《开曼 Cayman Islands VASP 虚拟资产服务牌照常见问题解答》

Frequently Asked Questions about Cayman Virtual Asset Services License (VASP)

（依据开曼群岛金融管理局 CIMA 最新公开法规/公告/FAQ/规则文件整理；含 2025 年 4 月 1 日起"Phase 2"牌照分轨：registration / licensing / waiver，以及 2025 修订法规引入/更新 Schedule 1A 与 Schedule 2 费用安排。）

国家/地区： 开曼群岛 Cayman Islands
主管机构： Cayman Islands Monetary Authority（**CIMA / "Authority"**）｜开曼群岛金融管理局（CIMA）
牌照/注册制度（以最新法规与CIMA公开口径为准）：

- 总体法律依据为《Virtual Asset (Service Providers) Act》（常见简称 **VASP Act / VASPA**，以修订版与修订法为准）。
- **Phase Two 自 2025年4月1日起生效：** 对在或自开曼提供**虚拟资产托管**与**虚拟资产交易平台**服务的 VASP，**从"注册/豁免"进入"必须持牌（Licence）"**。

  唐生一句话结论： 开曼VASP不是"一个名字叫VASP就完事"，而是 **"注册（Registered Person）+ 持牌（Licence）+ 受监管法下豁免（Waiver）"三轨并行**；2025/04/01后，**托管与交易平台**基本进入"必须持牌"的硬门槛。

本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐生（唐上永，Tang Shangyong）**｜**业务经理** 提供专业讲解。
服务商：仁港永胜（香港）有限公司｜Rengangyongsheng (Hong Kong) Limited

✅ 点击这里可以下载 PDF 文件：开曼 Cayman Islands VASP 虚拟资产服务牌照常见问题解答（FAQ）
✅ 点击这里可以下载 PDF 文件：开曼 Cayman Islands VASP 虚拟资产服务牌照申请注册指南
✅ 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）。

牌照信息

- **Virtual Asset (Service Providers) Act – Registration**（Registered Person / VASP Registration）
- **Virtual Asset (Service Providers) Act – Licence**（VASP Licence：重点适用于 **虚拟资产托管** 与 **虚拟资产交易平台** 等高风险类别；自 2025-04-01 起进入实质牌照阶段）
- **（如适用）VASP Waiver**（适用于已按其他监管法律受监管的"Supervised Persons"的豁免路径；CIMA 亦以 waiver 分轨表述，并发布 Licensing & Waiver Checklist）
- **监管机构**：Cayman Islands Monetary Authority（CIMA）
- **关键更新**：2025 修订法规将"牌照申请表 Schedule 1A"与"费用 Schedule 2（申请费+批复费双段）"制度化。

适用对象（Target Applicants）

适用于拟在或自开曼群岛开展、或以开曼为运营/集团枢纽并对外提供虚拟资产服务（"in or from within the Islands"）的机构，包括：

1. **虚拟资产托管（Custody）**：交易所托管、机构托管、钱包托管、密钥控制、MPC/多签托管等（2025/04/01 起通常进入"必须持牌"范畴）。
2. **虚拟资产交易平台（Trading Platform）**：订单簿撮合、撮合+结算、平台运营等（2025/04/01 起通常进入"必须持牌"范畴）。
3. **经纪 / OTC / 兑换 / 转移等 VASP 服务提供者**：多为注册（Registered Person）路径，但需按具体业务边界与CIMA口径确认。
4. **已在CIMA其他监管法下持牌/注册的金融机构**，拟"附带"提供虚拟资产服务：可能走 **Waiver（豁免）** 路径，但需要法律意见书与材料清单按要求提交。

常见问题解答｜开曼虚拟资产服务牌照（VASP）

Frequently Asked Questions about Cayman Virtual Asset Services License (VASP)

第一部分｜监管范围与牌照分轨（Perimeter & Licensing Track）

Q1：开曼 VASP 法（VASP Act）适用于哪些主体?
A（交付级写法）：

1. **适用对象**：任何在开曼群岛"**境内或自开曼（in or from within the Cayman Islands）**"提供虚拟资产服务（VAS）的实体或个人，都可能落入 VASP Act 的监管范围。
2. **判断逻辑（监管检查常用）**：不以"客户是否在开曼"'服务器是否在开曼"作为唯一标准，而以"**经营活动的实质连接点**"综合判断，例如：
   - 公司是否为开曼设立实体（Exempted Company/LLC 等）；
   - 董事会/高管/关键岗位是否在开曼进行决策与监督；
   - 关键系统控制（密钥、钱包、撮合规则、风控阈值）是否由开曼实体控制；
   - 是否以开曼名义对外招揽客户、签署客户协议、收取费用；
   - 是否从开曼组织运营团队、外包管理、客户支持与合规处置。
3. **交付建议**：在递交前制作《Perimeter Memo（监管边界说明书）》：用一页图把"实体/人员/系统/资金/客户"五要素落点画清楚，作为后续"走 Registration / Licence / Waiver"路径的论证底座。

Q2：什么是"虚拟资产服务（Virtual Asset Service / VAS）"?
A（交付级写法）：

1. **定义来源**：以 VASP Act 与 CIMA 对 VASP 的 FAQ 定义为准。
2. **实务归纳**：可将 VAS 拆解为四类"监管会问的交易功能"：
   - **Exchange（交换）**：币币/法币兑币/撮合兑换；
   - **Transfer（转移）**：代表客户发起链上转账/内部账转移；
   - **Custody（托管/控制）**：持有、控制或能动用客户虚拟资产或其控制权（如私钥/签名权）；
   - **Platform Operation（平台运营）**：运营撮合规则、订单簿、成交机制、上币与市场秩序。
3. **交付建议**：在业务说明书中将每一项产品功能映射到"是否构成 VAS"的定义条目，并标注"风险等级（Low/Medium/High）+ 对应控制措施"。

Q3：只做海外客户、服务器在海外，仍可能被认定为"in or from within Cayman"吗?
A（交付级写法）：

1. **答案**：可能。监管判断更看重"**经营实质**"，而不是单一技术部署地点。
2. **常见触发点**：
   - 以开曼实体签客户协议并收费；
   - 平台规则、风控阈值、上币决策由开曼董事会/管理层批准；
   - 客户资产（或关键密钥/签名权）由开曼实体或其外包方在开曼受控；
   - 合规处置（冻结、拒客、STR 决策）由开曼实体作出；
   - 对外宣传"开曼注册/开曼合规/受开曼监管"（即便营销，也形成强连接点）。
3. **交付建议**：若你希望降低被认定连接点，应在 Perimeter Memo 中明确：哪些控制权在何处；并配套"**控制权不在开曼**"的证据（合同、权限矩阵、董事会保留事项、系统管理员清单等）。

Q4：开曼 VASP 分为哪三条路径?
A（交付级写法）：

1. **Registration（Registered Person / 注册）**：通常适用于不属于"必须持牌"的高风险类别；完成注册后受持续监管与 AML/CFT 义务约束。
2. **Licence（VASP Licence / 牌照）**：重点面向 **Virtual Asset Custodians（托管）** 与 **Virtual Asset Trading Platforms（交易平台）** 等高风险活动，自 2025-04-01 起进入 Phase 2 实质落地。
3. **Waiver（豁免）**：面向已按其他监管法律受监管的 "Supervised Persons"，可以申请豁免路径（仍需满足 CIMA 对应清单/条件）。
4. **交付建议**：对外材料建议用三分轨图示：
   - 先做"是否 VAS？"；
   - 再做"是否 Custody / VATP？"；
   - 最后做"是否 Supervised Person 可 Waiver？"

Q5：Registered Person（注册）适合哪些业务?
A（交付级写法）:

1. **定位**：通常适用于相对低风险、且不触发"托管/交易平台必须持牌"的 VAS 活动。
2. **实务例子（需个案定性）**:
   - 某些仅提供撮合/经纪、但不控制客户资产、且不构成"平台运营"的模式;
   - 某些技术服务/代理服务（不掌握控制权）但仍可能构成 VAS 的边缘业务。
3. **监管会追问的三件事**:
   - 你是否"实际上控制客户资产"?（若是，可能升级 Licence）
   - 你是否"运营交易规则/撮合系统"?（若是，可能属于 VATP）
   - 你是否存在"资金池、统一钱包、代客户转移"?（若是，风险上升）
4. **交付建议**：注册路径也要按"可运行体系"准备 AML、风险评估、记录保存、外包治理等，不要把注册当"轻量备案"。

Q6：VASP Licence 重点覆盖哪些高风险类别?
A（交付级写法）:

1. **核心类别**:
   - **Virtual Asset Custodians（虚拟资产托管）**：对客户虚拟资产或其控制权（例如私钥/签名权）进行保管、控制或管理。
   - **Virtual Asset Trading Platforms（虚拟资产交易平台）**：运营撮合/订单簿/交易规则/市场秩序管理的交易场所。
2. **监管强度**：Licence 的尽调深度通常显著高于 Registration：系统证据链、钱包/密钥控制、对账、市场监控、外包审计权等都会被重点审查。

Q7：Phase 2 牌照制度何时实质生效?
A（交付级写法）:

1. **关键日期**：2025 年 4 月 1 日起，开曼虚拟资产监管进入"Phase 2"——托管与交易平台类活动进入实质牌照阶段（Licence 路径落地）。
2. **对项目管理的意义**:
   - 你的业务若触及 Custody/VATP，应以 Licence 目标倒推：人员、系统、制度、审计、保险、对账机制必须提前建设;
   - 如果仍按"仅注册"思路推进，后续补件与整改成本会急剧上升。

Q8：Waiver（豁免）适用前提是什么?
A（交付级写法）:

1. **适用逻辑**：若申请主体已在开曼按其他监管法律受 CIMA（或相关制度）监管，可能属于 "Supervised Person"，可申请 Waiver。
2. **核心证明**:
   - 你已受监管的事实（牌照/注册证明、受规管活动范围）;
   - 你提供的 VAS 活动如何被现有监管框架覆盖（治理、资本、客户资产保护、合规）;
   - 你仍能满足 CIMA 对应的文件清单与持续义务。
3. **交付建议**：制作《Waiver Justification Pack》：用 10–15 页说明"监管覆盖等效性"，并逐条对照 CIMA Waiver Checklist 的编号提交。

Q9：不注册/不持牌/不豁免提供 VAS 有何后果?
A（交付级写法）:

1. **监管风险**：构成违法，可能面临行政措施、刑事处罚、业务停止、声誉损害等后果。
2. **商业后果**：银行/通道/机构合作方通常会将"未合规准入"视为重大红线：可能直接终止合作、冻结账户或拒绝开户。
3. **交付建议**：对外客户沟通材料建议加入"合规状态声明（Compliance Status Statement）"模板，避免误导陈述。

Q10：CIMA 是否有专门的 VASP FAQ?
A：有。CIMA 发布 VASP FAQ，对适用范围、关键定义、注册/牌照/豁免路径等提供明确口径与解释。
（交付建议：把 FAQ 的关键定义引用进你的《Perimeter Memo》与《Business Plan》，并在文末列"监管引用清单"。）

第二部分｜关键概念定义（Custody / VATP / Control）

Q11：什么是"虚拟资产交易平台（VATP）"?
A（交付级写法）:

1. **实务定义**：若你运营一个"让买卖双方形成成交"的交易场所，并由你制定/执行交易规则（撮合、订单优先级、撮合引擎、停牌/熔断、上币/下架等），通常会被视为 VATP。
2. **监管关注点**：
   - 市场秩序：反操纵、反刷量、异常波动监控；
   - 透明度：撮合规则、费用披露、上币标准；
   - 客户资产保护：隔离、对账、处置机制。
3. **交付建议**：交易平台项目务必准备《Market Surveillance Framework（市场监控框架）》与《Listing/Delisting Policy（上币/下架制度）》作为申请附件。

Q12：什么是"虚拟资产托管（Custody）"?
A（交付级写法）：

1. **核心判断**：你是否"**控制**"客户虚拟资产或其控制权（例如私钥、签名权、转移权限、MPC 分片控制、提币审批权）——只要能影响资产转移，即为高风险托管特征。
2. **典型托管形态**：
   - 热/冷钱包托管；
   - MPC 托管；
   - 代客户管理密钥/恢复方案；
   - 统一钱包归集、内部账分配（即便声称"非托管"，也可能被认定托管）。
3. **交付建议**：托管申请包至少应包含：
   - 《Key Management Policy》
   - 《Wallet Architecture & Signing Workflow》
   - 《Access Control Matrix（权限矩阵）》
   - 《Withdrawal Approval SOP（提币审批流程）》
   - 《Reconciliation SOP（对账流程）》

Q13：钱包软件（纯技术）是否必然属于 VASP?
A（交付级写法）：

1. **不必然**：若仅提供非托管软件工具（用户自持钥、你不介入转移），可能不构成 VASP；但若你提供"代执行交易/代转移/代保管控制权"等服务，则可能落入监管范围。
2. **监管会问的四个问题**：
   - 你是否能单方或共同签名转移资产?
   - 你是否能冻结/解冻/改写提币白名单?
   - 你是否掌握恢复/重置机制?
   - 你是否对客户资产做归集/统一钱包?
3. **交付建议**：准备《Non-custodial Statement（非托管声明）》与系统证据（权限截图、密钥分布、恢复流程），避免"名义非托管、实质可控"的矛盾。

Q14：只做 OTC 是否一定是 VASP?
A（交付级写法）：

1. **大概率会触及 VAS**：OTC 往往涉及交换（exchange）与转移（transfer）。
2. **是否升级为高风险的关键点**：
   - 是否代客户收付、是否形成资金池；
   - 是否使用统一钱包归集；
   - 是否对客户资产有暂时控制；
   - 是否存在第三方代付、现金交易等高风险要素。
3. **交付建议**：OTC 业务应提交《Funds Flow Diagram（资金路径图）》+《Same-name In/Out Policy（同名出入金政策）》+《Large Transaction EDD SOP（大额交易EDD流程）》作为核心附件。

Q15：只做经纪撮合（不碰资产）是否可能仅注册而非持牌?
A（交付级写法）：

1. **可能**：若你不构成 VATP（不运营撮合引擎/订单簿/平台规则）且不控制客户资产，可能适用 Registration。

2. **但常见"被升级"的原因**：
    - 你虽不碰资产，但你运营撮合系统并制定规则 → VATP；
    - 你通过"统一结算、代收代付"形成控制权 → custody/transfer；
    - 你对交易对手方做集中报价、形成市场场所属性。
3. **交付建议**：在 BP 中明确：撮合仅限"介绍/撮合撮合"，成交与结算由第三方完成，并列出合同与权限边界证据。

Q16：做法币出入金（fiat on/off-ramp）如何定性？
A（交付级写法）：

1. **VASP 角度**：你通常会触及 exchange（法币兑币）与 transfer（代转移）要素。
2. **银行与监管角度**：法币环节会显著抬高 AML 风险：来源资金、第三方代付、欺诈退款、通道套现等都是高频问询点。
3. **交付建议**：必须提供：
    - 银行账户结构与收款主体说明；
    - 同名出入金规则与例外审批；
    - 退款/拒付处置流程；
    - 交易监控规则（拆分、快进快出、异常对手方）。

Q17：做"发行/推广虚拟资产"是否在 VASP 范围？
A：可能。若你提供与发行相关的服务安排（例如发行代理、承销式安排、代币发行平台服务、营销分发与收款结算），可能落入 VAS 定义范围；若代币具证券属性，还可能触及其他监管法律。
（交付建议：做《Token Classification Memo（代币属性分类备忘录）》与《Offering Controls（发行控制清单）》并纳入风险评估。）

Q18：同一公司能否同时做交易平台+托管？
A（交付级写法）：

1. **可行**，但监管期望更高。
2. **必须解决的三类冲突**：
    - 客户资产保护：平台运营与托管控制必须隔离（权限、岗位、审批链）；
    - 利益冲突：上币、做市、自营、清算收费需披露与管控；
    - 风险传染：技术/外包/事故响应必须分层与可隔离。
3. **交付建议**：监管递交常见"最佳实践"：平台实体与托管实体分设；或至少在同实体内设置"独立托管线"与独立审批链，并提供权限矩阵证明。

Q19：同集团多实体分别持牌是否更稳？
A（交付级写法）：

1. **常见结构**：HoldCo（控股）+ OpCo（平台运营）+ CustodyCo（托管）+ PaymentsCo（法币通道）。
2. **优势**：风险隔离、便于满足不同监管要求、降低单点事故影响。
3. **监管底线**：结构必须真实，不能仅"纸面分拆"；每个实体要有实质（人员、系统控制、董事会监督、合同与资金路径）。

Q20：CIMA 对"境内实质（substance）"敏感吗？
A（交付级写法）：

1. **敏感**：CIMA 行业评估与监管实践均强调治理、网络安全、外包监督等"可运行实质"。
2. **可验证的实质证据**：
    - 董事会纪要、KRI 报告、整改闭环台账；
    - 关键岗位任命文件与工作日志；
    - 系统访问控制与审批链记录；
    - 外包审计与供应商评估记录。
3. **交付建议**：建立《Substance Evidence Pack（实质证据包）》作为持续监管与银行尽调用。

第三部分｜路径选择与关键表格/费用（Forms & Fees）

Q21：是否必须在开曼设实体？
A：通常需要以开曼实体作为申请主体（结构形式由方案确定）。实际项目中还应同步考虑税务、银行开户、外包合同签署主体与数据/系统控制主体的一致性。

Q22：是否允许完全远程团队？
A（交付级写法）：

1. 可部分远程，但关键职能（治理、合规、资产控制、事故响应）需确保：
    - 可在监管要求下快速响应；
    - 可被检查与提供证据链；
    - 不因外包/远程导致"无人负责"。
2. 交付建议：准备《Resourcing Plan（人员配置计划）》：列岗位、职责、地点、时间投入、备份安排。

