西班牙 Spain（MiCA）加密资产服务提供商（CASP）牌照

常见问题（FAQ 大全）

Q1–Q400（Spain（MiCA）CASP｜西班牙 Spain版）

Frequently Asked Questions about the Spanish (MiCA) CASP License

本文由 **仁港永胜（香港）有限公司**拟定，并由 **唐上永（唐生，Tang Shangyong）提供专业讲解。**
西班牙监管口径提示：MiCA 自 2024-12-30 起适用，CNMV 在其 MiCA 授权手册中明确了可在 2024-09 起提前递交申请、并强调在 MiCA 适用日前不授权 CASP。
Travel Rule 依据 **Regulation (EU) 2023/1113**（西班牙 BOE/欧盟 EUR-Lex 均可查）。
DORA 自 **2025-01-17**起适用（对 CASP 的 ICT、外包、事件通报与韧性治理影响巨大）。

适用对象：**拟以**西班牙 Spain为 MiCA 申请国（Home Member State），申请并运营 **CASP（Crypto-Asset Service Provider）**，并通过 **MiCA 护照机制（passporting）**向全欧盟跨境展业的机构。
法律依据：MiCA（EU 2023/1114）统一授权与持续监管框架；并行适用 Travel Rule（EU 2023/1113）；与 DORA（EU 2022/2554）等欧盟合规底座协同。

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

牌照名称：西班牙 Spain（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

- 在西班牙根据 MiCA 框架，提供加密资产服务需获得的许可证通称为：
  CASP 牌照（Crypto-Asset Service Provider Licence）
  即：
  “Proveedor de Servicios de Criptoactivos autorizado bajo MiCA”
  或更简练称为：
  MiCA CASP 牌照 / MiCA 加密资产服务提供商授权
  这是一种由 CNMV 授权的许可，允许企业根据 MiCA 提供受监管的加密资产服务（例如交易、托管、订单执行等）。

补充说明

- 获得 CASP 牌照后，该许可将在欧盟范围内具有“护照效力”（passporting），允许牌照持有者在全 EU 27 个成员国范围内部署相关服务。
- 西班牙已经逐步停止旧的 VASP 注册体系，新实体需自 2024 年底起申请 MiCA CASP 授权，且过渡期计划于 2025 年结束。

主管机构：

- **西班牙国家证券市场委员会**
  西班牙语全称：**Comisión Nacional del Mercado de Valores**
  缩写：CNMV
  CNMV 是西班牙负责根据 MiCA 授权、监管和监督加密资产服务提供商（CASPs）的主管金融市场监管机构。
- **另一个相关机构（职责侧重不同）**
  对于 MiCA 范围内的 *资产参考代币（ARTs）* 和 *电子货币代币（EMTs）* 等方面的审慎监管，还涉及 **西班牙银行（Bank of Spain）** 的职责划分（尤其是针对货币类稳定币等分类）。

✅ 点击这里可以下载 PDF 文件：西班牙 Spain（MiCA）加密资产服务提供商（CASP）牌照申请注册指南
✅ 点击这里可以下载 PDF 文件：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）。

西班牙 Spain（MiCA）CASP 牌照常见问题（FAQ 大全）

A 分类｜牌照与范围（Licence, Scope & Strategy）

Q1：MiCA 下 CASP 牌照是什么？
A：MiCA（EU 2023/1114）下的 CASP 授权，是在欧盟统一框架内提供加密资产服务的"单一授权"，获批后可依护照机制跨境展业（仍需做跨境通报与本地营销合规补丁）。

Q2：在西班牙谁是 CASP 的核心主管机关？
A：以**证券市场行为监管口径**，CNMV 是 MiCA 体系下加密资产市场/服务的重要主管机关之一；你在实操中需把材料做成"行为监管可读"。CNMV 已发布 MiCA 授权手册并安排提前受理窗口。

Q3：Banco de España（西班牙央行）还管不管 CASP？
A：在 MiCA 落地期间，西班牙存在"既有登记/监管分工"与 MiCA 新体系并行理解的必要：**央行体系（含登记/支付/银行口径）+ CNMV 行为口径 + SEPBLAC AML 执行**，需要用"职责矩阵+流程图"讲清楚，避免材料口径冲突。

Q4：SEPBLAC 是什么角色？
A：SEPBLAC 是西班牙 AML/CFT 体系关键执行机构（FIU/监管检查/报告接收等），你必须把 AML、STR、制裁筛查、Travel Rule 作为"可运行系统"呈现，而非仅写制度。

Q5：MiCA 生效时间点对西班牙申请意味着什么？
A：CNMV 手册明确：MiCA 自 2024-12-30 起适用；在此日期之前不授权 CASP，但允许从 2024-09 起提前提交申请，以便加快审核。

Q6：MiCA 过渡期（grandfathering）对在西班牙运营的存量机构意味着什么？
A：如果你是存量 VASP/加密业务运营者，需判断是否符合西班牙适用的过渡安排与截止日；务必把"过渡期合规计划（Gap→里程碑→证据链）"写进申请/转轨包，避免"到期 cliff-edge"。

Q7：CASP 牌照能覆盖哪些业务？
A：MiCA 的 CASP 服务是按"服务类别"授权（如托管、交易平台、兑换、执行/传递、投顾/组合、转移等），你必须先确定服务边界，再写制度、资本、系统与人员。

Q8：能不能先申请少量服务，后续再扩项？
A：可以，策略上常用"先轻后重"：先做 RTO/Execution/Transfer 等，形成合规运营记录后，再扩到交易平台/托管等高复杂度服务；扩项相当于重大变更，需按监管程序与补件逻辑重走一轮证明。

Q9：交易平台（Trading Platform）与兑换（Exchange）能否视为同一类？
A：不能。平台类更强调市场秩序与监测（操纵、刷量、异常行情、上币治理、停牌熔断）；兑换更强调报价公平、费用披露、冲突管理与执行质量。

Q10：托管（Custody）为什么是"最难"之一？
A：因为监管关注资产隔离、密钥管理、权限、对账、保险/保障与责任边界；你必须提供"可演示证据链"（系统截图/日志/演练报告/审计口径）。

Q11：申请组合怎么选最稳？
A：按三层组合：

- 入门合规：RTO + Execution + Transfer（以 AML/Travel Rule 为核心）
- 平台组合：Trading Platform（以规则+监测+证据链为核心）
- 全栈组合：Custody + Exchange + Platform（资本、系统、安全、外包治理压力最大）

Q12：MiCA 与 Travel Rule 的关系？
A：MiCA 管"牌照+行为+治理+审慎"；Travel Rule（EU 2023/1113）管"转账信息随行+留存+对接+拒绝/延迟机制"，两者必须并行落地。

Q13：DORA 与 CASP 的关系？
A：DORA 自 2025-01-17 起适用，覆盖 ICT 风险管理、事件管理与通报、第三方风险、韧性测试等；平台/托管类 CASP 基本都会被监管以 DORA 标准"抬高审查预期"。

Q14：CNMV 是否有"申请窗口/操作手册"？
A：有。CNMV 发布了 MiCA 授权手册并明确申请前置提交安排与时间点。

Q15：西班牙是否有针对 MiCA 的市场滥用/监管趋同指引？
A：CNMV 网站收录 ESMA 与 MiCA 相关的监管趋同材料与指引动态（例如防范市场滥用的监管实践指引）。

Q16：白皮书/发行（Title II MiCA）与 CASP 授权是一回事吗？
A：不是。Title II 主要管加密资产发行/上市白皮书与通知流程；CASP 授权是服务提供商准入。CNMV 也发布了 Title II 通知流程资料。

Q17：是否能在未获 CASP 授权前向客户提供服务?
A：高风险。MiCA 适用后，未授权经营/超范围经营属于红线；过渡期内也要严格按允许范围与条件执行，并保留监管可审计证据。

Q18：申请前最重要的"第一张图"是什么?
A：服务映射图：把产品/流程拆解到 MiCA 服务类别，并标注每类对应的制度、系统、资本、人员与外包依赖。

Q19：申请前最重要的"第二张图"是什么?
A：数据与权限流图：KYC→风控→交易→托管→转账→对账→报告全链路，标出系统、供应商、数据字段、日志留存与访问控制。

Q20：申请前最重要的"第三张图"是什么?
A：集团穿透与控制权图：到自然人 UBO，列明投票权/否决权/委派权/协议控制与关联方关系。

B 分类｜实体与实质（Entity, Substance & Operating Model）

Q21：什么是"实质运营（Substance）"的监管底层逻辑?
A：监管要确认：决策与控制在本国主体可追溯；关键控制职能可有效履职；外包可控可审计可退出；检查时能立即调取客户与交易证据链。

Q22：西班牙落地通常需要哪些"最小实质"?
A：最低可解释模型：本国办公场所 + 管理层问责链 + 合规/AML/风险/信息安全负责人 + 可运行系统与留痕机制（至少能演示开户、EDD、监控、STR、转账、对账与投诉闭环）。

Q23：董事/管理层必须常驻西班牙吗?
A：不必机械"全员常驻"，但必须证明"有效管理（effective management）"与可用性：值勤安排、授权矩阵、会议纪要、签批链、应急授权链必须可审计。

Q24：集团在欧盟外，能否用西班牙空壳申请?
A：强烈不建议。监管对"空壳+全外包+全境外决策"敏感，往往会在 Substance、外包、数据可得性与审计权上卡死。

Q25：可以把 AML/合规外包给供应商吗?
A：可以外包"工具/执行环节"，但不能外包"责任与决策"。公司必须拥有规则库所有权、处置决策权、质量复核权与审计追溯能力。

Q26：客服、KYC 审核、链上分析可外包吗?
A：可外包，但要做：重要性分级、尽调、合同审计权、分包限制、数据访问与留存、事件通报、退出迁移计划，并设内部责任人。

Q27：申请主体应选择什么公司形态?
A：以能支持审慎与治理要求的实体为宜（可承担资本金、雇佣、合同、税务与审计），并能清晰隔离集团其他高风险业务。

Q28：是否需要单独的西班牙银行账户?
A：通常需要：资本注入、客户法币隔离、运营费用与税务缴付都要落在可审计账户结构上，并能输出月度对账与资金流水解释。

Q29：是否能先用 EMI/支付牌照主体来申请 CASP?
A：可行但复杂：需证明业务隔离、冲突管理、资本与风险不互相掏空，并处理监管交叉要求（支付/证券/加密/AML/DORA）。

Q30：Substance 最常见补件点是什么?
A：①关键岗位"挂名"②决策链不在本国③无法调取日志/客户档案④外包无审计权⑤无退出方案⑥人员不足以覆盖服务范围。

C 分类｜股东/UBO（Shareholding, UBO, SoF/SoW）

Q31：哪些人必须做股东/UBO 尽调?
A：≥10% 股东、控股股东、实际控制人、最终 UBO、董事、高管、关键岗位负责人（合规/AML/风险/信息安全/内审）都应纳入 Fit & Proper 与负面筛查范围。

Q32：为什么"10%/重大持股"是敏感线?
A：达到阈值即触发重大影响与控制审查；监管关心是否会被项目方/做市商/关联方"反向控制"，影响上币、风控或客户资产安全。

