



仁港永胜

协助金融牌照申请及银行开户一站式服务

网址: www.CNJRP.com 手机: 15920002080 地址: 香港环球贸易广场86楼 852 92984213 (WhatsApp)



正直诚信
恪守信用

荷兰 Netherlands (MiCA) 加密资产服务提供商 (CASP) 牌照 常见问题 (FAQ 大全)

Frequently Asked Questions about the Netherlands (MiCA) Crypto Asset Service Provider (CASP) License

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

(MiCA: Regulation (EU) 2023/1114 | DORA: Regulation (EU) 2022/2554 | 结合荷兰监管口径: AFM + DNB)

文档说明（交付与索取）：本指南适用于制作 BP、Programme of Operations、AML/ICT/Outsourcing 包、Fit & Proper/UBO 包与项目索引。如需 PDF 交付版 / 可编辑 Word 版 / Master Checklist Excel / RFI Q&A Pack / 面谈题库，可向仁港永胜唐生索取（有偿）。

点击这里可以下载 PDF 文件：[荷兰 Netherlands \(MiCA\) 加密资产服务提供商 \(CASP\) 牌照申请注册指南](#)

点击这里可以下载 PDF 文件：[关于仁港永胜](#)

1) 牌照名称

牌照名称：荷兰 MiCA 加密资产服务提供商牌照 | 加密资产服务提供商牌照 (CASP) (MiCAR Title V)

英文：Crypto-Asset Service Provider (CASP) Authorisation under MiCAR

主管机关（申请受理/行为监管主线）：AFM (Dutch Authority for the Financial Markets)

审慎/持股核准/稳定币部分监管：DNB (De Nederlandsche Bank) 对 CASP 的审慎监管、拟议持股 (qualifying holdings) 评估，并对 EMT/ART 发行人承担权限

服务商：仁港永胜（香港）有限公司

本文由 仁港永胜（香港）有限公司 拟定，并由 唐上永（唐生） 业务经理 提供专业讲解。

2) 牌照介绍与申请优势

2.1 MiCA 统一授权的核心价值

- **单一牌照 + 欧盟护照：**获批后可按 MiCA 护照机制在 EU 跨境展业（自由提供服务/设分支），形成“一个母牌照覆盖全欧盟”的合规底座。
- **行为、治理、客户保护、资本/保障、ICT、外包一体化：**监管审查从“文件齐全”升级为“可运行、可审计、可验证”。

2.2 荷兰的市场/监管优势（实操视角）

- **监管分工清晰 (AFM + DNB)：**CASP 主要由 AFM 负责受理与监管；DNB侧重审慎与拟议持股评估、以及 EMT/ART 发行人监管，有利于申请包按分工拆解交付。
- **过渡期窗口明确：**对“已在 DNB AML 注册”的机构，MiCAR 许可要求自 2025-06-30 起适用（等同给了 6 个月过渡缓冲）。
- **AFM 公开登记与透明度：**AFM 已设 **CASP register**，对外展示“获授权/已通知”的 CASP，利于对接银行、合作机构、做品牌背书。

3) 监管机构与适用法律 (NCA + 本国实施法/监管口径 + MiCA 主法)

3.1 主管机构 (Netherlands NCA)

- **AFM：**CASP 授权/通知、行为监管 (conduct) 主线；对外发布 MiCAR 关键节点与执法态度。
- **DNB：**
 - 对 CASP 进行审慎监管与拟议持股评估；
 - 对 EMT/ART (稳定币) 发行人承担主管权能。

3.2 主要适用法规（申请材料“法律依据段”建议写法）

- **MiCA 主法**: Regulation (EU) 2023/1114 (CASP 授权、持续义务、行为规范、客户保护、外包治理等)。
- **DORA**: Regulation (EU) 2022/2554, 自 2025-01-17 起适用, ICT 风险、事件、第三方外包与韧性测试要求显著增强。
- **荷兰 AML (Wwft) 框架**: 作为 AML/CFT 体系基础 (客户尽调、交易监控、STR、制裁筛查、记录保存等; MiCA 不替代 AML)。DNB “Crypto service providers” 监督口径亦强调 MiCAR 与既有监督主题衔接。

以下为《**荷兰 Netherlands (MiCA) 加密资产服务提供商 (CASP) 牌照常见问题 (FAQ 大全)**》

说明: 荷兰 MiCA 主管机关信息与过渡期节点, 以 AFM 官方专题页与其“Crypto-asset service providers”登记页为准; 荷兰过渡机制已于 2025-06-30 结束。

另: MiCA 作为欧盟统一法规, 自 2023-06-30 生效 (并分阶段适用)。

本文由 **仁港永胜 (香港) 有限公司** 拟定, 并由 **唐生** 提供专业讲解。

A | 荷兰MiCA CASP 牌照定位与监管框架 (Q1-Q20)

Q1: 荷兰 MiCA 下的 CASP 是什么?

A1: CASP (Crypto-Asset Service Provider) 指在 MiCA 框架下, 以专业方式向客户提供加密资产服务而需取得授权的机构; 获批后可用 EU 护照机制跨境展业 (需通报)。

Q2: 在荷兰申请 CASP, 主管监管机构是谁?