Q23：监管更关心"形式注册"还是"可持续运营能力"？
A：更关心可持续运营能力：制度是否能运行、系统控制是否可审计、治理是否能推动整改闭环。

Q24：注册与持牌的核心差异一句话？
A：**注册**是准入分轨的较低强度路径；**持牌**对应高风险活动（托管/平台）并需满足更强规则、系统证据链与持续监管要求。

Q25：是否存在"临时/过渡安排"？
A（交付级写法）：

1. 2025-04-01 起 Phase 2 实质落地，行业通常存在过渡沟通与监管安排（以 CIMA 公告与个案为准）。
2. 交付建议：若你处在过渡期，应准备《Transition Plan（过渡计划）》：时间表、里程碑、风险缓释、沟通记录。

Q26：是否可以先注册再申请 Licence？
A：可以；但如果业务本质已属于 Custody/VATP，建议以 Licence 要求倒推建设，不要把注册当"拖延牌照"的策略。

Q27：Licence 申请是否有专门表格？
A：有。2025 修订法规引入/更新 **Schedule 1A：Application for Licence**。

Q28：费用是否在 2025 修订中更新？
A：是。费用在 **Schedule 2** 中更新，并且 CIMA 公告明确了"申请费 + 批准后费用"的双段缴付机制。

Q29：是否存在 CIMA 的 Licensing & Waiver Checklist？
A：存在。该清单用于指导 Licence 与 Waiver 的材料递交结构与编号。

Q30：Checklist 对 Waiver 的材料要求与 Licence 一样吗？
A：不完全相同。Waiver 常仅需清单的部分章节，但仍须证明监管覆盖与持续义务可被满足。

第四部分｜规则要求：托管与交易平台（Rule Expectations）

Q31：VASP 是否必须遵守 AML/CFT？
A：必须。CIMA 对 VASP 的 AML/CFT 有明确监管说明（现场/非现场监督），且你需建立风险评估、KYC/EDD、监控、STR、记录保存等体系。

Q32：CIMA 是否针对托管与交易平台发布专门规则（Rule）？
A：是。CIMA 发布《Rule – Virtual Asset Custodians and Virtual Asset Trading Platforms》，对高风险类别提出更强要求。

Q33：该 Rule 的法律地位是什么？
A（交付级写法）：

1. 该 Rule 是 CIMA 在监管框架下发布的规则性要求，适用于相应类别主体，并作为审批与持续监管的关键基准。
2. 交付建议：在申请包中做《Rule Mapping Table（条款对照表）》：逐条对照 Rule → 你公司的制度章节 → 系统证据（截图/日志/报表）。

Q34：开曼 VASP 与基金/证券监管如何交叉？
A（交付级写法）：

1. 若你提供的产品或服务具有证券/基金/衍生品属性，可能触发其他监管法律义务（例如投资管理、发行分销等）。
2. 交付建议：并行准备《Regulatory Perimeter Matrix（监管边界矩阵）》：VASP Act / AML / 其他金融监管逐项勾稽，避免"只做 VASP 合规，忽略证券/基金边界"。

Q35：是否允许"只面向专业投资者"？
A：可以作为风险降低策略（如降低零售投诉与误导风险），但并不自动豁免 VASP 义务；仍需满足 VASP Act、Rule 与 AML/CFT。

Q36：CIMA 对"市场行为/披露"是否有要求?
A：有。尤其平台类被期望确保透明、公平、避免误导，并建立市场监控与利益冲突管理机制。

Q37：CIMA 是否关注网络安全与外包?
A：高度关注。CIMA 行业评估指出治理与网络安全、外包监督等存在差距，监管趋势偏向持续加强。

Q38：CIMA 是否会进行主题检查/行业评估?
A：会，并公开发布对行业控制缺口的观察（例如治理监督、网络安全、外包监督不足）。

Q39：一句话：开曼 VASP 合规最核心是什么?
A：**业务边界清晰 + 客户资产保护（隔离/对账/审批链）+ AML 证据链（识别—处置—报告—留存）+ IT/外包可审计。**

Q40：开始项目的第一份文件建议是什么?
A（交付级写法）：

- 《Perimeter Memo》：回答三件事：
  1. 是否构成 VAS；
  2. 属于 Registration / Licence / Waiver 哪条路；
  3. 是否触及其他金融监管边界（证券/基金/支付等）。
- 并附上"资金路径图、系统控制图、实体/人员职责图"三张图，作为后续所有材料的主索引。

第五部分｜申请包内容（Application Pack）与补件策略

Q41：注册申请的基本流程是什么?
A（交付级写法）：

1. 立项与边界定性（Perimeter Memo）；
2. 建立申请包：公司/股权/治理/业务/AML/IT/外包/财务；
3. 按 CIMA 指定方式递交（含清单编号与附件索引）；
4. 回应补件与监管问询；
5. 批准与缴费（含双段缴付逻辑）；
6. 登记生效与持续监管节奏建立（报告/审计/检查准备）。

Q42：Licence 申请流程与注册有何不同?
A：Licence 申请在"材料深度、系统证据链、控制强度、问询强度"上明显更高：

- 要求你不仅"写制度"，还要能"演示制度如何在系统里运行"；
- 托管/平台的 Rule 对照与证据包通常是成败关键。

Q43：Waiver 申请核心要点?
A（交付级写法）：

1. 证明"你是 Supervised Person"；
2. 证明"你提供的 VAS 在现有监管框架下可被有效监管"；
3. 按 CIMA Waiver Checklist 递交；
4. 明确豁免后仍遵守的 AML/CFT、记录保存与治理要求。

Q44：CIMA 对文件"编号/索引"有要求吗?
A：有强烈偏好。按照 Checklist 编号与附件索引递交，可显著减少补件沟通成本。

Q45：申请包通常包含哪些"六大件"?
A（交付级写法）：

1. **公司与股权**：注册文件、股权结构穿透到 UBO、SoF/SoW；
2. **治理与人员**：董事会架构、关键岗位（CO/MLRO/IT安全等）、职责与时间投入；
3. **业务与产品**：商业模式、目标客户、费用模型、资金路径与风险控制；
4. **AML/CFT**：风险评估、KYC/EDD、制裁筛查、监控、STR、记录保存；
5. **IT与安全**：钱包/密钥、权限矩阵、日志、对账、BCP/DR、渗透测试；
6. **财务与审慎**：财务预测、资本与资源、保险（如适用）、审计安排。

Q46：是否需要业务计划书（BP）？
A：通常需要，并建议 BP 至少覆盖：

- 产品矩阵（功能—监管映射—控制措施）；
- 资金路径（入金—交易—提币—退款—对账）；
- 组织与治理（董事会监督与三道防线）；
- 技术架构（钱包/权限/日志/对账/外包）；
- 风险评估与合规计划（年度节奏）。

Q47：是否需要组织结构图与穿透到 UBO？
A：需要。交付建议：

- 提供"法律结构图 + 控制链条图 + 资金来源说明（SoF/SoW）"；
- 若涉及多层控股或跨境股东，应准备"解释信（Structure Narrative Letter）"。

Q48：董事会层面需要哪些材料？
A（交付级写法）：

- 董事名单与履历、适当人选声明；
- 董事会保留事项清单（上币、外包、重大变更、资产政策等）；
- 会议频率与议程模板；
- KRI 报告模板与整改闭环（CAPA）台账模板。

Q49：关键人员一般包括哪些？
A：常见为：CEO/MD、CO（合规负责人）、MLRO、IT安全/系统负责人、运营负责人、财务负责人；平台/托管还应包含市场监控负责人、钱包安全负责人等（按规模适配）。

Q50：外包安排需要披露吗？
A：需要。且交付建议必须包含：

- 供应商清单（KYC/链上分析/云/托管/客服等）；
- 供应商尽调表；
- 合同关键条款摘要（审计权、监管访问权、事故通报、退出迁移、分包限制）；
- 外包监督计划（季度评估/年度审计/整改）。

Q51：系统说明要写多深？
A：写到"**可审计级别**"，监管问询常聚焦：

- 钱包架构、签名流程、权限矩阵；
- 日志字段（谁、何时、做了什么、审批链）；
- 对账机制（链上余额—内部账—差异处理）；
- 监控规则（AML/反欺诈/市场监控）；
- BCP/DR 与演练证据。

Q52：托管业务最关键的 5 份技术材料？
A：

1. 钱包架构图（热/温/冷、MPC/多签）；
2. 密钥管理政策（生成、存储、轮换、恢复、销毁）；
3. 权限矩阵与审批链（最小权限、双人复核）；
4. 提币流程 SOP（含风控、白名单、冷静期）；
5. 对账 SOP（频率、差异处理、报表样例）。

Q53：交易平台最关键的 5 份材料？
A：

1. 撮合规则与公平性说明；
2. 上币/下架政策与委员会机制；

3. 市场监控框架（反操纵/反刷量）；
4. 客户资产隔离与对账机制；
5. 订单/成交日志字段与导出样例。

Q54：需要提供政策制度清单吗？
A：需要。交付建议最低清单：AML/制裁、客户投诉、信息安全、外包管理、事件响应、利益冲突、市场行为、记录保存、变更管理、员工行为准则等。

Q55：申请费与批准后费用如何缴？
A：CIMA 公告明确"申请费 + 批准后费用"双段逻辑；项目预算必须按两段缴付与持续合规成本做现金流安排。

Q56：Schedule 2 的费用在哪里？
A：在 2025 修订法规（立法网站 PDF）中的 Schedule 2。

Q57：Schedule 1A（Licence 申请表）关键点是什么？
A：Schedule 1A 明确了 Licence 申请信息框架，并与 Registration 表格信息存在衔接关系（尤其当申请主体尚未注册时）。

Q58：可以先递交 Registration 再补 Licence 吗？
A：技术上可行，但若业务已确定为 Custody/VATP，建议以 Licence 标准一次性建设，避免后续"推倒重来"。

Q59：申请被退回/补件最常见原因？
A（交付级写法）：Top 6：

1. 业务边界不清（自称非托管但实质可控）；
2. 治理与关键岗位不匹配（CO/MLRO 经验不足或兼任不合理）；
3. SoF/SoW 解释不足；
4. IT 安全证据链不足（无渗透/无日志/无对账）；
5. 外包合同缺关键条款（无审计权/无监管访问权）；
6. 文件索引混乱，无法按 Checklist 快速核对。

Q60：CIMA 会要求面谈吗？如何准备？
A（交付级写法）：

1. **会**，尤其 Licence（托管/平台）项目，面谈常伴随系统演示与证据核验。
2. **面谈准备三件套**：
   - 《Regulator Q&A Bank（监管问答库）》：按主题列 100+ 常问点；
   - 《System Demo Script（系统演示脚本）》：KYC→监控→提币审批→签名日志→对账→事件响应；
   - 《Evidence Pack（证据包）》：截图、日志样例、报表导出、工单与整改台账。
3. **交付建议**：将面谈输出固化为《Management Presentation Deck（管理层演示稿）》与《Demo Walkthrough（演示走查文档）》用于复用。

第六部分｜时间表、项目管理与补件策略（Timeline & Remediation）

Q61：开曼 VASP 注册/持牌项目通常需要多长时间？如何做可交付时间表？
A（交付级写法）：

1. **时间不应只写"X 个月"**，监管更认可"里程碑驱动"的计划。建议按四段写：
   - **T0–T1（2–4 周）**：边界定性 + 申请包框架（Perimeter Memo、产品映射表、资金路径图、组织架构与岗位清单）。
   - **T1–T2（4–8 周）**：制度与系统证据链补齐（AML、钱包/密钥、权限矩阵、日志字段、对账报表、外包合同关键条款）。
   - **T2–T3（递交后 8–16+ 周）**：监管问询与补件（按轮次管理：Round 1/2/3）。
   - **T3–Go-live（4–8 周）**：银行/通道尽调、上线前演练（事件响应、提币演练、对账演练、STR 演练）。
2. **交付建议**：输出《监管申请甘特图 + 责任矩阵 RACI + 证据清单 Tracker》三件套，确保每次补件都能"可追踪"。

Q62：CIMA 可能提出几轮补件？怎样把补件变成"可控工程"？
A（交付级写法）：

1. 常见 1–3 轮（复杂 Licence 项目可能更多）。关键是你是否"按 Checklist 编号 + 证据链"递交。
2. **补件管理建议（可交付模板）**：

- 建立《Regulator Q Log（监管问题台账）》字段：问题编号、收到日期、责任人、答复要点、附件编号、证据类型（制度/截图/日志/合同/报表）、提交日期、是否关闭。
- 每一轮补件输出《Cover Letter（补件说明信）》：逐条回应、引用附件编号、说明改动点与生效日期。

3. **交付底线**：不要只"口头解释"，要提供**可验证证据**（日志样例、权限截图、工单记录、演练报告）。

Q63：如何避免"自称非托管但被认定托管"的补件风险?
A（交付级写法）：

1. 监管常用的"实质托管"判断：你是否能影响资产转移（签名权/审批权/恢复权/冻结权）。
2. **可交付证据包建议**：
   - 《Key Ownership Statement（密钥所有权声明）》：明确客户自持钥或第三方托管；
   - 《Signing Authority Evidence（签名权证据）》：MPC 分片分布、签名门限、管理员名单；
   - 《Recovery Process（恢复流程）》：说明你是否能单方恢复；
   - 《Admin Privilege Matrix（系统管理员权限矩阵）》：证明你无法绕开客户授权。
3. **最忌讳**：白皮书写"non-custodial"，但 SOP 写"可冻结/可重置/可代提币"——这会直接触发升级审查。

Q64：如何在申请阶段证明"制度可运行"，而不仅是"写得好看"?
A（交付级写法）：

1. 用"三证据链"证明可运行：
   - **流程证据**：SOP + 表单 + 审批链；
   - **系统证据**：权限截图、日志字段、报表导出；
   - **运营证据**：演练记录、培训签到、工单与整改闭环。
2. **交付建议**：每个核心制度（AML、提币、对账、事件响应、外包）都要配"**至少 3 个真实样例**"作为附件。

Q65：若公司计划先小规模试运营（Pilot），如何写"分阶段上线计划"?
A（交付级写法）：

1. 监管最关心：试运营是否引入"监管缺口"。
2. **分阶段上线写法**：
   - Phase A：只开白名单客户（机构/专业客户）、限制币种、限制提币额度；
   - Phase B：增加币种/客户、引入更多监控规则；
   - Phase C：全量功能开放（需证明监控与资源同步扩容）。
3. **交付建议**：输出《Go-live Readiness Checklist（上线就绪清单）》：KRI 门槛、回滚机制、事故升级路径、值班表、冷钱包演练通过标准。

第七部分｜申请材料深度（Deliverable-Grade Pack）

Q66：Licence（托管/平台）申请包最关键的"十个附件"是什么?
A（交付级写法）：

1. Perimeter Memo（边界说明）
2. Business Plan（含产品映射、客户与市场、收入模型）
3. Funds Flow Diagram（资金路径图）
4. Wallet & Key Architecture（钱包与密钥架构）
5. Access Control Matrix（权限矩阵）
6. Withdrawal SOP（提币审批 SOP + 表单）
7. Reconciliation SOP（对账 SOP + 报表样例）
8. AML/CFT Program（风险评估 + KYC/EDD + 监控 + STR）
9. Outsourcing Register & Contracts Summary（外包清单 + 合同关键条款摘要）
10. Incident Response & BCP/DR（事故响应 + 灾备演练记录）

交付提示：以上每一项建议写成"可直接作为制度章节"的格式，并附证据样例。

Q67：Schedule 1A（Licence 表）填报最常被问的点有哪些?
A（交付级写法）：

1. 业务范围描述是否与实际系统功能一致（最常见矛盾来源）。
2. 客户资产/私钥控制描述是否清晰（托管边界）。
3. 费用模型与资金路径是否闭环（谁收费、收哪、如何对账）。
4. 外包与第三方依赖是否充分披露（云、KYC、链上分析、托管技术）。
5. 关键人员能力与时间投入是否可信（兼职过多/无备份会被追问）。

交付建议：建立《Form–BP–Policy 三表一致性检查》：表格字段 → BP 段落 → 制度条款编号，避免自相矛盾。

Q68：股权结构穿透（UBO/SoF/SoW）要写到什么程度?
A（交付级写法）：

1. 建议穿透到自然人最终受益人（UBO），并提供：身份证明、住址证明、简历、资金来源与财富来源说明。
2. **SoF/SoW 写法**：
   - SoW：财富形成路径（职业/公司分红/股权出售/投资收益）；
   - SoF：本次注资/营运资金具体来源（哪家银行、哪笔资金、哪份合同/分红决议）。
3. **交付建议**：输出《UBO Due Diligence Pack》：证件+声明+银行流水摘要+解释信（避免"只有一句话"）。

Q69：关键岗位（CO/MLRO/IT安全负责人）需要哪些"可递交证明"?
A（交付级写法）：

1. 履历（CV）+ 资格证书（如 AML/合规/信息安全）
2. 任命书（Appointment Letter）与职责说明（Job Description）
3. 时间投入声明（Time Commitment）
4. 独立性声明（尤其 MLRO）
5. 备份安排（Deputy/Alternate）

交付建议：形成《Key Persons Pack》统一递交，避免分散导致补件。

Q70：董事会治理（Board Governance）应该准备哪些"硬材料"?
A（交付级写法）：

1. 董事会章程/议事规则（Terms of Reference）
2. 保留事项清单（Matters Reserved）
3. 董事会年度议程（Annual Board Calendar）
4. 风险委员会/合规委员会机制（如适用）
5. 会议纪要模板 + KRI 报告模板 + 整改闭环台账模板

交付建议：把"治理"写成可审计的"输入—决策—监督—整改"闭环。

第八部分｜系统与安全（IT, Cybersecurity, Evidence Chain）

Q71：监管为什么强调"日志（Logs）"，你需要提供哪些日志字段样例?
A（交付级写法）：

1. 因为日志是"可审计证据链"的核心：能证明谁批准了提币、谁改了白名单、谁调整了风控阈值。
2. 建议至少准备 4 类日志样例（导出 CSV/截图均可）：
   - 身份/KYC 操作日志（审核、拒绝、复核）
   - 权限变更日志（角色、管理员、临时授权）
   - 钱包/提币日志（发起、审批、签名、广播、TXID）
   - 风控/监控日志（命中规则、处置动作、升级/关闭工单）
3. **交付建议**：附《Log Retention Policy（日志留存政策）》：留存年限、不可篡改措施、访问控制、审计导出流程。

