评估是否向监管/执法通报、保存证据、禁止 tipping-off，按政策执行并记录。

Q198：如何处理 PEP 命中？
A：不一定拒绝，但要 EDD：高管批准、加强 SoW/SoF、持续监控、定期复核、交易异常阈值更低。

Q199：如何处理媒体负面新闻客户？
A：提升风险等级、加强尽调、必要时限制/终止关系，记录判断依据并评估 STR。

Q200：如何处理加密资产"来源证明"？
A：通过链上分析、交易所出入金记录、历史地址关联、购买凭证、矿工收入证明、OTC 合同等，形成合理解释与证据链。

Q201：如何处理跨链桥资产来源？
A：跨链桥增加溯源难度，通常提高风险。需更强链上分析、更多佐证文件、降低限额或拒绝高风险路径。

Q202：是否允许现金入金？
A：高风险。多数合规框架倾向限制或禁止现金相关路径，若存在必须极强控制与记录并评估监管接受度。

Q203：如何识别“结构化拆分”洗钱？
A：识别：多笔小额、短周期重复、多个账户协同、同一设备/IP/地址聚合；触发增强监控与调查。

Q204：如何识别“洗售交易/刷量”？
A：监控：自成交、关联账户对倒、异常订单撤单、成交集中度异常、费率套利；并可触发市场滥用调查与 AML 评估。

Q205：如何处理异常高频交易？
A：区分：正常做市/量化 与 可疑刷量；需要更强的客户分类、做市协议、风控阈值与监控模型。

Q206：是否需要保存通话/聊天记录？
A：若客户指令通过电话/聊天渠道形成，建议保留。至少保留关键指令与确认记录，满足可追溯与争议处理需要。

Q207：如何与 FIU 沟通？
A：通过 MLRO 统一口径；建立 STR 报送流程、回执管理、后续补充材料机制与保密制度。

Q208：STR 报送后还要做什么？
A：持续监控相关客户与交易、执行 FIU 指令（如冻结/延迟）、内部复盘与模型优化。

Q209：如何处理“误报 STR”的担忧？
A：合规上宁可合规报送也不要漏报。关键是：建立合理的怀疑阈值与决策留痕，确保你报送有依据。

Q210：MLRO 日常需要做什么？
A：风险评估更新、监控规则审查、STR 决策与报送、培训、政策更新、监管沟通、独立审查与整改跟踪。

Q211：如何做 AML 年度风险评估？
A：覆盖：客户、产品、渠道、地域、交易类型、链上风险、外包、制裁与欺诈；输出：风险矩阵+缓释计划+资源预算。

Q212：AML 与数据保护冲突怎么办？
A：需在 GDPR 合规框架下处理。通常 AML 属于法定义务基础，可处理必要数据，但仍需最小化、访问控制、保留期限与告知义务。

Q213：是否可以把 AML 完全外包？
A：不可以。可外包工具/部分操作，但责任在持牌实体。监管会审查外包治理与内部监督能力。

Q214：交易监控一定要上系统吗？
A：对规模化平台/托管，强烈建议系统化。仅人工监控无法覆盖与留痕，会被认为不可持续。

Q215：如何对接链上分析供应商？
A：需要：尽调、合同审计权、数据与模型透明度、可解释性、SLA、退出与替代供应商计划。

Q216：如何处理“客户拒绝补资料”？
A：按政策限制/终止服务、冻结或拒绝交易、记录并评估 STR；避免继续提供服务导致监管风险。

Q217：如何处理“长期不活跃客户”？
A：定期复核频率可降低，但若重新激活或出现异常交易，需要重新验证与更新 KYC。

Q218：如何识别恐怖融资风险？
A：关注：小额频繁、特定地缘、特定组织关联、资金流向异常、链上地址与已知风险实体关联；并执行制裁筛查与 STR 评估。

Q219：是否需要建立欺诈风控（anti-fraud）？
A：需要。包括：账户接管、SIM 交换、钓鱼、社工欺诈、API 滥用、退款欺诈等，与 AML/客户保护强相关。