Q33：SoF 与 SoW 的差别?
A：SoF（Source of Funds）解释"本次入资的钱从哪里来"；SoW（Source of Wealth）解释"整体财富如何累积形成"。两者都要可审计证据链。

Q34：SoF/SoW 一般需要哪些证据?
A：银行流水、审计报表、完税证明、股权/资产处置协议、分红决议、交易记录（含加密资产处置的合规证明）、融资协议（如有）等；并给出资金路径图（每一跳解释）。

Q35：如果资金来自加密资产收益，会被拒吗?
A：不必然，但审查会更严格：需证明交易所/钱包来源、反制裁与反混币风险、税务合规、资金链清洁度与可解释性。

Q36：股权结构多层控股能接受吗?
A：能，但必须穿透到自然人，并披露协议控制、否决权、委派权、质押/信托安排等"控制权结构"。

Q37：PEP/制裁命中怎么办?
A：要有"命中处置 SOP"：二次核验→升级→EDD→风险决策→必要时拒绝/终止→留痕与复核；对制裁命中一般采取冻结/拒绝与上报机制（依适用法与内部政策）。

Q38：股东中有项目方/做市商是否高风险?
A：是。需强化利益冲突管理、上币治理独立性、做市参数隔离与审批、信息墙与员工交易限制。

Q39：股东变更是否要事先批?
A：通常重大持股/控制权变化属于重大事项，应遵循事前通知或审批要求（以主管机关程序为准），并建立持续通知机制与监控触发器。

Q40：持续通知触发器怎么写?
A：至少包括：达到/跨越 10% 变化、控制权变化、UBO 变化、质押/信托变化、重大诉讼/处罚、资金结构重大变化、关键岗位变更等。

D 分类｜董事适任性与关键岗位（Fit & Proper, Key Functions）

Q41：董事会最核心的监管期待是什么?
A：可问责（accountability）+ 能力覆盖（competence coverage）+ 独立制衡（independence），并能对重大外包、客户资产保护、市场行为与重大事件承担治理责任。

Q42：董事会需要几个人才合适?
A：与业务复杂度匹配：平台/托管类至少要覆盖交易系统/安全/AML/风险/合规；小团队可用"外部独立董事+外包内审"补齐，但要真实履职证据。

Q43：哪些岗位是"必问模块"?
A：CEO/COO（运营与可持续）、合规负责人、MLRO、风险负责人、信息安全负责人、（可外包的）内审负责人。

Q44：MLRO 最容易被问什么?
A：风险评估方法论、规则库场景、STR 决策与质量控制、制裁/PEP 处置、Travel Rule 落地、培训与独立审查、与 SEPBLAC 沟通机制。

Q45：合规负责人最容易被问什么?
A：MiCA 行为义务落地、披露与营销审核、利益冲突、投诉处理、客户资产保护、政策更新机制、合规年度计划与监测指标。

Q46：信息安全负责人最容易被问什么?
A：密钥管理（MPC/HSM/多签）、权限分层、日志不可篡改、渗透测试与整改、事件响应与通报、BCP/DR 演练、第三方风险与云治理（DORA 口径）。

Q47：关键岗位能兼职吗?
A：可，但要证明资源充足与独立性：例如 MLRO 不应与业务销售同一 KPI；合规不得被商业目标"绑架"；并用 RACI 与升级路径固化。

Q48：关键岗位外包可行吗?
A：内审通常可外包；合规/AML 可外包支持但责任不可外包；信息安全可外包 SOC 但需内部 owner；所有外包都要审计权与退出权。

Q49：面谈准备的"标准答题卡"怎么做?
A：把每个岗位职责映射到 MiCA/DORA/TFR 条款→对应 SOP→对应系统证据→对应留痕与复核，形成 30–80 个高频问题的"一页答案卡"。

Q50：最常见不通过点?
A：岗位挂名、组织不成体系、缺少独立制衡、没有实际权限/数据访问权、无法解释规则库与阈值来源、缺少演练与整改闭环。

E 分类｜资本/保障/可持续经营（Prudential, Safeguards & Sustainability）

Q51：MiCA 下资本要求是怎么定的?
A：通常按"最低资本 + 固定开支比例/审慎保障"双轨取高（具体以 MiCA 对不同服务类别的要求为准），并要求持续满足而非一次性满足。

Q52：为什么监管要看现金流与压力测试?
A：因为平台/托管类合规成本高（AML 工具、Travel Rule、审计、SOC、渗透测试、外包审计权成本），纸面资本充足但现金流撑不住会导致违规风险。

Q53：资本金必须实缴吗?
A：实操上通常需要可验证入资证明（银行入资、验资/对账等），并解释资金来源与资金路径。

Q54：客户资产保护属于资本范畴吗?
A：属于审慎保障的核心：要证明客户资产隔离、托管结构、对账机制、错误更正与赔付安排、以及在破产/风控事件下的保护措施。

Q55：可以用保险替代部分保障吗?
A：视业务与监管接受度，保险可作为补强（冷/热钱包盗损、职业责任险等），但不能替代资产隔离、权限控制与对账等基础机制。

Q56：固定开支（Fixed overheads）怎么口径化?
A：把人力、外包、工具订阅、安全与审计、办公与法律税务、云与基础设施等纳入；并明确增长情景下的弹性成本与资本补充机制。

Q57：资本补充机制怎么写才"监管可读"?
A：写触发条件（亏损、增长、事件、监管要求升级）→补充方式（股东增资、可转换、融资承诺）→时限→董事会决议模板→资金到位路径。

Q58：如果申请多项服务，资本怎么取?
A：按 MiCA 逻辑通常"按服务类别取高"或叠加规则处理；策略上可先申请轻服务降低资本压力，后续扩项再补强。

Q59：财务模型至少做几年?
A：建议 3 年（P&L、BS、CF）+ 压力情景；并提供月度现金消耗（burn-rate）与最坏情景下持续经营说明。

Q60：监管最喜欢看到的财务"证据"是什么？
A：真实可验证的：银行对账、合同（外包/工具/办公）、人员薪酬结构、审计/法律预算、以及能落地的收费模型与客群增长假设。

F 分类｜AML/制裁/STR/Travel Rule（Financial Crime & TFR）

Q61：Travel Rule 的法律依据是什么？
A：Regulation (EU) 2023/1113（欧盟层面直接适用），对加密资产转账信息随行、留存、对接与处置作出要求。

Q62：Travel Rule 适用哪些场景？
A：涉及"加密资产转移/转账"的服务（含平台转出、托管提币、代表客户转移等），以及与其他 CASP/VASP 的信息交互。

Q63：Travel Rule 必须传哪些信息？
A：核心是"发起人/受益人信息 + 钱包/账户标识 + 交易信息"，并对缺失信息的拒绝/延迟/人工复核提出要求（字段以法规与行业消息标准落地为准）。

Q64：自托管钱包（unhosted wallet）怎么处理？
A：要做风险分级：收集与验证（在可行范围内）、强化监测、地址归属证明/小额验证、异常触发 EDD；并规定无法满足信息要求时的处置策略（拒绝/延迟/限额）。

Q65：AML 风险评估要做几层？
A：至少四层：企业级（EWRA）+ 客户（KYC/KYB）+ 产品/服务 + 地域/渠道；并每年复核、重大事件触发复核。

Q66：KYC/KYB 的最低要素？
A：身份、地址、税务居民、自我声明、UBO 穿透、经营性质（KYB）、资金用途、预计交易行为、制裁/PEP/负面筛查、风险评分与证据留存。

Q67：EDD 触发器怎么设？
A：高风险国家/行业、PEP、异常交易模式、混币/匿名增强工具、频繁自托管交互、快速进出、与已知风险地址交互、投诉与欺诈信号等。

Q68：交易监控"规则库"要包含哪些场景？
A：链上（高风险地址、跳转、混币、跨链桥、暗网标记等）+ 链下（充值/提现频率、分拆、阈值、关联账户、异常盈利等）+ 行为（多账号、设备指纹异常、IP/地理异常）。

Q69：STR/SAR 的流程要怎么写才可用？
A：告警→初筛→调查→升级→MLRO 决策→提交→后续跟踪→质量复核；每一步要有工单、证据附件与时限 SLA。

Q70：制裁筛查命中如何处置？
A：明确冻结/拒绝/终止/上报路径（按适用法与内部政策），并保留命中证据、误报复核记录与二线复核签批。

G 分类｜ICT/DORA/外包（Tech, Security, DORA, Outsourcing）

Q71：DORA 对 CASP 的关键影响是什么？
A：把 ICT 风险、事件管理与通报、第三方风险、韧性测试"制度化、证据化"，并且自 2025-01-17 起适用。

Q72：什么叫"可演示证据链"？
A：监管问你"怎么做"，你能立刻展示：系统架构图、权限矩阵、日志样例、告警工单、演练报告、渗透测试与整改闭环、对账报表、外包评估记录。

Q73：最小权限（RBAC）必须做到什么程度？
A：特权账号隔离、审批链、多因素、操作留痕、不可篡改日志、定期复核；冷钱包/签名权限要多签或 MPC 并具备紧急处置预案。

Q74：渗透测试/代码审计要多频？
A：建议至少年度 + 重大变更触发；并对高危漏洞设整改时限与复测报告。

Q75：事件响应要包含哪些内容？
A：分级标准、指挥链、隔离与止损、客户沟通、监管通报、取证与根因分析、复盘与整改闭环；并做桌面演练与实战演练留痕。

Q76：BCP/DR 最关键指标？
A：RTO/RPO、备份策略、恢复演练证明、关键供应商故障的替代方案；平台/托管类建议做双活/热备策略并记录演练结果。

Q77：外包为什么是监管"必卡点"？
A：因为一旦核心系统/数据/合规执行外包失控，就会直接引发客户资产风险与监管不可达。DORA 也强调第三方 ICT 风险治理。

Q78：外包合同必须有什么条款？
A：审计权、监管可访问性、数据权与留存、分包限制、事件通报 SLA、业务连续性要求、退出与迁移、终止交接、服务水平与赔偿机制。

Q79：云服务外包怎么做"合规论证"？
A：写清数据分类与驻留、加密与密钥控制、访问控制、监控与日志、供应商尽调、BCP/DR、退出迁移计划、以及监管访问与审计安排。

Q80：供应链风险怎么管？
A：建立第三方风险评估框架：准入尽调→合同控制→持续监控（KPI/KRI）→年度复评→事件管理→退出；并保留每次复评报告与整改闭环。

H 分类｜客户保护（Disclosures, Conduct, Complaints）

Q81：客户披露包至少包含什么？
A：费用披露、风险披露、执行方式、资产保管方式、利益冲突披露、投诉渠道、暂停/终止与强平规则（如适用）、硬分叉/空投处理、错误更正与赔付逻辑。

Q82：营销合规的红线是什么？
A：误导性表述、收益承诺、淡化风险、对零售客户不当激励；必须建立"营销审查流程+素材归档+投放受众分层+KOL/代理管理"。

Q83：零售与专业客户要分层吗？
A：建议分层。不同客群的风险提示强度、适当性测试、产品准入、杠杆/衍生品限制（如有）应不同，并记录客户确认。

Q84：适当性/合适性何时需要？
A：当你提供投顾/组合管理或具有类似性质的服务时，需要知识测评、风险承受评估、产品分层与再评估机制。

Q85：客户资产隔离要怎么"写给客户看"？
A：用可理解语言解释：链上地址归属、法币隔离账户、对账频率、冻结/扣划条件、破产隔离原则（如适用法支持）、以及客户自查渠道（对账单/交易记录）。

