《阿联酋•迪拜 UAE – Dubai VARA VASP 牌照 FAQ》

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生（唐上永，Tang Shangyong）提供专业讲解。
（本文定位：可直接用于客户说明、合规制度起草、申请材料编制与面谈答辩）

Virtual Assets Regulatory Authority（VARA）虚拟资产服务提供商（VASP）牌照

Dubai VARA Virtual Asset Service Provider (VASP) Licence Full Regulatory & Licensing Guide

Dubai VARA Virtual Asset Service Provider (VASP) Licence｜按业务活动分八大类
服务商：仁港永胜（香港）有限公司｜Rengangyongsheng (Hong Kong) Limited

牌照名称：阿联酋・迪拜 UAE – Dubai VARA牌照申请｜Dubai VARA License Application

✅ 点击这里可以下载 PDF 文件：阿联酋・迪拜 UAE – Dubai VARA 虚拟资产服务提供商牌照常见问题解答（FAQ）
✅ 点击这里可以下载 PDF 文件：阿联酋・迪拜 UAE – Dubai VARA 虚拟资产服务提供商牌照申请注册指南
✅ 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）。

A. 监管边界与适用范围（Q1–Q15）

Q1：VARA 管的是整个阿联酋的虚拟资产吗？还是只管迪拜？

A（交付级）：
VARA 的监管边界是 **"迪拜酋长国内（Dubai Emirate）"** 的虚拟资产及相关活动监管（覆盖迪拜的自由区与大陆），但**不包括 DIFC（Dubai International Financial Centre，迪拜国际金融中心）辖区**。因此判断第一步永远是：**业务实体注册地/经营地是否在 DIFC**；若在 DIFC，通常走 DIFC/DFSA 体系，而非 VARA。

Q2：什么叫 "VASP / VA Activity"？是不是只要碰到加密就算？

A：在 VARA 框架下，监管关注的是你是否提供**特定"持牌活动（Licensed Activities / VA Activities）"**，而不是你是否"提到加密"。例如：顾问、经纪、托管、交易所、借贷、资管投资、转移与结算等都属于需明确申请的活动类别。

Q3：在迪拜做加密业务，是否"必须"拿 VARA 牌照？

A：只要你在 VARA 辖区内从事 VARA 定义的 VA Activities，就应按其许可体系取得相应授权/牌照，否则属于未授权经营风险。实务上（银行开户、支付通道、托管/流动性合作）也会将"VARA 授权状态"作为硬门槛。

Q4：DIFC、ADGM、RAK DAO 与 VARA 有什么关系？能互认吗？

A：这是 UAE "多监管区并存"格局：

- **VARA：迪拜（除 DIFC）**
- **DIFC/DFSA：DIFC 金融自由区**
- **ADGM/FSRA：阿布扎比 ADGM**
  不同区**不自动互认**。你在 ADGM/DFSA 持牌不等于在 VARA 辖区可直接展业；反之亦然。对外营销必须清晰写明"在哪个监管区、哪类授权、可做哪些活动"。

Q5：我们是海外公司，没有迪拜实体，但网站给迪拜客户用，需要 VARA 吗？

A：需要做"监管触达/经营事实"评估：是否在迪拜**主动招揽/营销**、是否有本地团队/办公室、是否向迪拜居民提供服务、是否在迪拜设立经营实体或与自由区/DET 建立许可关系。交付建议：出具**Regulatory Perimeter Memo（监管边界备忘录）**，把"触达行为、客户范围、签约主体、收付款路径、服务器与运营团队所在地"逐项论证，避免被认定为在辖区内经营。

Q6：VARA 的 Rulebooks 是什么？必须全部遵守吗？

A：VARA 规则采用"**总则 + 通用强制规则书 + 活动规则书**"结构：

- Regulations 2023（监管框架总则）
- **Compulsory Rulebooks（强制适用）**：Company / Compliance & Risk Management / Technology & Information / Market Conduct
- **Activity Rulebooks（按你申请的活动适用）**：Advisory、Broker-Dealer、Custody、Exchange、Lending & Borrowing、VA Management & Investment 等
  只要你获 VARA 许可并从事相应活动，就必须符合对应 Rulebooks。

Q7："VASP 可以一次申请多个活动吗？还是一个活动一张牌？"

A：VARA 官方明确：VASP **可以申请多个活动并在一个总体许可下聚合**；但**涉及 Custody（托管）时会有更严格的独立性/隔离要求**（例如治理独立、或与其他活动的防火墙、甚至要求证明"arms-length association"）。因此"多活动组合"是可行的，但托管属于高敏感活动，组合结构要谨慎设计。

Q8：VARA 的"持牌活动"具体有哪些？

A：VARA FAQ/页面公开列示的活动类别包括（以官方清单为准）：

- VA Advisory Services（顾问）
- VA Broker-Dealer Services（经纪/交易撮合类中介）
- VA Custody Services（托管）
- VA Exchange Services（交易所）
- VA Lending and Borrowing Services（借贷）
- VA Management and Investment Services（资管/投资管理）
- VA Transfer and Settlement Services（转移与结算）
- VA Issuance（发行相关，含规则书/类别）
  申请时必须逐项勾选与满足该活动 Rulebook 要求。

Q9：我们只做"营销/社群/教育内容"，不碰客户资产，是否一定不需要牌照？

A：不一定。关键是你是否落入"受规管活动的实质提供"：例如是否提供投资建议、是否促成交易、是否代表客户下单、是否介绍并收取成功费/返佣、是否提供交易功能入口。交付建议：把"内容与行为"按活动定义逐条对照，必要时在对外材料里加入合规声明与地域限制。

Q10：我们做"钱包软件（非托管）"，用户自持私钥，还要 VARA 吗？

A：要看是否构成 VARA 下的"Custody / Transfer & Settlement / Exchange" 等活动：

- 纯"非托管软件工具"一般监管压力较低；
- 但只要你介入**交易执行、转移结算、代签名、托管、或提供法币出入金通道**，就可能落入牌照边界。
  交付建议：做"**Custody touchpoints**（托管触点）"清单：谁持私钥、谁能单方转移、谁能冻结、谁能恢复、谁能更改提币地址。

Q11：VARA 规则与 FATF Travel Rule 有什么关系？

A：VARA 的合规风控体系通常会要求 VASP 将 AML/CFT 与跨境金融安全作为核心原则，并在合规与风险管理规则书体系下落地（尤其是交易监控、可疑活动上报、客户尽调、记录保存、外包与技术控制等）。具体 Travel Rule 落地通常体现为：客户信息采集、交易附带信息传递、对接合规供应商与留存审计证据。

Q12：VARA 与 UAE 联邦 AML 法体系如何衔接？

A：实务上 VASP 在迪拜落地 AML/CFT 时，需要同时满足：VARA 的规则书要求 + UAE 联邦层面的 AML/CFT 法规框架（以及相关监管部门的通用期望）。交付建议：以 VARA Rulebooks 为主线，把联邦 AML 要求嵌入 KYC/EDD、交易监控、制裁筛查、记录保存与 STR/报告流程。

Q13：做 RWA（现实资产代币化）/证券型代币（STO）在 VARA 下如何定位？

A：要区分：

- 是否属于"虚拟资产发行（VA Issuance）"范畴；
- 是否触及证券/资本市场属性（可能同时触及其他监管框架）；

- 是否涉及托管/交易所/经纪等二级市场活动。
  交付建议：先出具"Token Classification Memo（代币分类备忘录）"，再确定申请的活动组合与披露/市场行为控制要求。

Q14：我们计划只服务机构客户（Professional/Institutional），合规会更简单吗？

A：不会"更简单"，而是"不同"。机构业务的监管关注点往往更聚焦：市场完整性、冲突管理、做市/自营边界、披露与报价公平性、托管控制、以及系统韧性。你仍需要完整的治理与证据链。

Q15：一页总结"是否需要 VARA 牌照"的判断方法？

A：交付级四步法：

1. **地域**：是否在迪拜（除 DIFC）经营/招揽？
2. **活动**：是否属于官方列示的 VA Activities？
3. **触点**：是否触碰客户资产/交易执行/转移结算/报价撮合？
4. **对外事实**：网站/APP/营销/合同/收付款路径是否指向迪拜客户？
   满足 1+2，通常就进入牌照路径；有争议则做监管边界法律意见。

B. 牌照类型、申请路径与阶段（Q16–Q35）

Q16：VARA 的申请起点是什么？是先注册公司还是先申请牌照？

A（交付级）：VARA 官方"Licence Applications"页面明确：**第一步通常是向 DET（Dubai Economy & Tourism）或相关 Free Zone 提交 IDQ（Initial Disclosure Questionnaire）**；之后按要求补充文件（含商业计划、UBO 与高管信息），并缴纳进入审查的初始费用（通常为许可申请费的 50%）。因此路径常见是：先确定落地实体/自由区或大陆许可载体 → 提交 IDQ → 进入 VARA 审查。

Q17：IDQ 一般会问什么？我们要准备哪些信息才"RFI-ready"？

A：交付建议把 IDQ 当成"监管尽调提纲"，至少准备：

- 业务模式：活动组合、目标客户、产品流程图
- 组织架构：股权穿透、UBO、董事会与高管简历
- 合规体系：AML/KYC、制裁、交易监控、投诉处理、记录保存
- 技术体系：钱包架构、密钥管理、数据安全、灾备
- 财务与资本：资金来源、预算、压力测试
  做到这些，后续补件（RFI）会显著减少。

Q18：VARA 申请是否有"分阶段（如 MVP/FMP）"的概念？

A：市场上确实存在"分阶段许可/逐步开放"的讨论与实践（如历史上的 MVP 概念、以及 Full Market Product 的推进），但对外交付时建议以 VARA 官方当期申请页面与规则书要求为准，并把"阶段性要求/试运营限制"作为条款化内容写进商业计划与上线路线图。

Q19：我们能不能先拿到"原则性批准"再找银行/托管合作？

A：实务上通常是"相互促进"：你需要银行/托管/支付伙伴来证明可运营与资金隔离；伙伴又需要你展示监管路径与进度。交付建议：

- 先做"合规能力包"（制度摘要+系统架构+控制证据）
- 同步推进 IDQ 与伙伴尽调
- 用阶段性材料（draft policies、技术方案、董事会决议）换取合作方有条件支持函。

Q20：申请周期一般多久？

A：周期高度取决于活动组合（托管/交易所更复杂）、材料质量与 RFI 往返次数。官方页面没有给固定天数承诺，交付建议采用项目管理法：以"里程碑+补件缓冲"排期，而不是用单一月份承诺客户。

Q21：申请费怎么理解？为什么说"通常先付 50%"？

A：VARA 官方说明：申请审查开始前通常需要支付初始费用，**通常为许可申请费的 50%**，以启动审查流程。交付建议把费用拆为：政府/监管费用 + 自由区/DET 费用 + 合规审计/测试费用 + 系统与外包成本四类预算池。

Q22：VARA 是否允许一家公司持多个活动？会不会要求分公司/隔离？

A：VARA 允许多个活动聚合在一个总体许可下，但明确提示：**托管相关活动可能需要隔离与独立治理**（例如与交易所/经纪的利益冲突隔离、权限隔离）。交付建议在组织架构上预留：托管子公司/独立董事/独立风控签名权的方案。

Q23：哪类活动是"高难度/高成本"的？

A：一般而言（按监管审慎与市场风险）：

- **Custody（托管）**：私钥控制、资产隔离、对账与审计、冷/热钱包治理
- **Exchange（交易所）**：市场完整性、撮合与公平、操纵监控、资产隔离、技术韧性
- **Lending & Borrowing（借贷）**：对手方风险、抵押品管理、清算机制、流动性风险
  交付策略通常是：先定商业边界，再选择"活动组合最小闭环"。

Q24：VARA 申请是否要求本地实体、办公室与人员？

A：VARA 规则书整体强调治理、责任与可监管性，实务上通常需要在迪拜建立可被监管触达的实体与"实质运营能力"（人员、办公、可审计系统与记录）。交付建议把"Substance（实质）"作为商业计划的单独章节说明。

Q25：董事、高管、RO/MLRO 的适当人选（Fit & Proper）要怎么证明？

A：交付包至少包含：

- 履历与资格证明（教育、从业经验、监管/合规背景）
- 无犯罪/无破产/无重大合规不良记录声明
- 利益冲突披露与回避机制
- 职责说明书（Job Description）与 KPI
  并在公司治理规则与合规风控规则书框架下形成证据链。

Q26：是否必须设立 MLRO、合规负责人、风险负责人、内审？

A：在 VARA 的合规与风险管理框架中，合规与风险管理是核心支柱；是否要求独立内审/独立审查通常取决于规模与风险，但"第二道防线（合规/风险）"与"可独立复核机制"是常见监管期望。交付建议采用"三道防线"写法并匹配岗位与外包方案。