Q72：对账（Reconciliation）要做到什么频率与粒度?
A（交付级写法）：

1. 监管关注点：链上余额、内部账、客户余额三者是否一致；差异如何发现与处理。
2. 建议写"三层对账"：
    - 日内/每日：热钱包与内部账；
    - 每周：冷钱包与资产总账；
    - 每月：客户余额、费用收入、通道结算全量核对。
3. **交付建议**：提供"差异处理"工单样例：差异原因分类、调查步骤、修正审批、复盘与预防措施。

Q73：钱包架构（Hot/Warm/Cold）在递交材料中怎么写才"像监管文件"？
A（交付级写法）：

1. 画一张 Wallet Architecture Diagram，标注：用途、额度上限、签名门限、人员角色、审批链。
2. 用表格列：钱包类型、资产支持、触发转移条件、风控阈值、是否自动化、是否人工复核。
3. 写"例外处理"：紧急提币、系统故障、密钥疑似泄露时的冻结与迁移流程。

交付建议：附《Cold Wallet Ceremony（冷钱包操作仪式）》：双人复核、录像、现场签到、封存与审计。

Q74：MPC 托管如何解释"控制权"？
A（交付级写法）：

1. 监管会问：分片在谁手里？门限是多少？是否存在"你能单方签名"的情况？
2. 交付写法：
    - 分片分布：公司/第三方/硬件/地理位置；
    - 门限策略：m-of-n，审批前置条件；
    - 恢复机制：谁能触发恢复、需要哪些审批。
3. 附证据：MPC 配置截图/供应商证明/权限矩阵。

Q75：灾备（BCP/DR）不是口号，怎样提供"可递交演练证据"？
A（交付级写法）：

1. 递交《BCP/DR Plan》之外，必须提供：
    - 演练计划（Drill Plan）
    - 演练记录（Drill Report）：场景、参与人、步骤、耗时、结果
    - 整改闭环（CAPA）：问题清单、责任人、完成日期
2. 典型演练场景：云故障、撮合引擎宕机、钱包服务不可用、密钥疑似泄露、KYC 供应商故障。
3. 交付建议：把演练频率写入董事会年度议程与 KRI。

Q76：渗透测试/漏洞管理需要提供哪些证据？
A（交付级写法）：

1. 渗透测试报告摘要（可脱敏）+ 关键漏洞修复证明（工单/补丁记录）。
2. 漏洞管理 SOP：分级（Critical/High/Medium/Low）、修复时限、复测机制。
3. 交付建议：附《Secure SDLC（安全开发生命周期）》：代码审计、CI/CD 权限、密钥管理、依赖库扫描。

Q77：平台类（VATP）市场监控要写哪些规则？
A（交付级写法）：

1. 异常交易监控：刷量、对倒、自成交、异常价差、异常撤单。
2. 市场操纵风险：拉盘砸盘、假消息联动、异常集中度。
3. 处置机制：预警—限制—暂停—调查—报告—复盘。
4. 交付建议：提供《Surveillance Rules Library（规则库）》样例：每条规则含阈值、触发条件、误报处理、升级路径。

Q78：交易规则披露需要写到什么程度？
A（交付级写法）：

1. 撮合优先级（价格优先/时间优先）、最小交易单位、手续费结构、撮合失败处理。
2. 暂停交易/熔断/下架标准与流程。
3. 订单类型与风险提示（市价单滑点、限价单不成交风险）。

4. 交付建议：形成《Trading Rulebook（交易规则手册）》作为客户协议附件之一。

Q79：客户资产隔离（Segregation）怎么写才"能过监管问询"？
A（交付级写法）：

1. 分三层说明：
    - 法律层：客户资产不应被视为公司资产（写入条款）；
    - 账务层：客户余额与公司自营/费用收入分账；
    - 钱包层：客户资产与公司运营钱包分离（或以清晰归集规则+对账补强）。
2. 交付建议：附《Client Asset Policy（客户资产政策）》+ "钱包地址/子账户结构示意图（可脱敏）"。

Q80：是否需要保险（Insurance）？
A（交付级写法）：

1. 视业务风险与监管期望而定；托管/平台通常更容易被问及：盗窃、内部舞弊、系统事故、职业责任等保障。
2. 若尚未投保，可提交：保险市场询价记录、计划购买的险种范围、预计保额与时间表。
3. 交付建议：把保险写入《Risk Treatment Plan（风险处置计划）》中，不要单独一段空话。

第九部分｜AML/CFT（可运行证据链）

Q81：AML/CFT 体系至少应包含哪 8 个模块？
A（交付级写法）：

1. 企业风险评估（BRA）
2. 客户风险评估（CRA）与分层 KYC
3. 制裁与 PEP 筛查
4. 交易监控（规则库 + 场景）
5. EDD（高风险客户/高风险地区/复杂结构）
6. STR/SAR 决策与提交流程
7. 记录保存与审计追踪
8. 培训与三道防线（业务—合规—审计）

    交付建议：每个模块至少附 1 个"运行样例"。

Q82：开曼 AML 里"Travel Rule"一定要做吗？
A（交付级写法）：

1. 是否"必须"取决于你提供的服务类型与适用要求（以及对手方、通道、行业实践）。
2. 即便未强制，监管与银行尽调通常会问：你是否具备"传递/接收必要信息、识别缺失信息、拦截高风险转账"的能力。
3. 交付建议：准备《Travel Rule Readiness Note（可执行说明）》：适用范围、字段、阈值、供应商方案、处置 SOP。

Q83：KYC 需要哪些"可递交表单"？
A（交付级写法）：

1. 自然人客户开户表（含风险问题与声明）
2. 法人客户尽调表（股权穿透、控制人、受益人）
3. EDD 问卷（高风险增强尽调）
4. SoF/SoW 解释信模板
5. 受制裁/PEP 命中处置表

    交付建议：把表单"字段—证据—系统录入—复核签名"做成闭环。

Q84：如何写"同名出入金（Same-name）政策"才能更容易通过银行与监管？
A（交付级写法）：

1. 原则：客户入金账户名需与平台开户名一致；不一致默认拒绝或触发 EDD。
2. 例外：机构集团资金归集、受监管托管账户、受信托安排等——必须列明例外条件、审批层级、留痕证据。

3. 交付建议：附《Same-name Exception Approval Form（例外审批表）》与"例外名册"。

Q85：OTC/法币通道的高风险点要如何在 AML 风险评估中体现？
A（交付级写法）：

1. 高风险点：第三方代付、现金/等值工具、快进快出、异常拆分、跨境高风险地区。
2. 风险缓释：限额、冷静期、增强监控、要求来源证明、对手方白名单、黑名单与拒客机制。
3. 交付建议：把这些落到"监控规则库"与"处置 SOP"，而不是只写在评估里。

Q86：STR/SAR 决策链怎么写才"像可运行机制"？
A（交付级写法）：

1. 三段式：触发（监控命中/人工发现）→ 调查（收集证据、问询、链上分析）→ 决策（提交/不提交/持续观察）。
2. 明确角色：调查员、MLRO、最终批准人；明确时限与升级路径。
3. 交付建议：附《STR Decision Memo Template（决策备忘录模板）》+ 2 个脱敏样例。

Q87：记录保存要写几年？要保存什么？
A（交付级写法）：

1. 通常建议按开曼 AML 监管期望设定较长留存（例如 5 年及以上，具体按适用规则与业务性质确定）。
2. 保存范围：客户资料、交易记录、监控命中、调查记录、审批链、对账报表、日志导出、培训记录。
3. 交付建议：形成《Record Retention Schedule（记录保存一览表）》：类别—留存年限—存储位置—访问权限—销毁审批。

Q88：如何证明"培训不是走过场"？
A（交付级写法）：

1. 培训计划（年度）+ 课件 + 签到 + 测验 + 通过率 + 补训记录。
2. 关键岗位（前线、客服、审核、风控、IT 管理员）要有岗位化课纲。
3. 交付建议：附《Training Matrix（岗位培训矩阵）》与至少一次演练（STR 演练/事故演练）报告。

Q89：制裁筛查要筛谁、筛什么、多久筛一次？
A（交付级写法）：

1. 筛查对象：客户、受益人、控制人、关键授权人、对手方（如适用）。
2. 筛查事件：开户、重大变更、定期复核、交易触发（大额/高风险/异常）。
3. 交付建议：附《Sanctions & PEP SOP》+ 命中处置表单 + 供应商 SLA。

Q90：链上分析（Blockchain Analytics）是不是必需？
A（交付级写法）：

1. 非必然，但托管/平台类通常会被问到"你如何识别涉诈、混币、暗网、被盗资金"。
2. 若你不使用链上分析工具，需要提供替代控制：风险评分、对手方白名单、人工调查能力与升级机制。
3. 交付建议：附《On-chain Investigation SOP（链上调查 SOP）》与样例报告。

第十部分｜外包治理（Outsourcing & Third-Party Risk）

Q91：外包清单（Outsourcing Register）要包含哪些字段？
A（交付级写法）：

- 供应商名称、服务类型、数据接触级别、关键性等级、地域、分包情况、合同期限、退出计划、审计权条款、事故通报时限、负责人。

  交付建议：外包清单要"可用于董事会季度审阅"。

Q92：外包合同最关键的 8 条条款是什么？
A（交付级写法）：

1. 监管访问权/配合检查条款
2. 审计权（含第三方审计）
3. 数据安全与保密

4. 事故通报时限与协作
5. SLA 与可用性指标
6. 分包限制与事前批准
7. 退出与迁移（Exit Plan）
8. 责任与赔偿/保险（如适用）

交付建议：递交"合同摘要"+"条款对照表"，即便合同保密也可脱敏提交。

Q93：云服务（Cloud）在申请包里怎么解释？
A（交付级写法）：

1. 说明数据分类（敏感/非敏感）、加密措施、访问控制、区域与备份策略。
2. 给出"云权限矩阵"（谁能开实例、谁能读日志、谁能导出数据库）。
3. 交付建议：附《Cloud Security Baseline》与"最小权限"截图证据。

Q94：KYC/制裁筛查供应商外包，监管会担心什么？
A（交付级写法）：

1. 命中误判/漏判风险；2) 数据泄露；3) 服务中断；4) 供应商模型不透明。
   交付建议：提交供应商尽调（资质、审计报告、SLA、事故历史）+ 你的"人工复核与兜底机制"。

Q95：托管技术外包（钱包/MPC/密钥管理），监管最关注什么？
A（交付级写法）：

1. 你是否仍"控制关键风险决策"（例如审批链、门限、权限授予）。
2. 供应商是否能绕过你单方操作客户资产。
3. 你是否拥有可迁移与退出能力（避免供应商锁定）。

交付建议：提供《Key Control Governance（关键控制治理）》：谁能变更门限、谁能启用紧急模式、如何审计。

Q96：外包退出计划（Exit Plan）要写多细？
A（交付级写法）：

1. 写到"可执行"：迁移步骤、时间窗口、数据导出格式、责任人、验收标准、回滚方案。
2. 明确触发条件：供应商违约、重大事故、监管要求、成本不可控。
3. 交付建议：附《Exit Drill（退出演练）》计划（即便尚未实施，也写出演练安排）。

第十一部分｜客户文件与披露（Client Terms, Disclosures, Complaints）

Q97：客户协议（Terms）至少要包含哪些合规条款？
A（交付级写法）：

1. 服务范围与限制（你做什么、不做什么）
2. 费用与收费方式
3. 风险披露（价格波动、技术风险、链上不可逆）
4. 客户资产政策（隔离、托管方式、提币规则）
5. KYC/制裁与信息提供义务
6. 冻结/限制/终止条款（涉嫌违法、制裁命中、欺诈风险）
7. 投诉处理与争议解决
8. 数据与隐私、外包披露（如适用）

交付建议：准备《Disclosure Schedule（披露附表）》把关键风险用清单呈现。

Q98：风险披露怎么写才"对监管与银行都有用"？
A（交付级写法）：

1. 不写空话，写"可量化/可场景化"风险：如滑点、极端波动、链上拥堵导致延迟、网络攻击导致暂停。
2. 写清"平台可以做什么处置"（暂停交易、限制提币、回滚交易？通常链上不可回滚）。

3. 交付建议：附《Incident Customer Notice Template（事故客户通知模板）》。

Q99：投诉处理机制要包含哪些步骤？
A（交付级写法）：

1. 受理（渠道、登记）→ 分类分级（交易/提币/账户/欺诈）→ 调查（证据收集、系统日志）→ 回复（时限、升级）→ 结案与复盘（改进措施）。
2. 交付建议：建立《Complaint Register（投诉台账）》+ 每月复盘报告给管理层。

Q100：平台暂停交易/下架资产的规则需要提前披露吗？
A（交付级写法）：

1. 建议披露。监管与客户纠纷的高频点正是"为何暂停、为何下架、是否公平"。
2. 交付建议：写《Suspension & Delisting Policy》：触发条件、委员会机制、客户通知、资产处置与时间表。

第十二部分｜持续监管"起步包"（Ongoing Compliance Starter Pack）

Q101：获批后第一天应该建立哪些"持续监管节奏"？
A（交付级写法）：

1. 月度合规例会：KRI、监控命中、投诉、重大事件、外包评估。
2. 季度董事会汇报：风险地图、整改闭环、审计/测试结果。
3. 年度计划：培训、BCP 演练、渗透测试、外包审计、政策回顾。

   交付建议：输出《Compliance Calendar（合规日历）》可直接执行。

Q102：KRI（关键风险指标）建议有哪些？
A（交付级写法）：

- KYC：拒绝率、复核率、EDD 占比、超时未完成 KYC 数量
- 交易监控：命中率、误报率、STR 比例、平均处置时长
- 钱包：提币失败率、人工审批比例、异常提币拦截数
- 安全：高危漏洞数量、修复时长、权限变更次数
- 外包：SLA 违约次数、事故通报延迟、审计整改完成率

  交付建议：把 KRI 阈值与升级路径写清楚（到什么数必须上报董事会）。

Q103：内部审计（Internal Audit）是否必须？
A（交付级写法）：

1. 视规模与监管期望而定，但高风险平台/托管通常需要独立审计或等效的独立评估机制。
2. 若没有内部审计部门，可采用外部第三方年度评估 + 管理层整改闭环。
3. 交付建议：出《Annual Assurance Plan（年度保证计划）》列明审计主题与频率。

Q104：政策制度多久复核一次？
A（交付级写法）：

1. 建议至少年度复核；发生重大变更（新产品、新国家、新通道、重大事故）应即时复核。
2. 交付建议：每份制度页脚写"版本号/生效日期/下次复核日期/审批人"。

Q105：重大事件（Material Change/Incident）如何界定与上报？
A（交付级写法）：

1. 典型重大事件：重大安全事件、客户资产损失、系统长时间中断、重大合规违规、关键外包故障、关键人员离任。
2. 交付建议：制定《Regulatory Notification SOP（监管通报 SOP）》：何时、向谁、以何形式、提供哪些信息、后续更新频率。

Q106：关键人员离任（尤其 MLRO/安全负责人）需要如何处置？
A（交付级写法）：

1. 立即启动"替补机制"（Deputy/Interim 任命）

2. 通知管理层与董事会，评估对风险与监管的影响
3. 如需对监管通报，按通报 SOP 执行
4. 更新权限矩阵、系统账户、签名权与审批链

交付建议：准备《Key Person Change Pack（关键人员变更包）》：任命文件、交接清单、权限回收证明。

Q107：新增币种/新增产品功能是否属于"重大变更"?
A（交付级写法）：

1. 对平台/托管而言通常属于高关注变更（风险画像变化、监控规则变化、技术变化）。
2. 交付建议：建立《New Product Approval SOP》：风险评估、合规评审、IT 安全评审、董事会/委员会批准、上线后监控。

Q108：如何做"上币尽调（Listing DD）"?
A（交付级写法）：

1. 项目背景：团队、法律结构、代币分配、治理机制。
2. 风险：制裁/违法、洗钱风险、技术漏洞、集中度与操纵风险。
3. 监控：链上风险评分、交易行为监控规则。
4. 交付建议：输出《Listing Committee Pack》+《Token Risk Rating Model（代币风险评级模型）》。

Q109：客户分级（Retail/Professional/Institutional）对合规有什么价值?
A（交付级写法）：

1. 决定 KYC 深度、限额、产品可用性、风险披露强度。
2. 交付建议：用《Customer Tier Policy》写清：分级条件、证据要求、复核周期、降级机制。

Q110：如何建立"拒客与黑名单机制"?
A（交付级写法）：

1. 拒客触发：制裁命中、虚假信息、拒不提供资料、涉嫌欺诈、异常资金来源。
2. 黑名单：账户/设备/地址/链上地址/收款账户多维度。
3. 交付建议：建立《Refusal & Blacklist SOP》+ 《Refusal Register》并能导出审计。

第十三部分｜银行与通道尽调（Banking & Counterparty DD）

Q111：为何银行尽调往往比监管申请更难?
A（交付级写法）：

1. 银行承担直接洗钱风险与声誉风险，审核更保守。
2. 银行会看：你的客户结构、资金路径、同名出入金、监控规则库、事故历史、外包控制。
3. 交付建议：准备《Bank DD Pack》：监管状态、制度摘要、资金路径、KRI 样例、审计/测试摘要。

Q112：银行最常问的 12 个问题是什么?
A（交付级写法）：

1. 你到底做什么业务？是否托管？是否交易平台?
2. 客户是谁？来自哪些国家？是否零售?
3. 资金怎么进出？是否第三方代付?
4. 是否同名出入金？例外怎么管?
5. 监控规则有哪些？命中如何处置?
6. STR 怎么做？谁批准?
7. 是否支持隐私币/混币？政策如何?
8. 外包哪些？供应商是谁？审计权条款?
9. 钱包与密钥怎么管？是否多签/MPC?
10. 事故响应与赔付机制?
11. 审计/渗透测试做过吗?
12. 预计月交易量与资金规模?