A2: 荷兰对 MiCA 的“加密资产服务提供商 (CASP)”相关监管与信息披露, AFM 已建立 MiCAR 专题页并维护相关登记信息; 实务上通常以 AFM 作为主要受理/主管窗口进行沟通与许可流程安排。

Q3: DNB (荷兰央行) 还管加密吗?

A3: 在 MiCA 前, 部分加密业务在荷兰需要 **DNB 注册** (与反洗钱框架相关), DNB 也持续发布对未注册经营的执法案例; 进入 MiCA 后, 许可逻辑转向 MiCA 授权, 但 AML/Wwft 等义务仍然关键。

Q4: MiCA 对 CASP 何时开始适用?

A4: AFM 明确 MiCA 于 2023-06-30 生效; CASP 授权要求分阶段实施, 荷兰也设置过渡安排并已结束 (见 Q5)。

Q5: 荷兰过渡期 (transitional regime) 是什么? 什么时候结束?

A5: AFM 登记页写明: 曾在 2024-12-30 前已按 DNB 注册的特定加密服务商, 可在荷兰 MiCA 过渡机制下继续服务至 2025-06-30; 并明确荷兰过渡机制已于 2025-06-30 结束。

Q6: 没有 CASP 牌照还能在荷兰继续做业务吗?

A6: 若已不在有效过渡安排内, 继续“向公众提供受规管加密资产服务”将面临重大合规风险 (包括执法与罚款); DNB 曾就未按当时法律要求注册而经营的情形作出罚款决定, 显示执法并非理论风险。

Q7: CASP 牌照覆盖哪些服务类型?

A7: 一般包括: 托管/管理、运营交易平台、加密兑法币/加密兑加密、执行/传递订单、转移服务、投顾与组合管理等; 申请必须“逐项勾选 + 逐项写流程与控制”。(服务分类以 MiCA 法定定义为准, 申请文件应逐条映射。)

Q8: 我只做撮合/经纪 (不碰客户资产) 算不算 CASP?

A8: 通常仍可能落入: 接收/传递订单、执行订单、运营平台或兑换等服务项; 关键取决于你在客户旅程中是否提供“受规管服务行为”(撮合方式、收费方式、是否代表客户执行、是否形成平台规则/订单簿等)。建议做“业务定性备忘录”锁定服务项边界。

Q9: 我只做托管钱包算不算 CASP?

A9: 是, 高概率属于“托管与管理加密资产”服务项; 托管对密钥管理、冷热钱包、权限分离、资产隔离、对账与审计轨迹要求最重之一。

Q10: 我只做加密兑加密需要牌照吗?

A10: 在 MiCA 下“兑换”类服务通常需要授权; 历史上荷兰 DNB 注册规则侧重某些类别 (例如法币兑换/托管), 但 MiCA 进入后应按 MiCA 服务表判断, 不建议沿用旧时代经验。

Q11: 如果我在别的欧盟国家拿了 CASP, 能来荷兰直接做吗?

A11: 可走 MiCA 护照通报机制在荷兰自由提供服务或设分支, 但仍要遵守荷兰消费者保护、营销合规、AML 义务与本地执法口径, 且需要按通报程序完成跨境落地。

Q12: 荷兰是否要求本地公司实体?

A12: 若你选择“在荷兰申请牌照”, 通常需要欧盟内实体并满足有效管理与可监管触达; 若你在他国持牌进入荷兰, 则取决于以“自由提供服务”还是“设分支”方式进入, 以及业务模式与本地运营安排。

Q13: 荷兰对“有效管理地”怎么看?

A13: 核心是: 关键决策、治理与控制职能要真实可核验 (董事会运作、合规/MLRO 履职、关键外包治理、系统与日志审计)。单靠形式注册地址/挂名人员很难通过实质审查。

Q14: MiCA 与荷兰 AML (Wwft) 关系是什么?

A14: MiCA 解决“牌照/行为规范/客户保护/审慎与治理/跨境护照”, 而 AML (如 Wwft、制裁法等) 决定“反洗钱与制裁筛查的底线”; DNB/CMS 等公开材料显示 Wwft 与制裁法在荷兰加密合规中长期是核心要求。

Q15：荷兰是否有官方登记/清单可查？

A15: AFM 提供“Crypto-asset service providers”登记页，并注明过渡机制结束时间与当时纳入过渡机制的机构范围。

Q16：申请材料英文可行吗？

A16: 实务中英文通常可用以利于跨境团队准备；但公证/认证、公司法文件、以及监管沟通语言要求应以 AFM 实操与项目安排为准（建议关键声明准备可认证译本）。

Q17：拿到 CASP 后是否自动能做所有加密业务？

A17: 不是。授权是“服务项颗粒度”——你获批哪些服务就只能做哪些；超范围展业是重大合规风险。

Q18：荷兰对“宣传/营销”有什么敏感点？

A18: 最敏感的是“暗示已获批/等同持牌/受监管保证收益”等误导性表述；在过渡期结束后，任何“申请中也可放心使用”等宣传更易触发执法关注。

Q19：荷兰会重点审什么？

A19: 通常集中在：股东/UBO 声誉与资金来源、董事与关键岗位适任性、AML/KYC 的有效性、托管/钱包安全与外包可审计性、客户资产隔离与披露、以及项目是否具备真实运营能力。