Q220：如何防止内部人员挪用资产？
A：权限分层、双人复核、冷钱包多签、操作日志不可篡改、定期审计、离职交接与权限回收。

Q221：如何管理“私钥接触人员”？
A：最小化原则：密钥生成与备份仪式、关键人分离、强身份认证、签名仪式记录、定期轮换与审计。

Q222：如何处理“客户要求绕过 KYC”？
A：拒绝。并记录沟通内容、风险评级上调，必要时评估 STR。

Q223：如何处理“第三方付款入金”？
A：高风险。通常限制或要求证明付款人与客户关系，并执行增强尽调与审批。

Q224：如何处理“公司账户由个人代操作”？
A：需授权核验：董事会决议/授权书/受权人身份验证，并监控异常行为。

Q225：是否需要建立客户黑名单？
A：建议。包括：欺诈、制裁、严重违约、拒不配合尽调、可疑行为等；并有复核与解除机制。

Q226：如何处理“误冻结客户资产”的投诉？
A：需要：条款依据、证据留存、内部复核、沟通话术、申诉机制与升级路径，确保合规同时减少争议。

Q227：如何管理“疑似市场操纵”的客户？
A：触发市场监控与 AML 调查，限制交易或冻结，记录证据并评估监管报告义务。

Q228：是否需要对客户进行教育？
A：建议。提供风险教育、诈骗提示、地址安全提醒、双重验证引导等，可降低投诉与欺诈风险。

Q229：如何处理“客户交易指令争议”？
A：保留指令证据：订单日志、IP/设备、时间戳、双重确认记录、客服沟通记录；并有争议处理 SOP。

Q230：AML 体系最关键的交付是什么？
A：不是手册，而是"制度+系统+证据链"：风险评估、KYC 工作流、监控工单、STR 决策记录、培训与审计整改闭环。

G｜ICT / DORA / 外包治理 / 钱包安全（Q231–Q280）

Q231：DORA 对 CASP 影响大吗？
A：非常大。DORA 要求 ICT 风险治理、事件管理、韧性测试、第三方风险管理更硬；监管审查会要求你提供可验证证据（不是口头）。