Q86：投诉处理机制为什么重要？
A：它是行为监管的"落地抓手"，必须有：受理时限、调查流程、升级路径、结案标准、统计复盘、整改闭环与证据留存。

Q87：ADR/争议解决怎么设计？
A：条款中明确管辖、仲裁/法院、语言、证据规则、客户资金/资产处置的临时措施、以及与监管投诉并行的处理机制。

Q88：客户协议（T&C）最关键的 10 条？
A：服务范围、费用、风险、执行、托管与资产归属、暂停/终止、错误更正与赔付、硬分叉/空投、数据与隐私、争议解决与适用法。

Q89：平台规则需要对外披露吗？
A：建议核心规则对外披露（订单类型、撮合原则、异常处理、停牌/熔断、费用），并保留版本控制与更新通知记录。

Q90：客户确认留痕怎么做？
A：点击确认+版本号+时间戳+IP/设备指纹+内容存档；重大更新要强制二次确认并保留差异对比。

I 分类｜护照与跨境（Passporting & Cross-border)

Q91：MiCA 护照机制能做什么？
A：在一国获批后，可向其他成员国跨境提供同范围服务（自由提供服务/设分支），但需做通报并遵守落地国消费者保护与营销规则补丁。

Q92：护照通报包应包含什么？
A：服务清单、目标国列表、跨境交付模式、客户文件多语言版本、投诉处理与客服安排、数据与隐私合规说明、当地营销合规清单。

Q93：跨境营销的最大风险是什么？
A：把"通报=可以随便拉客"误解。实际落地国对广告、KOL、冷呼、促销可能有额外限制；必须有本地合规审查与留痕。

Q94：设分支与跨境自由提供服务怎么选？
A：看客群规模、当地监管预期、运营与客服要求、税务与雇佣成本；大规模零售通常更适合分支/本地化运营。

Q95：跨境客户争议由谁处理？
A：主体仍由获批 CASP 负责，需建立多语言工单与升级机制，并明确与外部 ADR/监管投诉并行的内部处理标准。

Q96：跨境数据传输有什么注意？
A：需满足 GDPR 与本国隐私要求，尤其是 KYC/交易/Travel Rule 字段；对第三国传输要有合法基础与供应商合同条款。

Q97：跨境外包怎么解释监管可得性？
A：无论供应商在哪里，你都要保证监管可访问、可审计、可导出日志与客户档案，并能执行退出迁移。

Q98：跨境运营最常见补件点？
A：目标国清单不清、客户文件未多语言、投诉/客服安排不足、营销治理缺失、数据/外包安排不透明。

Q99：护照通报是否能"后补"？
A：可以分阶段：先在本国试运营形成证据链，再扩张通报；但任何对外营销与招揽前必须确保合规与通报路径正确。

Q100：如何用"第二阶段工程"管理护照？
A：建立护照路线图：目标国优先级→当地合规补丁包→多语言披露→客服与投诉→税务与数据→上线检查表。

J 分类｜运营与持续合规（Ongoing Compliance, Reporting, Change Control）

Q101：获批后最重要的持续义务是什么？
A：持续资本与审慎保障、持续 AML/制裁与 STR、持续 ICT/DORA 合规、持续客户保护与披露、持续记录保存与报告、重大变更通知与批准。

Q102：什么算"重大变更"？
A：服务范围扩项、股权/控制权变化、关键岗位变更、重大外包/云迁移、核心系统更换、托管结构变化、产品重大改动、定价与费用重大调

整。

Q103：持续合规怎么做"项目化管理"?
A：建立年度合规计划+季度治理报告+关键风险指标（KRI）+内审/独立审查+整改闭环；并把所有政策版本化、可审计化。

Q104：记录保存要保存什么?
A：KYC/KYB 全流程、风险评分、EDD 决策、交易与订单生命周期、链上/链下日志、监控告警与处置、客户确认与披露版本、投诉工单、外包评估与审计、演练与事件响应等。

Q105：记录保存多久?
A：按 AML、税务、MiCA 相关要求执行（不同项可能不同）；建议建立统一的"数据留存矩阵"，逐项列法规依据、保存期限、存储位置与访问控制。

Q106：如何证明"制度在运行"?
A：用 KPI/KRI 与抽样测试：例如 STR 质量抽查、告警处置时效、制裁误报率、外包 SLA、渗透测试整改完成率、对账差异处理时效。

Q107：内审一定要有吗?
A：需要独立审查机制。小机构可外包内审，但要独立性与审计权、审计计划、底稿与整改闭环。

Q108：如何管理员工交易与利益冲突?
A：员工交易政策、申报与审批、黑名单期、信息墙、礼品招待、关联交易审查、做市与自营隔离、违规处置流程。

Q109：上币/下币治理属于持续义务吗?
A：是平台类核心持续义务：评估模型、委员会决策、风险评分、持续监测、重大事件下架机制、信息披露与客户通知。

Q110：如何应对监管检查?
A：预先准备"检查应答包"：组织与职责、系统证据链、样本数据导出流程、合规报告、外包合同与评估、演练与事件记录、客户投诉与纠纷台账。

Q111：申请前是否建议与 CNMV 预沟通?
A：建议。你可以用"Pre-app pack（10–20页）"快速对齐：服务范围、架构、资本、关键外包、风控与 AML 证据链，从而减少正式递交后的补件回合。CNMV 已发布授权手册与申请安排。

Q112：CNMV 手册对"何时可递交"有什么关键点?
A：它明确：MiCA 适用在 2024-12-30；但可从 2024-09 起提交申请以便顺利过渡。

Q113：材料如何拆成"审慎包/行为包"?
A：即便西班牙主管机关口径以 CNMV 为核心，你也应把材料拆成：①治理/资本/外包/退出（审慎风格）②客户披露/平台规则/投诉/营销（行为风格）③系统证据链（IT/日志/演练）④AML/Travel Rule（金融犯罪包）。

Q114：申请材料的"索引（Index）"为什么关键?
A：因为 MiCA/ITS 递交通常是表格字段→附件编号→页码/段落的交叉引用；无 Index 会显著增加补件概率与审查时间。

Q115：申请材料如何做到"RFI-ready"?
A：每条潜在补件提前准备：条款依据→现状→措施→证据编号→责任人→完成日期；并保持版本控制与差异说明。

Q116：申请中最常见的 RFI 主题?
A：服务映射不清、Substance 不足、资本与现金流不真实、外包合同无审计/退出、平台监测不足、托管安全证据不足、AML/Travel Rule 不可运行。

Q117：是否必须提供系统演示?
A：强烈建议提供"演示脚本+截图证据"，尤其平台/托管/转账：开户、EDD、制裁命中、告警调查、提币审批、多签/MPC 签名、对账差异处理等。

Q118：可否用第三方系统证明合规?
A：可以，但你仍需证明：配置由你控制、规则库归你所有、日志可导出、审计权可执行、退出可迁移。

Q119：Substance 证据通常包括什么?
A：办公租赁/门禁工位/照片、雇佣合同、值勤表、会议纪要、授权矩阵、关键岗位在岗证明、内部系统访问权限记录。

Q120：监管如何判断你不是"挂名管理"?
A：看签批与决策留痕：风险豁免、EDD 决策、上币委员会决议、外包年度评估、事件响应复盘、资本补充决议等是否由本国主体完成。

C/D 延展：股东尽调、董事胜任力与"最小合格画像"

Q121：股东尽调包的最低清单?
A：UBO 穿透图、身份证明/住址证明、税务居民声明、无犯罪/无重大处罚声明、负面与制裁筛查报告、SoF/SoW 证据链、关联方清单、控制权说明。

Q122：如何做"控制权说明"?
A：不仅写持股比例，还要写：表决权差异、优先股、否决权、委派权、股东协议关键条款、质押/信托安排、资金方与实际控制人的关系。

Q123：如果股东是基金/信托结构?
A：必须穿透到最终自然人（或至少到可识别控制人），并披露受益人类别、受托人权限、变更机制与信息获取权。

Q124：董事胜任力的"证据链"怎么做？
A：监管版 CV（项目经验映射到 MiCA 服务）、任命决议、岗位说明书、培训记录、面谈题库答案卡、以及在岗履职证据（会议纪要/签批记录样本）。

Q125：董事会"三道防线"怎么落地？
A：1LOD 业务线自控；2LOD 合规与风险独立监督；3LOD 内审独立评估。用 RACI、DoA（授权矩阵）、委员会章程、年度计划与报告模板固化。

Q126：关键岗位的独立性如何证明？
A：汇报线直达董事会/审计委员会；绩效不绑定销售；拥有数据访问权与暂停/拒绝权；有预算与资源；有独立复核与升级路径。

Q127：小公司人员不足怎么办？
A：用"兼职+外包"组合补齐，但必须：职责边界清晰、独立性可证、外包有审计权与退出计划、内部 owner 对结果负责。

Q128：什么情形会被认为"不适任"？
A：重大犯罪或金融处罚史、破产/失信、被监管取消资格、重大诉讼未披露、明显利益冲突无法消除、资金来源无法解释等。

Q129：如何处理历史负面新闻？
A：做披露与解释：事实、处置、整改、复核；并给出持续监测与限制措施，避免"隐瞒"触发诚信问题。

Q130：董事/高管需要懂技术吗？
A：平台/托管类强烈建议至少一名管理层具备安全/系统/交易架构理解，否则在面谈中很难解释密钥、权限、日志与事件响应。

E/F 延展：资本测算、持续经营、AML/Travel Rule 细化

Q131：资本测算表需要包含哪些字段？
A：申请服务类别、最低资本档位、固定开支口径、取高规则、当前资本、差额、补足计划、持续监测频率、触发补充条件。

Q132：持续经营证明怎么写更有说服力？
A：把合规成本写实：KYC/制裁/链上分析/Travel Rule/SOC/SIEM/渗透测试/外包审计/法律审计税务；并提供最坏月度 burn 与融资承诺。

Q133：压力测试建议哪些情景？
A：行情暴跌与挤兑、链上拥堵与提现延迟、重大安全事件、关键供应商宕机、监管提高资本/合规要求、舆情冲击导致客户流失。

Q134：AML 风险评分模型要可解释吗？
A：要。提供方法论、权重、阈值来源、复核频率、模型变更审批与回测记录，避免"黑箱评分"。

Q135：STR 质量如何保证？
A：设质量门槛：叙事结构、证据附件、时间线、资金流、链上地址与交易哈希、处置动作；并进行抽样复核与培训闭环。

Q136：Travel Rule 无法获取对手信息怎么办？
A：按内部政策采取：拒绝/延迟/人工复核/限额/强化监测，并记录决策理由与证据；对高风险对手采取更严格策略。

Q137：与海外 VASP 对接 Travel Rule 通道怎么做？
A：建立对手方分级（合规成熟度、司法辖区、消息标准兼容性）、签署数据与安全条款、设异常处理与回退机制，保留消息记录与审计轨迹。