Q20：最先做什么文件最关键？

A20: 先定 **Programme of Operations**（运营方案/服务范围），因为它决定：资本/保险方案、岗位配置、系统与外包边界、客户条款披露、以及 AML 场景与监控规则库的深度。

B | 实体设立与实质经营（Q21–Q40）

Q21：是否必须有荷兰办公室？

A21: 不是“只看租约”，而是看是否能证明实质运营：本地可触达管理、合规/MLRO 履职、会议纪要与授权留痕、IT 运维与外包管理可审计。建议有可核验办公安排。

Q22：董事必须是荷兰居民吗？

A22: 通常不以国籍作为硬门槛，但会审查：是否足够时间投入、是否能在欧盟内有效管理、是否可被监管面谈与问责、是否存在利益冲突。

Q23：可以远程团队为主吗？

A23: 可以，但你必须交代并证明：远程访问控制、日志不可篡改、关键审批“四眼原则”、外包审计权、以及监管沟通可到场能力。

Q24：最低员工人数有要求吗？

A24: MiCA 更强调“与业务规模匹配的资源与控制能力”。关键岗位必须真实可履职（不是“挂名外包”）。

Q25：集团公司能用母公司资源替代本地资源吗？

A25: 可以体现集团支持（政策、系统、资金、审计资源），但申请主体仍需有足够控制力、责任边界、以及可监管触达的治理安排。

Q26：需要设立哪些治理委员会？

A26: 建议至少：董事会/管理层会议机制；合规与风险议题上会机制；重大外包审批机制；新产品审批（NPC）；重大事件（安全/合规）通报机制。

Q27：如何证明“有效管理（effective management）”？

A27: 用证据链：董事会章程 + 年度会议日程 + 授权矩阵（DoA）+ 纪要模板 + 决策留痕（投票/签字）+ KPI 与风险报告上会记录。

Q28：是否必须设内部审计？

A28: 可按规模内设或外包，但必须满足独立性、审计范围、审计权与整改闭环；外包不等于免责。

Q29：是否需要数据保护官（DPO）？

A29: 视业务规模与 GDPR 触发条件而定；即便不强制，也应明确数据保护治理责任人与数据处理协议（DPA）。

Q30：如果我同时做支付/法币收付怎么办？

A30: CASP 不等于支付牌照。法币收付多通过银行/EMI/PI 合作；你必须在运营方案中画清资金流、责任边界、对账与客户披露。

Q31：可以用代理/经纪渠道拓客吗？

A31: 可以，但需渠道尽调、合同约束、反洗钱与制裁要求传导、培训与抽查、以及营销话术合规审查。

Q32：我能在获批前先做“试运营”吗？

A32: 原则上避免形成“对公众提供受规管服务”的事实；可做内部测试、封闭白名单、技术演练，但对外宣传、开户、收款、撮合等行为要非常谨慎。

Q33：公司章程经营范围要怎么写？

A33: 建议覆盖拟申请的 CAS 服务项，并与业务描述一致；避免章程范围过宽导致监管追问“为何不申请这些服务”。

Q34：股权结构复杂会影响审批吗？

A34: 会增加穿透尽调与补件轮次；建议减少多层离岸控股、减少协议控制工具，或至少准备“控制权说明信 + 资金路径图 + 关联方披露”闭环。

Q35：是否需要在荷兰开公司银行账户？

A35: 不一定必须本地，但必须可审计、可对账、可监管触达；银行/EMI 合作方尽调也会影响项目周期。

Q36：对外包云服务有什么地域偏好？

A36: 优先欧盟区域部署更稳（数据、监管触达、审计权）；若用非欧盟云，需额外解释跨境合规与监管可获取性。

Q37：董事/高管能否同时管理其他受监管机构？

A37：可行但需披露兼职与时间投入；如与竞争对手或关键供应商存在利益冲突，要提前制定冲突管理与回避机制。

Q38：如何设计“退出/关停计划（Wind-down plan）”？

A38：必须涵盖：客户资产安全返还、未完成交易处理、关键外包退出与数据迁移、员工与访问权限撤销、监管通报与客户通知模板。

Q39：申请失败最常见“组织原因”是什么？

A39：治理空心化（关键岗位挂名）、外包不可审计、董事会缺乏可核验证据链、以及业务范围与系统能力不匹配。

Q40：如何降低补件（RFI）轮次？

A40：把申请包做成“可审计索引”：A-I Master Checklist、编号规则、交叉引用（BP ↔ AML ↔ ICT ↔ 客户协议 ↔ 财务/资本），并建立补件战情室机制。

C | 服务范围与运营方案（Programme of Operations）(Q41–Q60)

Q41：Programme of Operations 应包含哪些最小要素？

A41：服务项清单、客户旅程（开户-交易-托管-提现-投诉-关户）、交易/撮合逻辑、资金流与钱包流、外包清单与责任边界、关键控制点（AML/风控/权限）、以及跨境护照计划。