Q27：申请材料中"最容易被 RFI 追问"的部分是什么？

A：Top 7：

1. 股权穿透与 UBO 资金来源（SoF/SoW）
2. 业务流程是否真实可运行（而非 PPT）
3. 客户资产隔离与对账机制
4. KYT/交易监控规则与告警闭环
5. 钱包/密钥/签名治理（托管尤其关键）
6. 外包治理与退出计划
7. 灾备与事件响应（含演练证据）

Q28：我们没有历史运营记录，是不是更难？

A：不必然，但需要更强"可运行证明"：系统演示脚本、控制点配置、模拟工单、对账报表模板、演练记录（可用桌面演练）与关键人员到岗计划。

Q29：是否可以"先拿某个轻量活动牌照，再升级到交易所/托管"？

A：可以作为策略，但必须诚实披露路线图，并确保当前牌照范围内不"变相开展高风险业务"。交付建议把升级路径写成：阶段目标、控制增强清单、资本与人员增强计划。

Q30：VARA 会看我们用什么交易系统/钱包系统吗？

A：会关注"技术与信息控制是否满足规则书要求"：访问控制、日志留存、变更管理、漏洞管理、灾备等。系统是自研或外包不是核心，核心是：你是否能证明"安全、可控、可审计"。

Q31：是否必须做渗透测试/安全审计？

A：在 Technology & Information 与整体风险控制期望下，渗透测试、漏洞扫描、复测与报告通常是合规交付的重要组成。交付建议：把"测试—修复—复测—证据归档"固化为年度制度。

Q32：VARA 对营销/广告有什么要求？

A：市场行为规则书（Market Conduct）通常会对营销、披露、客户协议、投诉处理、投资者分类等提出要求。交付建议：建立"营销素材审批机制 + 禁止收益承诺清单 + 风险披露模板"。

Q33：客户协议（Terms）需要覆盖哪些要点？

A：至少覆盖：费用、风险披露、订单执行与滑点、托管与资产隔离说明、冻结/限制服务条件、投诉机制、数据使用与留存、争议解决、以及对第三方风险（外包/链上拥堵/稳定币脱锚）的披露。

Q34：VARA 规则书是否会更新？我们如何保持"最新合规"？

A：VARA Rulebooks 会发布更新与版本迭代（官方 Rulebooks 站点提供更新入口与文本）。交付建议：建立"规则更新雷达"：每月检查更新、影响评估、制度修订、员工培训、系统变更与证据归档。

Q35：一页总结申请路径？

A：选落地载体（DET/Free Zone）→ 提交 IDQ → 补充材料（BP/UBO/管理层/体系）→ 通常先付 50% 费用进入审查 → RFI 往返与系统演示 → 取得相应活动许可并持续合规。

C. 资本金、审慎监管与财务可持续（Q36–Q50）

Q36：VARA 是否有最低资本金要求？

A（交付级）：有。VARA Rulebook 中存在按活动划分的资本与审慎要求口径，通常采用"**固定金额门槛 vs 固定年度开支比例** 取其高者"的结构（不同活动不同）。例如在公开页面可见：Custody、Exchange、Lending & Borrowing 等活动有对应的最低资本计算方式。

Q37：最低资本是一次性存进去就行吗？

A：不建议这样理解。监管与银行更看重"持续满足"与"可持续经营证明"：现金流预算、压力测试、运营资本阈值、事故准备金、以及不得挪用客户资产。资本是底盘，不是摆设。

Q38：资本计算里的 "fixed annual overheads（固定年度开支）"怎么准备证据？

A：交付建议：预算表（按月）+ 合同与报价（办公室、人员、系统、审计、法律、KYT/KYC）+ 董事会批准记录。并将开支与活动规模绑定，避免低估导致资本不足。

Q39：交易所与托管组合时资本要求会叠加吗？

A：通常会按"最高风险/最高门槛"或按监管审查口径综合评估，且托管可能要求更严格的隔离治理。交付策略：在申请前做"资本与活动组合测算表"，向监管呈现审慎规划。

Q40：是否需要客户资产保险或托管保险？

A：不是所有情况下都"强制"，但作为高等级风险缓释措施会显著增强监管与合作方信任。交付要点：覆盖范围、免赔额、理赔流程、除外责任，不得夸大"全额兜底"。

Q41：VARA 对客户资产隔离有什么核心期望？

A：交付标准：

- 法币资金与公司运营资金分离（专户/备付安排）
- 数字资产钱包地址与权限分层（客户池 vs 运营池）
- 每日对账与差异闭环
- 提币审批分权与留痕
  托管/交易所场景尤为关键。

Q42：能否用 Proof of Reserves（PoR）替代审计？

A：不能替代。PoR 是加分项，审计/独立审查关注的是控制有效性、治理、记录保存与可取证性。

Q43：VARA 会不会要求我们证明资金来源（SoF/SoW）？

A：实务上属于高频要求：UBO 注资路径、银行流水、股权结构穿透、以及对资金"可解释性"的证明。交付建议：SoF/SoW 资料包 + 资金路径说明信。

Q44：如果股东资金来自加密资产出售/交易，怎么准备更稳？

A：需要更强证据链：链上交易证明、对手方信息、交易所出入金记录、税务与法律意见（如适用）、以及反洗钱来源解释。目标是"可审计、可复核、可解释"。

Q45：我们如何证明"持续经营能力"？

A：交付建议：12–24 个月现金流预测 + 压力测试情景（币价暴跌/挤兑/通道中断）+ 成本削减预案 + 追加注资承诺（如有）+ 董事会应急决议模板。

Q46：是否需要建立"运营资金最低阈值"？

A：建议必须。低于阈值触发：暂停扩张/削减成本/增资/限制某些高风险活动。把阈值写进治理制度与管理层 KPI。

Q47：客户法币出入金（bank/PSP）失败率高会影响合规吗？

A：会影响运营风险、投诉风险与欺诈风险。交付建议：通道监控指标（失败率/拒付率/平均处理时长）+ 异常处置SOP + 高风险代付拦截规则。

Q48：借贷业务的"流动性风险"如何交付？

A：必须形成制度：抵押品管理、强平机制、极端行情熔断、对手方集中度限制、风险准备金、以及客户披露。并做压力测试并归档。

Q49：交易所做市/自营会触发更高资本或更严治理吗？

A：通常会显著增加市场操纵与冲突风险，监管会更关注：做市账户隔离、信息隔离、价格公平、监控规则、以及披露。资本是否上调取决于活动与风险评估结果。

Q50：资本与审慎监管一句话结论？

A：资本不是数字，是一套"可持续经营证明"：预算 + 压测 + 阈值 + 预案 + 证据链。

D. AML/CFT、KYC/EDD、制裁与交易监控（Q51–Q65）

Q51：VARA 对 AML/CFT 的核心要求在哪个规则书？

A：核心落在 **Compliance and Risk Management Rulebook** 及其与 Regulations 2023 的衔接要求上（适用于所有获许可 VASP）。交付时应以该规则书为主线，形成 AML 程序、风险评估、监控与报告闭环。

Q52：KYC 要做到什么程度才算"可交付"？

A：交付最低标准：

- 客户分类（零售/专业/机构）与风险评分模型
- 身份核验与活体/反欺诈
- 受益所有人识别（机构客户）
- EDD 触发条件与证据清单
- KYC 更新与再认证机制
- 记录留存与可导出审计包

Q53：制裁筛查要覆盖哪些？

A：至少覆盖：客户姓名/别名、UBO、董事高管、受益人、交易对手（如可得）、钱包地址（链上制裁/高风险地址），并保留"命中—复核—处置—关闭"工单证据。

Q54：链上监控（KYT）一定要买吗？可以靠人工吗？

A：规模化业务不建议靠人工。交付建议采用"工具+人工复核"组合：工具负责地址风险评分与模式识别，人工负责 EDD 与结论留痕。监管与合作方更看重持续性与一致性。

Q55：什么情况下必须做 EDD?

A：常见触发：高风险国家/行业、PEP、制裁相关、异常交易模式、短期大额入金/出金、混币器/暗网关联、以及地址风险评分高。交付应把触发阈值写进制度并在系统可配置。

Q56：交易监控要监控哪些典型场景?

A：至少 12 类：分拆/聚合、快速进出、异常时间段交易、地址跳转链、同设备多账户、刷量/对敲、异常滑点套利、与高风险地址交互、可疑代付、拒付高发、异常 API 调用、以及"冻结后再尝试"行为。

Q57：STR/可疑活动报告流程要怎么写成"可交付制度"?

A：交付标准：告警→调查→EDD→MLRO 决策→（必要时）报告/协作→记录归档→规则更新。每一步有负责人、SLA、证据编号与升级条件。

Q58：记录保存要多久?

A：记录保存期限需结合 VARA 规则书与 UAE AML 法规的一般要求进行制度化（不同记录类型可能不同）。交付建议：统一设定最低保存期限并分类管理（KYC/交易/告警/审批/日志/培训/外包），确保可检索与可导出。

Q59：我们只做机构客户，还需要同样严格的 AML 吗?

A：机构客户不等于低风险。反而需要更强的 UBO 穿透、资金来源解释、对手方尽调与交易模式合理性证明。交付上仍要完整 AML 程序。

Q60：如何避免"AML 做了但证据链不全"?

A：用工单系统固化闭环：每个告警必须有调查笔记、结论、附件、审批与关闭原因；抽样能复盘就是合规。

Q61：高风险客户能不能不做?

A：可以"拒绝/退出客户"，但必须制度化：拒绝标准、记录保存、可解释原因与复核机制。拒绝不是随意，而是合规策略的一部分。

Q62：如何处理客户要求快速提币，但风控拦截?

A：交付话术与流程：解释触发规则（不泄露细节）、要求补充材料、设定复核 SLA、必要时冻结并升级 MLRO。全程留痕。

Q63：如何对接银行/PSP 的 AML 尽调?

A：提供"AML 能力包"：风险评估摘要、KYC/EDD 流程、制裁与 KYT 工具、告警 KPI、培训记录、独立审查/测试报告、以及事件响应机制。

Q64：AML 体系中最常见的失败点是什么?

A："制度和系统不一致"：制度写了 EDD 触发，但系统没规则；制度写了工单闭环，但没有证据；制度写了制裁筛查，但未覆盖 UBO/地址。

Q65：本模块一句话总结?

A：AML 的交付本质是"可验证证据链"：可抽样、可复算、可导出、可复盘。

E. 市场行为、营销合规、投诉与投资者保护（Q66–Q80）

Q66：Market Conduct Rulebook 主要管什么?

A（交付级）：市场行为规则书通常覆盖：营销与披露、客户协议、投诉处理、投资者分类、透明度与市场完整性相关要求等。交付建议：把对外传播（网站/社媒/销售话术）纳入合规审批。

Q67：我们能不能宣传"持牌、合规、安全、零风险"?

A：可以宣传"已获授权/申请中（如实）"，但禁止夸大或误导。**"零风险、保本、保证收益、政府背书"**属于高风险表述。交付建议：建立"禁用词清单 + 风险披露模板 + 素材审批流程"。

Q68：客户分层（零售 vs 专业）为什么重要？

A：它决定：适当性、披露深度、杠杆/衍生品可否开放、风险提示与冷静期等控制。交付建议：把客户分层与权限矩阵绑定到系统。

Q69：费用披露要做到什么程度？

A：交付标准：费率表（交易费/提币费/点差/融资费/托管费）+ 计算示例 + 费率变更通知机制 + 费率配置留痕。抽样订单能复算。

Q70：OTC 点差如何避免纠纷？

A：披露报价基准（指数/多源中位价/自有库存成本）、锁价时间、失效条件、异常行情处理（熔断/暂停报价），并保留客户确认记录。

Q71：滑点/插针/断线导致亏损，平台怎么自证？

A：交付证据：撮合日志可复算、系统监控与告警、事故时间线、参数变更记录、以及对客户的披露与补偿政策（如适用）。

Q72：投诉机制最低要包含哪些？

A：渠道、分级、SLA、证据留存、处理闭环、复盘整改、以及向管理层/董事会的定期汇总。投诉数据是监管与合作方极关注的运营指标。

Q73：如何避免客服承诺"越权"？

A：交付建议：客服话术库 + 禁止承诺清单（不可承诺收益/不可承诺即时放行/不可泄露风控规则）+ 抽检与问责机制。

Q74：市场操纵与刷量，VARA 会查吗？

A：交易所/经纪类业务必须具备市场监控能力：对敲、刷量、关联账户操纵、异常成交集中度等。交付上需形成监控规则库与处置记录。

Q75：我们做做市，怎样避免利益冲突？

A：账户隔离、信息隔离、风控隔离、做市策略的合规边界、披露与审批、以及对异常交易的独立监控。最好形成董事会批准的冲突管理政策。

Q76：客户资产损失（黑客/误转），平台要怎么处理才"合规"？

A：交付级：事件响应预案（止损、取证、通报、客户沟通）、责任认定流程、赔付政策（若有）、以及控制改进与复测证据。

Q77：如果我们暂停提币，会被认为违规吗？

A：关键看是否有明确触发条件（安全/合规/链上拥堵/通道故障）、是否有客户条款支持、是否公平对待客户、是否有公告与工单证据。暂停本身不是原罪，"无制度、无证据、无沟通"才是风险。