Q138：自托管钱包的"归属证明"有哪些做法？
A：签名验证、小额验证、地址白名单、设备绑定、来源分析、交易行为一致性校验；并结合风险分级决定是否允许提现。

Q139：制裁与反混币策略要写吗？
A：要。明确对混币/匿名增强工具、暗网标记地址、受制裁实体的拒绝策略与升级机制（欧盟规则强调相关风险）。

Q140：培训体系怎么设计？
A：岗位分层（前台/合规/AML/客服/技术/管理层）+ 年度计划 + 测试题库 + 通过标准 + 复训机制；并保留签到与成绩记录。

G/H 延展：平台/托管/外包/客户保护进一步颗粒化

Q141：平台必须有市场监测吗？
A：必须。包括刷量、操纵、关联账户、异常波动、内幕信息泄露风险；并建立告警→调查→处置→披露/停牌→复盘闭环。

Q142：上币评估至少包含哪些维度？
A：项目背景与治理、技术安全、流动性与做市安排、合规与制裁风险、信息披露质量、利益冲突、持续监测指标与下架触发器。

Q143：托管的钱包架构建议怎么写？
A：冷热分离、MPC/多签、HSM（如适用）、权限分层与双人复核、密钥轮换、备份与灾备、紧急冻结与恢复流程。

Q144：对账频率如何设？
A：至少日对账（平台/托管高频业务建议更高频或实时对账），并设差异处理、冲正、客户通知与补偿规则。

Q145：客户提币的控制点有哪些？
A：地址白名单、延迟提现、风控评分触发人工复核、双人审批、多因素、异常时间窗口限制、与 Travel Rule 信息校验联动。

Q146：外包年度评估要怎么做？
A：评分表（安全、SLA、事件、合规、财务稳健、分包风险）、现场/远程审计记录、整改追踪、替代方案与退出演练。

Q147：退出计划（Exit Plan）需要到什么程度？
A：不仅写原则，要写：迁移步骤、时间表、资源、数据导出与格式、客户沟通模板、替代供应商清单、演练记录。

Q148：客户披露必须"简单易懂"吗？
A：是。监管会看是否存在复杂条款掩盖风险。建议做双层披露：一页摘要 + 完整条款；并要求客户确认留痕。

Q149：费用披露要披露哪些？
A：交易费、价差、托管费、提现费、上币相关费（如向项目方收取需冲突披露）、潜在第三方费用、以及费用变更通知机制。

Q150：客户数据与隐私怎么写？
A：GDPR 合规基础、数据最小化、留存期限矩阵、第三方共享清单、跨境传输机制、数据主体权利与响应 SLA、数据泄露事件响应。

I/J 延展：持续报告、变更管理、检查应对

Q151：持续报告通常包含哪些主题？
A：资本与财务、重大事件、ICT 事件、外包重大事项、投诉统计与整改、AML 指标（告警/STR/命中率）、风险报告与 KRI。

Q152：政策与系统变更怎么管理？
A：建立变更委员会/流程：需求→风险评估→测试→上线审批→回滚预案→上线后监控→文档更新→培训→留痕。

Q153：如何做版本控制？
A：所有政策、客户文件、平台规则、系统配置都要版本号、变更摘要、批准人、发布日期与生效日期，并保留历史版本可追溯。

Q154：如何准备监管检查"样本数据"？
A：预设导出模板：客户样本（KYC/EDD/交易/告警/处置）、系统日志样本、对账样本、外包评估样本、演练样本；并确保可匿名化处理。

Q155：客户投诉 KPI 建议？
A：受理时效、首次回复时效、结案时效、复投诉率、赔付金额、根因分类、整改关闭率；并按月/季向董事会汇报。

Q156：如何处理重大舆情事件？
A：建立危机沟通 SOP：公告模板、客户 Q&A、媒体口径、监管沟通、客服话术、技术与风控止损动作，保留全过程记录。

Q157：如何管理关联交易与做市商？
A：做市协议披露与审批、参数变更审批、异常监测、关联方交易隔离、信息墙与利益冲突披露；必要时限制关联方影响上币与风控。

Q158：如何管理员工权限漂移（privilege creep）？
A：权限定期复核、离职立刻回收、特权账号最小化、审批链、操作日志审计、异常权限告警。

Q159：如何证明"合规不是纸面"？
A：把每项义务转成：指标（KPI/KRI）+工单+抽样+报告+整改闭环+董事会监督证据。

Q160：最典型的"监管喜欢看到"的闭环是什么？
A：安全事件演练：演练计划→执行记录→问题清单→整改→复测→董事会汇报；AML 亦同理（抽样→缺陷→整改→复核）。

Q161：CNMV 对 MiCA 相关程序的文件在哪里看？
A：CNMV 已发布 MiCA 授权手册及相关说明文件（其手册中包含申请时间点与安排）。

Q162：Title II 白皮书通知的程序在哪里看？
A：CNMV 发布了关于 MiCA Title II（白皮书/通知）流程的公告与指引文件。

Q163：CASP 申请是否可以"先交后补"？
A：可补件，但不建议依赖；正确做法是"RFI-ready"一次成型，减少往返回合与监管疑虑。

Q164：如果业务包含法币出入金，需要额外牌照吗？
A：可能需要与支付/银行体系并轨（合作银行、EMI/PI、或持牌机构通道）；在申请中应明确资金流与责任边界，避免被视为无牌提供支付服务。

Q165：稳定币相关（EMT/ART）对 CASP 有何影响？
A：涉及稳定币交易/发行/推广时，会触发 MiCA 对 EMT/ART 的额外要求与披露义务；CASP 需评估可交易资产清单与风险披露。

Q166：是否必须建立"资产准入清单（Token Governance）"？
A：平台类强烈建议：准入、持续监测、下架、重大事件响应、信息披露更新与客户沟通。

Q167：是否必须建立"市场滥用"防控机制？
A：是。尤其平台类应对操纵、刷量、内幕信息等建立监测与处置流程；监管趋同层面 ESMA 也推动相关指引实践。

Q168：是否需要 KYC 与交易数据的统一数据字典？
A：建议必须有。否则 Travel Rule、税务报告、监管报告会互相打架，导致抽取困难与数据质量问题。

Q169：如何满足 DAC8 税务信息交换导向？
A：建立税务字段（税号、税务居民、交易数据）与报告可抽取能力；把数据留存与质量控制写入治理制度。

Q170：客户资金/资产的"破产隔离"要怎么说明？
A：用法律意见+结构说明+对账与隔离证据解释：谁持有钥匙、谁有控制权、资产在链上/链下如何隔离、破产时如何处置与通知。

Q171：是否需要"独立审计师"？
A：通常建议有：财务审计、系统审计/渗透测试、外包审计等；用第三方报告增强可信度，但仍要内部闭环。

Q172：对外合作（经纪、代理、IB、KOL）怎么合规?
A：建立第三方营销政策：准入尽调、合规培训、素材审批、佣金披露、违规处罚与终止机制、投放记录留存。

Q173：客户适当性测评题库要做多细?
A：与产品复杂度匹配：基础知识+风险理解+经验与财务承受；并保留题库版本、答题记录与再评估机制。

Q174：如何处理未成年人/弱势群体?
A：设准入限制与加强披露；对高风险产品禁止向不适当客群营销。

Q175：是否需要电话录音/客服留存?
A：建议对关键沟通留存（尤其投诉与争议、风险提示确认、重大异常处置沟通），并满足数据保护要求。

Q176：如何管理"多账户/关联账户"?
A：设备指纹、IP/行为画像、KYB/UBO 关联校验、反欺诈模型；发现关联操纵风险时限制或冻结并记录处置依据。

Q177：如何处理欺诈与账户接管（ATO）?
A：MFA、异常登录告警、提现延迟与人工复核、设备绑定、黑名单与强制重置；并建立客户赔付与争议处理规则。

Q178：如何处理链上拥堵导致的延迟?
A：披露执行与确认的边界，设风险提示与工单机制，必要时限制或延迟高风险转账，并保留对客户的通知记录。

Q179：如何处理硬分叉/空投?
A：在客户协议中明确归属、支持标准、风险与税务提示、技术可行性与时间表；并建立内部评估与公告机制。

Q180：如何处理下架资产的客户清退?
A：提前通知、提供替代处置路径、设合理期限、对未响应客户设托管/变现/转移规则（符合法律与客户协议），并留痕。

Q181：如何管理价格源与指数?
A：披露报价来源、过滤异常报价、滑点机制、系统故障时的报价降级方案；并记录每次异常处置。

Q182：最佳执行政策需要吗?
A：如果提供代客执行/撮合/聚合报价，应建立并披露"公平/最佳执行"原则与监测指标。

Q183：如何避免"自营与客户交易冲突"?
A：自营与客户订单隔离、禁止抢跑、信息墙、顺序公平、参数审批与监控；必要时限制自营业务。

Q184：风控限额怎么设?
A：按客户等级、资产类别、风险评分设：单笔/日/月限额、提现限额、杠杆/高波动资产限制；并允许合规/风险部门一键调整并留痕。

Q185：如何管理流动性与挤兑?
A：准备流动性应急预案：提现队列机制、冷钱包调拨流程、风控限额、沟通模板；并做演练记录。

Q186：如何管理做市商失效风险?
A：多做市商备份、异常点差/深度告警、紧急切换、暂停交易规则；并披露市场异常处理机制。

Q187：如何处理系统升级导致的中断?
A：变更管理+公告+回滚预案+监控+事后复盘；重大升级建议在低峰窗口并进行演练。

Q188：如何管理数据质量?
A：数据字典、校验规则、异常数据工单、抽样复核、ETL 版本控制；确保监管/税务/内部报表一致性。

Q189：如何准备年度监管报告?
A：按监管要求建立报告日历、责任人、数据抽取路径、复核流程；并保留报送凭证与回执。

Q190：如何处理监管来函?
A：建立函件工单：问题拆解→责任人→证据编号→答复草稿→法务/合规复核→提交→后续跟踪；形成可审计闭环。

Q191：如何证明外包"可退出"?
A：不仅写 Exit Plan，还要做"退出演练（tabletop / dry-run）"，输出演练报告与改进项。

Q192：如何满足监管"可访问性"?
A：合同条款 + 实操路径：监管访问请求流程、数据导出格式、日志留存位置、审计接口；并进行年度测试。

Q193：如何管理跨境团队协作?
A：明确职责边界、数据访问权限、值班与应急链、跨境传输合法基础；避免"境外团队实控"导致 Substance 质疑。

Q194：如何处理客户资产误转/错账?
A：冲正 SOP、客户通知、赔付规则、内部责任追踪、根因分析与整改；并把案例纳入培训。

Q195：如何处理监管要求升级（例如新增 RTS/ITS）?
A：建立法规雷达与变更评估流程：识别→影响分析→改造计划→测试→上线→培训→留痕。

Q196：如何处理员工违规?
A：违规分级、调查流程、纪律处分、监管沟通（如需要）、整改与制度更新；并纳入董事会监督。

Q197：如何处理客户数据泄露?
A：事件响应+取证+隔离+客户通知+监管通报+补救；并与供应商责任条款联动。

Q198：如何处理黑客盗币?
A：立即止损、冻结、链上追踪、报警与法律行动、客户沟通、赔付评估、复盘与整改；并证明你事前控制（MPC/多签/权限/监控）充分。

Q199：如何处理"无法履约/破产风险"?
A：启动 Wind-down 计划：停止新增、保护客户资产、清退与迁移、对账与争议处理、档案封存、监管沟通与公告。

Q200：持续合规的"最终交付物"长什么样?
A：一套可运行的 GRC：政策库（版本化）+ 工单系统 + 指标看板 + 报告日历 + 证据库（可导出）+ 内审与整改闭环。