Q232：ICT 治理需要董事会参与吗？
A：需要。董事会应批准 ICT 风险框架、关键政策、外包策略与重大事件响应，并定期接收报告。

Q233：必须有 CISO 吗？
A：未必强制，但必须有明确责任人（ICT 风险责任人/安全负责人）与资源，能对渗透测试、漏洞管理、事件响应负责。

Q234：钱包安全的最低要求是什么？
A：冷/热分离、热钱包限额、多签、权限分层、MFA、日志审计、对账、异常提现审批、密钥管理与备份、事故响应与演练。

Q235：多签门限怎么设定？
A：常见 M-of-N（如 2/3、3/5），并要求关键人分离与替补机制；门限应与风险、资产规模与运营效率平衡。

Q236：是否必须用 HSM？
A：强烈建议用于关键密钥管理。若不用，需要解释替代控制与风险缓释，准备接受监管质疑。

Q237：冷钱包签名仪式要记录吗？
A：要。记录：参与人、时间、地点、签名目的、资产数量、授权审批、视频/日志（按政策），形成可审计证据链。

Q238：热钱包如何控制风险？
A：限额、白名单、地址风险评分、双人复核、大额提现延迟与人工复核、异常行为检测、即时告警。

Q239：如何做权限矩阵（RBAC）？
A：列明每个角色可做什么、审批链条、双人复核点、紧急权限使用与审计。敏感权限必须最小化与定期复核。

Q240：日志需要保存多久？
A：按本国要求与风险需要。关键日志应不可篡改、可检索、可导出，用于审计与事件取证。

Q241：是否需要 SOC / SIEM？
A：对平台/托管建议配置（自建或外包），实现集中日志、告警、事件联动与取证能力。

Q242：渗透测试频率？
A：至少年度；重大变更、上新系统、外包切换后应追加。要有整改闭环报告。

Q243：漏洞管理怎么做？
A：漏洞扫描→评级→修复→复测→关闭。要有 SLA（高危 24–72 小时等）与例外审批机制。

Q244：事件响应必须包含哪些内容？
A：事件分级、隔离与遏制、取证与日志保全、客户与监管沟通模板、恢复计划、复盘与改进。

Q245：是否需要事件演练？
A：必须。包括桌面推演与实战演练；记录演练结果、问题清单与整改完成情况。

Q246：BCP/DR 必须有 RTO/RPO 吗？
A：必须。定义关键业务与系统的恢复目标，并通过演练验证。

Q247：云服务外包需要注意什么？
A：尽调、合同审计权、数据所在地、加密与密钥管理、SLA、可用性、退出与迁移计划、分包商管理。

Q248：外包是否需要监管通知？
A：很多 NCA 要求对关键/重要外包进行通知或审批。必须建立外包登记册与重大外包变更通知流程。

Q249：什么是"关键外包"？
A：影响核心服务、客户资产安全、ICT 安全、合规执行的外包，例如：托管、交易核心、KYC、链上分析、云基础设施、客服核心系统等。