Q78：如何把营销、市场、合规三方协作做成制度？

A：交付机制：Marketing Compliance SOP（发起→合规审阅→法律审阅→审批→发布→留档→抽检）。并建立版本控制与撤稿机制。

Q79：我们是否需要对外提供"合规披露页"？

A：强烈建议。栏目固定化：授权状态（如实）、费用表、风险披露、投诉渠道、反欺诈提示、隐私与数据政策、重大公告与更新日志。

Q80：本页总结？

A：市场行为合规的核心是：不误导、可披露、可复算、可追责。

F. 技术与信息控制（Technology & Information）总框架（Q81–Q105）

Q81：VARA 对"技术合规"最核心的关注点是什么？

A（交付级）：核心不是你用什么系统，而是你是否具备 **可控、可审计、可恢复、可防护** 的技术治理：访问控制、日志留存、变更管理、漏洞管理、数据保护、BCP/灾备、事件响应与取证能力。交付上要把"规则要求"映射到"系统控制点"和"可导出证据"。

Q82：Technology & Information Rulebook 通常覆盖哪些模块？我们要交付哪些制度？

A：通常包括：信息安全治理、身份与访问管理（IAM）、系统开发与变更、基础设施与云安全、数据治理、网络安全监测、业务连续性与灾备、第三方/外包技术风险、日志与取证。交付建议形成"12件套制度"：ISMS 总纲、访问控制、密钥管理（如适用）、变更管理、漏洞管理、日志与留存、数据分类与加密、BCP/DR、事件响应、供应商安全、渗透测试与复测、权限审计与复核。

Q83：我们需要 ISO27001 才能申请吗？

A：不一定"强制"，但监管与银行/合作方往往把 ISO27001、SOC2、或等效控制框架视为强加分项。交付策略：即便不认证，也要采用同等结构输出控制：资产清单、风险评估、控制实施、审计与管理评审记录，让监管看到"体系化治理"。

Q84：云部署可以吗？VARA 会不会要求本地机房？

A：云可行，但必须证明：数据安全、访问控制、密钥治理、日志留存与导出、灾备切换、供应商审计权与监管配合义务。交付建议：输出"Cloud Security Pack"：云架构图、网络分段、加密与KMS、权限矩阵、日志方案、BCP 方案、以及供应商合同条款摘要。

Q85：系统访问控制最低要做到什么程度？

A：至少做到：最小权限（least privilege）、基于角色的 RBAC、关键操作强制 MFA、特权账号（admin）独立管理、定期权限复核、离职即刻回收。并形成"权限变更工单+审批链+导出报表"证据。

Q86：开发与上线（SDLC/DevSecOps）要怎么写成可交付？

A：交付级写法：需求→安全评审→代码审查→测试（含安全测试）→上线审批→上线后监控→回滚方案→复盘记录。关键点：每次版本发布都能导出"变更单、审批链、测试报告、上线记录、回滚演练证据"。

Q87：渗透测试（PenTest）要做到什么频率？

A：交付建议：年度渗透测试 + 季度漏洞扫描；高风险变更（钱包/签名方案/撮合引擎/核心权限体系）上线后必须复测。每次测试必须闭环：发现→修复→复测→风险接受（如确需）→董事会/管理层批准。

Q88：漏洞管理（Vulnerability Management）怎么证明"有效"？

A：不是"做一次扫描"。要有 SLA：严重漏洞 24–72h、重大漏洞 7–14d 等；同时保留工单证据：漏洞编号、影响范围、修复提交、复测截图/报告、上线时间、残余风险说明。

Q89：日志要留哪些？留多久？如何做到"不可抵赖"？

A：至少留：登录/权限变更、关键参数变更、订单/撮合/成交、钱包签名与提币审批、风控拦截、告警工单、数据导出与访问。交付建议：采用"集中日志 + 哈希固化/防篡改存储 + 访问审计"，并定义留存期限与检索SLA，确保抽样可复算。

Q90：数据分类与加密要做到什么程度？

A：交付建议三类：公开数据/业务数据/敏感数据（含KYC、密钥材料、钱包地址关联、交易监控结论）。敏感数据必须：传输加密、静态加密、访问最小化、密钥轮换与访问日志；并输出"数据字典+分类标记+访问矩阵"。

Q91：KYC 数据/身份文件能否外包给第三方 KYC Provider？

A：可以，但要满足外包治理：尽调、合同审计权、数据保护条款、跨境传输合规、退出与数据返还/销毁机制。交付建议：形成"供应商准入评分表 + 年度复核模板"。

Q92：VARA 是否会要求我们证明"数据在什么国家存储"？

A：可能会问，尤其当涉及跨境数据传输或敏感数据托管在境外。交付建议：准备"Data Residency & Flow Map"：数据从采集、处理、存储、备份、访问、导出到销毁的全链路图。

Q93：灾备（DR）要做到什么标准才算可交付？

A：至少明确：RTO/RPO、主备架构、备份频率、演练计划、切换步骤、演练结果与复盘整改。并输出"半年/年度演练报告 + 证据截图 + 复测记录"。

Q94：事件响应（Incident Response）制度必须包含哪些？

A：最小 8 要素：事件分级、响应角色（含负责人/联络人）、止损与隔离、证据保全、客户沟通、监管沟通、恢复与复测、复盘与整改闭环。交付建议：附"事件时间线模板、取证清单、公告模板"。

Q95：如果发生黑客盗币，监管会问什么？

A：会问：资产是否隔离、密钥是否被单点控制、提币审批是否失效、日志能否复盘、是否及时止损与通报、损失范围与客户保护、根因与控制改进。交付要点：把"事故复盘报告"做成可审计文档（含证据编号）。

Q96：是否必须有 SOC（安全运营中心）？

A：不必然要求"自建 SOC"，但必须有持续监控能力：告警收集、关联分析、升级与处置闭环。交付建议：小团队用 MSSP（托管安全服务）+ 自己的响应制度，也可达到可监管标准。

Q97：我们如何向 VARA 证明"系统不是纸面"？

A：用演示脚本：KYC→权限→下单→撮合→风控拦截→提币审批→链上监控→告警工单→对账报表→日志导出。监管看到"可运行、可追溯、可复算"才算过关。

Q98：系统与合规制度经常不一致，怎么避免？

A：做"控制映射表（Control Mapping）"：每条制度要求对应一个系统控制点、一个报表、一个证据文件。任何制度更新必须触发系统配置检查与回归测试。

Q99：能否用"截图+说明"替代系统导出？

A：只靠截图风险很高。交付建议：截图用于解释，证据以"系统导出（CSV/PDF）+日志条目+工单记录"作为主证明，确保可抽样复核。

Q100：第三方审计/独立评估是否必要？

A：强烈建议。尤其是交易所/托管/借贷等高风险活动：独立审查可显著提升监管、银行和机构客户信任。交付建议：年度独立审查 + 重大变更后专项评估。

Q101：我们要建立"技术合规年度计划"吗？

A：建议必须。计划包含：渗透测试、漏洞扫描、权限复核、BCP演练、外包复核、日志抽检、数据最小化审查、密钥轮换（如适用）、以及培训。

Q102：合规与技术团队如何分工才符合"三道防线"？

A：第一道：工程/运维负责控制实施；第二道：合规/风险负责规则、监督与抽检；第三道：内审/独立审查负责有效性评估。交付要点：每道防线都有记录与整改闭环。

Q103：VARA 会不会要求"源代码审计"？

A：不一定常态，但在重大事件或高风险模块（钱包签名、撮合、清算）可能要求更深审查。交付建议：对关键模块保留代码审查记录、测试报告与版本控制证据。

Q104：技术外包最常见的失败点是什么？

A：四个：没有审计权、无法导出数据、退出不可控、事故通报不及时。交付时必须把这些写进合同并能展示执行证据。

Q105：本模块一句话结论？

A：技术合规的交付标准是：能演示、能导出、能复盘、能切换、能问责。

G. 托管（Custody）、钱包与密钥治理（Q106–Q135）

Q106：什么情形会被认定为"提供托管（Custody）"？

A（交付级）：核心判断是：你是否能控制或影响客户虚拟资产的转移/处置（例如持有私钥/助记词、代签名、可单方冻结或转移、可恢复密钥并转走资产）。即便你不称自己为托管，只要具备上述控制触点，就可能落入 Custody 活动许可边界。

Q107：托管与交易所/经纪放在同一公司可以吗？

A：VARA 允许多活动组合，但明确提示托管可能需要更严格的独立性与隔离（例如治理独立、防火墙、独立风险签名权）。交付建议：采用"托管独立治理包"：独立负责人、独立审批链、独立报表与对账、独立密钥控制与监控。

Q108：冷热钱包比例怎么定才合理?

A：没有"一刀切"。交付建议用风险与运营数据驱动：日均提币需求、峰值、链拥堵、以及安全事件应对能力。通常做法：热钱包维持"最小运营余额"，其余进入冷钱包；并制定补充热钱包的审批与时窗策略。

Q109：多签（Multi-sig）是不是必须?

A：不是唯一方案，但监管与合作方通常期望"去单点控制"。交付级选择：多签或MPC均可，但必须证明：签名分权、密钥分片/隔离、审批链、以及在异常情况下的应急恢复与冻结机制。

Q110：MPC 钱包如何向监管解释?

A：交付要点：MPC 架构图、分片存储位置、参与方角色、阈值签名策略（m/n）、密钥轮换与备份、以及"任何单方无法转移资产"的证明（含演示脚本）。

Q111：私钥备份怎么做才不踩雷?

A：备份必须遵循：加密、分片、地理隔离、访问审批、多方见证、定期演练。交付建议：形成"密钥生成—分发—存储—使用—轮换—销毁"全生命周期 SOP，并附见证记录模板。

Q112：提币审批链最低要做到什么?

A：至少"双人复核 + 分权签名 + 风险拦截"。交付建议：

- 风险引擎先拦截（地址风险/额度/新地址冷却期）
- 再走人工审批（运营+风控/合规）
- 最后签名执行（独立密钥持有人）
  每一步都有工单、时间戳、证据导出。

Q113：新提币地址要不要冷却期?

A：建议设置，尤其对零售客户：新地址添加后 24–48 小时冷却，或需要额外验证（2FA/邮件/视频/白名单机制）。交付可显著降低社工盗币风险。

Q114：如何处理"客户要求紧急放行提币"?

A：交付话术与机制：合规风控优先，紧急放行只能在"预设例外机制"下执行（例如高级别审批、额外验证、额度限制、全程录音/留痕）。否则属于绕过控制的重大风险。

Q115：托管资产隔离要怎么做成"可审计"?

A：三件套：

1. 钱包地址分层（客户池/运营池/手续费池）
2. 账本分层（客户子账/总账）
3. 对账机制（链上余额 ↔ 内部账 ↔ 客户报表）
   交付要点是"每日对账报表 + 差异闭环工单"。

Q116：对账差异长期存在会怎样?

A：这是监管与银行极敏感红线：可能被视为资产混同、记录不实或控制失效。交付要求：对账差异必须有SLA清零（或有合理解释并经批准），并形成整改闭环。

Q117：Proof of Reserves（PoR）怎么做才合规不过度营销?

A：交付建议：PoR 作为透明度工具，但披露必须谨慎，明确范围、方法、时间点、限制与假设，避免对客户形成"全额担保/无风险"的误导。PoR 不能替代对账、审计与内控。

Q118：是否需要第三方托管（Qualified Custodian）?

A：视商业模式与监管审查而定。自托管需要更强控制与证据；第三方托管需要更强外包治理与审计权。交付策略：两条路径都准备，选择更符合成本与时间的方案。

Q119：托管业务需要哪些关键岗位?