A 分类｜牌照与范围（深化：边界、产品、变体、风险定位）

Q201：MiCA 下"加密资产服务"与"技术服务/软件提供"如何划界?
A：只做软件/基础设施（不触达客户资产、不代表客户下单、不撮合、不持有私钥、不做转移）可偏向技术服务；一旦你**代表客户执行、托管、转移、撮合、报价兑换**，就落入 CASP 监管范围。交付上用"功能清单 + 资金/密钥/订单责任边界表"定界。

Q202：同一产品里同时含"兑换+执行+转移"，申请时怎么拆?
A：按客户旅程拆解：报价→确认→执行→结算→转移→对账，每段对应 MiCA 服务类别、制度与证据。申请组合策略：优先把"最监管敏感"的段落（托管/平台）单独列明控制措施。

Q203：只做"法币入金→买币→提币到自托管钱包"，是否必然需要托管牌照?
A：不必然，但你要证明你**不持有/不控制客户私钥**（例如仅做兑换与执行，提币至客户自托管地址由客户自行控制），并对"临时控制/中转地址/热钱包代管"做彻底切割，否则会被视为事实托管。

Q204：做"OTC 大宗撮合"算平台吗?
A：看是否存在多边撮合、订单簿、规则化撮合与市场组织。纯双边 OTC、点对点报价执行可能偏兑换/执行；但如果你形成"多边撮合规则 + 交易设施"，就可能被认定为平台类服务。

Q205：做"经纪/代理下单（brokerage）"属于哪类?
A：通常落入"接收与传递订单/执行订单"类（具体按 MiCA 服务定义映射）。关键是：是否替客户下单、是否选择交易场所、是否收取回扣/返佣，需写清利益冲突与最佳执行政策。

Q206：做"聚合报价（aggregator）"算不算兑换?
A：若仅展示行情、不给客户成交、不给报价承诺，可偏信息服务；若你按你的报价成交、或你控制成交路径，就属于兑换/执行，必须具备对应授权与披露义务。

Q207：做"跟单/复制交易"如何定性?
A：通常会触发投顾/组合管理性质风险（甚至与证券类监管交叉），需要适当性/合适性、冲突管理、策略披露、回撤与风险提示；申请前要做监管定位与法律意见。

Q208：做"质押/借贷/理财"是否在 MiCA CASP 范围内?
A：MiCA CASP 并不自动覆盖所有"收益型产品"。若涉及证券化、集合理财或信用中介属性，可能触发其他欧盟/西班牙本地框架。策略：收益类产品先从牌照外隔离（SPV/合作方）或暂停，避免拖慢 CASP 主体获批。

Q209：若提供"稳定币支付/结算"，是否需要额外许可?
A：可能与支付/EMI/银行体系交叉（法币清算、客户资金隔离、收付结构）。交付要用"资金流（money flow）+责任边界+合作机构清单"解释，防止被认定为无牌支付。

Q210：如何证明你"不向零售客户推广高风险产品"?
A：用"受众分层规则 + 营销投放白名单 + KOL/代理条款 + 审批工单 + 留痕"证明；对高风险资产设置"零售禁售/限售规则"。

B 分类｜实体与实质（深化：组织、值勤、会议、有效管理）

Q211：监管如何判断"有效管理"而不是远程遥控?
A：看：董事会与关键委员会在本国召开（可混合但有主场）、关键决策签批在本国完成、重大事件响应链条可在本国启动、数据与系统访问权限在本国可控。

Q212：值勤安排（duty roster）需要到什么颗粒度?
A：至少覆盖：工作日/周末/节假日、交易时段、紧急事件（安全/挤兑/制裁命中）响应。输出"岗位→电话→备岗→升级路径→SLA"。

Q213：办公室是硬性要求吗？共享办公室可以吗?
A：不是"必须大办公室"，但必须能证明真实运营：工位、会议室使用、门禁/访客、设备、档案存放与安全管理。共享办公室可行但要补充证据链与保密措施。

Q214：远程办公是否被否定?
A：不否定，但要有安全与治理：VPN/MFA、设备管理、日志、数据分类、远程审批留痕、关键岗位可用性证明；并说明本国实体如何"最终掌控"。

Q215：最小团队配置怎么写才不被质疑?
A：按服务范围反推：平台/托管必须有安全、风控、合规/AML、运营与客服；只做轻服务可精简，但要说明峰值处理能力与外包补强（含审计权/退出）。

Q216：集团支持团队（海外）能参与吗?
A：可参与支持，但要写清：仅提供二线支持/技术维护/咨询；所有关键决策、客户处置、AML 决策与重大事件响应由本国主体负责并留痕。

Q217：如何证明"本国主体对外包有控制"？
A：合同条款只是基础，还要：配置控制权、规则库所有权、日志导出权限、审计与整改工单、季度评审会议纪要、退出演练记录。

Q218：实体运营模型（Operating model）必须包含哪些图？
A：三张必备：组织架构与汇报线、系统/数据流与权限流、外包与供应链关系图（含分包）。附"职责矩阵 RACI"。

Q219：如何写"客户资产与公司资产隔离"的运营落地？
A：用"四账一致"框架：客户法币账户/客户加密资产地址/内部台账/对外对账一致；并说明每日对账、差异处理、冻结与更正机制。

Q220：如何避免"一个人身兼数职"被质疑？
A：给出资源证明：工时分配、替补机制、二线复核、外部独立审查；并说明关键岗位独立性（例如 MLRO 不与销售 KPI 绑定）。

C 分类｜股东/UBO（深化：控制权、关联方、资金路径、持续监控）

Q221：UBO 穿透到哪里算"够"？
A：穿透到自然人（或明确无法穿透的法定情形并给出控制人/受益人说明），同时披露协议控制与委派权，做到"谁能最终拍板"一目了然。

Q222：如果存在股权质押/对赌条款要披露吗？
A：要。质押、对赌、回购、优先清算、否决权可能导致控制权变化或激励扭曲，属于重大披露点；并写明触发条件与通知机制。

Q223：股东为交易所/项目方/做市商，如何降风险？
A：建立信息墙、上币委员会独立、做市参数审批与监测、关联交易披露、员工交易限制；并在章程/股东协议中限制对业务的干预。

Q224：SoF/SoW 资金路径图要包含什么？
A：每一跳：来源账户→中转账户→入资账户；每跳对应证明文件（流水、协议、审计、完税/分红决议）；并解释任何现金/加密资产转换环节。

Q225：如果入资来自贷款/融资怎么办？
A：披露融资方、合同条款、还款来源、担保安排与关联方关系；并评估是否引入额外控制权或偿付压力影响持续经营。

Q226：如何处理"加密资产入资/以币换股"？
A：通常不建议直接以币入资（估值、反洗钱、税务与审计复杂）；更稳妥是合规处置为法币后入资，并保留处置证据链与税务说明。

Q227：持续监控股东风险怎么做？
A：设股东/UBO 年度复核、重大事件触发复核（诉讼、制裁、媒体负面、财务恶化、控制权变动），并保留筛查报告与董事会记录。

Q228：股东变更的内部审批流程如何写？
A：触发器→合规/AML/风险尽调→法律意见→董事会决议→（如需）监管沟通→实施→更新 UBO 与公告/通知→归档。

Q229：如何解释"最终受益人"与"名义持有人"？
A：通过声明、受托/代持协议披露、资金路径与控制权条款证明真实受益人；名义持有人必须披露并说明其权利限制与信息提供义务。

Q230：如何处理"PEP 关联股东"仍要入股的情况？
A：需要强化 EDD、持续监控、限制其影响业务的治理安排（例如不得参与上币/风控/客户资产决策），并保留董事会风险接受理由与条件。

D 分类｜董事/关键人员（深化：面谈、胜任力、独立性、问责）

Q231：面谈最常见"破防题"是什么？
A：请你用 3 分钟讲清：服务范围→风控→AML→客户资产保护→外包治理→证据链。答不清，监管会认为你"没掌控业务"。

Q232：关键岗位的胜任力如何"证明而非宣称"？
A：用"四件套"：监管版 CV（项目映射）+ 岗位说明书 + 面谈题库答案卡 + 履职证据样本（会议纪要/签批/工单/报告）。

Q233：合规与风险如何保持独立？
A：汇报线直达董事会/审计委员会；有否决/暂停权；绩效与奖金不绑定收入；拥有数据访问权与预算；并定期出具独立报告。

Q234：MLRO 能否由外部顾问担任？
A：可作为支持，但监管更偏好内部负责人（或至少内部 owner）承担最终决策与签批。若外部担任，必须证明可用性、权限与独立性，并设内部替补。

Q235：信息安全负责人必须是全职吗？
A：平台/托管强烈建议全职或至少拥有足够资源；兼职可行但必须有 SOC/安全团队支持与明确的责任边界、演练与整改闭环。

Q236：如何建立委员会体系？
A：至少：风险委员会、合规与 AML 委员会、外包与 ICT 风险委员会、上币委员会（如平台）。每个委员会有章程、议程模板、纪要与决议留存。

Q237：董事会"责任声明"怎么写更有用？
A：不是口号，必须对应：监管义务清单、年度计划、资源配置承诺、重大事项审批范围、问责机制与替补安排。

Q238：如何证明管理层能覆盖 24/7 运营风险？
A：值班表 + 自动监控（告警）+ 升级链 + 事件响应演练 + 备岗人员清单；并提供最近演练记录与改进项。

Q239：关键人员变更会触发什么？
A：通常触发监管通知/批准流程（视主管机关要求），内部要先做交接清单、权限回收与新任尽调，避免"控制真空"。

Q240：如何避免"关键人风险（key person risk）"？
A：岗位备份（deputy）、文档化 SOP、权限分层与双人复核、知识库与交叉培训；并在 BCP 中体现关键岗位缺位情景。

E 分类｜资本/保障/财务可持续（深化：取高、对账、保险、压力测试）

Q241：资本"取高规则"在交付里怎么呈现？
A：用"服务类别→最低资本档位→固定开支口径→取高结果→差额→补足计划"一页表，并附财务模型链接（3 年 + 压力情景）。

Q242：监管为什么会质疑"过于乐观的收入预测"？
A：因为合规成本与获客成本往往被低估。要提供"定价→客群→转化→留存→交易量"可解释假设，并给出保守/基准/乐观三情景。

Q243：平台类费用结构如何避免"隐性收费"风险？
A：建立费用披露矩阵：每项费用触发条件、计算方法、示例、对客户的展示位置与变更通知流程；并做营销素材一致性校验。

Q244：客户资产保障"对账"怎么写成监管可核查？
A：规定：对账频率、数据源、容差阈值、差异分类、升级时限、客户通知标准、补偿规则；并保留对账报表样例与差异工单。