Q250：外包合同必须包含哪些条款？
A：审计权、监管访问权、数据归属与访问、SLA、分包限制、事件通报、业务连续性、退出/迁移、保密与安全要求、责任与赔偿。

Q251：如何做外包尽调？
A：供应商背景、财务稳健、合规记录、信息安全认证、渗透测试与审计报告、数据处理能力、地缘风险、分包链条。

Q252：供应商宕机会怎样？
A：必须有应急：切换方案、降级服务、备用供应商、手工流程、客户沟通模板与监管通报流程。

Q253：API 安全怎么做？
A：认证授权、速率限制、防重放、IP 白名单、密钥轮换、异常调用监控、审计日志、最小权限。

Q254：如何防止内部滥用权限？
A：双人复核、权限分离、定期权限审计、操作留痕、异常告警、离职即时回收权限。

Q255：数据保护（GDPR）与日志保存冲突？
A：通过最小化、访问控制、保留期限、合法性基础（AML/安全义务）、脱敏与加密实现平衡。

Q256：是否需要数据分类分级？
A：建议。客户身份信息、交易数据、密钥材料、审计日志等应分级管理并有不同访问控制。

Q257：是否需要代码审计？
A：对自研系统建议；对外包系统，至少需要供应商提供安全审计与测试报告，并具备你方复核与验证能力。

Q258：如何管理变更（Change Management）？
A：变更申请→风险评估→审批→测试→上线→回滚计划→上线后监控→复盘。重大变更应通知合规与风险。

Q259：如何管理版本发布？
A：灰度发布、回滚、监控、发布记录、责任人、窗口期安排；关键系统发布需更严格审批与测试。

Q260：如何防止 DDoS？
A：CDN/WAF、限流、流量清洗、弹性扩容、监控告警、应急预案与演练。

Q261：如何防止账户接管（ATO）？
A：MFA、设备指纹、异常登录检测、登录地理位置/行为分析、密码策略、风险验证与冻结机制。

Q262：如何防止钓鱼与社工？
A：客户教育、反钓鱼码、客服验证流程、敏感操作二次确认、异常通道识别。

Q263：如何管理密钥轮换？
A：制定轮换策略、紧急轮换机制、轮换记录与审计；轮换需与业务连续性联动。

Q264：如何管理第三方库与依赖？
A：SBOM、依赖扫描、漏洞补丁、版本锁定、供应链安全审查。

Q265：如何做"安全指标（KRI）"？
A：事件数量、修复时效、渗透测试发现、异常登录率、提现拒绝率、供应商可用性、告警响应时间等。

Q266：是否需要定期向董事会报告 ICT 风险？
A：需要。建议月度/季度报告，重大事件即时报告，形成治理证据链。

Q267：如何做 IT 外包退出（Exit Plan）？
A：数据迁移、功能替代、并行运行、客户影响评估、时间表、责任分工、成本预算、回滚方案。

Q268：是否需要独立第三方安全审计？
A：强烈建议，尤其托管/平台。提供第三方审计报告可增强监管信任。

Q269：如何处理"钱包被盗"事件？
A：立即止损（冻结/暂停）、取证保全、内部调查、监管与客户沟通、赔付评估、漏洞修复、复盘与防再发。

Q270：如何处理"供应商数据泄露"？
A：按合同与事件流程：通知、隔离、评估影响、监管与客户通报（按 GDPR/DORA）、补救措施、必要时终止合作与迁移。

Q271：是否需要对员工进行安全培训？
A：必须。钓鱼演练、密码与设备安全、数据保护、事件上报流程等。

Q272：是否需要演练 DR 恢复？
A：必须。演练要验证 RTO/RPO，形成测试报告与改进计划。

Q273：如何管理移动端安全？
A：设备绑定、越狱检测、加密存储、反调试、证书固定、风控策略与异常检测。

Q274：如何管理交易系统的公平性？
A：防止操纵与内部滥用：撮合透明、优先级规则、延迟与撮合日志、异常监控、权限隔离。

Q275：如何证明"系统可审计"？
A：通过：完整日志链条、工单系统、权限与审批记录、对账记录、演练报告、第三方测试报告。

Q276：如何管理数据质量（报表所需）？
A：建立数据字典、ETL 记录、数据校验规则、报表口径一致性检查与追溯机制。

Q277：如何准备监管检查（on-site / off-site）？
A：准备：政策库、日志与工单导出、权限审计记录、外包合同与尽调、报表与审计包、培训与演练记录、投诉台账。

Q278：如何做业务监控与告警？
A：交易量异常、系统延迟、提现异常、KYC 失败率、欺诈告警、链上风险告警，形成监控看板与升级机制。

Q279：如何处理"系统与条款不一致"？
A：这是监管雷区。必须：条款与实际收费、限额、风控、处理时限完全一致；变更需合规审批与客户通知。

Q280：ICT/DORA 最常被问的 5 个问题？
A：1）关键外包如何控制？2）退出计划是否可行？3）BCP/DR 演练证据？4）钱包与密钥如何安全可审计？5）重大事件如何分级通报与复盘？

H｜客户保护、投诉、营销与持续监管（Q281–Q300）

Q281：客户条款（T&C）必须包含什么？
A：服务范围、费用与点差、资产归属与隔离、充提规则、风险披露、暂停/冻结条件、争议处理、数据处理、责任限制与赔付政策（如适用）。

Q282：是否需要"风险披露单独文件"？
A：建议。面向零售客户尤其要清晰、可理解，避免把风险埋在长条款中导致被认为误导。

Q283：投诉处理流程怎么设计？
A：受理→分类→调查→回复→升级→复盘。设定 SLA（如 2 个工作日受理确认、15 个工作日内回复等），并保留台账与证据。

Q284：投诉数据要上报吗？
A：部分 NCA 会要求统计与报送，至少内部要作为风险指标向董事会报告，形成改进闭环。

Q285：营销宣传的红线是什么？
A：不得误导、不得暗示"保本/保证收益"、不得夸大监管背书、不得虚假披露费用或风险、不得对未获授权国家开展不合规招揽。

Q286：KOL/代理营销如何合规？
A：必须：合同化、披露关系与佣金、脚本合规审查、违规监控与处罚、留存发布记录与素材。

Q287：如何管理"交易暂停/下架公告"？
A：制定模板：原因、影响范围、客户资产处置、恢复时间预估、客服渠道、风险提示；保留审批与发布记录。

Q288：如何处理"客户资产冻结"争议？
A：条款依据 + 证据链 + 内部复核 + 申诉机制 + 合规保密（避免 tipping-off）。必要时提供第三方审计或监管沟通记录摘要（可披露范围内）。

Q289：获牌后需要提交哪些报表？
A：各国会有差异，但趋势是：年度审计报表、监管定期报表（业务量、客户资产、投诉、事件）、重大事件通报、关键外包通知等。建议按"报表日历"管理。

Q290：获牌后是否会被现场检查？
A：可能。尤其当业务规模上升、发生重大事件、投诉较多或存在市场风险。必须保持可审计证据链与快速导出能力。

Q291：重大事件需要通知监管吗？
A：一般需要（具体按本国规则与 DORA 事件分类）。重大安全事件、客户资产风险、系统中断、重大外包事故、重大合规违规等应及时通报。

Q292：如何准备年度审计？
A：提前建立：财务与业务数据口径一致性、对账机制、日志与工单、外包合同与执行证据、合规培训与监控记录，避免审计季"补档"。

Q293：是否需要年度合规报告？
A：强烈建议。包括：合规监控结果、重大问题与整改、培训、投诉、监管沟通、下一年度计划。

Q294：如何做员工年度培训计划？
A：分层：全员 AML/合规、敏感岗位专项（钱包操作/客服/风控）、管理层专题（治理/外包/事件响应），每次培训有材料、测试与记录。