交付建议：把这 12 问做成《Bank Q&A》可直接用于开户面谈。

Q113：如何把"监管合规包"改造成"银行可读版本"？
A（交付级写法）：

1. 监管版偏全量细节；银行版偏"风险可控与证据摘要"。
2. 银行版建议 30–50 页：
   - 业务概览 5 页
   - 资金路径图 2 页
   - AML 框架摘要 10 页
   - 规则库样例 5 页
   - 钱包/对账/权限摘要 10 页
   - 外包与审计摘要 5 页
3. 交付建议：附"证据索引"，银行若要深看可快速定位。

Q114：支付通道/OTC 对手方尽调应包含哪些内容？
A（交付级写法）：

1. 对手方牌照/注册状态与业务范围
2. AML 体系与 STR 机制
3. 资金结算周期、退款/拒付机制
4. 数据共享与审计权
5. 事故通报与联合调查机制

交付建议：建立《Counterparty Due Diligence Checklist》。

Q115：为何"资金路径图（Funds Flow Diagram）"是监管与银行共同的关键？
A（交付级写法）：
因为它能一眼看出：谁收款、谁持币、谁结算、谁对账、哪里可能形成资金池与混同风险。

交付建议：资金路径图要包含：账户名、币种/法币、触发条件、对账点、风险控制点（KYC/限额/审批）。

第十四部分｜经营范围边界与灰区处置（Perimeter Edge Cases）

Q116：做"仅撮合，不代结算"仍可能被认定 VATP 吗？
A（交付级写法）：

1. 若你运营"订单簿/撮合引擎/交易规则"，即便结算由第三方完成，也可能被视为平台运营。
2. 交付建议：若坚持仅做撮合，应提供证据：
   - 你不控制撮合规则（由第三方平台控制）或你只是"介绍撮合"；
   - 成交、结算、资产控制完全不在你手里；
   - 你不提供"交易场所功能"。

Q117：做"转账/支付"类服务一定属于 VASP 吗？
A（交付级写法）：

1. 若你代表客户转移虚拟资产（transfer），通常属于 VAS。
2. 若只是提供链上工具、客户自发起且你无控制权，可能不构成。
3. 交付建议：用"控制权测试"逐条论证，并形成《Transfer Perimeter Note》。

Q118：是否可以在对外宣传中写"受 CIMA 监管/持牌"？
A（交付级写法）：

1. 必须谨慎，避免误导。只有在确有对应的注册/许可状态时才可使用相应表述，并应准确写明类别（Registered / Licensed / Waiver）。
2. 交付建议：制定《Marketing & Communications Policy》：哪些措辞可用、哪些不可用、审批流程、留痕。

Q119：如果业务模式变化（例如从经纪升级到托管/平台），应该怎么做？
A（交付级写法）：

1. 先内部启动"重大变更评估"：是否触发 Licence；
2. 更新 Perimeter Memo、风险评估、制度与系统；
3. 按通报 SOP 处理监管沟通（如适用）；
4. 做上线前演练与培训。

交付建议：建立《Change Management SOP》与"变更台账"。

Q120：如果监管/银行问你"你凭什么说自己是 non-custodial？"最佳回答结构是什么？
A（交付级写法）：
用"**三段式证据回答**"：

1. **制度声明**：客户资产控制权归客户，平台不持钥/不掌握单方转移能力（引用制度条款编号）。
2. **系统证据**：展示 MPC/多签门限、权限矩阵、提币审批链、管理员无法绕过客户授权的截图/日志。
3. **运营证据**：展示一次提币流程的完整日志链（发起→审批→签名→广播→对账→归档），证明过程可审计、不可单方操控。

第十五部分｜费用预算与成本模型（CapEx / OpEx / Fee Map）

Q121：开曼 VASP 注册/持牌的费用与预算应该如何"对外可交付"呈现？
A（交付级写法）：

1. 建议拆成"三层费用地图"：
   - **监管法定费用**：按法规 Schedule 2（对应 registration/licence/waiver 等类别），并注明"**不可退**/触发时点"。（Phase 2 后 fees 以 Schedule 2 列示并更新。）
   - **专业服务费**：法律顾问、合规顾问、审计/独立评估、渗透测试、外包尽调等。
   - **运营持续费用**：合规人力、KYC/制裁筛查、链上分析、云资源、安全监控、值班与培训。
2. **交付建议**：输出《预算总表 + 分项说明 + 假设条件（Assumptions）》，每一项都写清：计费方式（一次性/按月/按量）、成本驱动因素（客户量/交易量/币种数/国家数）。

Q122：监管费用（CIMA fees）如何在文件中写得既准确又不踩雷？
A：

1. 监管费用应以"**法规 Schedule 2 / CIMA 公告口径**"为准，文件里写：
   - "政府收费以递交当日 CIMA 最新 Schedule 2/REEFS 显示为准"；
   - 并在预算表中列"区间/占位符"，避免写死被更新。
2. **交付建议**：在《费用说明》里引用"Phase 2 修订已将费用纳入 Schedule 2"。

Q123：CapEx（上线前一次性）通常包含哪些项目？
A：

- 制度文件与申请包编制（BP、Perimeter Memo、Funds Flow、Policies）
- 系统合规改造：权限分层、日志字段、报表对账、提币审批链
- 安全建设：渗透测试、漏洞修复、密钥管理（HSM/MPC）
- 外包合同整改：审计权、事故通报、退出计划（Exit Plan）
- 上线演练：BCP/DR、事故响应、STR 演练与证据归档

交付建议：CapEx 要按"可交付成果"列（Deliverables），让客户知道钱花在哪、交付拿到什么。

Q124：OpEx（持续费用）通常包含哪些项目？
A：

- 合规团队（CO/MLRO/风控/调查）与值班安排
- KYC/制裁筛查按量费用
- 链上分析工具（如使用）
- 云与安全运营（SIEM、告警、日志留存）
- 定期审计/独立评估与年度培训

- 外包供应商续约与 SLA 管理

  交付建议：OpEx 用"业务量驱动模型"表达（客户数、月交易笔数、国家数、币种数）。

Q125：如何把"合规成本"写成董事会能决策的格式？
A：

1. 建议输出《合规资源与预算论证》：
   - 风险画像（custody/VATP/OTC）→ 对应控制措施 → 对应成本与人力。
2. 给董事会的"决策表述"：
   - "若要开放零售/增加国家/增加币种/开杠杆，则 OpEx 需增加 X 类投入（监控规则、EDD、人手、审计频率）"。
3. **交付建议**：把成本与 KRI 阈值绑定（比如误报率上升→增加调查人手）。

第十六部分｜Phase 2（2025-04-01）Licence 强制点与路径选择

Q126：Phase 2 生效后，哪些业务必须从 registration 走向 licence？
A：

1. CIMA 已公告：自 **2025-04-01** 起，**提供虚拟资产托管（custody）与虚拟资产交易平台（VATP）服务**的 VASP 必须取得 licence。
2. 交付写法：在《Perimeter Memo》里把你的业务功能逐条映射到 custody / VATP / 其他 VAS，明确"为什么要 licence / 为什么仍可 registration"。

Q127：如果我已是 Registered Person，申请 licence 后会发生什么？
A：

- CIMA FAQ 明确：若 licence 获批，**现有 VASP registration 会被取消**（被 licence 替代）。

  交付建议：在项目计划中预留"注册转许可"的窗口期与对外披露措辞，避免宣传口径混乱。

Q128：Waiver（豁免）适用对象是谁？
A：

- CIMA FAQ 口径：仅 **Supervised Persons**（已在其他监管法下受 CIMA 许可/注册，但不在 VASP Act 下许可/注册）可申请 waiver。

  交付建议：若考虑 waiver，必须先证明"你已受其他监管法监管 + VASP 活动只是附带/例外"。

Q129：Licence 申请表为什么强调 Schedule 1A？
A：

- 2025 修订法规明确：**section 8(1) licence 申请应使用 Schedule 1A 的表格**，并且 fees 参照 Schedule 2。

  交付建议：建立《Schedule 1A 字段—BP 段落—制度条款》三表一致性检查，避免"表格写 A、BP 写 B、制度写 C"。

Q130：CIMA 是否提供"Licensing & Waiver Checklist"？有什么价值？
A：

- CIMA 发布了 **VASP Licensing and Waiver Checklist（New Applicants）**，并指出只有在收到所列必需文件后才开始处理许可申请。

  交付建议：把该 Checklist 转成你内部的"证据链 Tracker"，每一项都要有附件编号、责任人、完成日期与版本号。

第十七部分｜"Rule / Guidance"合规映射（Rule Mapping）

Q131：为什么说"Rule for Virtual Asset Custodians and Trading Platforms"是 licence 项目必读？
A：

1. 该 Rule 明确适用于 **虚拟资产托管人与交易平台**，用于说明持续监管义务与最低要求。
2. 交付建议：将 Rule 的关键条款映射到你的制度章节：
   - Custody：资产隔离、提币控制、对账、私钥治理、记录保存
   - VATP：市场监控、交易规则披露、冲突管理、客户资产与平台自营边界

Q132：如何做"Rule Mapping 表（可递交）"?
A（交付级写法）：

- 列三列即可：
    1. Rule 条款编号/主题
    2. 你的制度条款编号（Policy/SOP）
    3. 证据附件编号（截图/日志/报表/合同）

  交付建议：不要做成空表；每条必须能落到"证据链"。

Q133：托管类最常被追问的 6 个控制点是什么?
A：

1. 私钥控制权与签名门限（谁能签、谁能改门限、谁能恢复）
2. 提币审批链与白名单机制
3. 冷/热钱包额度与迁移规则
4. 对账频率与差异处理闭环
5. 资产隔离（法律、账务、钱包层）
6. 事故响应（密钥疑似泄露、被盗、内部舞弊）

   交付建议：每个点至少给 1 个"运行样例"（日志导出/工单）。

Q134：VATP 平台类最常被追问的 6 个控制点是什么?
A：

1. 市场监控规则库（对倒/刷量/自成交/异常撤单）
2. 交易规则披露与暂停/下架流程
3. 利益冲突（平台自营/做市/上币利益）
4. 客户资产与平台资产边界
5. 上币尽调（Token risk rating）与持续监测
6. 重大事件通报与客户通知机制

   交付建议：把这些写成《Trading Rulebook + Surveillance Policy + Listing Policy》三件套。

第十八部分｜监管面谈高频"刁钻问题库"第一批（Q135–Q165）

说明：以下问题建议你在申请前用"**三段式**"准备：**制度条款** → **系统证据** → **运营样例**。

Q135：你们到底是否托管？请用一句话定义并给证据。
A：一句话先定性（是否持钥/是否能影响转移），随后立即给"签名门限/权限矩阵/提币日志链"三证据。

Q136：谁能改提币限额？改一次需要几级审批?
A：写清：参数归属（风控/合规/董事会）、审批链、变更日志字段与复核频率。

Q137：如果 MLRO 不在，STR 谁批准？多久必须做出决定?
A：写清：Deputy MLRO 任命、升级路径、时限（内部 SLA）、决策备忘录模板。

Q138：你们如何避免内部人员盗币?
A：最小权限、双人复核、分权（MPC 分片/多签）、操作录像/签到、异常告警与审计导出。

Q139：你们如何处理"混币/暗网/涉诈地址"入金?
A：链上风险评分（或替代控制）、冻结/限制策略、EDD、STR 决策链与客户沟通模板。

Q140：你们是否允许第三方代付/代充?
A：原则禁止；例外条件、审批表、证据要求、监控规则与黑名单机制。

Q141：资金路径中哪里会形成资金池？如何证明不混同?
A：资金路径图 + 对账报表样例 + 分账规则（客户/公司/费用）+ 差异处理工单。

Q142：你们的对账发现过差异吗？差异如何关闭?
A：给 1 个脱敏样例：差异原因、调查步骤、审批与复盘（CAPA）。

Q143：你们如何决定上币？谁在上币委员会?
A：Listing Committee TOR、风险评级模型、利益冲突声明、持续监测与下架阈值。

Q144：你们如何处理客户投诉？是否能提供月度统计与复盘？
A：投诉台账 + SLA + 分级处置 + 月度复盘报告模板。

Q145：外包供应商宕机怎么办？你们能否切换？
A：Exit Plan、替代供应商策略、演练计划与"降级运行模式"。

Q146：你们的日志能否做到不可篡改？谁能导出日志？
A：WORM/权限限制/导出审批/审计留痕；导出样例与访问控制矩阵。

Q147：你们是否有任何自营交易/做市？如何控制冲突？
A：冲突政策、隔离墙、披露、监控与董事会监督。

Q148：你们如何界定重大事件？多久通知监管/客户？
A：事件分级矩阵、通报 SOP、客户通知模板、演练记录。

Q149：你们如何证明制度是"有效"而非"文件化"？
A：三证据链：制度条款编号 + 系统截图/日志字段 + 运营样例（工单/演练/培训）。

Q150：你们如何确保宣传不误导（licensed/registered/waiver）？
A：营销合规政策、审批流程、措辞白名单、发布留档。

Q151：你们如何处理新增国家/新增客户类型？
A：新市场评估 SOP、国家风险评级、产品可用性分级、KYC/EDD 升级策略。

Q152：你们如何设置交易监控规则？误报率如何管理？
A：规则库 + 阈值治理 + 误报复盘 + KRI（误报率、处置时长、STR 比例）。

Q153：你们如何限制单一客户多账户/关联账户？
A：设备指纹/受益人穿透/关联规则/黑名单；触发 EDD 与限制策略。

Q154：你们如何确保董事会"看得懂、管得住"？
A：董事会季度包：KRI、事故、外包、审计、整改闭环；年度议程与保留事项。

Q155：你们如何证明"客户资产隔离"？
A：条款（法律）+ 分账（账务）+ 钱包结构（技术）+ 对账证据（运营）。

Q156：你们是否允许匿名币/隐私币？
A：明确政策（通常倾向限制/禁止），并提供监控与拒绝策略。

Q157：你们如何处理高波动导致的强制平仓/爆仓风险（若有衍生品）？
A：若不提供衍生品应明确"不提供"；若提供需额外风险管理、披露与监控机制。

Q158：你们如何处理冻结/扣押/执法协作请求？
A：LE request SOP、合法性审查、最小披露、审计留痕与客户通知规则（如适用）。

Q159：你们如何保存记录？保存多久？
A：记录保存表（类别/年限/位置/权限/销毁审批）+ 导出演示。

Q160：你们如何处理员工权限离职回收？
A：Joiner-Mover-Leaver 流程、即时禁用、复核与审计。

Q161：你们如何管理 API 权限与第三方接入？
A：API key 生命周期、速率限制、IP 白名单、日志与异常检测、紧急吊销。

Q162：你们的客户资金是否经过银行？银行如何尽调你们？
A：Bank DD Pack（制度摘要、资金路径、监控规则、审计/测试摘要）。

Q163：你们如何验证资金来源（SoF）？
A：SoF 分层触发、证据清单、拒绝与例外审批、留档与复核周期。

Q164：你们如何处理关联方交易（集团内资金/自有账户）？
A：关联方政策、披露、审批、对账与审计。

Q165：如果 licence 获批，你们对外怎么表述监管状态？
A：严格按"licensed under VASP Act（具体类别）"；并与 FAQ 口径一致处理注册取消等事项。

第十九部分｜申请包一致性与"可交付核查"方法（Q166–Q180）

Q166：如何做"申请包一致性检查"（最容易救命的一步）？
A：建立三张表：

1. Form（Schedule 1A/REEFS）字段表
2. BP（Business Plan）段落索引
3. Policy/SOP 条款索引
   要求：任何一个关键点（托管/提币/对账/监控/外包）三表必须一致，且能指向证据附件。

Q167：哪些内容一旦前后矛盾，最容易触发补件甚至"升级审查"？
A：

- 是否托管、是否可冻结、是否可代提币
- 资金路径（谁收款、谁结算）
- 客户类型（零售/机构）与 KYC 深度
- 外包范围与审计权
- 权限矩阵与实际系统截图

交付建议：做"矛盾点自检清单"并作为内部 QA。

Q168：Licence 申请中"最该先写好"的三封信是什么？
A：

1. Cover Letter（申请说明信：业务定性+附件索引）
2. Perimeter Memo（监管边界说明：为何 licence/为何不 licence）
3. Governance Statement（治理与三道防线声明）
   并在每封信里引用附件编号与版本号。

Q169：Checklist（CIMA Licensing & Waiver Checklist）如何转为你的内部交付流程？
A：

- 把 Checklist 每一项变成"任务卡"：产出物、负责人、证据、审核人、完成标准。
  CIMA 明确：收齐所需文件才开始处理许可申请。

Q170：如何准备"监管问询 Round 1"预案？
A：

- 预先写好 30 个高频问答（就像本页 Q135–Q165），并给出证据链索引；
- 准备 5 个演示脚本：提币、对账、权限变更、监控处置、STR 决策链。

Q171：如何写"持续经营（Going Concern）与资源充足性"以增强可信度？
A：

- 写 12–24 个月财务预测（收入、成本、合规支出、应急预算）；
- 列出关键资源（人员、系统、外包）与备份；
- 把"扩张触发成本"写清（客户量翻倍→合规人力/规则库/审计频率增加）。

Q172：如果暂时没有银行账户或通道，申请包怎么写才合理？
A：

- 坦诚写"计划与时间表"，并给尽调材料框架（Bank DD Pack）；
- 写"无银行情况下不开展法币出入金"的控制与上线门槛；
- 监管与银行通常更看重"你是否先建体系再上线"。