Q245：保险安排如何写才不被认为"甩锅"？
A：明确保险覆盖范围、免赔额、理赔流程与时效、与内部控制的关系（保险是补强，不替代控制），并披露给客户的边界。

Q246：如何证明你有能力承担"黑天鹅事件"？
A：压力测试 + 流动性应急预案 + 冷钱包调拨 SOP + 提现队列机制 + 沟通模板 + 演练记录；并说明董事会授权与快速决策机制。

Q247：审计安排如何规划？
A：财务审计（年度）、合规独立审查（年度/半年度）、安全渗透测试与整改（至少年度+变更触发）、外包审计（年度复评）。

Q248：如何证明"资本不是借来的临时摆拍"？
A：展示长期资金稳定性：股东承诺函、资本补充触发器、资金在账时间、资金来源证据链、以及与运营现金流的匹配。

Q249：如果业务增长过快，资本如何动态跟上？
A：设增长触发：客户数、交易量、外包成本、告警量、客服工单量；触发后启动增资/扩编/升级系统容量的三联动计划。

Q250：如何处理"亏损期持续经营"监管担忧？
A：给出 runway（月度 burn + 现金储备可支撑月份）、融资路径、成本压缩预案（但不得削弱关键合规控制）、以及客户资产保护优先级。

F 分类｜AML/制裁/STR/Travel Rule（深化：自托管、对手方、规则库、质量控制）

Q251：EWRA（企业级风险评估）最容易缺什么？
A：缺"量化与证据"。要有风险因子、权重、评分、数据来源、年度复核与变更审批，并与交易监控规则库一一映射。

Q252：客户风险评分模型如何避免歧视与不一致？
A：使用可解释因子（地域、产品、行为、资金来源、链上风险、历史告警），避免不当敏感因子；并设人工纠偏与复核机制。

Q253：KYB 的 UBO 验证怎么做？
A：公司文件 + 董事/股东名册 + 受益人声明 + 穿透到自然人 + 公共登记/可信数据源校验；高风险企业加做资金与交易目的核验。

Q254：自托管钱包风险控制"最小合规包"是什么？
A：地址归属证明（签名/小额验证/白名单）、链上风险评分、提现限额与延迟、异常触发 EDD、Travel Rule 信息处理策略、拒绝/上报路径。

Q255：与其他 CASP/VASP 的对手方管理怎么做？
A：建立对手方白名单/灰名单/黑名单：合规成熟度、司法辖区、制裁风险、消息标准兼容性、历史拒绝率、事件记录；并签署数据与安全条款。

Q256：链上分析工具输出能直接当证据吗？
A：可作为线索证据，但必须结合客户资料、交易目的、资金路径解释形成完整叙事；并保留工具配置、版本与审计日志。

Q257：规则库阈值怎么解释才不被质疑"拍脑袋"？
A：用历史数据回测、同业基准、风险偏好声明（RAS）与案例复盘来证明阈值合理；每次调参要有审批与回测记录。

Q258：STR 叙事结构怎么写最"监管可读"？
A：时间线→参与方→资金流→链上证据（地址/哈希）→触发原因→调查步骤→结论与建议行动→已采取措施；附件编号化。

Q259：如何处理误报（false positive）过高？
A：做规则优化与分层：先降噪再聚焦；用二级规则与风险模型减少误报，同时确保对高风险场景零容忍。

Q260：如何处理"客户拒绝提供信息"？
A：设分层处置：限制服务/限额/冻结/终止/上报；并记录你请求信息的合理性、客户拒绝、内部决策与通知记录。

G 分类｜ICT/DORA/外包（深化：日志不可篡改、权限、第三方、韧性测试）

Q261：日志"不可篡改"如何落地？
A：采用 WORM/集中日志平台、特权账号隔离、日志哈希校验、访问审计；并设定保存期限与导出流程，确保监管检查可复现。

Q262：权限矩阵（DoA/RBAC）要细到什么程度？
A：至少覆盖：开户/KYC、风控配置、提现审批、密钥操作、上币/参数、费用调整、客户资料修改、告警处置、报告导出。每项对应角色、审批人、留痕字段。

Q263：密钥管理"最低交付证据"是什么？
A：钱包架构图、MPC/多签策略、密钥生成/备份/轮换 SOP、访问控制、审批与日志、应急恢复流程、演练记录。

Q264：渗透测试报告能直接交监管吗？
A：通常可提供摘要与整改证明（避免过度暴露敏感细节），关键是：发现→修复→复测闭环证据，以及董事会监督记录。

Q265：DORA 下第三方 ICT 风险评估要包含哪些要素？
A：关键性评估、集中度风险、分包链、数据驻留与访问、事件通报 SLA、审计权与监管访问、退出迁移计划、韧性测试要求。

Q266：如何做"韧性测试计划"？
A：年度测试日历：备份恢复、故障切换、压力测试、事件响应演练、第三方宕机演练；每次输出测试报告与改进项。

Q267：供应商宕机导致客户损失怎么办？
A：合同赔偿条款只是底线，核心是业务连续性：降级模式、切换方案、客户公告模板、工单与补偿政策、事件复盘。

Q268：如何证明云配置安全？
A：基线（CIS/自定义基线）、IaC 变更控制、密钥与凭证管理、网络分段、最小权限、监控告警、审计日志、定期审计。

Q269：外包是否可以"再外包"（分包）？
A：可以，但必须受控：分包需事先批准、同等审计权与安全条款、分包清单透明、关键分包不得未经许可变更。

Q270：如何做数据泄露通报与客户通知？
A：事件分级→取证→影响评估→监管通报→客户通知→补救→复盘；输出"通报模板+联系人清单+时限 SLA"。

H 分类｜客户保护（深化：披露可读性、营销治理、投诉与赔付）

Q271：披露文件如何做到"写给客户看"？
A：双层披露：一页摘要（关键风险/费用/资产归属/投诉）+ 完整条款；用示例说明费用与滑点；避免复杂术语堆砌掩盖风险。

Q272：费用变更怎么通知才合规？
A：提前通知、差异对比、客户确认留痕；重大变更提供退出/终止权安排，并保存投递与确认记录。

Q273：如何管理 KOL/代理营销？
A：准入尽调、合规培训、素材审批、禁语清单、投放受众限制、佣金披露、违规处罚与终止；保存素材版本与投放证据。

Q274：如何避免"收益承诺/保本暗示"？
A：设置审核红线：不得承诺收益、不得淡化风险、不得用误导性案例；所有宣传语必须可证据支撑，并保留审查工单。

Q275：客户适当性测试失败怎么办？
A：不得硬推；可提供教育材料与冷静期，或限制高风险资产/功能；并保存测试结果与限制措施的记录。

Q276：客户资产归属争议如何处理？
A：先对账与冻结争议资产，启动争议工单；必要时要求警方/法院文件；同时保持客户沟通留痕与监管沟通记录（如触发）。

Q277：赔付政策需要公开吗？
A：需要明确边界与条件：哪些情形可赔、哪些不赔、证据要求、处理时限、争议解决路径；并避免承诺超出能力范围。

Q278：如何处理客户"错误转账到错误地址"？
A：披露不可逆风险；提供尽力协助流程（链上追踪、联系对方平台等）；但明确不保证追回。保留客户确认与处理记录。

Q279：投诉与纠纷如何形成治理闭环？
A：投诉分类→根因分析→制度/系统改进→复核→向董事会报告；建立 KPI（结案时效、复投诉率、赔付金额等）。

Q280：如何证明客服有能力覆盖高峰？
A：提供人员排班、工单系统、SLA、知识库、升级机制、历史峰值数据与扩容计划；并与重大事件沟通模板联动。

I 分类｜护照与跨境（深化：通报、当地营销补丁、数据与税务）

Q281：护照通报最容易被忽视的点？
A：营销与客户文件本地化（语言、费用展示、投诉渠道）、当地消费者保护差异、KOL/广告限制、税务信息字段准备。

Q282：跨境服务如何避免"未通报先营销"？
A：建立"上线闸门"：未完成通报与本地合规补丁不得投放/招揽；所有投放需合规审批工单与受众证明。

Q283：设分支机构的触发条件是什么？
A：客户规模大、需要本地客服/投诉处理、当地监管预期更强、税务与雇佣需求；并评估分支治理成本与数据驻留要求。

Q284：跨境数据传输如何合规化？
A：建立数据分类与传输清单、第三国传输合法基础、供应商合同条款、加密与访问控制、数据主体请求处理 SLA。

Q285：跨境外包与本地监管检查冲突如何处理？
A：合同写入监管访问与审计权；准备"本地可导出"方案；将关键数据与日志确保可从西班牙主体快速导出。

Q286：跨境客户税务信息收集如何做?
A：在开户收集税务居民与税号、声明与更新机制；将交易数据与身份数据打通，保证可按税务报告需求抽取。

Q287：护照扩张的"最稳路线图"?
A：先单一语言/相近市场试点→复制"本地合规补丁包"→扩大；每扩一国做一份"差异清单+材料版本库+运营 SLO"。

Q288：跨境 KYC 能统一吗?
A：可以统一底座，但要允许本地差异：文件类型、验证方式、税务字段、投诉渠道；并做版本管理与差异说明。

Q289：跨境客户争议管辖如何写?
A：在 T&C 里明确适用法与争议解决机制，但同时尊重落地国强制性消费者保护规则；并准备当地语言摘要告知。

Q290：跨境营销素材需要多语言一致性吗?
A：必须一致。建立"母版→翻译→合规复核→发布"流程，保存翻译版本、复核记录与发布时间戳，避免信息差导致误导。

J 分类｜持续合规与变更管理（深化：报告、检查、重大事项、退出）

Q291：获批后的"监管日历"怎么做?
A：把所有义务做成日历：资本与财务报告、AML 年度复核、培训、外包年度评估、渗透测试、BCP/DR 演练、客户披露更新、内审计划与整改复核。

Q292：重大事项通知的内部触发器怎么设?
A：服务扩项、股权/控制权变化、关键岗位变更、核心外包/云迁移、重大安全事件、重大投诉/赔付、重大诉讼与处罚、财务持续经营风险。

Q293：如何建立政策版本库?
A：每份政策：编号、版本号、变更摘要、批准人、发布日期、生效日期、关联流程与表单、归档位置；历史版本可回溯。

Q294：如何管理产品上线（product governance）?
A：上线评审：合规/风险/安全/运营/客服共同签批；上线前完成披露、监测规则、客服脚本、应急预案与回滚方案。

Q295：如何证明"持续监测有效"?
A：KRI 看板 + 抽样测试报告 + 告警处置时效 + STR 质量复核 + 外包 SLA 报告 + 安全事件演练记录，形成月度/季度治理报告。

Q296：监管检查来临时，你的"应答包"要有什么?
A：组织与职责、系统证据链、样本导出模板、对账报表、外包合同与评估、事件响应记录、投诉台账、政策版本库索引、董事会/委员会纪要。

Q297：如何处理监管来函（RFI/问询）?
A：工单化：问题拆解→责任人→证据编号→答复→复核→提交→跟踪；建立统一格式（引用条款+附件编号+结论+后续动作）。

Q298：如何做年度合规总结?
A：按模块汇总：资本、AML、客户保护、ICT/外包、投诉、培训、内审与整改、重大事项；并附 KPI/KRI 数据与改进路线图。

Q299：如何设计"有序退出（wind-down）"可执行?
A：触发条件（财务/事件/监管）→停止新增→保护客户资产→对账与清退→迁移/替代服务→客户通知→争议处理→档案封存→监管沟通。附时间表与责任人。