Q42：我可以只申请“最省成本”的服务项吗？

A42：可以，但必须与真实业务一致；若实际运营超范围，风险极高。建议采用“分阶段服务扩张”策略（先单项、后增项）。

Q43：交易平台与执行订单有什么区别？

A43：平台通常涉及订单簿/撮合规则/市场监控与透明披露；执行订单偏向为客户在外部场所执行。不同服务项对系统、记录与市场监控要求不同。

Q44：OTC 业务如何在文件中定义？

A44：必须明确：是否报价做市、是否撮合第三方、是否代表客户执行、是否持有客户资产、是否经由自营钱包中转；OTC 常被监管视为 AML 高风险场景。

Q45：如果不碰法币，只做 crypto-to-crypto，会轻松吗？

A45：不一定。AML、链上风险、制裁筛查、市场滥用与钱包安全仍然严；尤其若提供托管/平台，ICT 要求不会因为不碰法币而降低。

Q46：可以把 KYC、链上分析、客服都外包吗？

A46：可以外包，但不能外包责任。你必须提供：供应商尽调、合同/SLA、审计权、数据与安全要求、退出预案、以及内部监督与 KPI。

Q47：外包最容易被问哪些问题？

A47：谁拥有最终决策权？是否可审计？是否可替代？数据在哪里？是否有重大集中度风险？如何监控 SLA？退出怎么做？

Q48：我要做衍生品/杠杆怎么办？

A48：MiCA 主要聚焦现货加密资产服务；衍生品往往涉及其他金融监管框架（例如 MiFID 等），需单独法律定性，不建议在 CASP 申请中模糊带过。

Q49：我要做 RWA/证券型代币怎么写？

A49：需先判断是否属于 MiCA 范围或落入金融工具监管；若可能为金融工具，应走对应证券监管路径，避免“MiCA 申请但实际是证券发行/交易”的监管雷区。

Q50：收费模型要披露到什么程度？

A50：要做到“可核验、可对账、可对客户解释”：交易费、点差、托管费、提现费、第三方费用、返佣/做市利益冲突披露、费用变更通知机制。

Q51：如何证明“最佳执行/公平撮合”？

A51：若涉及执行订单/平台撮合，应有撮合规则、订单优先级、异常交易处置、系统时间戳与日志、以及对外披露机制。

Q52：是否需要市场滥用监控（刷量/操纵）？

A52：平台型业务强烈需要：异常交易规则、关联账户识别、做市/自营隔离、公告与处置流程、记录留存。

Q53：我要做 staking/收益产品，能放进 CASP 吗？

A53：要谨慎：收益类产品可能触发额外消费者保护与产品治理要求，甚至落入其他监管分类；应先做法律定性与风险披露框架。

Q54：客户分类（零售/专业）怎么做？

A54：设定专业客户认定标准、证明材料清单、审批与复核周期；并在条款中明确不同保护水平与限制措施。

Q55：营销合规最小控制是什么？

A55：建立“Marketing Approval Log”：所有广告/推文/落地页/销售话术必须过合规审批，禁止误导性表述与夸大收益。

Q56：跨境提供服务最常见踩坑点？

A56：未完成护照通报、在目标国违反消费者保护/语言披露要求、以及跨境招揽触发第三国规则或制裁风险。

Q57：我能否只做 B2B（机构客户）降低要求？

A57：B2B 可在客户保护与适当性上相对更可控，但 AML、制裁、ICT、外包、治理并不会消失；仍要证明风险可控与披露清晰。

Q58：我要接入银行/EMI 通道，申请包要写什么？

A58：合作结构、责任边界、资金流与对账、拒付/冻结规则、数据共享与隐私、以及合作方尽调与退出预案。

Q59: Programme of Operations 写多长合适?

A59: 宁可“按流程与控制点写细”，也不要空泛；监管最怕“看不出怎么运营、怎么控制风险、怎么审计”。

Q60: 运营方案和 BP (商业计划) 怎么分工?

A60: 运营方案回答“做什么、怎么做、如何控制”；BP 回答“为什么可行、资源与预算、财务预测、持续经营与资本/保险覆盖”。

D | 股东/UBO 与适任性 (Fit & Proper) 总则 (Q61-Q80)

Q61: 10%/重大持股的门槛怎么理解?

A61: 一般以“重大影响/重大持股”作为触发更严格尽调与持续通知义务的门槛；实务建议：任何可能构成控制或重大影响的股东均按金融监管标准准备全套 DD。

Q62: 股权穿透要到什么层级?

A62: 穿透至最终自然人 UBO，并解释控制链条（投票权、协议控制、可转债/期权等潜在控制工具）。

Q63: 资金来源 (SoF) 与财富来源 (SoW) 有什么区别?

A63: SoW 解释“财富怎么积累”；SoF 解释“这笔出资的钱从哪里来、怎么流到申请主体”。两者必须闭环、可核验、可对账。

Q64: 监管最爱补件的 SoF 问题是什么?

A64: 资金路径断点（中间账户缺流水）、“借贷/代持”解释不清、资产处置证明不足、以及大额现金/第三方付款无法自证。

Q65: 可以用加密资产作为出资/资本吗?

A65: 极不建议作为主要形式；监管偏好稳定、可计量、可审计的资金。若必须涉及，应准备估值、流动性、处置与风险控制说明。

Q66: 股东背景调查要做哪些维度?

A66: 诉讼/破产/监管处罚、不利媒体、制裁与 PEP、商业关系与关联方、以及是否存在金融犯罪/洗钱风险。

Q67: 董事/高管适任性四要素是什么?