A：交付建议至少：托管负责人、信息安全负责人、风控/合规负责人、钱包运营主管、对账与财务控制岗、以及独立审查/内审（可外包）。关键是职责分离与可问责。

Q120：托管的"客户资产不得挪用"怎么制度化？

A：写进：公司治理红线、财务与钱包权限矩阵、禁止将客户资产用于自营/质押/借贷（除非客户明确授权并披露）、以及对违规的纪律处分条款。并设置技术限制：运营池与客户池不可混用。

Q121：托管与借贷结合（如质押收益）会更复杂吗？

A：会显著提高风险：抵押品管理、再质押、清算机制、客户披露与同意、以及流动性与挤兑风险。交付上需单独制度包：产品治理、风险揭示、压力测试与隔离方案。

Q122：钱包黑名单/冻结功能要不要？

A：建议具备。用于制裁命中、诈骗资金、可疑地址交互等场景。交付要点：冻结触发条件、复核机制、申诉机制、解除条件与记录留存。

Q123：托管业务如何处理"硬分叉/空投"？

A：交付制度应明确：支持标准、风险评估、客户通知、资产归属与处理方式、以及在技术不可行或风险过高时的拒绝机制。避免客户纠纷。

Q124：链上拥堵导致提币延迟，如何防投诉？

A：交付建议：披露网络风险、提供状态追踪、设定SLA与分级（普通/紧急），并在异常时发布公告。对外沟通要留痕，避免"客服口头承诺"。

Q125：密钥轮换（Key Rotation）如何做才安全？

A：交付流程：触发条件（人员变动/供应商变动/安全事件/周期到期）→ 新密钥生成见证 → 地址迁移计划 → 对账确认 → 旧密钥销毁证明。全程可审计。

Q126：如果关键签名人离职怎么办？

A：交付要点：离职即刻权限回收、签名阈值应急机制（避免单点）、备用签名人名单、以及董事会批准的应急变更流程。必须可在不影响客户资产安全前提下恢复运营。

Q127：托管系统如何满足"最小可行监管演示"？

A：演示脚本：地址分层→权限矩阵→提币审批→签名执行→链上交易→对账报表→差异闭环→日志导出→异常冻结与解冻流程。

Q128：托管业务最常见的失败点是什么？

A：单点密钥控制、对账不闭环、提币审批被绕过、外包无审计权、日志不可取证。这些都会引发监管严重关切。

Q129：托管业务是否需要更高资本或额外审慎要求？

A：托管通常属于高风险活动之一，资本与审慎要求会更严格（按活动规则与审慎口径计算）。交付时要把资本测算与运营预算绑定。

Q130：托管能否同时支持法币与虚拟资产？

A：可以作为产品形态，但法币部分往往涉及银行/PSP/备付安排与资金隔离。交付建议：法币资金流图 + 账户结构 + 对账机制 + 反欺诈与拒付控制。

Q131：托管客户协议中必须披露哪些风险？

A：至少：私钥风险、链上风险、第三方协议风险、硬分叉/空投处理、提币延迟风险、冻结与合规协作条件、费用与收费方式、以及赔付/责任限制（不得误导）。

Q132：托管与交易所内部划转是否需要记录？

A：必须。内部划转是审计与监管抽查重点。交付证据：划转工单、审批链、链上/账本记录、以及对账报表反映。

Q133：我们可以把托管完全外包给第三方吗？

A：可以，但你仍然对客户与监管负责。交付要求：第三方尽调、合同审计权、监管配合条款、数据导出、事故通报、以及退出切换计划（最关键）。

Q134：退出托管业务（wind-down）要怎么准备？

A：交付级：客户公告、资产迁移与对账、未决交易处理、费用结算、投诉处理、数据留存、以及监管沟通归档。提前准备"清退计划"可显著降低重大事件风险。

Q135：本模块一句话结论？

A：托管的合规核心是：密钥去单点、提币强控制、资产强隔离、对账强闭环、日志强取证。

H. 交易所（Exchange）、撮合与市场完整性（Q136–Q160）

Q136：什么时候会被认定为"交易所（Exchange）活动"？

A（交付级）：你提供撮合/交易执行机制，使买卖双方在你的规则下成交（无论订单簿、RFQ、聚合撮合、或撮合引擎驱动），通常都接近交易所活动边界。即便你宣称"只是技术平台"，只要你制定交易规则、撮合逻辑与市场秩序，就属于高监管关注活动。

Q137：撮合规则必须披露到什么程度？

A：交付建议披露到"可理解且可复核"：优先级（价格/时间）、订单类型、部分成交、撤单规则、异常行情处理、系统故障处理、以及费用计算方式。并保留撮合日志可复算。

Q138：VARA 会看我们的撮合引擎代码吗？

A：未必常态看源码，但会要求你能证明撮合公平性、参数变更受控、以及成交与账本一致。交付关键：版本控制、变更审批链、测试报告、撮合日志导出与复算样例。

Q139：如何防止"插针、异常K线、行情源污染"？

A：交付控制：多源行情聚合、异常值过滤、熔断与价格带、撮合参数保护、以及事故复盘机制。并把"行情源更换/参数调整"纳入变更管理。

Q140：市场操纵监控要覆盖哪些典型行为？

A：至少覆盖：对敲/刷量、拉盘砸盘、Spoofing、Wash trading、关联账户操纵、异常集中度、异常撤单率、以及做市账户与普通账户的异常交互。交付要点：监控规则库 + 告警处置记录 + 处罚/限制措施。

Q141：做市（Market Making）能做吗？需要额外披露吗？

A：可以，但会显著提升冲突风险。交付建议：做市账户隔离、策略审批、禁止内幕信息使用、报价公平性与记录留存、以及对客户披露"平台可能作为流动性提供者"的事实。

Q142：自营交易（Proprietary Trading）与交易所能共存吗？

A：可以但非常敏感。交付必须具备：信息隔离、防止优先成交、独立监控与审计、以及清晰披露与冲突管理政策。

Q143：上币（Listing）机制怎么做才可交付？

A：交付"上币评审机制模板"：项目尽调、代币分类、合规风险、技术风险、流动性与操纵风险、披露文件、上市后监控与定期复审。并形成上币委员会纪要与决议。

Q144：是否需要"产品治理/适当性"机制？

A：建议具备，尤其面向零售客户时：风险分级、权限矩阵（杠杆/衍生品/高波动资产）、风险揭示、冷静期（如你采用）、以及客户教育记录。

Q145：订单执行与滑点纠纷怎么降低？

A：交付要点：订单执行政策（Execution Policy）、滑点披露、异常行情处理、系统故障处理、以及可复算的订单与撮合日志导出。发生纠纷时用证据说话。

Q146：撮合系统的"时间戳"需要多精确？

A：交付建议：统一时间源（NTP）、毫秒级或更高精度、并防篡改记录。监管抽样复核时，时间线越清晰越容易通过。

Q147：是否必须做 KYC 才能允许交易？

A：合规上通常需要按风险分级执行 KYC/EDD，在客户身份、制裁筛查、风险评分未完成前不应开放完整交易权限。交付建议：权限矩阵与系统控制绑定（未KYC不可交易/不可提币/限额）。

Q148：如何控制"同一客户多账户"与"关联账户"风险？

A：交付控制：设备指纹、IP/行为分析、证件重复检测、受益人重复识别、以及关联账户图谱分析。并制定"发现关联—限制—复核—处置"流程。

Q149：API 交易如何防止滥用与操纵？

A：交付机制：API key 分级权限、速率限制、异常调用告警、白名单/固定IP、以及对高频策略的监控与熔断。并保留API日志可导出。

Q150：客户资金/资产在交易所业务里最关键的控制点是什么？

A：资产隔离与对账闭环：客户资产不进入运营资金池；每日对账；提币审批分权；撮合—清算—账本一致。任何一个失效都可能引发严重监管与声誉风险。

Q151：交易所是否需要"清算/结算"机制说明？

A：需要。交付应说明：成交确认、清算时点、失败处理、异常回滚、以及在链上转账时的确认策略（确认数/拥堵策略）。

Q152：如果我们提供杠杆/保证金交易，会更难吗？

A：会显著复杂：追加保证金、强平机制、价格源与风险参数、客户披露、以及极端行情下的损失分配机制。交付建议：单独"杠杆产品风险治理包"。

Q153：衍生品/永续合约属于 VARA 范畴吗？

A：需要按 VARA 对具体活动的定义与许可边界评估，并考虑是否触及其他监管框架。交付建议：先做产品分类与法律意见，再决定是否纳入许可范围。

Q154：交易所发生系统故障导致无法交易，如何合规处理？

A：交付制度：故障分级、公告机制、订单处理原则（撤单/保留）、补偿政策（如适用）、以及事故复盘与改进。关键是透明、可追溯、可复盘。

Q155：交易所如何处理"市场异常波动"？

A：交付机制：熔断/暂停交易、价格带、风险参数上调、限制高风险订单类型、加强监控与人工干预审批（有记录）。并把触发阈值写入制度。

Q156：如何证明"我们没有操纵市场"？

A：交付证据：市场监控规则库、告警工单、处置记录（限制/封禁/下架）、做市账户隔离与审计、以及成交日志可复算。监管更信"证据链"而非口头解释。

Q157：交易所业务最容易被 RFI 追问的三件事？

A：

1. 客户资产隔离与对账
2. 市场监控与操纵防控
3. 撮合公平性与系统韧性
   交付应优先把这三块做成"可演示、可导出"的材料包。

Q158：是否建议建立"上币与市场行为委员会"？

A：建议。委员会负责：上币决策、市场异常处置、重大参数变更审批、以及冲突管理。交付上体现公司治理成熟度。

Q159：交易所如何与托管协同才不混乱？

A：交付建议用"三流图"：订单流（撮合）、资产流（钱包/链上）、账务流（客户子账/总账）。并把权限与责任边界写清：谁能动客户资产、谁能改账、谁能放行提币。

Q160：本模块一句话结论？

A：交易所合规的核心是：公平撮合 + 市场监控 + 资产隔离 + 系统韧性 + 可复算证据链。

I. 外包与第三方风险治理（Outsourcing & Third Parties）（Q161–Q190）

Q161：VARA 允许把关键功能外包吗？哪些最常见？

A（交付级）：允许外包，但**责任不外包**。常见外包：KYC/KYB、KYT/链上监控、云基础设施、托管技术（含 MPC 提供商）、撮合引擎/行情源、客服、渗透测试与安全运营（MSSP）、合规独立审查等。交付重点是"可控、可审计、可退出、可应急"。

Q162：什么算"关键外包（material outsourcing）"？

A：满足任一即可视为关键：

1. 影响客户资产安全（托管/签名/提币）；
2. 影响交易执行与市场秩序（撮合/风控/行情）；
3. 影响 AML/CFT 合规有效性（KYC/KYT/制裁筛查）；
4. 影响数据安全与可用性（云/IAM/日志）；
5. 一旦中断会导致业务无法持续（单点供应商）。
   交付建议：做"关键外包清单 + 风险评级 + 替代方案"。

Q163：外包尽调（Vendor Due Diligence）要做哪些？

A：交付级尽调包至少包括：

- 公司资质与财务稳定性
- 安全合规（ISO/SOC、渗透测试、漏洞管理）
- 数据处理与隐私（数据驻留/跨境/子处理方）
- 业务连续性（SLA、DR、RTO/RPO）
- 审计权与监管配合条款
- 事故通报与取证协作
- 退出/迁移与数据返还/销毁机制
  并形成评分表与批准纪要。

Q164：外包合同里必须写哪些"监管友好条款"？

A：交付建议至少写入 10 条红线：

1. 审计权（你/独立审查/监管可审阅）
2. 数据所有权与可导出权（随时可导出）
3. 子处理方披露与审批
4. 安全事件通报时限（如 24h 初报）
5. 漏洞修复 SLA
6. 业务中断应急支持与切换
7. 合规协作（KYC/KYT 证据、日志、工单）
8. 服务终止后的数据返还/销毁证明
9. 变更管理与提前通知（重大变更需批准）
10. 争议解决与持续服务义务（避免"突然断供"）

Q165：第三方如果在境外存储数据，会有问题吗？

A：不必然，但必须可解释：数据类别、加密方式、访问控制、跨境传输合规、以及监管/审计可访问性。交付建议提供"Data Flow & Residency Map"，并在合同里锁定：数据位置、备份位置、访问主体与审批。

Q166：KYC/KYB 外包的最大合规风险是什么？

A：“做了但不可验证”。监管抽样时若你无法导出：身份证明、核验记录、EDD 证据、复核人、时间戳与版本记录，就会被视为合规失败。交付要求：第三方必须支持“证据导出+工单闭环”。

Q167：KYT 工具供应商如何选择更稳？

A：交付评估维度：地址覆盖率、风险标签透明度、规则可配置、误报率/召回率、与制裁名单对接、工单闭环、API 稳定性、数据导出能力、以及发生误判时的复核机制。最好做 POC（概念验证）并形成评估报告。

Q168：如果我们用第三方托管（custodian），“客户资产隔离”怎么证明？

A：交付证据：托管协议（资产归属/隔离条款）、钱包地址与账户结构、对账报表、权限矩阵（你能做什么/不能做什么）、以及托管方的审计/合规报告摘要。并确保：你能在合理时间内获取数据以响应监管询问。

Q169：撮合引擎外包的风险点？

A：三大风险：

- 公平性不可证明（无法导出撮合日志/规则）
- 参数变更不可控（供应商随意改）
- 故障处置不可控（无法快速回滚/修复）
  交付要求：撮合规则与日志可导出、变更需你审批、故障有SLA与回滚机制。