Q300：BCP/DR 与 wind-down 的区别?
A：BCP/DR 是"继续经营的恢复"；wind-down 是"停止经营的安全退出"。两者都要演练与证据，但目标不同、触发不同、沟通对象不同。

处罚与风险红线（高频问答｜MiCA 风险地图化）

Q301：什么是 MiCA 的"超范围经营"红线?
A：未获授权提供 CASP 服务、或获批后超出授权服务范围提供服务。交付上用"服务白名单 + 系统功能开关 + 上线闸门"确保不超范围。

Q302：未按 Travel Rule 执行会导致什么风险?
A：会触发 AML/制裁合规缺陷，可能导致监管处罚、业务限制与声誉风险；必须用"端到端流程 + 记录留存 + 异常处置"证明执行。

Q303：客户资产混同的风险?
A：极高。会导致客户资产保护失败与重大处罚。必须实现链上地址隔离/台账隔离/对账机制，并有差异处理与审计证据。

Q304：虚假或误导性营销的风险?
A：行为监管高压区：收益承诺、淡化风险、隐性收费、KOL 违规。必须有营销审批与素材归档，违规快速下架机制。

Q305：平台操纵与刷量未监测会怎样?
A：可能被认定为市场秩序失守。必须有监测规则、告警处置、停牌/熔断与调查机制，并保留证据链。

Q306：利益冲突未管理最典型情形?
A：向项目方收费但不披露、关联方做市干预、内部人员抢跑/自营与客户冲突、上币决策不独立。必须建立信息墙、披露与审批机制。

Q307：关键岗位挂名的处罚风险?
A：监管会认为治理失效，可导致拒批/限业/要求整改；获批后可能触发重大缺陷整改甚至许可风险。

Q308：外包无审计权的风险？
A：监管不可达、检查不可执行、退出不可行。必须补齐合同审计权、分包控制与退出迁移计划。

Q309：日志缺失/不可追溯的风险？
A：无法证明合规执行，监管可直接认为内部控制缺陷。必须建立集中日志、不可篡改、导出流程与留存期限矩阵。

Q310：数据泄露/安全事件不通报的风险？
A：触发 ICT 与隐私合规双重风险；必须有事件分级、通报与客户通知 SOP，并做演练与复盘。

Q311：如何把"交易平台规则"写成一份可对外发布的规则书？
A：结构：定义→订单类型→撮合原则→优先级→费用→异常行情→停牌/熔断→取消与更正→上币/下币→申诉与争议→版本更新与公告。附监测与执法（调查/处置）章节。

Q312：如何建立"上币评估机制模板"？
A：评分卡：团队/治理、技术安全、合规与制裁风险、代币经济、流动性与做市、披露质量、持续监测指标、下架触发器；并设委员会决议模板与冲突披露表。

Q313：如何把"托管责任边界"写清？
A：明确：谁控制私钥、谁可发起签名、谁可修改白名单、谁承担盗损/操作失误责任、保险覆盖边界、客户需承担的自托管风险。写入 T&C 与风险披露。

Q314：如何设计"提币审批流程"？
A：自动风控→风险评分→触发阈值人工复核→双人审批→签名→广播→链上确认→对账→客户通知；每步留痕字段与日志来源。

Q315：如何设计"账户冻结/解冻机制"？
A：触发器（制裁命中、欺诈、STR、司法请求、风控异常）→冻结范围→客户通知规则→复核与解冻条件→记录留存→监管沟通（如需）。

Q316：如何建立"异常交易调查工作台"？
A：工单结构：告警原因→交易明细→链上证据→客户资料→调查动作→结论→处置→STR 建议→复核签批。确保可导出。

Q317：如何建立"员工交易与内幕信息"制度？
A：员工账户申报、黑名单期、预先批准、禁止抢跑、信息墙、违规处分；并保留审批记录与抽查记录。

Q318：如何处理"客户多账户"风险？
A：设备指纹/行为画像/关联 UBO 校验；发现关联则合并风控视图、限制或冻结；并记录关联证据与处置依据。

Q319：如何处理"链上高风险地址交互"？
A：规则：自动拦截/延迟/人工复核/EDD/限制提现；并提供处置理由与证据（链上标签、交易图谱、历史行为）。

Q320：如何做"客户教育（risk education）"并留痕？
A：入门课程+测验+确认；高风险功能开启前再做二次教育与确认；保存内容版本、学习记录与测验结果。

申请与补件打法（"审查通过率"导向）

Q321：如何让申请材料"像监管文件而不是市场文案"？
A：每段都要：条款依据→风险→控制→证据→责任人→频率；避免泛泛而谈。用编号化附件索引与交叉引用。

Q322：补件（RFI）怎么回最有效？
A：三段式：1）直接回答结论；2）引用条款与解释逻辑；3）列附件编号与证据位置；最后给"整改计划与完成日期"（如适用）。

Q323：遇到"口径冲突"（不同文件说法不一致）怎么办？
A：建立"单一事实源"：一份主控说明（Operating model + 服务映射）统一口径；其余文件引用主控说明段落编号，避免多头叙述。

Q324：如何用"演示脚本"加速审查？
A：准备 30–60 分钟演示：开户→EDD→制裁命中→告警调查→STR 决策→提币审批→对账→投诉工单→外包审计记录→事件演练报告。

Q325：如何证明"系统不是 PPT"？
A：提供截图、日志样例、工单样例、对账报表样例、演练记录与整改闭环；并能现场导出（脱敏）样本数据。

Q326：如何准备"监管面谈题库"？
A：按岗位分：CEO/COO、合规、MLRO、风险、信息安全、运营。每题配"答案卡+证据编号+可演示点"。

Q327：申请被卡在 AML 怎么办？
A：通常是"不可运行"。补强：EWRA/规则库/STR 决策/Travel Rule 对接/自托管策略/培训与质量复核；并给出系统证据链。

Q328：申请被卡在外包怎么救？
A：补强合同条款（审计权/分包/退出/监管访问/事件通报），补齐尽调与年度评估记录，补一份退出演练计划与资源预算。

Q329：申请被卡在平台监测怎么救？
A：补一套市场监测框架：操纵/刷量/异常波动/关联账户/做市监管；补告警处置 SOP 与证据留痕（调查报告模板）。

Q330：申请被卡在托管安全怎么救？
A：补齐密钥管理、权限矩阵、签名策略、对账、灾备恢复、渗透测试与整改闭环、以及可演示证据链。

运营维持

Q331：如何建立季度治理报告（Quarterly Governance Pack）？
A：固定章节：资本与财务、风险与 KRI、AML 指标（告警/STR/命中）、客户投诉与赔付、外包 SLA、ICT 事件与演练、上币/下币决策、重大事项与整改进度。

Q332：如何管理"政策更新频率"？
A：至少年度复核；重大事件/新法规/新产品触发更新。每次更新保留变更摘要、批准记录、培训记录与生效通知。

Q333：如何把合规 KPI/KRI 设得"不会被打脸"？
A：用可衡量指标：告警处置时效、STR 决策时效、误报率、渗透整改完成率、外包 SLA 达成率、对账差异关闭时效、投诉结案时效。

Q334：如何处理"增长导致的合规容量不足"？
A：建立容量触发器：客户数/交易量/告警量/客服工单量/提现量；触发后自动启动扩编、系统扩容与规则优化计划。

Q335：如何建立"合规预算"并可解释？
A：按模块分摊：AML 工具、Travel Rule 通道、链上分析、审计与测试、SOC/SIEM、法律税务、外包审计、培训与认证；并与财务模型联动。

Q336：如何证明"客户资产保护持续有效"？
A：定期对账报告 + 抽样核查 + 差异闭环 + 冷钱包盘点 + 权限复核 + 独立审查报告。

Q337：如何应对"监管突然要求补充材料"？
A：建立"证据库"(Evidence vault)：所有关键证据按模块归档，可快速导出；并维护监管联系人、答复模板与内部审批流程。

Q338：如何处理"系统供应商涨价/服务调整"？
A：外包合同要有变更通知与退出条款；内部要评估集中度与替代方案，必要时启动迁移计划并做演练。

Q339：如何处理"客户集中度过高"？
A：风险评估与限额策略：对高集中客户设更严格的 SoF/SoW、交易监测与提现控制；并评估声誉与合规风险。

Q340：如何处理"单一链/单一稳定币依赖"？
A：做集中度风险评估，准备降级模式与替代路线（多链、多通道、多做市/流动性来源），并向客户披露风险。

Wind-down/BCP（退出与连续性更细）

Q341：Wind-down 计划必须包含"客户沟通"吗？
A：必须。包含：何时通知、通知渠道、客户资产提取路径、争议处理、客服承接、时间表与常见问题模板。

Q342：Wind-down 计划必须包含"数据与档案封存"吗？
A：必须。包括：KYC/交易/告警/STR/投诉/对账/外包审计/事件响应记录保存期限、存储介质、访问控制与监管取证路径。

Q343：BCP/DR 必须包含"供应商失效"情景吗？
A：必须。关键供应商失效要有降级模式、切换方案、客户公告模板、事件工单与复盘闭环。

Q344：如何定义 RTO/RPO 并让监管相信？
A：按关键系统分级：交易撮合、钱包签名、KYC、监控、工单、对账。每项给出 RTO/RPO、备份策略、演练记录与改进项。

Q345：如何处理"清退时客户不配合"？
A：在 T&C 里预先约定清退机制与期限；对长期不响应设保管/托管与最终处置规则（需符合法律），并保留通知与尝试记录。

Q346：Wind-down 是否需要资金预算？
A：需要。估算：客服、人力、法律、审计、系统维持、链上手续费、对账与清退成本；并证明你有资金支撑退出执行。

Q347：如何处理"退出期间的欺诈冲击"？
A：退出期是高风险期：加强监控、限额、人工复核、延迟提现、白名单策略；并准备客户沟通与报警/上报路径。

Q348：如何处理"退出期间的市场波动导致挤兑"？
A：设队列、分批、冷钱包调拨 SOP、风险提示与公告模板；并保留对客户的公平处理证据，避免差别对待。

Q349：如何证明"退出不伤害客户"？
A：以客户资产保护优先：资产可提取、对账透明、投诉与争议可解决、客户沟通充分、时间表清晰、数据与凭证可追溯。

Q350：退出完成后的"关闭义务"有哪些？
A：监管通知、客户最终结案、档案封存、外包合同终止与数据回收、财务清算与审计、遗留争议处理机制保留。

终局：把风险地图化为"红线清单 + 控制清单"

Q351：请给出 MiCA/CASP 常见 20 条红线清单（摘要）？
A：未授权经营、超范围经营、客户资产混同、虚假营销、隐性收费、不披露冲突、平台操纵不监测、托管密钥控制不当、对账缺失、日志不可追溯、外包无审计权、无退出方案、AML 不可运行、STR 不提交/质量低、制裁命中处置不当、Travel Rule 不执行、重大事件不通报、关键岗位挂名、重大变更不通知、数据泄露治理缺失。

Q352：如何把红线转成内部控制清单？
A：每条红线对应：控制措施→责任人→证据→频率→抽样与复核→整改闭环。形成"合规控制矩阵（Control matrix）"。