Q295：是否需要演练（BCP/DR/事件响应）年度计划？
A：需要。至少年度一次全流程演练，并对关键外包参与方进行联合演练或接口测试。

Q296：业务变更（新增服务/新国家）要做什么？
A：变更评估（法律+合规+AML+ICT）→董事会批准→监管沟通/通报→更新条款与披露→系统与流程上线→培训→留档。

Q297：如何管理"新产品上线审批"？
A：产品委员会机制：合规审查、风险评估、AML 影响评估、ICT 安全评估、客户披露与营销审批、试运行与复盘。

Q298：如何衡量合规体系有效性？
A：KRI/KPI：STR 质量、监控覆盖、审计发现、整改关闭率、投诉率、事件响应时效、培训完成率、权限审计结果等。

Q299：监管最喜欢看到什么？
A：可解释、可验证、可审计的体系：

- 文件与系统一致
- 决策留痕清晰
- 外包可控
- AML 可运行
- 事件响应与演练真实
- 报表按时且口径一致

Q300：成功获批 CASP 的"一句话秘诀"？
A：把申请做成"可运营的合规系统"，而不是"好看的文件包"：服务定性清楚、股东适任与资金来源闭环、AML 可运行、ICT/DORA 可审计、客户保护可验证、持续报表能力可落地。

15）我司服务建议与配套说明（交付包/流程/沟通节奏）

15.1 仁港永胜交付模式（从"拿牌"到"可持续运营"）

（1）Preparation：结构与差距评估（2–3 周）

- 业务定性与服务范围定稿（决定资本/系统/岗位）
- 股东/UBO 尽调路线与 SoF/SoW 证据链设计
- ICT/DORA 架构蓝图与外包清单（含合同条款框架）
- 输出：差距清单 + 项目计划甘特图 + 预算表

（2）Application：文件与系统证据链交付（6–10 周）

- Programme of Operations + Business Plan（可递交版）
- AML/CFT 手册 + STR 决策树 + 风险评估 + 培训计划
- ICT/DORA：钱包安全说明书、权限矩阵、日志与审计轨迹、BCP/DR、渗透测试计划
- Fit&Proper + 股东/UBO 包（CV 改写、声明、证据链、解释备忘录）
- 建立 RFI 应答机制（Q&A Log + 战情室）

（3）Post-Licence：获批后持续合规（长期）

- CASP Return 报送支持与审计包协同（按 MFSA 指引）
- 重大变更报备、外包通知、年度培训与演练、内审与整改
- 护照通报与跨境营销合规（Article 65 通报路径与材料包）

15.2 沟通节奏（建议）

- 每周项目例会（合规/法务/技术/运营四方）
- 关键里程碑评审（服务范围、外包、BP、AML、ICT、递交包、RFI 回合）
- 文档版本管理与证据链归档（便于监管抽查）

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

16.1 MiCA 下的持续合规主轴（CASP 维度）

- 治理与内部控制：三道防线、利益冲突、投诉、营销合规
- 审慎保障：持续满足资本/保障与风险覆盖，财务预测与压力测试动态更新
- 客户保护：资产隔离、披露透明、客户协议与费用结构一致性
- 外包治理：关键外包登记、审计权、退出机制、重大外包变更通知（MFSA 外包通知表）

16.2 马耳他 MFSA 的"报表化"要求（CASP Return）

MFSA 已发布 CASP Return，并提供"编制指引"，其中明确：

- **AACR（审计年度报表）须在会计参考日后 6 个月内提交，并附 Audit Pack**；
- 报送通过 LH Portal 递交，并强调按年度累计口径等编制要求。

16.3 AML（本国 AML 法 + 欧盟 AML 趋势）落地要点

- 风险评估（客户/产品/地域/渠道/交易/链上风险）
- CDD/EDD、UBO 穿透、SoW/SoF、制裁/PEP 筛查
- 交易监控（规则库+报警工单+人工复核）与 STR 决策留痕
- 记录保存、培训、独立审查