A67: 胜任能力（经验可核验）、诚信与声誉、时间投入、利益冲突管理。

Q68: CV 怎么写才“监管友好”?

A68: 写可核验事实：职责、规模、团队人数、系统与合规成果、风控/安全治理经验；避免空话。并附证明材料（任职证明/推荐信/证书）。

Q69: 关键岗位（合规/MLRO/ICT）必须全职吗?

A69: 不一刀切，但必须证明“资源充足、可履职、独立汇报线成立”；对高风险/平台/托管类项目，关键岗位兼职更容易被追问。

Q70: 可以让外部顾问兼任 MLRO 吗?

A70: 不建议作为唯一安排。即便允许外包，监管通常要求内部责任人承担最终责任，外包仅作为支持；并且要有审计权与替代机制。

Q71: 董事会技能矩阵（Skill Matrix）为什么重要?

A71: 它是监管判断“治理能力是否匹配业务风险”的快速工具；平台/托管/安全/AML/合规/金融运营等能力要覆盖。

Q72: 时间投入怎么证明?

A72: 时间投入声明 + 兼职披露 + 年度会议安排 + KPI/报告上会记录；并在面谈中能解释你如何覆盖关键职责。

Q73: 利益冲突常见场景有哪些?

A73: 自营交易与客户撮合、做市与平台运营、关联方提供关键外包、股东向平台导流/返佣、以及关键人员在供应商/竞争对手任职。

Q74: 如何做利益冲突管理?

A74: 冲突登记册 + 回避机制 + 披露机制 + 定价与费用透明 + 交易隔离（自营/做市/客户）+ 审计抽查。

Q75: 重大持股变更需要通知吗?

A75: 通常需要，且需要预先评估与监管沟通；建议建立“股权变更预警机制 + 资料包模板”。

Q76: UBO 是 PEP 会怎样?

A76: 不是自动否决，但需要更强 EDD、财富/资金来源核验、持续监控与更高治理层批准，并准备不利信息解释备忘录。

Q77: 股东来自高风险国家会怎样?

A77: 风险评级会显著上升，需更强的 EDD、资金路径证据、交易与制裁风险控制；部分情形可能影响银行/EMI 合作。

Q78: 董事/高管有历史处罚记录怎么办?

A78: 必须披露并解释整改与当前控制；隐瞒是致命问题。应准备“事件说明 + 证据 + 改善措施”。

Q79: 董事/高管可以在非欧盟吗?

A79: 可以但会被追问“有效管理地、可监管触达、到场面谈、日常履职与安全管理”。建议核心管理与控制职能尽量在欧盟内可触达。

Q80: 最常见“人员原因”失败点?

A80: 关键岗位资历与业务风险不匹配、治理空心化、兼职过多时间投入不足、以及无法解释系统与 AML/安全控制如何落地。

E | 资本/保险/审慎保障 (Q81-Q100)

Q81: MiCA 对资本/审慎保障的逻辑是什么?

A81: 核心不是“给一个统一数字”，而是按服务范围与风险，证明：你有足够的自有资金/等效保障（含保险等）覆盖运营风险与客户保护相关风险，并能持续经营。

Q82：是否必须买保险？

A82：取决于服务项与监管口径；常见做法是“资本+保险/等效保障”的组合，关键是覆盖范围、免赔额、理赔机制与承保人资质可核验。

Q83：托管业务对审慎保障有什么特殊性？

A83：托管涉及客户资产安全事件与赔付预期；审慎保障文件要明确：密钥控制、保险覆盖、赔付政策、事件响应与复盘机制。

Q84：财务预测要做几年？

A84：建议三年（P/L、BS、CF）+压力测试；并把合规、人力、审计、ICT、安全、外包成本计入，避免“预算不真实”。

Q85：压力测试要覆盖哪些情景？

A85：价格剧烈波动、挤兑/提现潮、系统宕机、重大安全事件成本、合作通道中断、以及监管整改成本。

Q86：亏损企业能申请吗？

A86：可以，但必须证明资本与保障持续满足、资金链稳、风控与合规有效、以及有可行的持续经营计划。

Q87：客户资金（法币）在谁的账上？

A87：若无支付/EMI 资质，通常在银行/EMI/PI；你要画清资金流、对账、冻结/退回规则与客户披露。

Q88：可以让股东“承诺注资”替代资本吗？

A88：承诺可作为支持材料，但通常不等于已到位的资本；监管更看重已实缴与可验证的保障安排。

Q89：审慎保障文件怎么写更容易过？

A89：用“风险→控制→覆盖→证据”结构：列风险（运营/安全/欺诈/外包/法律）、列控制（制度+系统）、列覆盖（资本/保险/准备金）、列证据（计算表+合同+报告）。