Q353：如何给监管展示你"能自我纠错"？
A：展示：内审/独立审查报告、问题台账、整改计划、完成证明、复测结果、董事会监督纪要。

Q354：如何建立"合规文化"的证据？
A：培训记录、举报机制、违规处分案例（脱敏）、管理层讲话与年度合规目标、绩效不以收入单一导向。

Q355：如何处理员工离职造成的控制缺口？
A：权限回收 SOP、交接清单、知识库、岗位替补、临时授权与限制措施；并保留离职流程工单与审计记录。

Q356：如何处理外包人员可访问客户数据的风险？
A：最小权限、数据脱敏、访问审批与审计、合同保密条款、监控告警、定期复核；高敏数据原则上不开放或仅开放受控视图。

Q357：如何应对监管对"集中度风险"的问询？
A：提供集中度评估（供应商、链、稳定币、客群、做市）、替代方案与迁移计划、以及测试/演练记录。

Q358：如何应对监管对"系统可扩展性"的问询？
A：提供容量规划、峰值压力测试、自动扩容策略、降级模式、监控指标与告警；并证明已测试并有记录。

Q359：如何应对监管对"客户保护"不足的问询？
A：补强披露（双层披露）、投诉闭环、费用透明、风险教育、受众分层与适当性机制；提供客户确认留痕与工单样本。

Q360：如何应对监管对"收益类产品"质疑？
A：先隔离：主体不提供/不推广，或通过合作方并做清晰披露与责任边界；提供法律意见与产品治理文件，避免拖累 CASP 主体授权。

最后 40 题：把"交付落地包"写到可直接复制成目录

Q361：如果我要做一份"西班牙 CASP 申请交付清单"，目录怎么排？
A：建议：服务映射→组织与治理→资本与财务→股东/UBO→人员胜任力→AML/Travel Rule→平台规则/托管安全→ICT/DORA/外包→客户文件→报告与持续合规→BCP/DR→Wind-down→证据库索引。

Q362：最关键的 10 份政策文件是什么？
A：AML/CFT 手册、制裁政策、Travel Rule 程序、客户资产保护政策、平台规则书、上币治理政策、信息安全政策、事件响应政策、外包治理政策、投诉与争议处理政策。

Q363：最关键的 10 个模板表单是什么？
A：风险评估表、EDD 记录表、STR 决策表、制裁命中处置表、外包尽调表、外包年度评估表、事件响应报告、渗透整改闭环表、对账差异工单、投诉结案报告。

Q364：最关键的 10 个系统证据截图是什么？
A：KYC 流程、制裁筛查命中、告警列表、调查工作台、提币审批、多签/MPC 签名、权限矩阵、日志导出、对账报表、投诉工单系统。

Q365：如何把"证据库"做成可检索？
A：按模块（A–J）+ 附件编号 + 关键词标签 + 版本号；建立索引表（Index）一键定位证据。

Q366：如何把"合规培训"做成可证明？
A：年度计划、课件版本、签到、测验、通过标准、补训记录；对关键岗位加做案例演练与口试记录。

Q367：如何把"监管沟通"留痕？
A：会议纪要、参会名单、议程、问题清单、答复材料、后续行动项与完成证明，全部归档入证据库。

Q368：如何确保"客户披露与内部政策一致"？
A：建立一致性检查：政策条款→客户文件→营销素材三方比对；变更时同步更新并强制客户确认。

Q369：如何处理"系统变更导致合规规则失效"？
A：变更评估必须包含合规影响；上线前回归测试（KYC/监控/Travel Rule/对账）；上线后监控告警；保留测试报告与审批记录。

Q370：如何为监管检查准备"脱敏样本包"？
A：预设脱敏规则与导出模板；保证可复现流程与证据链（保留哈希、时间戳、工单号），既保护隐私又可验证。

Q371：如何做"合规年度预算"最稳？
A：按模块列明固定成本与弹性成本，并设置增长触发；预留审计、渗透测试、外包审计、法律意见与突发事件预算。

Q372：如何证明"董事会真的监督合规"？
A：提供季度治理报告、董事会审议记录、整改跟踪表、重大事项审批记录、资源配置决议。

Q373：如何管理"新资产类别/新链/新桥"的引入？
A：产品治理流程：风险评估→安全评估→合规评估→监测规则→客户披露→上线审批→上线后复盘。每步留痕。

Q374：如何管理"跨链桥"风险？
A：设白名单桥、链上监测、限额与延迟提现、异常告警；并向客户披露桥风险（合约漏洞、拥堵、回滚等）。

Q375：如何管理"隐私币/匿名增强资产"？
A：通常风险极高：限制/禁售、强化 EDD、严格监测与提现控制；并在政策与客户披露中明确立场。

Q376：如何管理"做市与自营"合规？
A：做市规则透明、参数审批、异常监测、关联披露、信息墙；自营与客户订单隔离，禁止抢跑与利益冲突。

Q377：如何管理"价格操纵指控"?
A：保留监测证据、调查报告、处置记录（暂停/限权/下架）、与客户沟通与申诉记录；必要时与监管沟通留痕。

Q378：如何管理"客户资产追回请求"?
A：建立协助流程（链上追踪、联系对手方平台、执法协作），但明确不保证追回；并保留协助记录与客户确认。

Q379：如何管理"司法/执法请求"?
A：设专门通道：合法性校验→冻结/保全→数据导出→留痕→客户通知（如允许）→后续跟踪；并保护数据最小披露。

Q380：如何管理"高风险行业客户（博彩/成人/跨境换汇等）"?
A：行业分级、强化 KYB/UBO、交易目的核验、限额、持续监控与更高频复核；必要时拒绝并留痕。

Q381：如何管理"代理商带来的客户"风险?
A：代理商尽调、培训、素材审批、佣金披露；客户仍需你方独立完成 KYC/KYB 与风险评估，不能把审核外包给代理。

Q382：如何管理"退款/拒付（chargeback）"与欺诈?
A：法币通道配合反欺诈规则、设备与行为风控、提现延迟、黑名单与调查；并保留证据以支持争议处理。

Q383：如何管理"客户资产被盗后的赔付决策"?
A：启动事件响应→取证→责任归因→保险理赔→赔付委员会决议→客户沟通→整改；赔付规则必须事前披露并可执行。

Q384：如何管理"员工社会工程攻击"?
A：安全培训、双人复核、特权操作强审批、钓鱼演练、零信任访问；并保存演练与改进记录。

Q385：如何管理"API 客户/机构客户"风险?
A：API 权限分层、速率限制、异常行为监控、机构 KYB 与技术对接尽调、事件通报机制；并将 API 行为纳入交易监控。

Q386：如何管理"量化交易/高频"对市场秩序影响?
A：设置限频、风控阈值、异常策略识别、断路器、参数审批；并披露相关规则，避免对零售形成不公平环境。

Q387：如何管理"费用回扣/返佣"合规?
A：披露返佣规则、避免诱导性激励、建立审批与会计留痕；对关联返佣加强冲突披露与董事会批准。

Q388：如何管理"客户数据主体权利（GDPR）请求"?
A：建立工单：身份核验→范围确认→导出/更正/删除（如允许）→法定保留例外→回复时限→留痕归档。

Q389：如何管理"数据删除与法定留存冲突"?
A：用"留存矩阵"说明：哪些数据必须留存（AML/税务/监管）不得删除，其他数据可按政策删除；并向客户透明披露。

Q390：如何管理"内部模型（风控/评分）偏差"?
A：模型治理：回测、偏差监控、人工复核、变更审批、版本控制；并对高影响决策保留可解释性记录。

Q391：如何管理"审计发现事项"的整改?
A：问题台账→根因→整改计划→责任人→截止日→完成证明→复核→关闭；重大问题上报董事会并记录监督。

Q392：如何管理"监管处罚案例学习"?
A：建立案例库：同业处罚原因→你方差距→整改措施→培训；并纳入年度合规计划与审计重点。

Q393：如何管理"新法规/RTS/ITS 发布"带来的变更?
A：法规雷达→影响评估→项目计划→测试上线→培训→留痕；确保每次变更都有证据链与董事会知悉记录。

Q394：如何管理"跨境团队访问生产数据"?
A：最小化访问、脱敏、只读、时间窗授权、全量审计；关键数据原则上由西班牙主体掌控并可随时撤权。

Q395：如何管理"供应商集中度（single point of failure）"?
A：识别关键供应商→替代方案→合同退出条款→迁移演练→分散采购策略；并在季度治理报告中持续跟踪。

Q396：如何管理"客户资产地址变更/白名单变更"的欺诈?
A：变更延迟生效、强 MFA、二次验证、客服回访（高风险）、设备指纹校验；并保留变更工单与验证证据。

Q397：如何管理"多链资产对账复杂性"?
A：统一台账与数据字典、链上数据源校验、多链对账引擎、差异处理 SOP；并设链上异常数据的人工复核。

Q398：如何管理"停机维护"对客户的影响?
A：提前公告、维护窗口、受影响功能列表、紧急联系渠道、回滚预案；并保存公告与客户触达记录。

Q399：如何管理"监管口径变化"导致的材料重写?
A：保持主控说明（Operating model）为单一事实源，所有文件引用主控编号；口径变化时只改主控并同步派生文件，减少系统性返工。

Q400：如果让我用一句话概括"西班牙 CASP 过审的关键"，是什么?
A：**把业务边界讲清，把责任链做实，把 AML/Travel Rule 与 ICT/外包"跑起来并留痕"，再用可演示证据链把一切证明出来。**

仁港永胜建议（西班牙 CASP｜可执行清单）

1. **先定服务边界**：把业务拆到 MiCA 服务类别，形成"服务映射图 + 制度/系统/资本/人员对照表"。
2. **材料按监管可读组织**：建立 ITS 表格字段→附件编号→页码/段落的 Index；所有关键声明必须有证据附件。
3. **Travel Rule 做到端到端可运行**：字段、对接、异常处置、留存与审计轨迹一体化（EU 2023/1113）。

4. **把 DORA 当硬门槛**：事件响应、第三方风险、韧性测试、日志与权限等用"可演示证据链"呈现（2025-01-17 起适用）。
5. **先做 RFI-ready**：把最常见补件主题（Substance、外包、资本、系统安全、AML/STR）预先做成"条款依据→措施→证据→责任人→日期"的应答包。

选择仁港永胜的好处（核心优势）

- **监管导向写作 + RFI 补件能力强**：把技术/风控落成监管可读证据链与附件编号体系，显著降低补件回合。
- **模板库可直接落地**：Master Checklist（A–I）、BP/财务模型、AML/Travel Rule SOP、ICT/DORA 与外包治理制度、平台规则/上币评估、面谈题库等。
- **跨境护照与集团结构经验**：护照通报包、多国营销合规补丁、UBO/SoF/SoW 证据链与资金路径图一体化交付。

关于仁港永胜（Rengangyongsheng）

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、外包与退出）

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。

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。内容依据欧盟与西班牙公开信息整理（包括 CNMV MiCA 授权手册、EU 2023/1113 Travel Rule、DORA 等），仅作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、审查要点与费用以主管机关及最新法规/RTS/ITS 为准。

如需进一步协助（西班牙/欧盟 CASP 申请、收购并购、材料编制、系统合规与持续维护），欢迎联系唐生获取专业支持。