Q170：云服务商（IaaS/PaaS）是否也算外包？

A：是。交付要求：云架构安全、权限控制、日志与监控、DR、以及对监管/审计的可配合性。把云供应商纳入“关键外包清单”。

Q171：客服外包会影响合规吗？

A：会。客服是“对外承诺”高风险入口。交付要求：话术库、禁用承诺清单、工单留痕、抽检与培训、以及升级通道（投诉/冻结/MLRO 升级）。客服外包合同也应包含录音/记录留存与审计权。

Q172：第三方被黑客攻击，我们要承担什么？

A：监管与客户通常仍会追责你是否尽到了：供应商尽调、合同控制、持续监控、应急处置与通知义务。交付建议：建立“第三方事件响应”章节：触发条件、通报流程、证据请求清单、以及替代切换方案。

Q173：如何做“持续性供应商监控”才算有效？

A：交付机制：季度KPI（可用性、告警响应、数据导出SLA、事故次数）、年度复核（安全报告、渗透测试摘要、BCP演练）、重大变更审批（架构/子处理方/数据驻留改变），并形成供应商管理台账。

Q174：我们必须准备“退出（Exit）与替代方案”吗？

A：强烈建议，尤其关键外包。交付要求：

- 退出触发条件（成本/风险/监管要求/事故）
- 数据迁移计划（格式、周期、校验）
- 并行期（双跑）与回滚
- 客户沟通与对账
- 退出完成证明（含数据销毁）
  这部分是监管与银行尽调常问。

Q175：外包治理最常见的失败点是什么？

A：五个：无审计权、数据不可导出、子处理方失控、退出不可行、事故通报不及时。交付时要逐条封堵。

Q176：我们能把合规/MLRO 外包吗？

A：可采用外部顾问支持，但关键职责与问责链必须清晰（谁签字、谁决策、谁上报）。交付建议：内部指定负责人（CO/MLRO），外部顾问提供制度、培训、抽检、独立评估支持。

Q177：独立审查（Independent Review）可以外包吗？需要什么产出？

A：可以。交付产出建议：年度审查报告（范围、抽样方法、发现、评级、整改建议）、整改跟踪表（Owner、截止日、证据）、以及董事会/管理层审阅纪要。

Q178：外包与信息安全如何衔接？

A：交付应把外包纳入信息安全体系：供应商风险评估、访问控制、最小权限、接口加密、日志留存、以及定期权限复核。外包不是"黑箱"，必须能被监控与取证。

Q179：第三方提供的"黑盒算法"会有问题吗？

A：可能。若用于风险评分、交易监控或撮合排序，监管可能要求解释性与可复核性。交付建议：要求供应商提供方法论说明、可配置阈值、审计日志与抽样复核能力。

Q180：外包风险如何向监管"可视化呈现"？

A：交付建议用一张"外包治理矩阵"：供应商—功能—关键性等级—数据类别—审计权—SLA—DR—退出方案—负责人。监管最喜欢"结构化台账"。

Q181：如果供应商拒绝提供审计权怎么办？

A：交付结论：原则上不应选择该供应商承担关键功能；或必须通过架构调整降低关键性（例如把关键数据与控制留在你侧），否则合规风险过高。

Q182：我们要不要做"外包前监管沟通"？

A：当涉及托管/撮合/核心KYC等关键外包时，建议在申请材料与面谈中主动披露并说明控制与退出方案。交付策略是"透明 + 可控证据"。

Q183：第三方数据导出格式要怎么定？

A：交付建议：CSV/JSON + 字段字典 + 时间戳 + 唯一ID + 版本号。这样才能支持对账、审计与监管抽样。

Q184：第三方访问我们系统的权限怎么管？

A：交付要求：独立账号、最小权限、强制MFA、跳板机/堡垒机、会话录屏（如适用）、到期自动失效、以及所有访问写入集中日志。

Q185：外包下的"责任边界"如何写进客户协议？

A：可以披露使用第三方服务，但不能以此推卸核心责任。交付建议：披露第三方风险、事故处理与通知机制、以及你对客户资产与服务的总体责任承诺边界（避免误导）。

Q186：外包 KPI 与罚则怎么设？

A：交付建议：可用性（≥99.9%）、响应时限、事故通报、数据导出时限、漏洞修复SLA等；并设置服务抵扣/赔偿/终止权。关键是"可执行"。

Q187：外包与费用预算如何向董事会说明？

A：交付建议：把外包成本与风险对照：降低招聘成本 vs 增加第三方风险；并以"关键外包优先确保审计权/退出方案"为预算原则，避免只选最便宜。

Q188：外包与合规检查如何衔接？

A：交付机制：合规抽检时同时抽样第三方记录（KYC/告警/日志），并把整改要求传导至供应商（合同里要有协作义务）。

Q189：外包治理需要董事会批准吗？

A：建议对关键外包实行董事会/高级管理层批准，并记录在纪要中。监管抽查时，"谁批准、为何批准、风险如何控制"是高频问题。

Q190：本模块一句话结论？

A：外包合规=审计权 + 数据可导出 + 退出可执行 + 事故可协作 + 责任不外包。

J. 公司治理、三道防线与 RFI/面谈打法（Q191–Q215）

Q191：VARA 最看重的公司治理是什么？

A（交付级）：看重"可问责的治理链"：董事会监督、管理层执行、合规与风险独立性、以及重大事项（上币、托管变更、关键外包、风险参数）有审批、有记录、有复盘。

Q192：三道防线怎么写成"监管可接受"的交付文本？

A：交付结构：

- 第一线（业务/运营/技术）：控制执行与日常监控
- 第二线（合规/风险/MLRO）：制度制定、监督抽检、风险评估、STR决策
- 第三线（内审/独立审查）：年度评估、专项审查、整改跟踪
  每道防线都要有：职责、报告路径、产出物（报表/纪要/审查报告）。

Q193：CO/MLRO/风险负责人是否必须"完全独立不兼任"？

A：小机构可出现兼任，但必须证明：独立性不被业务KPI绑架、关键事项有升级机制、以及必要时引入独立审查。交付建议：即便兼任，也要用制度"隔离职责与审批权"。

Q194：治理文件清单（最小可交付）有哪些？

A：建议至少 12 份：董事会章程、授权矩阵（DoA）、冲突管理、风险管理政策、合规计划、AML/CFT手册、投诉处理、外包管理、信息安全与技术治理、事件响应、记录保存、以及产品治理/上币政策（如适用）。

Q195：RFI（补件）最常问哪些？

A：高频 8 类：UBO/资金来源、活动组合边界、客户资产隔离、KYC/EDD与KYT、密钥治理与提币审批、外包审计权与退出、系统韧性与DR、以及市场行为/营销披露。

Q196：如何把材料做成"RFI-ready（一次过）"？

A：交付技巧：每份制度都附"证据清单与输出报表样例"，并做交叉引用（例如 AML 手册引用客户分层与权限矩阵；技术手册引用日志导出；外包制度引用合同条款摘要）。监管最怕"孤立PPT"。

Q197：面谈最好的结构是什么？

A：交付建议：

1. 业务模型与活动组合（2页）
2. 客户资产与资金流（3张流程图）
3. AML/KYC/KYT闭环（含工单演示）
4. 技术与密钥治理（含提币审批演示）
5. 外包与退出（台账+合同条款摘要）
6. 治理与问责（DoA+三道防线）
   全程用"可导出证据"支撑。

Q198：系统演示（Demo）应该演示到什么粒度？

A：监管演示不是产品秀，是控制点验证：登录/MFA→权限矩阵→关键操作审批→日志留存→告警工单→对账报表→导出证据。演示必须可复刻（给出脚本、账号权限、样例数据）。

Q199：如何准备"证据编号体系"让材料更像交付件？

A：交付建议：Evidence Register（证据登记表）：E-001起，按模块分类（AML、Tech、Custody、Outsourcing等），每条证据写：名称、来源系统、生成方法、保存路径、责任人、更新频率。监管抽样时可秒级定位。

Q200：董事会/管理层会议纪要为什么重要？

A：因为它证明治理是真实运作：风险上报、重大决策、整改闭环。交付建议：固定议程模板（风险、合规、事件、投诉、外包、上币/产品变更），并保留附件（报表、审查结果）。

Q201：冲突管理（Conflict of Interest）要覆盖哪些?

A：至少覆盖：自营/做市与客户交易冲突、托管与交易冲突、上币利益冲突、员工交易与内幕信息、供应商回扣/关联关系。交付要点：披露→回避→审批→监控→处罚。

Q202：如何证明"合规独立性"?

A：交付证据：合规负责人直线汇报路径、否决权/升级机制、合规抽检报告、整改跟踪、培训记录、以及合规KPI不与纯营收绑定。

Q203：如何做年度合规计划（Annual Compliance Plan）?

A：交付模板：按季度列出抽检主题（KYC、制裁、告警、对账、权限复核、外包复核、营销抽检、投诉复盘、DR演练），每项写：样本量、方法、输出物、责任人、截止日。

Q204：员工培训最低要怎么做才可交付?

A：交付标准：入职培训 + 年度复训 + 重点岗位专项（客服/托管运营/风控）+ 测验与通过记录 + 培训材料版本控制。监管抽查时能拿出"人—课程—成绩—日期"。

Q205：客户投诉与监管投诉的区别?

A：客户投诉是内部闭环；监管投诉/重大事件上报通常有更高时效要求与材料标准。交付建议：投诉分级（普通/重大）与升级条件（涉及资产损失、系统故障、欺诈、制裁命中等）。

Q206：重大事件（material incident）如何定义?

A：交付建议按影响定义：影响客户资产安全、影响大量客户服务、影响市场秩序、影响数据泄露、或触发执法/媒体关注。每类事件都有响应SOP与通报模板。

Q207：如果我们改变业务范围（新增活动），需要做什么?

A：交付原则：先做影响评估（资本、人员、系统、制度），再走相应许可变更/新增申请流程，并在对外披露上严格按获批范围表述。避免"先上车后补票"。

Q208：如何处理"监管现场检查/抽样审阅"?

A：交付建议：建立"监管检查应对手册"：联络人、资料清单、证据导出SOP、抽样应答模板、以及"48小时内可提供"的核心报表包（KYC、告警、对账、权限复核、外包台账）。

Q209：哪些指标（KPI/KRI）建议定期向管理层报告?

A：交付建议至少 15 项：KYC完成率、EDD比例、制裁命中与处置时长、告警量与关闭SLA、STR数量、提币拦截率、对账差异次数、系统可用性、重大事件次数、投诉数量与解决时长、拒付率（如有）、外包SLA达成率、权限异常次数、渗透测试问题闭环率、DR演练结果。

Q210：如果监管问"你们如何确保客户资产不被挪用"，最佳回答结构?

A：三段式交付：

1. 法律/制度：客户资产隔离与禁止挪用条款
2. 组织/权限：分权审批与独立签名
3. 技术/证据：钱包分层、对账报表、日志留存与抽样复核
   并用证据编号现场展示。

Q211：如果监管问"你们如何防止洗钱"，最佳回答结构?

A：同样三段式：

1. 风险评估与客户分层
2. KYC/EDD + 制裁筛查 + KYT
3. 告警工单闭环 + STR 决策与记录留存
   再补一句：年度独立审查与培训。

Q212：如果监管质疑"你们没有足够本地经验"，怎么答?