Q90：资本与客户资产隔离是什么关系？

A90：资产隔离是客户保护底座；资本/保险用于覆盖运营与意外损失。监管通常会联动审查两者是否一致。

Q91：能否用集团担保？

A91：可作为增信，但仍需满足申请主体自身要求；担保条款需可执行、可审计、并明确触发条件。

Q92：资本到位时间点是什么？

A92：通常在获批前/上线前需要满足；项目计划应把“注资/保险出单/开户/验收”作为 Go-Live 前置条件。

Q93：费用（收费）与资本要求有关吗？

A93：收费模式影响风险与财务预测；高频交易/高波动产品/高杠杆宣传会提高监管对风险覆盖与客户保护的要求。

Q94：做市/自营交易会提高资本压力吗？

A94：会显著提高风险与利益冲突审查强度；需要更强隔离、限额、风控与披露，也可能影响审慎保障论证。

Q95：审计师在资本与财务预测中扮演什么角色？

A95：年度审计与可能的独立审查（AML/ICT）会成为持续合规证据链的一部分；成本应纳入预算。

Q96：资本证明用什么文件？

A96：银行入资证明、验资/审计证明（如适用）、财务报表、资金路径证据、以及董事会决议/股东决议。

Q97：是否必须设立客户资产信托/第三方托管结构？

A97：不一定，但必须证明客户资产隔离与可对账；若采用第三方托管，要说明密钥控制与责任边界。

Q98：安全事件赔付政策必须写吗？

A98：建议写清：触发条件、调查流程、是否全额/部分赔付、保险索赔路径、上限与排除条款、以及客户沟通模板。

Q99：监管会看“资金用途”吗？

A99：会。资金用途与预算必须支撑合规与安全落地（人、系统、审计、外包治理），否则会被质疑“拿牌后无法运营”。

Q100：资本/保障最常见补件点？

A100：保险覆盖不匹配服务项、财务预测过度乐观、成本漏项（合规/安全/审计）、以及资金来源证据不闭环。

F | AML/KYC/制裁与 STR (Q101-Q120)

Q101：荷兰 AML 的核心法律框架是什么？

A101：申请与运营需满足 MiCA 相关义务外，荷兰长期以 **Wwft（反洗钱与反恐融资）** 与制裁相关要求作为底线合规框架；公开法律指引亦强调 Wwft 与制裁法对加密服务商的重要性。

Q102：KYC 最小闭环是什么？

A102：客户身份核验（自然人/法人）→ 受益人识别（法人）→ 风险评级 → PEP/制裁筛查 → 持续监控与定期复核 → 记录保存与可调阅。

Q103：交易监控必须系统化吗？

A103：强烈建议系统化。监管通常要求“制度+系统+证据链”；仅文档不落地会在抽查与面谈中暴露。

Q104：链上分析工具必须买吗？

A104：若涉及转移/托管/平台/兑换，链上风险监控几乎是必需能力（识别制裁地址、黑产关联、混币暴露、异常路径）。可自建或外包，但要可解释、可审计。

Q105：STR（可疑交易报告）流程怎么设计？

A105：规则触发 → 一线复核 → 合规/MLRO 评估 → 决策（报/不报）→ 留痕 → 复盘；要保留“不报原因”记录，避免事后无法解释。

Q106：MLRO 是否必须独立？

A106：必须具备独立判断与直达董事会的汇报线；不应被业务 KPI 绑架。

Q107：如何管理制裁风险？

A107：客户、UBO、交易对手、链上地址多维筛查；命中处置（冻结/拒绝/上报）；并保留截图/报告与处置工单。

Q108：PEP 怎么管理？

A108：增强尽调（EDD）+ 财富/资金来源核验 + 管理层审批 + 更高频监控与复核周期。

Q109：高风险国家客户可以做吗？

A109：可做但风险极高：需更强 EDD、限额、加强监控、必要时拒绝；并考虑银行/EMI 合作方的风险偏好。

Q110：自托管钱包（unhosted wallet）怎么控？

A110：地址风险评分、额外核验、限额与分级控制、链上追踪、异常报警、以及在条款中明确客户责任与风险披露。

Q111：是否需要“钱包归属验证”？

A111：荷兰公开合规讨论中，制裁法框架下对钱包所有权核验曾被提及为监管关注点之一；实务上建议建立“地址归属证明”流程（签名验证/小额验证/声明+抽查）。

Q112：记录保存多久？

A112：按 AML/制裁/税务与监管报送要求综合设定统一留存策略，并确保可检索可导出。

Q113：AML 培训怎么做才合格？

A113：年度计划 + 入职培训 + 岗位专项培训 + 案例复盘 + 测验与记录留存（签到、课件、成绩、整改）。

Q114：可以把 KYC 全外包吗？

A114：可外包执行，但不可外包责任；必须有内部监督、抽查、SLA、审计权与替代方案。

Q115：OTC/现金场景最容易出问题在哪里？

A115：第三方付款、资金来源难核验、线下交割缺证据链；应设更严格 EDD、限制现金/第三方、增强监控与录像/留痕。

Q116：如何应对监管抽样检查？

A116：准备“抽查包”：客户档案、风险评级记录、报警处置记录、STR 决策记录、制裁命中工单、培训与独立审查报告。

Q117：必须做独立 AML 审查吗？

A117：强烈建议（内审或外部独立审查），形成年度整改闭环，提升续期/持续监管应对能力。

Q118：如何管理代理/介绍人渠道 AML 风险？

A118：渠道尽调、合同义务传导、培训、抽查、违规退出机制、以及对客户来源与交易行为的强化监控。

Q119：欺诈/账户接管怎么管？

A119：MFA、异常登录检测、设备指纹、提现风控、冻结流程、取证留痕与客户通知模板。

Q120：AML 失败最常见原因？

A120：风险评估空泛、监控规则不可执行、STR 没留痕、外包不可审计、以及制裁筛查不覆盖链上地址。

G | ICT/安全/外包（对齐 DORA 思路）(Q121-Q150)**Q121：DORA 与 CASP 有什么关系？**

A121：DORA 为欧盟金融实体 ICT 风险管理与外包韧性框架，CASP 在申请与运营中普遍采取“DORA 化”的 ICT/外包治理写法更容易满足监管对可审计与韧性的预期。