仁港永胜建议：把 AML 做成"制度+系统+证据链"，并把 STR 决策链条（未报送原因）纳入可审计文档库。

17）税务与法律配套（CIT/VAT/预提税/雇佣/架构建议）

- CIT（企业所得税）：利润口径、集团费用分摊与转让定价、持续经营与资本规划联动
- VAT：平台费/托管费/API 费/会员费/点差/服务费的 VAT 属性与跨境处理

- WHT：向非居民支付服务费/特许权使用费/利息等的预提税与税协适用
- 雇佣：本地雇员成本、社保、远程雇佣与 PE 风险
- 法律文件：客户条款、隐私/GDPR、外包合同（审计权/退出）、公司治理文件、AML 政策库

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
适用对象：拟在马耳他申请 **MiCA CASP 牌照**（交易平台 / 托管 / 兑换 / 经纪 / 投顾 / 组合管理 / 转账等）

17）税务与法律配套

（CIT / VAT / 预提税 / 雇佣 / 架构建议｜监管 + 实操）

本章目标：**让 CASP 在“合规持牌”的同时，实现税务可控、结构可持续、跨境不踩雷。**
监管核心关注：**是否存在“空壳”或“税务套利式结构”**，是否与 MiCA 的 **substance（实质经营）** 要求相冲突。

17.1 企业所得税（CIT｜Corporate Income Tax）

（1）马耳他名义税率与实际税负逻辑

- **名义企业所得税率：35%**
- 但马耳他实行**股东退税（Tax Refund）制度**：
  - 合规分红后，非居民股东可申请 **6/7、5/7、2/3 或 100%** 不同类型退税
  - **实际有效税率可降至约 5%–10% 区间**（取决于收入性质）

⚠ **MiCA + MFSA 实操重点**：

> **退税≠监管套利**
> 若 CASP 被认定为“无实质运营，仅为税务通道”，将直接影响：

- 牌照审批（substance 不足）
- 持续监管（被要求增加本地资源）
- 与银行/审计师合作

结论：
马耳他 CASP 应以“合规实质 + 税务优化”并行，而非极端税务导向结构。

（2）CASP 常见应税收入类型

收入类型	税务属性
交易手续费 / 点差	经营性收入（CIT）
托管费 / 钱包管理费	服务收入（CIT）
API / 技术服务费	可能涉及转让定价
自营交易收益	需特别区分是否允许
利息 / 其他投资收益	分类处理

强烈建议：
在 **Business Plan + Transfer Pricing 文件**中清楚界定各类收入归属与定价机制。

17.2 增值税（VAT）

（1）加密资产相关 VAT 基本原则（欧盟）

- **加密货币本身的兑换（类似法币）通常免 VAT**
- 但以下**不一定免税**：
  - 平台服务费
  - 技术服务费
  - 托管服务
  - 会员费 / 订阅费

（2）马耳他实操重点

- 是否向 **欧盟客户**提供服务

- 是否触发 **OSS / IOSS** 或跨境 VAT 申报
- 是否存在 **B2C 数字服务** 属性

建议：
在 BP 中明确：

- 收费模式
- 客户地域
- VAT 处理逻辑（免税 / 标准税 / 反向收费）

17.3 预提税（WHT｜Withholding Tax）

（1）马耳他优势

- **对分红一般不征收预提税**
- 对多数服务费 / 利息支付，预提税压力较低
- 与多国有良好的 **双边税收协定（DTA）网络**

（2）监管与合规注意

- 向关联方支付技术费、管理费、品牌费
  → 需有**真实服务 + 转让定价文件**
- 避免被认定为 **利润转移（BEPS 风险）**

17.4 雇佣、人员与社保

（1）本地雇佣要求（Substance）

- MFSA 在 MiCA 下**高度关注本地实质**：
  - 合规负责人
  - MLRO
  - ICT / 风险 / 管理层
- 纯“名义董事 + 外包团队”模式风险极高