A：交付答法：

- 展示关键岗位履历与职责分离
- 引入外部专家/独立审查（不替代问责）
- 用制度与证据链证明可运行
- 给出上线路线图与人员到岗计划（日期、岗位、KPI）

Q213：治理类最常见雷区是什么？

A："有制度无执行"。没有会议纪要、没有抽检报告、没有整改闭环、没有证据导出，都会被认为是纸面合规。

Q214：我们如何把"整改闭环"做成监管友好？

A：交付模板：Issue Log（问题登记）→根因→整改措施→Owner→截止日→证据→复测→关闭。每月向管理层汇报一次，形成纪要。

Q215：本模块一句话结论？

A：治理交付=三道防线可运行 + 决策有纪要 + 控制有证据 + 整改可闭环。

K. 借贷（Lending & Borrowing）与资管（VA Management & Investment）高频（Q216–Q240）

Q216：什么情形属于"Lending & Borrowing"活动？

A（交付级）：你向客户提供以虚拟资产为标的的借贷、撮合借贷、利息/收益安排、抵押借款、或把客户资产出借给第三方获取收益等，通常落入借贷活动边界。该活动风险高，监管会重点看：抵押品、清算、流动性、披露与挤兑风险。

Q217：借贷业务最关键的风险点是什么？

A：四类：对手方风险（借款人违约）、抵押品风险（波动/折价/流动性）、流动性风险（客户集中赎回/挤兑）、以及操作与清算风险（强平失败）。交付必须把这些写进风险框架并配置系统参数。

Q218：抵押品管理制度要怎么写才可交付？

A：交付要点：抵押率（LTV）与折价（haircut）、追加保证金阈值、强平触发与执行步骤、价格源（oracle/指数）与异常处理、以及在链拥堵/价格断层时的应急措施。并附参数表与审批机制。

Q219：强平机制如何避免争议？

A：交付建议：

- 触发阈值透明披露
- 强平顺序与分批执行规则
- 价格源异常与熔断
- 交易执行日志可复算
- 客户通知与时间戳留痕
  争议发生时，证据链决定胜负。

Q220：借贷产品的客户披露必须包含哪些？

A：至少：利率与费用、抵押品波动风险、强平风险、极端行情下可能产生剩余欠款、链上/技术风险、以及平台是否再质押/出借客户资产（如有必须明确同意）。

Q221：能否对客户资产进行再质押（rehypothecation）？

A：这是高敏感事项。交付原则：若存在再质押/再出借，必须有清晰的客户授权、披露、风险隔离与对账机制；否则极易触发重大合规与声誉风险。建议以"尽量不再质押"为稳健路线。

Q222：如何做借贷业务的压力测试？

A：交付情景至少 5 个：币价暴跌 40%/60%、抵押品流动性枯竭、价格源中断、链上拥堵导致无法及时强平、以及客户集中赎回。每个情景给出：损失估算、应急动作（暂停借贷/上调保证金/限制提币等）与责任人。

Q223：借贷业务是否需要单独的资本与流动性缓冲？

A：强烈建议。借贷对流动性要求高。交付策略：风险准备金、流动性池、以及"赎回排队/限额/暂停"机制（必须在条款中披露并有触发条件）。

Q224：借贷与托管结合，会不会更难？

A：会。因为你同时承担"资产控制"与"风险转移"。交付必须做更强隔离：客户资产池、抵押品池、平台风险池分层，对账与审批更严格。

Q225：什么情形属于"VA Management & Investment"？

A：你代表客户管理其虚拟资产组合、提供委托投资/资产管理、基金/组合策略、或以受托方式进行投资决策与调仓，通常进入资管/投资管理活动边界。监管会重点看：受托责任、适当性、利益冲突、估值与托管安排。

Q226：资管业务的"受托责任"如何体现在制度里？

A：交付应明确：投资授权范围、风险预算、资产配置边界、止损与风控规则、估值与计费、报告频率、以及当发生冲突时的处理（优先客户利益/披露/回避）。

Q227：资管业务必须有客户适当性评估吗？

A：建议必须。交付模型包括：财务状况、投资经验、风险偏好、投资目标、可承受亏损、以及专业投资者认定（如采用）。并把结果绑定到产品权限与策略选择。

Q228：资管估值（Valuation）怎么做才可交付？

A：交付要点：估值政策（价格源、异常价处理、停牌/流动性不足处理）、估值频率（每日/每周）、估值复核、以及对客户的估值报表模板。若涉及非流动资产/RWA，更需要独立估值与披露。

Q229：管理费/绩效费如何披露与计提？

A：交付标准：费率、计提周期、计费基数（AUM/净值）、高水位线/回拨（如有）、以及例子可复算。最好提供"费用计算示例表"，避免纠纷。

Q230：资管与交易所/经纪同集团，会有哪些冲突风险？

A：冲突包括：优先成交、费用输送、内幕信息、上币利益冲突。交付必须：信息隔离、交易分配政策、最佳执行政策、以及独立监控与审计。

Q231：资管是否必须使用独立托管？

A：视模式与监管审查。独立托管能显著降低挪用风险与提升可信度；自托管则需要更强隔离与对账。交付建议：优先"独立托管 + 明确授权"，或至少实现集团内托管独立治理。

Q232：客户报告（Reporting）最低要提供哪些？

A：交付建议：持仓与变动、收益与回撤、费用明细、重大风险事件、以及对策略偏离/风险超限的解释。报告频率写入合同并可导出留存。

Q233：资管策略使用 DeFi/质押收益，需要额外披露什么？

A：交付必须披露：智能合约风险、协议治理风险、清算与脱锚风险、流动性风险、以及可能的无法退出/延迟退出风险。并在投资授权中明确"可用协议白名单/限额"。

Q234：客户赎回机制如何设计更稳？

A：交付建议：赎回频率、赎回通知期、赎回定价点、以及在极端行情/链上拥堵/流动性不足时的延期/分期安排（必须事先披露并设触发条件）。

Q235：资管业务如何做"重大事项通报"？

A：交付制度：重大偏离、重大损失、重大安全事件、重大策略变更、关键外包变更等触发通报；并规定对客户与监管（如适用）的沟通时限与模板。

Q236：资管业务最常见的失败点是什么？

A：三类：适当性不足（卖错产品）、估值与费用不透明（不可复算）、以及冲突管理失效（集团利益优先）。交付要把"透明与证据"做到极致。

Q237：借贷与资管如何在同一体系下管理风险？

A：交付建议：统一风险框架（风险偏好声明、限额体系、压力测试、事件响应），但对借贷和资管分别设"专属风险参数表"和"审批权限矩阵"。

Q238：如果我们只做机构客户，借贷/资管会更容易吗？

A：不会更容易，只是控制点不同：机构客户更看重风险披露、对账、审计、以及法律条款可执行性。监管仍会要求你具备完整治理与证据链。

Q239：借贷/资管如何向监管证明"我们能控得住极端行情"？

A：交付证据：压力测试报告、参数调整机制（上调保证金/限额/熔断）、应急预案、演练记录、以及历史模拟回测结果（方法论与假设披露）。

Q240：本模块一句话结论？

A：借贷/资管交付=清晰授权与披露 + 参数化风控 + 压测与应急 + 估值与费用可复算 + 冲突隔离可审计。

L. 记录保存与数据留存（Record-Keeping & Data Retention）（Q241–Q270）

Q241：VARA 对记录保存的总体要求是什么？

A（交付级）：核心不是"留多久"，而是**是否完整、可检索、可复核、不可篡改**。记录必须支持监管抽样、事故复盘、客户纠纷与审计需要，覆盖业务、合规、技术、财务与治理全链路。

Q242：通常需要保存哪些类别的记录？

A：至少包括：

- 客户（KYC/KYB/EDD/制裁筛查）
- 交易（订单、撮合、成交、清算）
- 钱包与资产（地址、提币审批、签名、对账）
- AML（告警、调查、STR 决策）
- 技术（登录、权限、变更、日志、告警）
- 外包（尽调、合同、SLA、事故）
- 治理（董事会/管理层纪要、审批）
- 投诉与纠纷处理

Q243：记录保存期限有没有统一年限？

A：VARA 规则通常要求**不少于若干年（常见为 5–8 年）**，并以"业务关系结束后起算"。交付建议：统一采用**不低于 8 年**的集团标准，避免不同模块年限不一致。

Q244：电子记录是否可以替代纸质？

A：可以，且更受欢迎，但必须满足：完整性、可读性、不可篡改、可导出。交付建议：集中存储 + 权限控制 + 哈希/防篡改机制 + 备份。

Q245：日志（Logs）是否也属于法定记录？

A：是，尤其是**安全、权限、关键业务日志**。监管常通过日志判断"控制是否真实运作"。日志必须可检索、可导出、可关联业务事件。

Q246：记录可以只保存在第三方系统吗？

A：风险很高。交付原则：即便外包，也要确保你**随时可导出**完整记录，并在退出时可迁移与留存。

Q247：如何防止记录被篡改或删除？

A：交付手段：

- 只读存储（WORM）
- 哈希校验
- 访问审计
- 删除审批与留痕
- 备份与异地存储

Q248：如果发生系统升级，旧记录怎么办？

A：交付要求：迁移计划、校验报告、样本复核、以及迁移完成证明。旧记录必须可追溯，不得因升级而丢失。

Q249：监管抽样时，通常会抽哪些记录？

A：高频抽样：

- 随机客户的 KYC/EDD
- 某日/某币对的订单—成交—对账
- 某次提币的审批—签名—链上记录
- 一条 AML 告警的完整闭环
- 最近一次重大变更的审批与日志

Q250：如何把记录保存做成"检查友好"？

A：交付技巧：建立 **Evidence Index（证据索引）**，每类记录有固定路径、命名规则、负责人和导出步骤。监管抽样时"即点即出"。

Q251：聊天记录、客服记录要不要保存？

A：要。客服往往是承诺与纠纷源头。交付建议：客服系统留痕、话术版本控制、录音/聊天记录留存与抽检。

Q252：删除客户数据是否允许？

A：在满足法定留存期后、且不影响未决纠纷/调查的前提下才可。交付要有"数据销毁审批与证明"。

Q253：如果客户要求"删除我的数据"，如何处理？

A：交付答法：区分**隐私权**与**法定留存义务**。可删除营销/非必要数据，但法定留存数据需保留并向客户说明法律依据。

Q254：记录保存失败的最常见原因？

A：三点：记录分散不可检索、外包数据不可导出、权限混乱导致日志缺失。交付要逐一封堵。

Q255：我们需要"记录保存政策（Record Retention Policy）"吗？

A：必须。交付政策应列明：记录类型、保存年限、存储位置、访问权限、销毁流程与责任人。

Q256：如何证明记录"真实反映业务"？

A：交付证据：系统生成（非手工）、时间戳、权限审计、抽样复算、以及独立审查结果。

Q257：记录保存与审计如何衔接？

A：交付机制：审计抽样直接基于留存记录；审计发现进入整改闭环；整改证据再次留存，形成"证据的证据"。

Q258：记录保存需要董事会关注吗？

A：建议至少年度汇报一次记录保存与信息安全状况。重大事件（数据泄露、记录丢失）必须升级。

Q259：跨境业务的记录是否要区分司法辖区？

A：建议区分并标记。交付做法：在记录元数据中标注适用司法辖区，方便回应不同监管询问。

Q260：记录保存模块一句话结论？

A：记录保存不是"存起来"，而是"随时能被监管复盘"。

M. 监管报告、通知与通报（Regulatory Reporting & Notifications）（Q261–Q280）

Q261：持牌后需要定期向 VARA 报告吗？

A（交付级）：是。报告形式包括：定期报告、事件通报、临时信息披露。频率与内容取决于活动类型与风险等级。

Q262：常见的定期报告有哪些？

A：可能包括：

- 业务与交易量摘要
- 客户与资产规模
- AML 指标（告警、STR）
- 重大风险与事件
- 外包与技术变更
  具体以 VARA 要求与牌照条件为准。

Q263：什么算"必须立即通报"的事件？

A：通常包括：

- 客户资产安全事件
- 严重系统故障
- 数据泄露
- 重大欺诈或洗钱事件
- 关键人员变动
- 关键外包或控制失效

Q264：通报有时间要求吗？

A：有。交付建议：**24 小时内初报 + 后续详细报告**。关键是"及时 + 准确 + 持续更新"。

Q265：通报内容要包含哪些？

A：交付模板通常包括：事件摘要、影响范围、即时止损措施、初步原因、客户影响、后续行动与时间表。

Q266：通报是否等同于承认违规？

A：不是。及时、透明通报通常被视为**良好合规行为**，有助于降低处罚风险。

Q267：如果事件仍在调查中，如何通报？

A：交付答法：明确"初步判断""仍在调查"，避免确定性结论；承诺更新时间点并按期补充。

Q268：未通报或迟报的后果？

A：可能比事件本身更严重，包括罚款、附加条件、声誉风险。交付原则：**宁早不晚**。

Q269：监管报告由谁负责签署？

A：通常由指定负责人（如 CEO/CO/MLRO）签署。交付要明确责任人与替代人。

Q270：监管报告模块一句话结论？

A：监管不怕你出事，怕你不说或说不清。

N. 客户协议、条款与披露（Client Agreements & Disclosures）（Q271–Q295）

Q271：客户协议在 VARA 合规中有多重要？

A（交付级）：极其重要。协议是监管判断**你是否误导客户、是否合理分配风险**的核心文件之一。

Q272：客户协议至少要覆盖哪些内容？

A：

- 服务范围与许可边界
- 费用与收费方式
- 客户资产归属与隔离
- 风险披露
- 提币与结算规则
- 冻结、限制与终止
- 投诉与争议解决
- 责任限制与免责边界

Q273：风险披露可以"模板化"吗？

A：不建议千篇一律。交付级风险披露应**与具体业务、产品、技术和司法辖区匹配**，避免被认定为误导或不足。

Q274：是否必须披露"平台可能暂停服务"？

A：是。交付应明确暂停条件（技术、合规、市场异常）与客户通知机制，避免纠纷。

Q275：费用披露最容易出问题的点？

A：隐性费用、不清晰的计费基数、动态调整未披露。交付要提供**费用示例**，让客户可复算。

Q276：责任限制可以写得很宽吗？

A：不可过度。若被认定为不公平条款，监管与法院可能不支持。交付建议：责任限制需与风险控制能力相匹配。

Q277：客户协议需要 VARA 事前批准吗？

A：通常不需逐条批准，但在审查或投诉中会被重点检查。交付要确保版本控制与历史留存。

Q278：营销材料与客户协议不一致怎么办？

A：这是重大风险。交付原则：**营销不得超出协议与获批范围**；发现不一致要立即整改并留痕。

Q279：多语言协议如何处理？

A：交付建议：指定**法律效力语言版本**；其他语言为参考。避免翻译歧义。

Q280：客户协议模块一句话结论？

A：客户协议是"你对监管的承诺书"，不是纯商业合同。

O. 营销、推广与对外沟通合规（Marketing & Promotions）（Q296–Q320）

Q296：VARA 对营销的核心要求是什么？

A（交付级）：真实、清晰、不误导。不得暗示"保本""保证收益""监管背书"，必须与实际获批业务范围一致。

Q297：官网、白皮书、路演资料都算营销吗？

A：是。任何面对公众或潜在客户的材料都可能被视为营销内容。

Q298：可以用"Regulated by VARA"作宣传吗？

A：需谨慎且准确。交付建议：仅陈述事实（持牌状态与许可范围），不得夸大或暗示官方推荐。

Q299：是否可以在获批前预热营销?