Q122：ICT 材料最小清单是什么？

A122：系统架构图、数据流、访问控制（RBAC/MFA）、密钥管理、冷热钱包策略、多签与签名仪式、日志与审计轨迹、事件响应、BCP/DR、渗透测试与漏洞管理、外包登记册与合同要点。

Q123：冷热钱包怎么写才“监管友好”？

A123：分层策略 + 权限最小化 + 多签门限 + 关键人分离 + 签名留痕（录像/日志/纪要）+ 定期轮换 + 对账与资产证明机制。

Q124：多签（Multi-sig）要写哪些细节？

A124：门限设置、参与角色、备份与恢复、紧急替代流程、密钥生成与保管、签名审批流程与记录留存。

Q125：密钥管理必须用 HSM 吗？

A125：不一定强制，但需证明达到同等安全水平；若不用 HSM，要给出替代控制（分片、离线保管、访问控制、审计）。

Q126：渗透测试必须做吗？

A126：强烈建议；并形成整改闭环与复测报告。上线前应将其作为验收包核心。

Q127：日志要做到什么程度？

A127：不可篡改、可检索、可导出、留存期明确；覆盖关键操作（权限变更、提现、密钥操作、审批、报警处置）。

Q128：如何证明系统“可审计”？

A128：日志策略 + 权限矩阵 + 双人复核 + 审计追踪导出能力 + 对账可回溯 + 变更管理记录。

Q129：BCP/DR 要多细？

A129：RTO/RPO、灾备地点、恢复步骤、演练频率、通讯机制、关键供应商中断预案；并保留演练记录。

Q130：发生安全事件如何处理与通报？

A130：识别→分级→隔离→取证→通报→恢复→复盘；准备监管与客户沟通模板，并保留根因分析与整改证据。

Q131：外包哪些属于“关键外包”？

A131：KYC/制裁筛查、链上分析、托管/冷库、撮合引擎、云基础设施、支付/出入金通道、核心客服与工单系统等通常都可能被视为关键外包。

Q132：关键外包合同必须包含哪些条款？

A132：SLA/KPI、审计权与穿透审计、数据与安全义务、分包限制、事件通报时限、退出与迁移、业务连续性、监管可获取性。

Q133：供应商尽调要做什么？

A133：资质与声誉、财务稳健、信息安全（ISO/SOC 报告）、数据所在地、分包链条、事故历史、以及替代方案可行性。

Q134：可以把核心系统放在非欧盟吗？

A134：可行但更难；需解释跨境数据合规、监管可触达、审计权执行、以及供应链风险；实务建议优先 EU 区域。

Q135：开源组件能用吗？

A135：能用，但要做代码审计、版本与补丁管理、供应链安全评估、以及漏洞响应机制。

Q136：内部人员作恶怎么防？

A136：权限分离、四眼原则、行为监控、强制休假与轮岗、关键操作录屏/留痕、审计抽查。

Q137：平台刷量/操纵怎么控？

A137：监控规则、关联账户识别、异常交易报警、处置流程、信息披露与申诉机制。

Q138：上线前验收包建议包含什么？

A138：安全基线、权限矩阵、对账机制、压力测试、渗透测试报告、DR 演练记录、日志审计演练、外包 SLA 验收。

Q139：数据治理为什么会被问？

A139：因为监管越来越关注报表可生成、字段一致性与可追溯；应准备数据字典、字段来源图（lineage）与留存策略。

Q140：客户资产证明（Proof of Reserves）需要吗？

A140：未必是法定统一要求，但“可对账、可证明、可审计”是托管与平台的核心；可准备内部 PoR 报告机制与审计接口。

Q141：如何管理第三方访问权限？

A141：最小权限、临时授权、审批留痕、定期复核、离职/撤权流程、以及供应商运维操作审计。

Q142：DORA 化写法的核心是什么？

A142：资产清单→风险评估→控制措施→监控指标→事件响应→演练→证据留存；把外包纳入统一治理与登记册。

Q143：SOC/7×24 监控必须自建吗？

A143：不一定，可外包，但要有告警处置记录、SLA、审计权与替代方案。

Q144：如何处理数据泄露与 GDPR？

A144：隐私政策、DPA、跨境传输评估、加密与访问控制、数据主体权利流程、以及事件通报与补救。

Q145：交易对账要怎么做？

A145：链上链下对账、客户分户台账、异常差异调查流程、对账频率与责任人、以及审计导出。

Q146：钱包地址黑名单怎么维护？

A146：来源（制裁/情报/链上分析）、版本管理、更新频率、命中处置工单、以及误报复核机制。

Q147：如何避免“系统与制度脱节”？

A147：把制度条款映射到系统控制点（规则引擎、阈值、审批节点、日志字段），并做“制度-系统一致性测试”。

Q148：核心系统变更需要怎么管理？

A148：变更评审、回滚计划、测试与验收、变更窗口、记录留存；重大变更需评估是否触发监管报备。

Q149：外包退出（exit plan）要怎么写？