（2）雇佣成本

- 薪俸税（PAYE）
- 社会保险（Social Security）
- 董事与高级管理层需明确：
  - 雇佣关系 or 服务合同
  - 税务居民身份

建议：
提前设计 **“最低可接受本地团队配置模型”**，避免被要求临时补人。

17.5 推荐公司与集团架构（示例）

（1）标准合规结构（推荐）

```
控股公司（HK / EU / Offshore）
↓
马耳他 CASP 持牌公司
（实质经营 / 系统 / 合规）
```

（2）集团支持模式（可行）

- IT / 开发 / 客服：可集团共享（需外包治理）
- 合规与 MLRO：**核心必须在马耳他**

- 钱包或托管：可集团，但需**完全透明 + 审计权**

⚠ **绝对不建议**：

- 马耳他“空壳”+ 全部海外操作
- 无清晰转让定价与外包治理

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

（ESMA Level 2/3｜AMLA｜DAC8｜未来 3–5 年）

- **ESMA Level 2/3（RTS/ITS/Guidelines）持续强化“模板化、数据化、可审计”**：申请材料与持续报表会越来越强调字段一致性、日志与证据链、披露与系统执行一致。
- **DORA 驱动 ICT 与外包监管从“有制度”走向“可验证韧性”**：渗透测试、事件分级、第三方风险、退出预案会更硬。
- **DAC8（加密税务信息交换）将推动税务数据字典与客户税务自证流程前置**：建议在开户与数据治理阶段预留字段与报表能力。

18.1 ESMA Level 2 / Level 3：

MiCA 正在从“原则监管”走向“模板监管”

核心趋势

- 更多 **RTS / ITS / Guidelines**：
  - 报表字段统一
  - 文件模板化
  - 风险指标量化

对 CASP 的影响：

- **BP、AML、ICT 文件必须“字段级可对齐”**
- 系统日志、监控数据将成为监管重点

18.2 AMLA（欧盟反洗钱管理局）

AMLA 将带来：

- 更统一的欧盟 AML 执法
- 对高风险 CASP 的直接介入
- 对 STR、制裁、链上分析的更高要求

结论：
AML 不是“文件工程”，而是长期系统工程。

18.3 DAC8（加密税务信息交换）

- 强制加密资产服务商向税务机关报送：
  - 客户身份
  - 交易金额
  - 钱包地址
- 数据将自动交换至客户税务居民国

影响：

- KYC 字段前置
- 数据治理与报表系统升级
- 客户隐私合规（GDPR）要求更高

18.4 DORA（数字运营韧性法案）

- ICT 外包
- 云服务
- 钱包托管
- 灾备与演练

未来监管口径：

> “你能不能抗住一次真实事故？”

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

第一阶段｜Preparation（准备期）

目标：一次性把“方向”定对

- 服务范围定性（避免选错 CAS 服务）
- 股东/UBO 穿透与 SoF/SoW 路径设计
- ICT 架构与外包清单（DORA 思路）
- 本地团队配置模型
- 预算与时间轴

失败案例 80% 死在这里没做清楚

第二阶段｜Application（申请期）

目标：监管可读、补件可控

- Programme of Operations + BP
- AML/CFT 全套制度 + STR 决策链
- ICT / 钱包 / BCP / DR
- Fit & Proper 包（董事/MLRO/高管）
- 建立 **RFI 战情室**

核心：**回应速度 + 证据链完整性**

第三阶段｜Post-Licence（获牌后）

目标：不被吊销、不被限制、不被罚

- 定期监管报送
- 年度审计 + AML 独立审查
- 培训与演练
- 重大变更报备
- 护照扩展与跨境营销审查

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

20.1 申请阶段

- MiCA CASP Business Plan（监管版）
- Programme of Operations（流程图级）
- Master Checklist（A–I）
- 股东/UBO SoF/SoW 路径包
- Fit & Proper 文件包

- RFI Q&A Pack（补件专用）

20.2 合规与系统

- AML/CFT 手册（含 STR 决策树）
- Risk Register（含 KRI / KPI）
- ICT / DORA 合规包
- 外包治理与合同条款库
- 钱包安全与权限矩阵