A：风险极高。交付原则：未获批前只能做**公司层面介绍**，不得推广具体受规管服务。

Q300：营销审批流程要怎么设?

A：交付建议：营销材料必须经**合规/法务审批**，留存审批记录与版本号。

Q301：KOL/代理推广是否允许?

A：可以，但你对其行为负责。交付要求：签署合规条款、提供话术指引、定期抽检与违规处罚。

Q302：社交媒体发言需要合规审查吗?

A：建议纳入审查或事后抽检。监管已多次通过社媒内容认定误导宣传。

Q303：可以对比其他平台或暗示"更安全"吗?

A：不建议。交付原则：避免比较性、贬损性或无法证实的表述。

Q304：客户教育内容（Education）是否算营销?

A：通常不算，但内容必须中立、风险充分披露，避免变相推广。

Q305：营销违规的常见处罚?

A：警告、罚款、强制整改、限制业务甚至吊销许可。交付要把营销列为重点风险。

Q306：如何监控营销合规?

A：交付机制：审批台账、发布清单、抽检、KOL 监控、以及违规纠正记录。

Q307：重大市场事件发生时，能否发营销内容?

A：极不建议。交付原则：此时应优先客户沟通与风险提示，而非获客宣传。

Q308：营销与客户协议冲突的处理顺序?

A：立即下架/更正营销 → 通知客户 → 内部复盘 → 记录整改。拖延风险极高。

Q309：营销合规模块一句话结论?

A：营销是"放大器"，放大合规也放大违规。

P. 持续监管、年审与日常合规（Q310–Q335）

Q310：取得 VARA 牌照后，监管是否"放松"?

A（交付级）：不会。持牌后进入**持续监管阶段**：年审、定期报告、事件通报、现场/非现场检查、主题审查（thematic review）都会发生。合规强度取决于**活动类型与风险画像**。

Q311：年审（Annual Review）通常覆盖哪些内容?

A：

- 业务范围是否与获批一致
- AML/CFT/KYT 运作有效性
- 客户资产隔离与对账
- 技术与信息安全（含 DR/BCP 演练）
- 外包与第三方治理
- 治理与三道防线

- 投诉、事件与整改闭环

Q312：年审材料的"最小交付清单"是什么?

A：年度合规报告、风险评估更新、独立审查/内审摘要、关键指标（KPI/KRI）、重大变更清单、事故/投诉汇总、整改跟踪表、董事会/管理层纪要。

Q313：是否需要年度独立审查（Independent Review）?

A：**强烈建议**。尤其交易所、托管、借贷、资管等高风险活动。独立审查能显著降低执法风险并提升银行/机构信任。

Q314：年审中最容易被点名的问题?

A：

- 记录不可导出/不完整
- 外包审计权与退出方案缺失
- 提币审批被绕过
- AML 告警闭环不完整
- DR 演练"只写不练"

Q315：年审不通过会怎样?

A：可能要求限期整改、附加条件、加强报告频率，严重者可触发执法。

Q316：VARA 是否会做"主题审查"?

A：会。常见主题：托管安全、营销合规、KYC/EDD、市场操纵防控、外包治理。需提前准备主题证据包。

Q317：如何准备"随到随查"的非现场检查?

A：建立 **48 小时可交付包**：KYC 抽样、提币样本、对账报表、告警闭环、权限复核、外包台账、最新 DR 演练证据。

Q318：年内发生重大变更，是否要等年审再报?

A：不应等待。**重大变更需事前/事后及时通报**，避免被认定为隐瞒。

Q319：持续监管中，谁对接 VARA 最合适?

A：指定 **单一监管联络人**（CO/MLRO/合规负责人），避免多头沟通。

Q320：持续监管一句话原则?

A：**"持续合规比一次获批更重要。"**

Q321：VARA 在持续监管中，是否会区分"活跃期机构"与"低活跃机构"?

A（交付级）：会。VARA 在实际监管中会基于**交易量、客户规模、风险活动（托管/交易所/借贷）对机构进行风险分层监管**。

- **活跃/高风险机构**：更高频报告、更多主题审查
- **低活跃机构**：报告频率相对降低，但**不等于放松要求**
  交付建议：即便业务量低，也要维持**全套可运行合规体系**，避免被认定为"空壳持牌"。

Q322：如果公司已获 VARA 牌照但暂未正式上线业务，是否仍受监管?

A：是。**持牌即受监管**。
即便未上线，也必须：

- 保持合规制度有效
- 提交必要报告（如零业务报告）

- 及时通报重大变更
  实务雷区：很多机构误以为"未运营 = 不用管"，这是**高风险误解**。

Q323：VARA 是否会关注"实际业务与商业计划的偏离"？

A：非常关注。
若出现以下情形，极易触发问询：

- 实际业务明显偏离获批商业计划
- 风险活动占比显著变化（如突然重心转向托管/借贷）
- 客户结构与风险假设严重不符
  交付建议：建立**年度商业计划偏离评估**，形成书面说明与董事会纪要。

Q324：监管如何判断一家 VASP 是否"实质运营（substance）不足"？

A：常见判断指标包括：

- 本地关键岗位是否真实履职
- 决策是否在迪拜完成
- 系统、合规、客户支持是否完全外包
- 本地是否只有"牌照壳"
  交付要点：准备**实质运营证据包**（人员、会议、系统权限、决策记录）。

Q325：VARA 是否会审查董事会或高管的"实际参与度"？

A：会。
监管会通过：

- 会议纪要
- 决策文件
- 重大事件签批记录
  判断董事/高管是否**真正参与治理**，而非"挂名"。
  交付建议：董事会/管理层会议**必须有风险与合规议题**，且有讨论与指示痕迹。

Q326：如果合规负责人（CO/MLRO）长期依赖外部顾问，会有问题吗？

A：可能有问题。
VARA 允许外部支持，但**不接受"完全外包合规责任"**。
合规红线：

- 内部必须有明确问责人
- 外部顾问只能"支持"，不能"替代"
  交付建议：明确内部签字权与升级路径。

Q327：VARA 如何看待"合规 KPI 与业务 KPI 的冲突"？

A：这是监管重点。
若合规岗位 KPI 与营收/增长强绑定，可能被认定为**独立性不足**。
交付建议：

- 合规 KPI 以**质量、及时性、闭环率**为主
- 明确写入薪酬与绩效政策

Q328：监管是否会要求机构提供"历史合规问题清单"？

A：在年审、主题审查或扩展业务时，**经常会要求**。
交付级做法：

- 建立 **Compliance Issue Register（合规问题台账）**
- 记录：问题 → 根因 → 整改 → 复测 → 关闭
  这是**成熟机构的重要加分项**。

Q329：如果发生轻微违规但已内部整改，是否仍需上报？

A：取决于**性质与影响**。
但在以下情况下，建议上报：

- 涉及客户资产或数据
- 涉及 AML/制裁
- 可能被第三方或客户察觉
  原则：**不确定时，宁可保守通报**。

Q330：VARA 如何评估一家机构的"合规文化"？

A：并非看口号，而是看：

- 员工培训是否真实
- 合规是否能否决业务
- 是否主动发现问题
- 是否有持续改进
  交付关键证据：培训记录、拒绝客户/业务的案例、整改闭环。

Q331：监管是否会关注"客户画像与营销策略是否匹配"？

A：是。
若你声称"只做专业客户"，但营销内容明显面向零售，将被质疑**风险披露不足或误导**。
交付建议：

- 客户分层 × 营销内容 × 产品权限三者必须一致。

Q332：VARA 是否会复核历史营销内容？

A：会，尤其在投诉或执法调查中。
实务要点：

- 营销材料需版本管理
- 下架内容也要留档
- 能说明"何时、为何、由谁批准"

Q333：监管是否关注 IT 与合规之间的协作机制？

A：高度关注。
若 IT 无法配合导出数据、设置控制点、支持调查，监管会认定合规**不可执行**。
交付建议：

- 建立 IT–合规联动流程
- 明确响应 SLA 与优先级

Q334：VARA 如何看待"快速扩张但合规滞后"的机构？

A：这是**高风险画像**。
监管更偏好：**稳健扩张 + 合规先行**。
交付策略：扩张前做**合规影响评估（CIA）**，并留痕。

Q335：是否建议在持牌后进行"合规成熟度评估"?

A：强烈建议。
交付方式包括：

- 内部成熟度自评
- 外部独立评估
- 与监管最佳实践对标
  这类报告在年审与扩展业务中非常有说服力。

Q. 执法、处罚与合规后果（Q336–Q360）

Q336：VARA 的执法工具有哪些?

A：警告、罚款、附加条件、业务限制、暂停或吊销许可、公开通报。
VARA 真正监管的不是“制度文本”，而是“一家机构是否具备自我约束、持续改进与真实运营的能力”。

Q337：哪些违规最容易被罚?

A：

- 误导性营销
- 未通报重大事件
- 客户资产隔离失败
- AML 严重缺陷
- 未经批准的业务扩展

Q338：罚款是否有上限?

A：按法规与个案裁量，**可叠加**（多项违规、多次发生）。

Q339：主动通报是否有助于减轻处罚?

A：通常是**减轻因素**。迟报/不报往往加重后果。

Q340：监管如何认定“管理层失职”?

A：看是否存在：知情不报、忽视内控、纵容违规、未推动整改。

Q341：个人会被追责吗?

A：可能。关键岗位（董事、CO/MLRO）在严重失当时存在个人责任风险。

Q342：处罚会影响银行/合作伙伴吗?

A：会。公开执法常触发银行重新评估甚至终止合作。

Q343：如何把“处罚风险”前移管理?

A：季度风险评审、独立审查、证据化留存、董事会监督、红线清单。

Q344：被处罚后还能继续经营吗?

A：取决于性质与整改。轻微违规可整改继续；严重者可能被限制或退出。

Q345：执法模块一句话结论?