Q173：如何定义"上线门槛"（Go-live Gate）？
A：

- 门槛示例：KYC/制裁/监控规则库上线；提币审批链与白名单生效；对账报表跑通；事故响应演练通过；关键岗位到位与培训完成。

Q174：如何把"Rule for Custodians & Trading Platforms"落到制度目录？
A：

- 以 Rule 为主线：客户资产/私钥治理/对账/市场监控/披露/冲突/外包/记录/事故；
  并将每章附"证据链附件"。

Q175：如何准备"监管现场或远程演示"（Evidence Demo）？
A：

- 用"演示脚本 + 截图点位 + 日志导出点位 + 失败场景处置"四件套；
- 每个演示结束必须能导出：工单号、审批链、日志、报表、归档位置。

Q176：哪些"最低限度制度"必须先定稿再递交？
A：

- AML/CFT Program（含 STR）
- 提币与钱包治理（含权限与签名）
- 对账与客户资产隔离
- 外包治理与退出计划
- 事故响应与 BCP/DR
  （托管/平台 licence 项目尤其要按 Rule 逻辑完整覆盖。）

Q177：如果你希望未来扩展到更多牌照/司法辖区，申请包怎么写更"可扩展"？
A：

- 用模块化制度（Policy library）+ 参数化规则库（thresholds）+ 版本控制；
- 把"新增国家/币种/产品"写成独立的变更管理 SOP。

Q178：如何在申请文件中体现"合规文化"（不是口号）？
A：

- 三道防线、董事会年度议程、KRI 报告、培训与演练、整改闭环（CAPA）——用"记录与模板"证明，而不是用形容词。

Q179：最常见的"自我否定式写法"有哪些？
A：

- "我们不托管"但写"可冻结/可代提币/可重置密钥"；
- "我们不做零售"但营销文案写"面向所有用户"；
- "我们不接高风险国家"但 KYC 没有国家评级与拦截规则。

  交付建议：在递交前做一次"红队审稿"：专找矛盾与监管敏感点。

Q180：若要把本 FAQ 进一步升级成"可直接递交的制度包"，建议下一步做什么？
A（交付级行动清单）：

1. 选定你的业务类型（Registered / Licensed custody / Licensed VATP / Waiver）并在首页"定性声明"固定。
2. 依据 CIMA Checklist 生成你的《申请材料 Master Tracker》。
3. 依据 CIMA Rule 生成《Rule Mapping》与证据链目录（截图/日志/报表/合同）。
4. 准备监管演示脚本（5 个）+ 面谈问答库（本页 Q135–Q165 做底稿）。
5. 输出"外部版（递交版）+ 内部版（操作版）"两套文件（内部版包含更细 SOP 与参数）。

第二十部分｜跨境展业与客户地理风险（Cross-border & Geo-Risk）

Q181：开曼 VASP 能否面向全球客户？是否会触发其他国家牌照？
A（交付级写法）：

1. **VASP（开曼）许可/注册 ≠ 全球通行证**。你可以"跨境提供服务"，但客户所在国可能要求：本地牌照、注册、豁免或营销限制。
2. **可递交表述**：在 BP 中写"Cross-border Compliance Approach"：
   - 目标国家分层（A：可直接展业；B：需法律意见/注册；C：禁止/限制）；
   - 营销与招揽边界（主动/被动招揽区分）；
   - 当地触发点（本地员工、办公室、本地支付通道、本地广告）。
3. **交付建议**：输出《国家合规准入矩阵（Country Matrix）》并纳入变更管理流程（新增国家必须走审批）。

Q182：如何定义"高风险国家/地区"，并落地到系统拦截？
A：

1. 建议采用多源评级（FATF、制裁清单、内部风险情报、银行要求），形成内部"国家风险分级"。
2. 落地方式：
   - KYC 阶段：自动拦截/触发 EDD/要求额外证明；

- 交易阶段：来自高风险地区的出入金、链上对手方与法币对手方都要加强监控。

3. **交付建议**：提供《Country Risk Methodology》+《国家清单版本控制》+ 系统拦截截图/日志。

Q183：什么是"被动招揽（reverse solicitation）"？能否作为跨境合规策略？
A：

1. 作为策略可以提，但**不能当"万能挡箭牌"**。监管与银行通常会看：你是否在该国做广告、是否有本地语言投放、是否有本地渠道合作。
2. **可递交表述**：写《Marketing Boundary Policy》：哪些国家仅允许被动招揽、网站/APP 如何做地理限制（geo-block）、客服如何应答。
3. **交付建议**：保留证据：营销审批记录、投放排除名单、地理限制配置截图。

Q184：如果客户来自受制裁国家，但其本人不在制裁名单，能否开户？
A（交付级写法）：

1. 不同制裁框架对"地域/居民/实体"限制不同，需按你适用的制裁制度与银行要求执行。
2. **可递交机制**：
   - 制裁命中 → 自动拒绝；
   - 高风险辖区 → 强制 EDD + MLRO 审批；
   - 例外 → 必须出具法律意见与管理层批准，并记录原因与证据。
3. **交付建议**：形成《Sanctions Decision Tree（决策树）》与"例外审批表"。

Q185：如何处理跨境税务/旅行规则信息字段（客户资料、转账信息）的数据合规？
A：

1. 你需要把"数据合规"写成可运行机制：哪些字段必收、收集目的、留存期限、对外共享规则（例如 Travel Rule/执法请求）。
2. **交付建议**：输出《Data Governance Policy》：数据分类、最小化收集、加密、访问控制、导出审批、跨境传输评估。

第二十一部分｜数据治理与隐私（Data Governance & Privacy）

Q186：申请包里"数据地图（Data Map）"要包含什么？
A：

- 数据类别：身份资料、交易数据、日志、KYC 文件、链上分析报告、投诉与调查材料
- 数据流向：从前端 → 后端 → 第三方供应商 → 存储（云/本地） → 备份
- 权限与角色：谁能看、谁能导出、谁能删除

交付建议：给监管/银行一个"可读版本"的 Data Map（脱敏），再提供内部详细版用于审计。

Q187：怎样证明"最小权限（least privilege）"不是口号？
A：

1. 用三类证据：
   - 权限矩阵（按角色列出可执行动作）；
   - 权限变更日志（谁在何时授予/撤销）；
   - 定期复核记录（季度/半年）。
2. **交付建议**：提供《Access Review Report》样例（脱敏）：发现问题、整改闭环（CAPA）。

Q188：日志与客户数据保存多久？能否应客户要求删除？
A（交付级写法）：

1. 合规记录通常必须留存（满足 AML/审计/监管期望），因此"被遗忘权/删除请求"往往不能完全满足。
2. **可递交表述**：制定《Data Retention Schedule》与《Data Subject Request SOP》：
   - 哪些可删除（营销偏好等）；
   - 哪些必须保留（AML/交易/日志）；
   - 如何匿名化/最小化披露。
3. **交付建议**：提供"删除请求处理单"模板与样例。

Q189：如何管理"数据导出"（CSV/报表/截图）造成的泄露风险？
A：

1. 规定导出权限、导出审批、导出水印/加密、导出目的与留存。
2. 交付建议：制定《Data Export Control SOP》并可展示导出审批工单与审计日志。

Q190：第三方供应商拿到客户数据时，必须有哪些控制条款？
A：

- 数据使用目的限制、保密、加密、事故通报时限、分包限制、审计权、退出与销毁证明。

  交付建议：做《Supplier Data Processing Addendum（DPA 附录）》条款对照表。

第二十二部分｜持续监管：报送、变更、年度节奏（Ongoing Supervision）

Q191：获批/注册后第一年最容易"踩雷"的是什么？
A：

1. "变更未管理"：新增币种/新国家/新通道/新外包，没走变更审批。
2. "制度未落地"：没有证据链（日志、工单、培训、演练）。
3. "对账与资产隔离不严"：差异积累，审计时爆雷。

   交付建议：第一年以"治理与证据链建设"为主线，不以扩张为主线。

Q192：哪些变更属于重大变更（Material Change）需要升级处理？
A（交付级写法）：

- 业务范围：从经纪升级到托管/平台
- 客户范围：从机构扩展到零售
- 地理范围：新增高风险国家
- 关键外包：更换 KYC/托管/云/撮合核心服务商
- 关键人员：CO/MLRO/安全负责人离任

  交付建议：把上述写入《Change Management SOP》并设置"变更门槛与审批层级"。

Q193：如果我想新增功能（staking、借贷、衍生品），在开曼 VASP 体系下怎么写合规路径？
A：

1. 先做 perimeter 评估：是否仍属于 VASP Act 框架，是否触发其他监管法/牌照。
2. 输出《New Product Approval Pack》：风险评估、客户披露、监控规则、系统安全评审、法律意见（如需要）。
3. **交付建议**：对外材料必须写"是否提供/不提供"，避免宣传误导。

Q194：年度审计/独立评估怎么组织，才能对监管与银行都有用？
A：

1. 将年度保证计划分成三块：财务/客户资产、AML、IT 安全与业务连续性。
2. 交付建议：输出《Annual Assurance Plan》+《整改闭环台账（CAPA）》并纳入董事会季度审阅。

Q195：如何设计"年度合规日历（Compliance Calendar）"？
A：

- 每月：KRI、监控命中、投诉、外包 SLA、STR 统计
- 每季：董事会风险报告、权限复核、外包复核、演练
- 每年：政策复核、培训、渗透测试、BCP/DR 大演练、审计

  交付建议：日历要对应"谁负责、输出什么文件、保存在何处"。

Q196：如何处理"客户资产不足/挤兑风险"的压力测试（Stress Test）？
A：

1. 托管/平台应做场景：链上拥堵、极端波动、集中提币、通道冻结。
2. 交付建议：提供《Liquidity & Withdrawal Stress Test Report》：假设、结果、缓释措施（限额、分批、冷钱包调拨计划）。

第二十三部分｜处罚、执法协作与风险地图（Enforcement & Risk）

Q197：CIMA 对 VASP 可能采取哪些监管措施?
A（交付级写法）：

1. 典型手段包括：要求整改、限制业务、暂停/撤销许可、公开通报等（具体以适用法律与个案为准）。
2. **交付建议**：建立《Regulatory Breach SOP》：如何识别违规、内部升级、补救、通报、复盘。

Q198：如何处理执法机关/法院要求冻结或提供资料?
A：

1. 必须建立"合法性审查"步骤：请求主体、法律依据、范围、时限。
2. 形成《LE Request SOP》：最小披露、证据留痕、内部审批、是否通知客户（视法律与请求限制）。
3. **交付建议**：保留"请求登记台账"与"资料交付清单"。

Q199：如果发生被盗/系统漏洞，第一小时应该做什么?
A：

- 启动事件响应（IR）：隔离、冻结、切换、证据保全
- 通知关键岗位：CO/MLRO/安全负责人/管理层
- 启动客户沟通预案与监管通报评估
- 保留链上证据与系统日志（不可篡改）

  交付建议：准备《1-hour Playbook》与演练记录，能显著提升可信度。

Q200：如何向客户解释"链上不可逆"与平台责任边界，避免纠纷?
A：

1. 在客户协议与风险披露中明确：链上交易不可逆、地址错误责任、平台可协助但不保证追回。
2. 交付建议：提供《Wrong Address / Scam Handling SOP》与客户话术模板。

第二十四部分｜30 个"最容易被拒/被补件"的雷区清单（第一批：Q201–Q230）

Q201：雷区 1｜"我们不托管"但 SOP 写"可代提币/可冻结/可重置密钥"。怎么办?
A：立刻做"三表一致性修复"：Form/BP/Policy 同步改；并用权限矩阵+日志证明你做不到"单方控制"。

Q202：雷区 2｜资金路径图缺失，或对账点写不清。
A：补齐 Funds Flow Diagram + 对账报表样例 + 差异处理工单闭环。

Q203：雷区 3｜外包未披露或合同无审计权/无退出计划。
A：建立 Outsourcing Register + 合同摘要对照表 + Exit Plan，并纳入董事会监督。

Q204：雷区 4｜没有"运行证据链"，只有漂亮制度。
A：每个核心制度至少补 3 个样例（截图/日志/工单/演练/培训）。

Q205：雷区 5｜关键岗位兼职过多且无备份。
A：补 Deputy 安排、时间投入声明、交接与离任权限回收流程。

Q206：雷区 6｜交易监控规则写得空泛，无法落地。
A：给出规则库：阈值、触发条件、误报处理、升级路径；附命中样例。

Q207：雷区 7｜上币政策缺失或不含利益冲突控制。
A：Listing Policy + Committee TOR + 冲突声明 + 下架阈值。

Q208：雷区 8｜同名出入金不严格、第三方代付缺控制。
A：Same-name Policy + 例外审批表 + 黑名单机制 + 监控规则。

Q209：雷区 9｜国家风险评级没有版本控制。
A：Country list 版本号、生效日、变更审批、系统拦截证据。

Q210：雷区 10｜日志无法证明"谁做了什么"。
A：补齐关键字段（用户、时间、动作、对象、结果、IP/设备）与导出流程。

Q211：雷区 11｜对账频率与粒度不足（链上/内部账/客户余额不闭环）。
A：三层对账（每日/每周/每月）+ 差异处理与复盘。

Q212：雷区 12｜BCP/DR 没演练。
A：演练计划+报告+整改闭环（CAPA），至少一次大演练证据。

Q213：雷区 13｜漏洞管理没有时限与复测。
A：分级、修复 SLA、复测记录与管理层汇报机制。

Q214：雷区 14｜营销文案写"持牌受监管"，但实际仅注册或尚在申请。
A：制定 Marketing Policy + 措辞白名单 + 审批留痕。

Q215：雷区 15｜客户协议缺乏暂停/下架/冻结条款。
A：补齐客户协议与披露附表，明确处置边界与通知机制。

Q216：雷区 16｜投诉机制不完整或无台账。
A：Complaint SOP + 台账 + 月度复盘模板。

Q217：雷区 17｜STR 机制不清晰，MLRO 决策无备忘录。
A：STR Decision Memo 模板 + 时限 + 升级路径 + 样例。

Q218：雷区 18｜KYC/EDD 表单缺失或字段不够。
A：补齐个人/法人/EDD/SoF/SoW 模板与系统录入流程。

Q219：雷区 19｜API 权限/第三方接入没有安全策略。
A：API key 生命周期、速率限制、IP 白名单、异常检测、紧急吊销 SOP。

Q220：雷区 20｜数据导出失控（员工随意导出客户资料）。
A：Data Export Control SOP + 审批工单 + 审计日志。

Q221：雷区 21｜外包供应商宕机没有降级方案。
A：替代方案、降级运行模式、演练计划与责任人。

Q222：雷区 22｜"被动招揽"无证据，实质在当地做推广。
A：营销排除名单、geo-block 配置、投放记录与审批证据。

Q223：雷区 23｜客户分级缺失，零售与机构同一套 KYC/限额。
A：Customer Tier Policy + 分级证据 + 定期复核。

Q224：雷区 24｜关联方交易不披露。
A：关联方政策、披露、审批、对账与审计跟踪。

Q225：雷区 25｜密钥恢复机制过于强大（你能单方恢复）。
A：重设计恢复门限与审批链，证明你不能单方控制。

Q226：雷区 26｜资金来源核验只靠一句"客户声明"。
A：分层触发 SoF 证据清单、抽样复核、拒绝与例外审批。

Q227：雷区 27｜缺少"变更管理"导致上线后无序扩张。
A：Change SOP + 变更台账 + 上线门槛（Go-live Gate）。

Q228：雷区 28｜事件响应只有文档，没有 1 小时行动方案。
A：1-hour Playbook + 演练记录 + 客户通知模板。

Q229：雷区 29｜规则库没有误报治理，调查资源不足。
A：误报复盘机制、阈值治理、资源扩容触发点。

Q230：雷区 30｜"证据链文件命名混乱、版本不可追踪"。
A：建立文档版本控制：版本号、变更记录、附件编号、归档目录结构。

第二十五部分｜收口：把本 FAQ 变成"可递交文件包"的落地步骤（Q231–Q240）

Q231：我已经有 FAQ 了，如何快速生成"递交版制度目录"?
A：以 CIMA Rule/Checklist 为骨架（如你走 Licence），把 FAQ 的主题映射到制度章节：AML、Wallet/Withdrawal、Reconciliation、Market Surveillance、Outsourcing、Records、Incidents、Governance，并给每章附证据链索引。

Q232：如何建立"证据链目录"（Evidence Index）？
A：三列：附件编号、证据类型（截图/日志/工单/报表/合同/演练）、对应制度条款编号。

交付建议：附件编号必须稳定，补件时只更新版本，不改编号体系。

Q233：如何准备"监管演示脚本"（Demo Script）让面谈更稳?
A：建议 6 个脚本：

1. 开户/KYC/EDD 走一遍

2. 提币：发起→审批→签名→广播→归档
3. 对账：导出→差异→工单→关闭
4. 监控：规则命中→调查→升级→STR 决策
5. 权限变更：授予/撤销/日志
6. 事故响应：告警→冻结→通报→复盘
   每个脚本都要能导出证据。

Q234：如果我暂时还没完成系统改造，是否可以先递交？
A（交付级写法）：
可以递交"过渡方案"，但必须写清：

- 当前能力与缺口
- 具体改造计划与时间表
- 上线门槛（未达门槛不得上线相关功能）
  并在补件时按计划逐项关闭缺口。

Q235：如何把"外包治理"写成董事会可监督的机制？
A：季度外包报告（SLA、事故、审计、整改），外包清单更新必须走审批；关键外包变更需董事会/委员会批准。

Q236：如何把"客户资产隔离"写成可审计闭环？
A：法律条款 + 分账规则 + 钱包结构 + 对账报表 + 差异工单 + 审计抽样，六件套缺一不可。

Q237：如何把"跨境国家矩阵"与系统控制结合？
A：国家矩阵（政策层）→ 系统 geo-block/拦截（技术层）→ 审批与例外台账（运营层）→ KRI 与复盘（治理层）。