20.3 获牌后

- 年度合规日历
- 监管报表模板
- 培训材料
- 演练方案
- 护照通报文件包

21）唐生结论：马耳他在 MiCA 版图中的定位

马耳他适合两类项目：

1. **希望在欧盟做"可持续合规运营"而不是"低门槛套利"的团队**：MFSA 已把 MiCA 申请、外包、报表与持续义务做成可下载、可递交、可审计的体系（Rulebook + Forms + CASP Return + Outsourcing Notification）。
2. **既有 VFA 体系背景、计划迁移到 MiCA 的主体**：马耳他通过 Chapter 647 推动 VFA 退场并设置过渡安排；对"迁移路线"更友好，但对"证据链"要求也更硬。

成功关键不在"写得漂亮"，在于四件事：

- 股东/UBO SoF/SoW 闭环与声誉风险可控
- 关键岗位真实可履职（独立性 + 资源 + 汇报线）
- ICT/外包按 DORA 级别一次性建好（可审计、可演练、可退出）
- 把 AML 做成"制度+系统+证据链"(STR 决策留痕可解释)

马耳他在 MiCA 版图中的定位

一句话总结：马耳他不是“最快”，但非常适合“长期合规运营的 MiCA 中枢”。

21.1 适合谁?

- 真正打算在欧盟长期经营的 CASP
- 有交易平台 / 托管 / 机构客户目标的团队
- 重视银行、审计、机构合作的项目

21.2 不适合谁?

- 想“低成本、空壳拿牌”的项目
- 无法提供本地实质与合规团队的团队
- 只想短期套利或转卖牌照的结构

22）项目执行计划与甘特图（里程碑）

- Week 1–2：服务范围定稿 + 差距评估 + 预算
- Week 3–6：公司/实质/岗位与外包清单定稿
- Week 7–14：BP + AML + ICT/DORA + 合同披露 + 股东/适任性包定稿
- Week 15：LH Portal 递交
- Week 16–28：完整性审查 + RFI 补件 + 面谈（如有）

- Week 29–36：条件落实（注资/保障/系统验收/培训演练）→ Go-live
  （如为迁移主体，需按过渡安排倒排节点，避免错过窗口。）

23）监管审查重点矩阵（资本/适任性/AML/ICT/客户保护/护照）

审查模块	监管关注点	申请人必须提交/展示
运营方案	服务定性、客户旅程、资金/资产路径可审计	Programme of Operations + 流程图/对账逻辑
资本/保障	风险覆盖与持续经营	资本方案 + 3 年预测 + 压力测试
董事适任性	胜任/诚信/时间投入/冲突	CV + 声誉声明 + 授权矩阵
股东/UBO	穿透 + SoF/SoW 闭环	结构图 + Money Trail Map + 解释备忘录
AML	风险评估、监控、STR 留痕	AML 手册 + 规则库 + STR 决策树
ICT/外包	DORA 级别治理与韧性	架构图 + 权限矩阵 + BCP/DR + 外包治理
客户保护	披露透明、投诉、资产隔离	客户协议 + 披露文本 + 投诉机制
护照/跨境	通报材料与营销合规边界	护照通报包 + Marketing Approval Log

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（唐生建议）

1. **先定服务范围，再定系统与制度深度**：服务选错 = 资本、岗位、钱包与报表全错。
2. **股东/UBO 资料必须闭环可核验**：SoF/SoW + 资金路径图 + 不利信息解释备忘录，是最常见补件点。
3. **ICT 直接按 DORA 标准做**：外包治理、渗透测试、BCP/DR 演练证据要"可审计"。
4. **AML 做成"制度+系统+证据链"**：STR 决策链条、未报送原因、工单留痕必须可解释。
5. **建立 RFI 战情室**：补件速度与质量决定周期与成功率。

24.2 为何选择仁港永胜（核心优势）

- **一体化交付**：MiCA/CASP 申请文件 + AML + ICT/DORA 外包治理 + 客户条款披露 + 护照通报，避免多团队碎片化。
- **强模板库与可复制工具**：BP/PoO、Risk Register、STR 决策树、外包尽调清单、面谈题库、RFI 应答包、护照通报包等可直接落地。
- **监管逻辑导向**：按"可审计、可证据化、可解释"的结构组织材料，提高通过率与审查效率。
- **获牌后持续合规能力**：报表（CASP Return）、审计包、培训演练、重大变更报备、外包通知全套长期支持。

关于仁港永胜

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

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 技术标准及马耳他主管机关（Malta Financial Services Authority（MFSA））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。