A：“合规缺口拖得越久，代价越大。”

R. 牌照变更、扩展与退出（Wind-down）（Q361–Q385）

Q361：新增业务活动需要重新申请吗？

A：通常需要**变更/新增许可**。必须先做影响评估，再走审批流程。

Q362：更换 UBO、董事或关键岗位要报吗？

A：要。**关键人员与所有权变更**需及时通报并可能需事前批准。

Q363：集团重组或跨境迁移如何处理？

A：需提交结构图、控制与风险评估、数据与资产安排，确保不削弱监管可见性。

Q364：技术或托管架构重大变更怎么办？

A：提前评估并通报；必要时提供演示与独立评估。

Q365：如果决定停止业务，是否需要“清退计划”？

A：必须。**Wind-down Plan** 是监管重点。

Q366：清退计划要包含哪些？

A：客户通知、资产迁移与对账、未决交易处理、费用结算、投诉处理、数据留存与销毁、监管沟通时间表。

Q367：清退期间可以继续营销或吸收新客户吗？

A：不应。应限制新增风险并保护现有客户。

Q368：清退失败的最大风险？

A：资产迁移混乱、对账不清、沟通不透明，易引发投诉与执法。

Q369：是否需要独立第三方协助清退？

A：高风险业务建议引入（托管/审计/法律），提升可信度。

Q370：退出完成后是否仍需留存记录？

A：是，按法定年限继续留存。

Q371：牌照暂停与吊销的区别？

A：暂停为临时限制；吊销为终止。后者影响更深远。

Q372：被吊销还能再申请吗？

A：难度极高，需充分整改与时间间隔。

Q373：变更与退出模块一句话结论？

A：“退出同样需要合规设计。”

S. 跨境经营、集团结构与数据（Q386–Q395）

Q386：VARA 是否限制跨境服务？

A：允许跨境，但必须遵守**服务地法规**与数据/制裁要求。

Q387：集团多牌照如何避免冲突？

A：明确业务边界、客户分层、信息隔离、冲突管理与披露。

Q388：跨境数据传输的合规要点？

A：数据分类、加密、访问控制、审计权、跨境依据与记录。

Q389：不同司法辖区的营销如何管理？

A：按目的地法规区分；不得以 VARA 牌照误导其他市场。

Q390：如何向监管解释“集团协同”不削弱控制？

A：提交治理与控制映射：谁决策、谁执行、谁审计、证据在哪。

Q391：跨境模块一句话结论？

A：“全球协同，单点问责。”

T. 实操清单、最终结论与交付收官（Q396–Q400）

Q396：VARA VASP 合规的“五大支柱”？

A：

1. 资产安全（托管/对账/审批）
2. AML/CFT（KYC/KYT/STR）
3. 技术韧性（安全/DR/日志）
4. 治理与问责（三道防线）
5. 透明沟通（报告/营销/事件）

Q397：最快拉开合规差距的做法？

A：证据化：**把制度变成可导出的报表与日志**。

Q398：面向董事会的一句话建议？

A：“把合规当成基础设施，而不是成本中心。”

Q399：对准备申请或已持牌机构的最终提醒？

A：先定业务边界 → 先建系统与证据 → 再提交申请/扩展；持续演练、持续改进。

Q400：全文终极结论？

A：VARA 关注的不是“你写了什么”，而是“你是否每天都在按你写的去做”。

关于仁港永胜

---

1) 仁港永胜建议

1.1 先定“受规管活动组合”，避免范围漂移

VARA 采取“活动分轨（activity-based）”监管：不同活动（Exchange、Broker-Dealer、Custody、Advisory、Management & Investment、Transfer & Settlement、Lending & Borrowing 等）会触发不同规则与审查重点。建议先用 **Scope Matrix** 固化：

- 你做什么 / 不做什么
- 面向谁（零售/机构/专业投资者）
- 资金流与资产流

- 风险等级与控制点
  并让商业计划、客户协议、营销材料、系统权限“四件套”完全一致。

1.2 把“合规管理系统 CMS”做成可运行系统，而不是文件夹

VARA 明确要求 VASP 建立并维持有效的 **Compliance Management System（CMS）**：覆盖运营全链路、具备独立性、对董事会可视、能及时发现并上报重大不合规。建议交付时直接落成：

- 合规制度包（Policy Suite）
- 证据索引（Evidence Index）
- 抽检与整改闭环（Issue Log → Root Cause → Remediation → Retest → Close）
- 48 小时可交付监管资料包（RFI Pack）
  （监管问的不是“有没有写”，而是“能不能导出证据”。）

1.3 把“客户资产安全”当成第一产品（Custody/Key/Wallet/Recon）

客户资产与记录保存是 VARA 核心审查点之一：必须做到**可隔离、可对账、可审计、可追溯**。建议交付落地：

- 钱包分层（热/温/冷）与签名策略（MPC/多签）
- 提币审批链（四眼原则/分权）
- 日对账/差异处理 SOP
- 应急冻结与事故响应流程
- 关键外包（如托管商/云/安全服务）审计权+退出方案
  （“责任不外包”是底线。）

1.4 AML/CFT：用“实时监控 + goAML + STR 闭环”建立可解释体系

VARA 规则体系要求 VASP 的 AML/CFT 计划可运行并与联邦 AML 法框架一致。建议交付重点放在：

- 客户风险分层（KYC/KYB/EDD）
- 链上监控（KYT）规则库 + 告警工单闭环
- STR 决策与留痕（含升级路径、持续监控）
- 监管信息请求 48 小时响应机制（RFI SLA）

1.5 营销合规：宁可克制，不可“暗示监管背书/保本收益”

Marketing Regulations 2024 对“误导性宣传、超范围宣传、风险披露不足、对零售不当营销”等高度敏感。建议交付落地：

- 营销审批流程（合规/法务签批 + 版本管理）
- KOL/代理合规条款与抽检
- 声明模板（不保本、不保证收益、不暗示官方推荐）
- 与客户协议一致性核查（Marketing vs T&C）

---

2) 为何选择仁港永胜

1. **交付级文件体系**：不止“制度文本”，而是“制度 + 证据输出 + 演示脚本 + 闭环台账”一体化，直接满足 CMS 与 RFI 需求。
2. **活动分轨打法**：按 VARA activity-based Rulebooks 为骨架，帮助你把 Exchange/Custody/Broker/Advisory 等不同活动的重点控制“提前装配”。
3. **技术合规落地**：从权限矩阵、密钥治理、日志留存到 DR 演练，提供可审计证据链，而非泛泛建议。
4. **年审与执法风险前置管理**：用 Top 50 高危问题清单 + 10 分钟面谈速查表，把“最可能被罚的点”提前封堵。

---

3) 关于仁港永胜

仁港永胜（香港）有限公司｜Rengangyongsheng (Hong Kong) Limited
定位：面向虚拟资产与金融科技机构的**合规许可申请、制度搭建、持续监管与年审陪跑**服务商。
交付风格：以监管条文为底座，输出可递交、可审计、可复盘的“交付件”，并将关键控制点落到系统与证据链。

---

4) 联系方式

—— **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

服务方向：Dubai VARA / EU MiCA / 香港 SFC / 香港 MSO / 全球 VASP 与支付合规

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）

业务经理｜合规与监管许可负责人

- 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**完整可编辑 Word / PDF 版本、制度模板、清单包**交付件，可向仁港永胜唐生 **有偿索取**（用于监管递交与内部落地）。

---

5) 服务（VARA 交付版服务菜单）

依据 VARA 的 Regulations + Rulebooks 体系（含 CMS、执法与营销要求）设计服务包。

5.1 牌照申请与活动范围设计

- 受规管活动组合策略（Scope Matrix）
- 商业计划书（监管版）+ 风险画像
- 组织结构与问责链（Board / SMF / CO / MLRO）

5.2 合规制度与证据链落地（CMS 一体化）

- CMS 主文件（合规治理、独立性、报告路径）
- AML/CFT+KYT 制度包与工单闭环
- 记录保存与证据索引体系（Evidence Index）
- 事件通报与监管沟通 SOP

5.3 技术与安全合规（可演示）

- 密钥治理与钱包分层、提币审批链
- 权限矩阵（IAM）与日志留存（可导出）
- DR/BCP 演练方案与记录模板

5.4 年审与持续监管陪跑

- 年度合规计划（Annual Compliance Plan）

- 独立审查/内审对接与整改闭环
- 监管检查 48 小时资料包（RFI-ready）

5.5 营销合规与对外材料审阅

- Marketing 审批流程与话术红线
- KOL/代理合规条款与抽检机制
- 官网/白皮书/路演材料合规审阅

---

6) 免责声明

本文为一般性信息与实务指引，不构成法律意见或对监管结果的保证。具体适用应以 **VARA 最新法规、规则书（Rulebooks）及个案沟通结果**为准；并可能同时受到阿联酋联邦 AML/CFT 法规及其他主管机关要求的影响。

仁港永胜不对因单独使用本资料而产生的任何直接或间接后果承担责任。

仁港永胜保留对本文内容更新与修订的权利。

---

7) VARA 年审/执法高危问题 Top 50 清单（交付版｜直接用于自查与董事会汇报）

这些问题对应 VARA 最常“抽样验证”的控制点：**CMS、客户资产、AML、外包、营销、事件通报、记录保存**等。

A. 许可范围与实际经营（1–8）

1. 你是否开展了未获批活动/变相活动?
2. 客户协议/官网/营销是否与获批范围一致?
3. 是否存在零售导向营销但自称只做机构?
4. 重大业务模型变更是否及时通报?
5. 实际客户/交易量是否远超商业计划假设且未调整控制?
6. 是否存在“集团协同”导致监管不可见/不可控?
7. 是否存在绕开风控的“特殊客户通道”?
8. 牌照条件（conditions）是否全部落实并留证据?

B. CMS 与合规独立性（9–16）

9. CMS 是否独立于业务线？CO 是否能否决?
10. 是否有重大不合规的升级机制与记录?
11. 合规 KPI 是否被营收绑定（独立性受损）?
12. 是否具备 48 小时 RFI 响应能力（证据导出）?
13. 是否有年度合规计划与执行证据?
14. 是否有合规抽检与整改闭环台账?
15. 董事会/管理层是否定期审阅合规报告并形成纪要?
16. 关键岗位是否“挂名不履职”?

C. 客户资产、托管与对账（17–26）

17. 客户资产是否清晰隔离与可证明归属?
18. 钱包分层与签名策略是否记录化、可审计?
19. 提币是否严格审批（四眼/分权）且全程留痕?
20. 是否存在“后台直提/紧急口令提币”未留痕?
21. 是否进行日对账？差异是否闭环?
22. 托管外包是否有审计权与退出方案?
23. 价格源/估值异常是否有熔断机制?

24. 客户资产相关事故是否及时通报?
25. 权限矩阵是否定期复核?
26. 冷钱包应急流程是否演练并留证据?

D. AML/CFT + KYT + STR（27–36）

27. 风险评估是否更新？客户风险分层是否真实执行?
28. KYT 规则库是否匹配你实际链上暴露?
29. 告警工单是否闭环（调查、结论、措施）？
30. STR 决策是否有升级路径与留痕?
31. 制裁命中处置是否及时且可复核?
32. 高风险国家/行业是否有额外控制?
33. 是否存在“为业务放宽 EDD”的记录?
34. 交易监控是否足够及时（实时/近实时）？
35. STR 后是否持续监控而非“一报了之”？
36. goAML/监管沟通责任人是否明确?

E. 外包与第三方（37–43）

37. 关键外包是否已分类并获管理层批准?
38. 合同是否包含审计权、子处理方、事故通报、数据导出、退出?
39. 云/托管/撮合等关键供应商是否有 DR 与切换方案?
40. 是否做持续供应商监控（SLA/KPI/年度复核）？
41. 外包数据是否可随时导出与迁移?
42. 供应商事件响应是否演练?
43. 供应商拒绝审计权是否仍被用于关键功能?

F. 营销合规与客户披露（44–50）

44. 是否存在“保本/保证收益/官方背书”暗示?
45. 风险披露是否清晰、显著、与产品匹配?
46. KOL/代理是否发布违规内容且你无监控证据?
47. 营销审批是否留痕（版本管理）？
48. 下架内容是否留档以备追溯?
49. 客户协议与营销内容是否一致（费用/风险/限制）？
50. 投诉处理是否及时、记录完整并可复盘?

---

8) 监管面谈问答速查表（10 分钟版本）

用于 **VARA 面谈/现场检查/临时问询**。建议配合你们的“证据索引编号”边讲边展示。

8.1 我们是谁、做什么（30 秒）

- 我们获 VARA 授权开展的活动是：**（列明）**
- 我们不开展：**（列明红线）**
- 目标客户：**（机构/专业/零售）**，营销与条款完全一致。

8.2 客户资产如何保护（90 秒）

- 资产隔离：客户资产与自有资产分层管理、独立账簿与对账机制。
- 密钥治理：MPC/多签 + 分权审批 + 最小权限。
- 提币控制：四眼原则、风控规则、异常拦截、全程日志。

- 证据：钱包策略、审批日志、对账报表、权限矩阵导出。

8.3 AML/CFT 如何运作（120 秒）

- 风险评估与分层：KYC/KYB/EDD，定期复核。
- 监控：KYT 规则库 + 实时/近实时告警。
- 闭环：告警→调查→处置→（必要时）STR→持续监控。
- 证据：样本客户 KYC 包、告警工单、STR 决策记录、培训记录。

8.4 合规如何独立（60 秒）

- 我们建立 CMS，合规独立于业务线，CO 有升级与否决机制。
- 董事会/管理层按季度审阅合规与风险报告并留纪要。

8.5 外包怎么管（60 秒）

- 关键外包清单与分级；合同含审计权、事故通报、数据导出、退出方案。
- 供应商季度 KPI + 年度复核 + 重大变更审批。

8.6 营销如何避免误导（45 秒）

- 所有营销材料合规审批与版本管理；不暗示保本、收益保证或官方背书。
- KOL/代理有合规条款与抽检记录。

8.7 事件与通报（45 秒）

- 重大事件 24 小时初报、持续更新；保留事故处置与复盘证据。
- 48 小时内可响应监管 RFI（资料包已预制）。

8.8 最后一问：你们如何证明“不是纸面合规”（30 秒）

- 我们所有控制点都有系统日志与报表输出；抽样可复算；整改闭环可追溯。

全文讲解完