Q238：如何把"红队审稿（找矛盾）"制度化？
A：递交前做一次"矛盾点审查"：托管边界、资金路径、客户类型、外包范围、权限矩阵、营销口径，形成审查纪要与整改闭环。

Q239：本 FAQ 的"对外交付版本"与"内部操作版本"应如何区分？
A：

- 对外版：制度条款 + 证据摘要（可脱敏）
- 内部版：更细 SOP、阈值参数、规则库明细、供应商合同细节、调查话术库
  两版共用同一套编号体系，便于监管问询快速定位。

Q240：如果你要我（仁港永胜）把这套内容升级为"开曼 VASP 申请可递交整包"，交付件清单应包括哪些？
A（交付级清单）：

1. Perimeter Memo（含 licence/registration/waiver 路径结论）
2. Business Plan（含资金路径、客户/国家矩阵、收入模型）
3. Governance Pack（董事会/三道防线/KRI/年度日历）
4. AML/CFT Program（含 STR/Travel Rule readiness）
5. Wallet/Withdrawal Pack（密钥治理、权限矩阵、提币 SOP）
6. Reconciliation & Client Asset Pack（对账、隔离、差异工单）
7. VATP Pack（如适用：交易规则、监控、上币、冲突）
8. Outsourcing Pack（清单、合同摘要、DPA、Exit Plan）
9. Incident Response & BCP/DR Pack（1-hour playbook + 演练）
10. Evidence Index（证据链目录 + 附件归档）
    并按 CIMA Checklist 顺序装订，便于审查。

第二十六部分｜Registration vs Licence：怎么"选"、怎么"写"、怎么"证明"（Q241–Q260）

Q241：我到底该走 Registered Person 还是 VASP Licence？一句话怎么定性？
A（交付级写法）：

- 你只要回答三个问题：
  1. **你是否"控制或持有客户虚拟资产的转移能力"**（例如持钥/可单方影响转移/代提币）？

2. 你是否运营或提供 **交易平台**（撮合、订单簿、撮合规则、市场监控）？
3. 你的服务是否属于"高风险核心环节"(托管/平台通常就是）？

- **可递交结论**：把答案写入《Perimeter Memo》，并把"系统证据"附在 Evidence Index（权限矩阵、签名门限、提币链路)。

Q242：最常见的"误判路径"是什么？
A：

- 口头说"不托管"，但实际上：
  - 钱包由你创建；
  - 你能冻结/恢复/重置；
  - 你能代客户提币；
  - 你能单方更改签名门限。

交付建议：先做一次"红队审稿"，专找"事实托管"痕迹，再定路径。

Q243：如果我目前是注册（Registered)，未来要做托管/平台，策略上怎么写？
A（可递交结构)：

1. **阶段 1（注册)**：仅提供低风险服务（例如某些中介/技术服务)，明确"不触及托管/平台"。
2. **阶段 2（升级许可)**：上线托管/平台前必须完成：
   - 私钥治理、提币控制、对账、监控、外包治理、事故响应演练；
   - 并提交 Licence 申请。
3. 关键：写清"**上线门槛（Go-live Gate)**"，未达门槛不得上线相关功能。

Q244：如果我既做托管又做平台，申请文件怎么避免"写乱"？
A：

- 用"**服务拆分法**"：
  - Custody 模块：资产隔离、签名门限、提币审批、对账、钱包政策
  - VATP 模块：交易规则、监控、上币、冲突、市场公平
- 用"**责任边界图**"：谁负责撮合、谁负责清算、谁负责托管、谁负责法币通道。

交付建议：不要一份 SOP 同时涵盖两类核心控制；分册更容易通过审查。

Q245：Waiver 路径什么时候值得考虑？
A（交付级写法)：

- 仅当你已在其他监管法下是受监管机构，且 VASP 活动是"附带/例外"，才有讨论价值。
- 实务上，Waiver 论证需要：
  1. 现有牌照范围与监督事实；
  2. VASP 活动的边界、规模、风控隔离；
  3. 不申请 licence 的合理性（风险不相称)。

交付建议：准备 1 份外部法律意见（Legal Opinion）增强说服力。

Q246：如何在 BP 中写"监管状态披露"才稳？
A：

- 用固定措辞：
  - "Registered under the VASP Act as a Registered Person（如适用)"
  - "Licensed under the VASP Act for custody/VATP（如适用)"
- 禁止使用模糊夸大词：如"fully regulated / guaranteed / government endorsed"。
- 建立 Marketing 合规模板与审批留痕。

Q247：Licence/Registration 选择对银行开户影响大吗？
A：

- 银行更看重：

1. 资金路径是否清晰；
2. 是否托管、托管怎么控；
3. AML/制裁/可疑交易处置是否可运行；
4. 外包与事故响应是否成熟。

交付建议：无论走哪条路径，都要做一份《Bank DD Pack》：制度摘要+证据链摘要+资金路径图。

Q248：如何把"业务不确定性"写成监管可接受的表述？
A：

- 不要写"以后可能做任何事情"。
- 写成"**产品路线图 + 风险门槛**"：
  - 未来扩展功能 → 必须先走 NPA（New Product Approval）+ 法律评估 + 监控规则/披露升级 +（如需要）申请许可变更。

Q249：如果使用集团公司/多实体结构，怎么写更容易被接受？
A：

- 监管最关注：**谁对客户负责、谁持资产、谁做关键控制**。
- 交付级写法：
  1. 结构图（UBO 穿透 + 各实体职责）
  2. 服务分工表（RACI）
  3. 客户合同签署主体与争议解决
  4. 资金路径与对账归属

关键：避免"空壳主体申请、实际由海外团队运营"但无治理与控制证据。

Q250：Licence vs Registration 的"最终自检清单"是什么？
A（可复制清单）：

- 是否持钥/是否能影响转移？
- 是否提供撮合/订单簿/撮合规则？
- 是否提供法币出入金通道？
- 是否向零售开放？是否高风险国家较多？
- 关键控制是否已有证据链（权限/日志/对账/监控/演练）？
  满足越多"高风险特征"，越应走 licence 并提前补齐控制。

第二十七部分｜托管（Custody）深水区：把"可运行控制"写出来（Q261–Q280）

Q261：什么叫"私钥治理（Key Governance）"交付级写法？
A：至少包含 8 个要素：

1. 生成（key ceremony）
2. 存储（HSM/MPC/冷存）
3. 使用（签名门限、角色分离）
4. 备份与恢复（谁能触发、门限）
5. 轮换（rotation）
6. 作废（revocation）
7. 访问控制（JML：入转离）
8. 审计与证据（日志、录像、见证人签字）

交付建议：提供"Key Ceremony 记录表"模板与一次演练样例（可脱敏）。

Q262：冷热钱包怎么设"额度与迁移规则"才像真的？
A（可递交机制）：

- 热钱包：仅用于日常小额提币；设置单日/单笔上限；超限自动转冷审批。
- 冷钱包：大额储备；迁移需要双人复核 + 多签门限 + 变更日志。

- 设"极端行情"策略：拥堵时分批/延迟/提币公告模板。

  交付建议：把额度写成"参数表"并纳入变更管理。

Q263：提币（Withdrawal）控制最容易被问到的 10 个点？
A：

1. 地址白名单与新增地址冷静期
2. 设备指纹与异常登录
3. 风险评分（链上/行为/制裁）
4. 分级限额（按客户等级/KYC等级）
5. 双人复核/多签
6. 批量提币的分拆与审批
7. 失败重试与重复广播控制
8. 客户通知与确认机制
9. 紧急冻结与解冻流程
10. 全链路日志可追溯

  交付建议：用"一笔提币的证据链样例"把以上点串起来。

Q264：客户资产隔离（Safeguarding）怎么写到"可审计"？
A（六件套）：

1. 法律隔离：客户协议条款明确客户资产归属
2. 账务隔离：客户分账/子账户规则
3. 钱包隔离：客户钱包/池化钱包结构说明
4. 运营隔离：提币审批、费用扣除、冲突控制
5. 对账闭环：每日对账 + 差异工单
6. 审计抽样：定期抽样验证与报告

  交付建议：提供"对账报表样例 + 差异工单样例"。

Q265：对账（Reconciliation）必须对哪些账？频率怎么写？
A：

- 至少三层：
  1. 链上余额 vs 钱包内部账
  2. 内部账 vs 客户余额明细
  3. 费用/手续费 vs 平台收入账
- 频率：可写"每日自动对账 + 每周人工复核 + 每月审计抽样"。

  交付建议：把"差异阈值"写清：超过阈值必须升级到 CO/管理层。

Q266：如果采用池化托管（omnibus pooling），如何降低质疑？
A：

- 解释为什么池化（效率/链上成本），同时给出强控制：
  - 客户分账明细可实时核对
  - 提币必须在客户层面校验余额与风控
  - 对账与审计抽样更严格

  交付建议：对外说清"池化≠混同"，用对账证据证明。

Q267：MPC/多签到底怎么选？监管会怎么问？
A：

- 监管更关心：**门限设置是否合理、是否能避免单点控制、恢复机制是否过强**。
- 交付建议：写清：

- 门限（m-of-n）与角色分配
- 谁保管分片/签名权
- 恢复触发条件与审批
- 任何变更必须留痕并复核

Q268：托管业务是否建议购买保险？文件怎么写？
A：

- 可以写"评估并在可行时配置保险/赔付安排"，但不要承诺"100%赔付"。
- 交付建议：把保险写成风险缓释之一：与冷存比例、门限控制、事故响应并列。

Q269：如何处理链上拥堵导致提币延迟，避免投诉与挤兑？
A：

- 预案三件套：
  1. 客户公告模板（原因、预计时间、替代方案）
  2. 分批提币策略（优先级、限额）
  3. 投诉与升级通道（SLA）

  交付建议：把"极端行情处置"写进 BCP/IR 的附件。

Q270：如果发生盗币，最关键的"证据保全"是什么？
A：

- 固定链上证据（TX、地址、时间线）
- 固定系统证据（日志、权限变更、工单、告警）
- 固定人员证据（值班记录、审批链）

  交付建议：准备《Theft Incident Evidence Pack》模板，发生事件可直接启用。

Q271：如何证明"员工无法单独完成盗币"？
A：

- 用"分权"证明：
  - 发起人与审批人不同
  - 签名权分散
  - 关键操作需双人复核
  - 所有操作有不可篡改日志

  交付建议：在制度里写"控制目标"+"技术措施"+"审计验证方法"。

Q272：托管服务是否能允许客户自己持钥（non-custodial）？
A：

- 可以，但必须写清：
  - 你不持钥时的责任边界
  - 你仍要做哪些 AML/监控（例如交易监控与制裁筛查）
  - 客户误操作的处理

  交付建议：把 non-custodial 作为独立产品线写，不要与 custodian 混写。

Q273：托管类最容易忽略的"费用扣除"风险是什么？
A：

- 平台自动从客户资产扣费，容易被质疑"混同/未经授权"。
- 交付建议：
  - 合同中明确费用类型与扣除规则
  - 扣费必须可对账、可追溯、可申诉

Q274：如何写"钱包地址管理"（Address Management）才像合规成熟？
A：

- 地址创建、标签、用途限制、白名单、风险评分、禁用/冻结、审计复核。

  交付建议：附"地址台账样例（脱敏）"。

Q275：如何处理"灰产资金误入"但客户声称无辜？
A：

- 写清"调查—限制—申诉—结论—记录保存"的闭环；
- 明确可疑时优先保护系统与客户群体利益，必要时提交 STR 并冻结处置。

  交付建议：提供《Case Management SOP》与台账字段定义。

Q276：托管类的"重大事件"定义建议包含哪些？
A：

- 私钥疑似泄露、异常签名、冷钱包迁移异常、对账差异超阈值、批量提币异常、供应商泄露、制裁命中批量上升。

  交付建议：用"事件分级矩阵"写通知链路与时限。

Q277：托管类如何做"供应商依赖"风险缓释？
A：

- 核心依赖（MPC、链上分析、KYC）必须：
  - SLA、审计权、事故通报、分包限制、退出计划
  - 每年复核与演练（例如切换方案）

  交付建议：外包清单必须"版本化"。

Q278：托管业务的"客户适当性/风险披露"需要写到什么程度？
A：

- 至少披露：链上不可逆、地址错误风险、市场波动、网络拥堵、监管变化、平台限制与冻结条件。

  交付建议：把披露写成"签署确认 + 可追溯记录"。

Q279：托管业务是否必须做渗透测试？如何写才稳？
A：

- 建议写"定期开展安全测试（含渗透测试）并形成整改闭环"。
- 交付建议：不要只写"会做"；要写"频率、范围、整改 SLA、复测要求"。

Q280：托管模块最强的"交付式结尾"怎么写？
A："本机构以客户资产隔离与可验证控制为核心设计原则，采用分权签名、提币审批链、三层对账与不可篡改日志，确保任何关键操作均可追溯、可审计、可复盘；并通过外包治理、事件响应与年度保证计划持续验证控制有效性。"

第二十八部分｜交易平台（VATP）深水区：市场公平与冲突管理（Q281–Q300）

Q281：什么算"交易平台服务"（VATP）？最容易被问到哪一句？
A：

- 只要你提供撮合机制（订单簿/撮合规则/撮合引擎）并让用户之间交易，你就要把"平台规则与市场监控"写完整。

  交付建议：写清你是 CEX、OTC 撮合、RFQ，还是仅技术转发；不同模式控制不同。

Q282：交易规则（Trading Rulebook）最低要包含哪些章节？
A（交付级目录）：

1. 订单类型与撮合规则
2. 交易时段与暂停机制
3. 异常波动与熔断/限价

4. 市场监控与禁止行为
5. 费用与优先级（是否存在手续费返佣）
6. 争议处理与更正
7. 上币/下币规则与披露
8. 冲突管理（做市/自营/关联方）

交付建议：把 Rulebook 当成"监管与客户都会看"的文件写，语言要可读可执行。

Q283：市场监控（Surveillance）规则库怎么写才不空？
A：

- 至少列出 12 类典型行为与触发逻辑：
  - wash trading、self-trade、layering、spoofing、pump & dump、异常撤单、异常成交量、跨账户关联交易、价格偏离、异常 API 频率等。
- 交付建议：给 1 个"命中—调查—结论—处置"的脱敏案例样例。

Q284：如果平台有做市商（market maker），如何避免被质疑操纵？
A：

- 交付级写法：
  1. 做市资格与合同条款（禁止操纵、报送义务）
  2. 平台内部冲突隔离（信息隔离墙）
  3. 做市监控（价差、深度、撤单、成交占比）
  4. 披露：向客户披露是否存在做市与可能影响

关键：不要"既做市又上币审批又监控"，必须分权。

Q285：平台自营（proprietary trading）能不能做？怎么写才稳？
A：

- 可行性取决于具体监管判断与风险控制，但就文件而言必须：
  - 强披露、强隔离、强监控、强审批；
  - 明确禁止利用客户订单信息牟利。

交付建议：如果你想降低复杂度，直接声明"不做自营"，并写制度如何保证。

Q286：上币（Listing）尽调最核心的 10 项是什么？
A：

1. 代币经济模型与集中度
2. 项目主体与治理结构
3. 技术安全（审计、合约风险）
4. 法律属性与限制（证券属性风险）
5. 合规风险（制裁、诈骗、黑客历史）
6. 流动性与市场操纵风险
7. 透明度与信息披露
8. 交易与托管支持能力
9. 退市触发条件
10. 持续监测计划

交付建议：把这些做成《Token Risk Rating》评分表，可直接纳入制度附件。

Q287：退市（Delisting）最容易引发纠纷，怎么写？
A：

- 写清：
  - 触发条件（合规风险、技术漏洞、流动性枯竭、欺诈）
  - 通知期限与紧急退市例外

- 客户处置窗口（提币/平仓）
- 公告模板与客服话术

交付建议：提供退市演练流程，证明可执行。

Q288：平台的价格形成与指数来源怎么披露？
A：

- 披露：撮合规则、参考价来源、异常行情处理、系统故障时的处理。

交付建议：把"价格偏离阈值"写清并纳入监控告警。

Q289：如何处理 API 高频交易带来的操纵与系统风险？
A：

- API key 生命周期、速率限制、IP 白名单、异常行为识别、紧急吊销、限频与熔断。

交付建议：附 API 滥用处置案例样例（脱敏）。

Q290：如果提供杠杆/衍生品，文件要增加什么？
A：

- 若不提供：明确"不提供"。
- 若提供：必须新增：强适当性、强风险披露、强制平仓规则、保证金与风险引擎、异常波动处置。

交付建议：衍生品会显著提升审查强度，建议先把现货平台控稳再扩展。

Q291：平台如何防止"关联账户多开"与"刷量"？
A：

- 设备指纹、受益人穿透、行为关联规则、交易模式识别、返佣政策控制。

交付建议：把"返佣"纳入合规审批，返佣极易诱发刷量。

Q292：客户资产在平台与托管之间如何交互才不混乱？
A：

- 定义清楚：
  - 交易账户余额与托管钱包余额的映射
  - 内部划转规则、权限与日志
  - 对账如何覆盖内部划转

交付建议：画一张"Trade-to-Custody 资金路径图"。

Q293：平台是否需要"市场滥用调查"台账？
A：必须有。字段建议：触发规则、涉及账户、交易对、时间线、调查动作、结论、处置、是否 STR/是否通知监管。

交付建议：每月至少做一次抽样复盘。

Q294：平台重大事件（中断、撮合异常、价格异常）如何对外沟通？
A：

- 预设公告模板：中断原因、影响范围、客户操作建议、恢复时间、补偿政策（如有）。
- 交付建议：公告必须经过合规/法务审批并留档。

Q295：平台如何处理"错误成交/系统 bug 造成的不公"？
A：

- 写清：纠正条件、纠正范围、证据标准、客户申诉渠道、最终裁决机制与记录保存。

交付建议：建立"更正委员会/审批链"。

Q296：如何管理"上币相关利益冲突"（投资、顾问费、持币）？
A：

- 上币委员会成员必须声明：是否持有项目权益/代币/顾问关系；冲突则回避；所有决定留痕。

  交付建议：附《Conflict Declaration Form》模板。

Q297：平台如何证明"监控不是摆设"？
A：

- 给三类证据：
  1. 规则库清单
  2. 命中样例（脱敏）
  3. 处置闭环（限制/冻结/退市/STR）

  交付建议：最好准备一段演示脚本：从命中到结案的全流程。

Q298：平台如何确保客户披露"足够清晰"？
A：

- 披露要包括：撮合规则、费用、做市/自营（如有）、风险、暂停/退市、投诉机制。

  交付建议：用"客户确认记录"证明客户已阅并同意。

Q299：平台是否需要"治理与监督"的董事会材料？
A：

- 需要。建议每季度董事会包至少包含：KRI、市场监控统计、投诉、重大事件、外包、审计与整改。

  交付建议：把"董事会看板"模板作为制度附件。

Q300：VATP 模块的交付式结尾如何写？
A："本机构通过交易规则披露、市场监控规则库、上币与冲突管理机制、以及重大事件处置与复盘闭环，确保交易平台运行透明、公平、可审计；并以证据链与董事会监督持续验证控制有效性与市场完整性。"

第二十九部分｜AML/CFT 体系：从"文件"到"可运行证据链"（Q301–Q320）

Q301：CIMA 最想看到的 AML 体系"不是哪份文件"，而是什么？
A（交付级回答）：是你能证明 **"持续运行"**：

- 风险评估（Risk Assessment）每年复核；
- KYC/EDD 有分层触发与审批链；
- 监控规则库可配置、可复盘；
- STR 决策有 MLRO 备忘录与台账；
- 制裁筛查与命中处置有证据；
- 培训、抽检、审计、整改闭环（CAPA）持续存在。

  交付建议：每一项至少给出 1–3 份"样例证据"（截图/日志/工单/报告）。

Q302：AML 风险评估（EWRA/BRRA）最低应包含哪些维度？
A：建议至少 7 维：客户（零售/机构/高净值）、产品（托管/平台/法币通道/OTC/RFQ）、国家地区、交付渠道（线上/代理/API）、交易对手（链上/法币）、资金来源/财富来源、外包依赖。

可递交写法：明确每维的**评分规则**、**权重**、**触发 EDD 阈值**与**复核频率**。

Q303：如何写"客户分层（Customer Tiers）"才可执行？
A：按 **KYC 完整度 + 风险评分 + 行为稳定性** 三因素分层：

- Tier 1：低额度、低功能（不开放提币到未白名单地址等）
- Tier 2：标准额度（增强监控）
- Tier 3：高额度/机构（强 EDD + 定期复核 + MLRO/CO 审批）

交付建议：把每层的**限额、功能开关、触发 EDD**写成"参数表"，纳入变更管理。

Q304：KYC 最小字段集（个人客户）建议有哪些？
A（可复制）：身份信息（姓名、DOB、国籍、居住地）、身份证明、地址证明、职业与雇主、资金来源 SoF、财富来源 SoW（视风险）、PEP 声明、制裁/负面信息筛查结果、受益人/代理人情况（如适用）、用途与预期交易概况。

Q305：法人客户（机构）KYC/UBO 穿透要做到什么程度？
A：做到"可解释且可验证"：

- 注册文件、董事股东名册、章程、良好存续；
- **UBO 穿透到自然人**（或解释为何无法穿透并提供替代证据）；
- 授权签字人、董事/UBO 身份与制裁/PEP 筛查；
- 业务性质、主要收入来源、对公银行账户、主要交易对手。

交付建议：输出《Corporate KYC Pack Checklist》与"缺口处理规则"（何时拒绝）。

Q306：什么时候必须做 EDD？
A（交付级阈值示例）：

- PEP/制裁相关、负面新闻高风险；
- 高风险国家/行业（博彩、暗网相关、匿名工具强使用等）；
- 交易行为异常（突增、集中、链上高风险对手方）；
- 机构结构复杂或 UBO 不透明。

建议写清：EDD 内容清单 + MLRO 审批 + 定期复核频率。

Q307：如何把 SoF/SoW（资金/财富来源）做成"可审查模板"？
A：给出分层证据清单（低/中/高风险）：

- 工资/奖金：工资单、税单、雇佣证明、银行流水
- 经营收入：财报、合同、发票、纳税证明
- 投资收益：券商对账单、基金赎回记录、交易所记录
- 资产出售：买卖合同、过户证明、收款流水

交付建议：每类给"可接受/不可接受"示例，减少一线随意性。

Q308：交易监控（TM）规则库怎么写才不像"空话"？
A：用"规则卡（Rule Card）"写：

- 规则名称、触发逻辑、阈值、适用客户层级、误报处理、升级路径、结案标准、复盘频率。

交付建议：至少列出 20–40 条规则（链上 + 法币 + 行为）。

Q309：链上分析（Blockchain Analytics）要如何嵌入流程？
A：三点：

1. 入金地址风险评分（来源类别：mixers、黑客、暗网、制裁地址等）；
2. 出金对手方风险评分；
3. 调查工单必须引用链上报告编号。

交付建议：调查结案报告中必须附"链上证据摘要"。

Q310：制裁筛查要筛哪些对象？
A：至少四类：客户本人、UBO/董事高管、受益人/收款人（如适用）、链上地址/对手方（结合链上分析）。

交付建议：把"筛查频率"（开户、定期、触发时）写清。

Q311：如何处理"部分命中/疑似命中"（false positives）？
A：必须有 SOP：

- 二次核验字段（DOB、国籍、地址、证件号）
- 升级审批（CO/MLRO）

- 记录留存（为什么判定非命中）

交付建议：建立《Sanctions Hit Review Memo》模板，审计最爱看。

Q312：什么时候要冻结（freeze）或限制账户？
A：典型触发：制裁命中、欺诈/盗币强迹象、执法请求、STR 评估中需要防止资金外流。

注意：冻结与限制必须有**权限链与日志**，且与客户沟通模板配套。

Q313：STR（可疑交易报告）决策必须留什么证据？
A（交付级清单）：

- 触发来源（规则命中/投诉/银行退单/链上报告）
- 调查动作（问询、补充材料、链上追踪）
- 结论与理由（为何可疑/为何不报）
- 处置措施（限制/终止/冻结）
- MLRO 决策备忘录 + 台账条目

交付建议：STR 是否提交属于敏感信息，对外披露策略要写清（通常不告知客户）。

Q314：如果客户强烈反对提供 SoF/SoW，怎么处理？
A：写清"拒绝即限制/终止"的规则：

- 在合理期限内不提供 → 降级限额/冻结出金 → 最终关闭账户并保存记录；
- 需要时提交 STR。

交付建议：准备"客户沟通话术"与升级路径，减少前线摇摆。

Q315：如何做"持续尽调（Ongoing CDD）"？
A：三条主线：

- 定期复核（按风险：半年/一年/两年）
- 触发复核（额度突变、国家变更、行为异常）
- 资料更新（证件过期、UBO 变更）

交付建议：用系统提醒 + 台账证明"确实做了"。

Q316：员工培训要如何写得"可审查"？
A：分层培训：董事会/高管、前线、AML 调查员、技术与安全、客服。

- 频率：入职 + 年度 + 重大制度更新
- 证据：课件、签到、测验、补训记录。

交付建议：把"考试不合格处理"写进制度。

Q317：独立审计/评估（AML）应覆盖哪些？
A：风险评估方法、KYC 样本抽检、监控规则有效性、STR 台账与决策质量、制裁筛查、记录保存、外包合规、整改闭环。

交付建议：输出《AML Audit Plan》与《CAPA 台账》。

Q318：如何管理"代理/介绍人/渠道合作"带来的 AML 风险？
A：三件套：

- 渠道尽调（DD）与持续复核
- 合同条款（合规义务、审计权、禁止误导营销）
- 客户责任归属（最终 KYC 责任不外包）

交付建议：建立《Introducer Oversight SOP》。

Q319：如何处理"混币器/mixer"相关入金？
A：建议写成强控制：

- 触发 EDD 与资金解释
- 必要时拒绝/限制并提交 STR
- 建立明确阈值（比例、频次、金额）

交付建议：把 mixer 视为"高风险来源类别"写入规则库与风险评估。

Q320：AML 记录保存需要哪些"必须字段"?
A：客户资料、交易明细、监控命中、调查工单、STR 决策、制裁筛查结果、培训记录、审计与整改。

交付建议：把"保存期限、存放位置、访问权限、导出审批"写成 Data Governance 附录。

第三十部分｜Travel Rule（旅行规则）落地：字段、阈值、供应商与证据（Q321–Q340）

Q321：Travel Rule 在开曼 VASP 的"递交版"写法要点是什么?
A：用一句话：**"我们对可转移的虚拟资产转账，采集并传递必要的发起人/受益人信息，并对无法完成信息交换的交易实施限制或增强尽调。"**

交付建议：写成"分场景 SOP + 系统证据链"，而不是泛泛陈述。

Q322：Travel Rule 信息字段通常包括哪些?
A（交付级字段示例）：

- 发起人：姓名、账户标识/钱包、地址或身份证明信息、出生日期/国籍（视制度）
- 受益人：姓名、账户标识/钱包

交付建议：字段以你采用的 Travel Rule 方案与合作方要求为准，并写明"字段缺失时的处置"。

Q323：Travel Rule 适用于哪些交易?
A：通常聚焦 **"对外转账（外部钱包/其他 VASP）"**，内部划转不在同一强度，但仍应留痕。

交付建议：在 SOP 中明确：VASP-to-VASP、VASP-to-unhosted、unhosted-to-VASP 三类路径分别怎么做。

Q324：什么是 unhosted wallet（自托管钱包）场景的核心难点?
A：你无法从对方 VASP 获取信息，因此你需要：

- 地址所有权验证（sign message/小额验证/白名单冷静期）
- 强化 EDD（用途、对手方、资金解释）
- 交易后监测与抽检

交付建议：把"验证失败/拒绝提供信息"的处置写得非常具体（限制、延迟、拒绝、STR 评估）。

Q325：Travel Rule 供应商（TRP）接入时，监管/银行会问什么?
A：

1. 供应商是否能覆盖主要对手方网络?
2. 信息交换失败怎么处理?
3. 数据存储在哪里？跨境传输与加密如何做?
4. 审计权、事故通报、退出计划有没有?

交付建议：把 TRP 纳入 Outsourcing Register，并提供合同摘要与 DPA。

Q326：Travel Rule "失败交易"如何处置才稳?
A（可递交规则）：

- 可容忍失败：仅限低风险、小额、且有补救流程
- 不可容忍失败：高风险国家/高金额/异常行为 → 必须阻断或升级审批

交付建议：设置"失败率 KPI/KRI"，超过阈值升级到董事会/风险委员会。

Q327：如何证明你真的"传递了信息"?
A：保存 3 类证据：

- TRP 交换回执/日志编号
- 转账交易哈希（TX）与对应信息索引
- 例外审批（如果没传递）

交付建议：做一份"Travel Rule Evidence Pack 样例"（脱敏）。

Q328：Travel Rule 与制裁筛查如何联动？
A：在信息交换前后都要筛：

- 受益人信息与地址风险
- 发起人信息与地址风险
  若命中 → 阻断/冻结/升级 MLRO。

交付建议：SOP 中写明"筛查点位"（pre/post）与日志字段。

Q329：如何处理"对手方 VASP 不在网络里/不配合"？
A：三层策略：

1. 白名单合作方优先（可交换信息）
2. 非合作方：限额 + EDD + 事后抽检
3. 高风险非合作方：拒绝或需 MLRO 特批

交付建议：维护"对手方 VASP 名单"与版本控制。

Q330：Travel Rule 与隐私/数据最小化冲突如何写？
A：写明：

- 仅收集必要字段
- 仅用于合规目的
- 加密、最小权限、留存期限
- 数据主体请求的处理边界（合规记录通常不得删除）

交付建议：把这一段放入《Data Governance Policy》并与 Travel Rule SOP 交叉引用。

Q331：Travel Rule 是否需要写入客户条款与披露？
A：必须。披露：你可能会收集并向对手方 VASP/供应商分享必要信息用于合规；客户不同意可能无法转账。

交付建议：披露要"可读"，并保留客户确认记录。

Q332：如何设置 Travel Rule 的"上线门槛（Go-live Gate）"？
A：建议门槛：

- 覆盖主要链与主要对手方
- 失败处置可运行（阻断/升级）
- 证据链可导出
- 演练至少一次（含失败场景）

交付建议：把门槛写入变更管理与产品上线流程。

Q333：如果你提供法币出入金，Travel Rule 与银行信息怎么衔接？
A：建立"法币-链上"统一案件视图：

- 法币入金来源信息 → 链上入金地址 → 链上风险评分 → 提币 Travel Rule 信息交换 → 法币出金受益人核验

交付建议：输出一张"端到端资金路径图"，便于银行尽调。

Q334：Travel Rule 是否影响提币时效？如何回应客户？
A：会影响。可递交写法：

- 高风险/信息缺失 → 延迟/人工复核
- 低风险/信息齐全 → 自动放行

交付建议：准备客户公告与客服话术，避免投诉升级。

Q335：Travel Rule 对 OTC/RFQ 模式也适用吗？
A：只要存在"可转移的虚拟资产转账"就要纳入你的 Travel Rule/信息收集与传递机制。

交付建议：把 OTC/RFQ 的对手方尽调写得更强。

Q336：Travel Rule 的审计抽样怎么做？
A：每月抽样：

- 成功交换的样本（验证字段齐全、回执存在）
- 失败样本（验证处置符合 SOP）
- 高风险样本（验证升级与 MLRO 决策）

交付建议：输出《Travel Rule QA Report》模板。

Q337：Travel Rule 与黑名单/拒绝名单如何联动？
A：对"持续拒绝交换信息/高失败率/反复异常"的对手方：加入限制名单，自动限额或拒绝。

交付建议：名单更新必须走审批与版本控制。

Q338：Travel Rule 供应商退出/替换如何做业务连续性？
A：必须有 Exit Plan：

- 数据迁移/销毁证明
- 替代方案（临时人工流程、限额策略）
- 切换演练计划

交付建议：把 TRP 视为"关键外包"，纳入 BCP/DR。

Q339：Travel Rule "最常见 10 个补件点"是什么？
A：

1. 场景拆分不清（VASP-to-VASP / unhosted）
2. 字段清单缺失
3. 失败处置不具体
4. 没有证据链（回执/日志）
5. 没写与制裁联动
6. 没有客户披露
7. 没有 QA/抽样
8. 没有供应商治理
9. 没有上线门槛
10. 没有 KRI 指标

交付建议：逐条补齐"制度条款 + 证据样例"。

Q340：Travel Rule 模块的交付式结尾怎么写？
A："本机构已建立涵盖 VASP-to-VASP 与 unhosted wallet 场景的旅行规则合规机制，包括信息采集、信息交换、失败处置、制裁联动、证据链留存与抽样复核；并通过关键外包治理与业务连续性预案确保机制稳定运行。"

第三十一部分｜监管问询 Round 2：更刁钻但必须答得"可审查"（Q341–Q360）

Q341：你如何证明 AML 不是"写在纸上"，而是"系统里跑起来"？
A：提交 3 类证据：

- 系统配置截图（规则阈值、限额、审批链）
- 日志/工单样例（命中→调查→结案）
- 月度/季度报告（KRI、STR 统计、整改闭环）

Q342：你如何避免"同名出入金"被第三方代付破坏?
A：写明：

- 原则：同名为主；
- 例外：必须 EDD + 关系证明 + MLRO/CO 审批 + 限额；
- 持续监控：第三方代付频次与关联网络识别。

Q343：你如何处理"稳定币出入金"的合规风险?
A：稳定币不等于低风险：要做发行方与储备透明度评估、链上风险、对手方风险、以及赎回/冻结风险披露。

交付建议：把"稳定币名单管理"纳入上币/资产准入制度（与平台上币类似逻辑）。

Q344：你如何处理"链上地址=客户身份"的关联证明?
A：采用地址所有权验证（签名/小额验证/冷静期），并记录验证证据；验证失败则限制出金或升级 EDD。

Q345：如果监控规则误报率很高，你怎么治理?
A：建立"误报治理机制"：

- 每月误报复盘（阈值、特征、例外）
- 规则调整走变更审批
- 调查资源与 SLA 触发扩容阈值

交付建议：提供"规则变更记录"。

Q346：你如何定义"异常行为"，并避免一线主观判断?
A：把异常行为参数化：

- 金额突增、频次突增、夜间集中、地址更换频繁、跨国频繁切换、与高风险类别地址关联等。

交付建议：异常必须触发工单，不允许口头放行。

Q347：你如何处理"客户拒绝解释链上来源"的灰区?
A：明确：拒绝解释/证据不足 → 限制出金/关闭账户 → STR 评估 → 记录保存。

Q348：你如何证明 MLRO 具备独立性与资源?
A：提供：岗位职责、汇报线（可直接向董事会/委员会）、资源配置、案件量统计、备份安排、培训与资格证明。

Q349：你如何处理"执法请求"与客户隐私冲突?
A：按《LE Request SOP》：合法性审查→最小披露→审批留痕→交付清单→是否通知客户（按法律限制）。

Q350：如果发生重大事件，你向监管报告的触发标准与时限是什么?
A：用事件分级矩阵写：

- 一级：资产风险/制裁相关/大规模泄露 → 立即升级与评估通报
- 二级：系统中断/监控失效 → 限时通报与整改

同时把"调查与复盘"纳入 CAPA。

Q351：你如何管理"关键外包"导致的 AML/Travel Rule 断点?
A：关键外包（KYC/TRP/链上分析/云）必须：SLA、事故通报、替代方案、退出计划、演练与年度复核。

Q352：你如何证明你了解并遵守 CIMA 对 Custodians / Trading Platforms 的持续义务?
A（递交级回答）：我们将 **Rule + Statement of Guidance** 的条款逐条映射到制度章节与证据链索引，并设定季度董事会监督与年度保证计划。

Q353：Phase 2 下申请 Licence 的材料装订逻辑是什么?
A：以 **Schedule 1A** 为主线，配套提交"完成并签署的 Licensing & Waiver Checklist"，并按清单编号装订、编号、归档。

Q354：REEFS（线上提交）对申请人意味着什么?
A：意味着你要把材料做成"结构化、可定位"的包：清单编号一致、附件可直接点开、版本可追踪，补件才能快速闭环。（CIMA 对新申请亦强调线上门户与清单提交口径。）

Q355：你如何避免"宣传口径"与"监管状态"不一致引发风险?
A：建立 Marketing SOP：

- 监管状态措辞白名单
- 合规审批留痕
- 重大变更（例如 Licence/Registration 状态变化）自动触发更新

交付建议：附 1 份"合规审稿记录样例"。

Q356：你如何证明"客户投诉机制"有效？
A：投诉台账 + SLA + 处理闭环 + 月度复盘 + 重大投诉升级董事会；并保留沟通证据。

Q357：你如何处理"高风险客户仍能通过"的质疑？
A：回答逻辑：不是一刀切拒绝，而是 **风险为本（RBA）**：高风险=强 EDD+强限额+强监控+更高审批层级；若无法满足证据→拒绝。

Q358：你如何证明"数据导出/截图"不会泄露客户信息？
A：最小权限 + 导出审批 + 水印/加密 + 审计日志 + 定期权限复核；并提供导出工单样例。

Q359：你如何处理"跨境展业"带来的牌照触发风险？
A：国家矩阵分层（A/B/C）+ geo-block + 营销排除 + 新国家上线审批（NPA + Legal check）+ 证据留痕。

Q360：本页 AML/Travel Rule 模块如何一键转成"递交版附件包"？
A（交付清单）：

1. AML Program（含 RBA、CDD/EDD、TM、Sanctions、STR、Training、Audit）
2. Travel Rule SOP（分场景 + 字段 + 失败处置 + 证据链）
3. Rule Library（规则卡）+ 命中样例
4. STR 台账 + MLRO 决策备忘录模板
5. Sanctions Hit Review Memo 模板
6. Evidence Index（对应清单编号）
7. 外包治理（TRP/KYC/Analytics）+ Exit Plan
   并按 Schedule 1A/Checklist 编号体系归档，便于审查与补件。

第三十二部分｜资本与审慎：怎么写"可解释、可审查、可持续"（Q361–Q380）

Q361：监管问"你的资本是多少"，你应该怎么回答才稳？
A（交付级结构）：

1. **资本水平**（数字）
2. **来源与到位证据**（出资证明、银行入账、审计/会计确认）
3. **资本用途与预算**（12–24 月运营成本覆盖）
4. **压力测试**（极端行情/盗币/银行通道中断）
5. **触发补充资本的阈值**（KRI：客户资产规模、交易量、事件发生等）

Q362：CIMA 对 custodian / trading platform 的"审慎关注点"主要是什么？
A：重点不是"形式资本"，而是：

- 是否能覆盖运营与安全风险（盗币/赔付/诉讼/罚款）
- 是否有可执行的风险治理（Rule + Statement of Guidance 的要求）

Q363：资本方案（Capital Plan）最低应包含哪些栏目？
A（可复制目录）：

- 基准情景财务模型（12/24 月）
- 压力情景（交易量下滑、手续费下降、黑天鹅事件成本）
- 流动性计划（现金管理、银行备用账户/备用 PSP）
- 资本补充机制（股东承诺/备用授信）
- 资本触发阈值与升级路径（提交董事会、限制业务、暂停上新）

Q364：监管可能会追问"你能承担盗币损失吗"？怎么写？
A：不要空口说"能"。写成"三层风险缓释"：

1. **预防**：门限签名、提币审批、对账闭环、监控规则
2. **侦测与响应**：IR/取证/冻结/协作流程
3. **财务缓释**：保险（如适用）/自留风险准备/赔付政策边界
   并声明"赔付取决于事实与条款，不做无限承诺"。

Q365：客户资产规模增长时，资本与风控如何跟着升级？
A：写明"规模触发升级表"：

- 客户资产 > X：增加冷存比例/提升门限/增强审计频率
- 日提币 > Y：增加人工复核/扩大监控团队
- 新链/新资产上线：必须完成 NPA + 安全评估 + AML/Travel Rule 评估

Q366：如何写"费用收入模型"以支持资本合理性？
A：把收入写清：交易费、提币费、托管费、上币费（如有）、做市返佣（如有）。
关键：上币费/返佣必须在**冲突管理**与**披露**下运行，避免被质疑"利益驱动上币"。

Q367：监管问"你是否挪用客户资产"，如何用制度证明"绝不"？
A（递交式）：

- 合同条款：客户资产归属
- 钱包与账务：客户分账/池化但可核对
- 内控：费用扣除授权与对账
- 审计：抽样核验
- 董事会监督：季度 safeguarding 报告
  （与 custodian / trading platform Rule 与 Guidance 的 safeguarding 原则一致。）

Q368：有没有"最低资本"固定数字？
A：CIMA 更强调风险为本与材料完整性（尤其 Phase 2 对托管/平台的许可要求）。你应避免对外宣传"固定最低资本=XX"这种过度简化表述；更稳的写法是：**按业务风险、客户资产规模与运营模型制定资本计划，并提供可验证到位证据**。

Q369：如何写"资金隔离账户/银行安排"才好过银行尽调？
A：写清 4 点：

- 公司自有资金账户 vs 客户资金账户（如涉及法币）
- 资金路径图（入金→对账→出金）
- 账户权限与审批链（双人复核）
- 备用通道（备用银行/PSP/限流策略）
  并准备《Bank DD Pack》。

Q370：财务报表与审计在 VASP licence 申请中怎么讲？
A：以"可审查"为目标：

- 财务预测与假设可追溯
- 费用预算覆盖合规、人力、安全、外包
- 若已有历史运营：提供审计/管理账与差异解释

  交付建议：把"预算—控制—实际—复盘"做成季度董事会固定包。

Q371：如何写"风险准备金/拨备"更像成熟机构？
A：按风险分类设准备金逻辑：

- 运营风险准备金（系统中断、外包事故）
- 合规风险准备金（审计整改、法律咨询）
- 安全风险准备金（应急响应、取证、第三方安全服务）
  并写"动用审批"。

Q372：监管追问"你是否能在极端行情维持服务"？
A：用 BCP/DR + 限流策略回答：

- 拥堵时提币延迟/分批

- 临时提高风控阈值
- 客户公告模板与投诉 SLA
- 系统扩容与应急值班
  （BCP 与重大事件处置要与 Rule/Guidance 的运营稳健性一致。）

Q373：如何把资本方案写进董事会治理?
A：写成"董事会每季度审批/复核":

- 资本充足与流动性
- 风险 KRI（提币、监控命中、投诉、外包事故）
- 重大事件与整改
- 新产品/新国家上线审批（NPA）

Q374：监管问"你为什么选择现在申请 licence"，怎么答?
A：答"因为 Phase 2 已生效，且我们提供 custody/VATP 服务"。并引用 CIMA 官方口径：自 2025-04-01 起，custody 与 VATP 必须取得牌照。

Q375：现有 registered person 转 licence 的"时间要求"怎么写?
A：CIMA FAQ 明确提到：Phase 2 生效后，相关主体需在规定窗口期内提交申请与 Schedule 1A 文件等（并会提供/要求相应清单）。

Q376：资本、保险、赔付政策三者关系如何写得不踩雷?
A：

- 资本：保证持续经营
- 保险：缓释特定风险（受条款限制）
- 赔付政策：按事实与合同条款处理，不承诺"无条件全赔"。

  交付建议：对外 marketing 禁止承诺性措辞。

Q377：监管问"你赚上币费会不会乱上币"，如何回应?
A：用上币治理回答：上币委员会、冲突声明与回避、风险评分表、持续监控与退市机制；费用披露透明且与决策隔离。

Q378：如何写"客户资产证明（Proof of Reserves）"?
A：若你要做 PoR：写清方法论、频率、覆盖范围、审计/第三方验证、客户理解提示（PoR≠无风险、≠保险）。

不做 PoR：写清替代控制（对账、审计抽样、治理报告）。

Q379：资本模块最终交付式结尾怎么写?
A："本机构以风险为本制定资本与流动性计划，确保在正常与压力情景下持续满足运营、合规与安全投入；并通过董事会监督、阈值触发机制与持续复盘，动态匹配业务规模与风险暴露。"

Q380：资本模块最常见补件点是什么?
A：

- 资本来源证据不足（SoF/SoW）
- 财务预测假设不可追溯
- 压力测试缺失
- 没有触发阈值与升级机制
- 与业务范围不匹配（说做托管却没预算安全与对账团队）

第三十三部分｜治理、IT、外包、BCP、Wind-down：监管收官刁钻题（Q381–Q400）

Q381：三道防线怎么写成"能落地"?
A：

- 第一线：业务与运营（执行 KYC、监控、客户沟通）
- 第二线：合规/风险（制定规则、抽检、审批、报告）
- 第三线：内部审计/独立评估（抽样验证与整改）
  并给出 RACI 表与例会机制（周/月/季）。

Q382：董事会/委员会 TOR（章程）最低要包含什么？
A：职责范围、会议频率、法定人数、决议机制、冲突回避、报告清单、升级机制、记录保存。

交付建议：至少设：风险/合规委员会、上币委员会、技术安全委员会（或同等职能）。

Q383：MLRO 独立性怎么证明？
A：汇报线可直达董事会/委员会；有资源与替代安排；STR 决策留痕；不受业务 KPI 绑架。

Q384：CO/MLRO/CTO 的"关键岗位备份"怎么写？
A：写"副职/代理"制度：触发条件（休假/离职/事故）、授权范围、交接清单、临时报告机制。

Q385：如何证明 IT 安全控制不是 PPT？
A：提供证据链：

- 权限矩阵（JML 流程）
- 日志与告警样例
- 渗透测试/整改闭环
- 钱包签名门限配置与变更记录
- 事故响应演练记录

Q386：外包清单（Outsourcing Register）最低字段有哪些？
A：供应商名称、服务范围、数据接触、关键性评级、SLA、审计权、分包限制、事故通报、退出计划、年度复核日期。
（与 Rule/Guidance 的外包与运营稳健性要求保持一致。）

Q387：监管问"你怎么防止供应商锁定（vendor lock-in）"？
A：写 Exit Plan：数据迁移/销毁、替代供应商、临时手工流程、切换演练、业务降级策略。

Q388：REEFS 门户提交意味着什么？
A：材料必须结构化、编号一致、可定位、版本可追溯；CIMA 已明确 VASP 相关申请通过 REEFS 路径与表单流程管理，并对表单版本有更新要求。

Q389：Licence 申请包怎么装订最像"专业交付"？
A：以 **Checklist 编号体系**为目录：

- 每个编号对应文件/章节
- 文件名含编号与版本
- Evidence Index 一页定位
  （CIMA 的 VASP Licensing & Waiver Checklist 明确要求按清单编号组织文件。）

Q390：监管问"你如何处理客户投诉与争议"，怎么答？
A：投诉台账 + SLA + 升级链（客服→合规→管理层）+ 复盘与纠正（CAPA）+ 重大投诉董事会汇报。

Q391：BCP/DR 最低要写哪些情景？
A：系统中断、链上拥堵、钱包供应商故障、KYC/TRP 故障、银行通道中断、数据泄露、关键人员不可用。
每个情景写：触发→应对→客户沟通→恢复→复盘。

Q392：Wind-down（有序退出）计划必须包含什么？
A：客户资产安全处置（提币窗口/通知）、业务终止时的交易处理、数据留存与隐私、员工与供应商退出、监管沟通与最终报告、第三方审计（如需要）。

交付建议：把 Wind-down 作为"随时可启用"的独立手册。

Q393：如何处理"资产冻结/执法协作"与客户权利？
A：写 LE Request SOP：合法性核验、最小披露、审批留痕、交付清单、保密与是否通知客户（依法处理）。

Q394：监管会问"你如何避免市场操纵"，最终怎么答？
A：用 Rulebook + Surveillance + Case Management + 处置闭环回答：

- 规则库、命中证据样例
- 案件台账（调查→结论→处置）
- 退市/限制/冻结/STR 机制联动

Q395：如何证明"上币治理"有效?
A：

- Token Risk Rating 表
- 上币委员会纪要与冲突声明
- 持续监控与退市演练
- 信息披露与客户确认留痕

Q396：监管问"你会不会把客户订单信息拿去自营套利"，怎么答?
A：若不做自营：明确禁止，并说明技术/制度如何防止（访问控制、日志审计、隔离墙）。
若做自营：必须写强披露、强隔离、强监督与审计验证——难度显著增加。

Q397：你如何管理"跨境营销触发当地牌照风险"?
A：国家矩阵 + geo-block + 营销排除 + 新国家上线审批（NPA + 法律评估）+ 留痕。

Q398：Phase 2 下"新申请"与"存量转换"路径有何差异?
A：新申请：若提供 custody/VATP，自 Phase 2 起应走 licence 轨；存量 registered person 若涉及 custody/VATP 则按 CIMA FAQ 口径在规定窗口期内提交 licence 申请与 Schedule 1A 文件等，并配套清单。

Q399：本 FAQ 如何直接转成"递交版最终包"?
A（交付式目录）：

1. Perimeter Memo（服务范围与定性）
2. AML Program + Travel Rule SOP + 规则库
3. Custody 手册（Key Governance、提币、对账、隔离）
4. VATP Rulebook + Surveillance + Listing/Delisting
5. Outsourcing Register + Exit Plan
6. BCP/DR + Incident Response + Wind-down
7. Board Pack（TOR、三道防线、季度报告模板）
8. Evidence Index（按 Checklist 编号）
   （Checklist 编号装订是"减少补件"的关键做法。）

Q400：一句话收官：监管最终要什么?
A：**清晰边界 + 可运行控制 + 证据链 + 治理监督 + 可持续资源**。
你写得再漂亮，没有证据链与运行闭环，也会被补件"打回重做"。

仁港永胜建议（唐生｜可执行清单）

1. **先定性再写材料**：先做《Perimeter Memo》把你到底是注册还是许可、是否涉及 custody/VATP 写死，并与系统事实一致。
2. **用 Checklist 编号倒推材料**：按 CIMA 的 **VASP Licensing & Waiver Checklist** 编号装订（文件名含编号+版本+日期），极大减少补件。
3. **Phase 2 项目化推进**：若涉及 custody/VATP，自 2025-04-01 起就是 licence 赛道，按 Schedule 1A/FAQ 口径准备。
4. **证据链优先于制度文本**：每章至少准备 3 份证据（权限矩阵/日志/工单/演练记录/对账样例）。
5. **把银行尽调当"第二监管"**：提前做 Bank DD Pack（资金路径图、AML摘要、证据链摘要、外包清单与退出计划）。
6. **上线门槛（Go-live Gate）写进制度**：Travel Rule、提币控制、对账闭环、监控规则库未达标不得上线。
7. **董事会要"看得懂、管得住"**：季度固定包（KRI、STR、投诉、外包、重大事件、整改闭环）+ TOR + 纪要留存。
8. **合规服务：**选择一间专业专注的合规服务商协助牌照申请收购及后续维护及合规指导尤为重要，在此推荐选择仁港永胜。

为何选择仁港永胜（核心优势）

- **交付级写法**：按监管清单/编号体系输出，可直接装订递交。
- **证据链思维**：不仅写制度，还把"截图/日志/工单/演练记录"做成可审查包。
- **全链路实操**：Perimeter 定性 → AML/Travel Rule → Custody/VATP 深水区 → Outsourcing/BCP/Wind-down → 董事会治理。
- **对接银行/审计/律所协同**：为尽调准备"可复用材料包"，减少多方重复劳动与口径冲突。

关于仁港永胜（香港）有限公司｜联系方式

我们仁港永胜在全球各地设有专业的合规团队，提供针对性的合规咨询服务。我们为受监管公司提供全面的合规咨询解决方案，包括帮助公司申请初始监管授权、制定符合监管要求的政策和程序、提供季度报告和持续的合规建议等。我们的合规顾问团队拥有丰富经验，能与您建立长期战略合作伙伴关系，提供量身定制的支持。

—— **合规咨询与全球金融服务专家** ——

公司中文名称：仁港永胜（香港）有限公司
公司英文名称：Rengangyongsheng (Hong Kong) Limited

我们专注于：

- 全球金融牌照与虚拟资产合规
- 多司法辖区持牌结构设计
- AML/CFT、IT、治理体系落地
- *监管沟通与长期合规支持*

服务覆盖：
香港｜毛里求斯｜欧盟｜英国｜中东｜离岸司法辖区

总部地址：
香港特别行政区西九龙柯士甸道西 1 号
香港环球贸易广场（ICC）86 楼
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

联系人： 唐生（唐上永，Tang Shangyong）

- 香港 / WhatsApp：+852 9298 4213
- 深圳 / 微信：+86 159 2000 2080
- 邮箱：Drew@cnjrp.com
- 官网：www.jrp-hk.com

来访提示：请至少提前 24 小时预约。
注：本文所涉模板、清单、Word/PDF 可编辑交付件，可向仁港永胜唐生有偿索取。

免责声明

1. 本 FAQ 为一般性合规研究与项目交付参考材料，不构成法律意见、审计意见或任何监管承诺。
2. 监管实践可能随法律修订、监管指引更新、个案事实差异而变化；具体申请策略与材料口径应以 CIMA 最新公开文件、REEFS 表单要求及个案沟通为准。
3. 任何对外宣传不得夸大"监管背书/保证获批/无限赔付"等内容；涉及客户资金与虚拟资产风险披露应以正式条款与适用法律为准。

—— 《**开曼 Cayman Islands VASP 虚拟资产服务牌照 FAQ Q1–Q400（实用交付版）**》——