A149：迁移步骤、数据导出格式、双运行期、客户影响评估、替代供应商预选、以及合同终止触发条件。

Q150：ICT 失败最常见原因？

A150：外包不可审计、权限控制薄弱、日志不可追溯、DR 演练缺失、以及钱包密钥管理方案不清晰。

H | 客户保护、资产隔离、条款披露（Q151-Q190）

Q151：MiCA 下“客户保护”核心抓哪几件事？

A151：核心是：信息披露真实透明、客户资产隔离与可对账、利益冲突可识别可治理、投诉与纠纷可处理可留痕、以及营销不误导。

Q152：必须把客户资产与自有资产隔离吗？怎么证明？

A152：通常需要“法律与会计意义的隔离 + 运营隔离”。证明方式：分户台账、钱包分层/分地址策略、对账报表、权限矩阵、以及审计可导出记录。

Q153：如果是托管（custody），客户资产隔离如何落地？

A153：建议采用“客户分户/分组钱包 + 内部分户账 + 日对账”，并设：提现审批四眼原则、多签、冷库签名仪式留痕、异常冻结流程。

Q154：交易平台不托管客户资产，就不用隔离吗？

A154：仍需隔离“自营 vs 客户撮合”的规则、订单与成交记录不可篡改、费用与点差披露、以及客户资金/加密资产在第三方托管或通道方的责任边界说明。

Q155：客户条款（T&Cs）至少要覆盖哪些模块？

A155：服务范围、费用结构、订单执行规则、资产托管与风险、提现与冻结、冲突披露、投诉流程、数据隐私、事件通知、终止/关户、法律适用与争议解决。

Q156：风险披露（Risk Disclosure）怎么写才合规？

A156：要做到“具体且与产品/服务匹配”：价格波动、流动性风险、技术/链上风险、托管与私钥风险、对手方与外包风险、制裁与冻结风险、税务风险。

Q157：费用披露需要披露到什么程度？

A157：必须“可计算、可对账、可解释”：交易费/点差、托管费、提现费、网络费、第三方费用、返佣/渠道费用（如影响客户价格需披露）、费用变更机制与提前通知。

Q158：点差（spread）属于费用吗？要披露吗？

A158：在客户保护框架下，点差是客户成本的一部分；建议披露点差形成机制、是否动态调整、以及可能产生的利益冲突（做市/自营）。

Q159：适当性/适配性（suitability/appropriateness）要做吗？

A159：若提供投顾/组合管理等服务，适当性评估基本属于“必做”；即使只是零售平台开户，也建议做最小化风险测评与分级限制（尤其高风险产品/功能）。

Q160：零售客户需要设置交易限制吗？

A160：建议分级：新手限额、杠杆/复杂功能限制、冷静期/风险提示弹窗、强制阅读确认、以及“高风险币种/小市值资产”更严格规则。

Q161：客户同意（consent）如何留痕？

A161：页面勾选 + 版本号 + 时间戳 + IP/设备信息 + 条款存档；条款更新要做版本管理与差异说明。

Q162：如何处理客户资产被监管/制裁冻结？

A162：制度必须写清：冻结触发条件、内部审批、客户通知模板、证据留存、解除条件、以及与监管/执法机关沟通路径。

Q163：是否需要客户资产的“日常对账”？

A163：强烈建议至少“日对账 + 月结对账”，对账对象：链上余额、内部账、第三方托管/通道方账；差异要有工单与根因分析。

Q164：平台是否需要“资产证明/储备证明”机制？

A164：不一定强制统一格式，但监管关注“可对账、可审计、可证明”；建议至少具备内部 PoR 报告与审计接口（尤其托管/平台型）。

Q165：客户资产是否可以再质押/再利用（rehypothecation）？

A165：如涉及，必须非常清晰披露并取得明确同意；同时要评估是否触发额外法律属性与更强客户保护要求，实务上建议谨慎或避免。

Q166：客户资金（法币）如何保护？

A166：若无支付牌照，通常通过银行/EMI/PI；要在文件中明确资金流、分户机制、冻结与退款规则、以及对账与异常处理责任人。

Q167：交易执行与撮合规则要公开到什么程度？

A167：至少披露：订单类型、撮合优先级、部分成交、取消规则、系统中断处理、价格来源/指数、以及异常行情处理机制。

Q168：是否要披露“自营交易/做市参与”？

A168：要。必须披露做市/自营与平台之间的隔离、利益冲突、价格形成、以及内部监控与限制（限额/黑名单/审批）。

Q169：如何防止“内部交易员抢跑/内幕优势”？

A169：交易权限隔离、敏感信息屏蔽、行为监控、强制休假与轮岗、审计抽查、以及违规处置制度（含即时冻结权限）。

Q170：客户投诉机制必须有哪些要素？

A170：渠道（网页/邮件/电话）、受理时限、调查流程、回复时限、升级路径、补偿/纠纷处理、记录保存、以及趋势分析与整改闭环。

Q171：投诉记录需要保留哪些字段？

A171：客户标识、时间线、问题分类、证据附件、处理人、决定依据、最终结果、补偿金额、以及是否触发监管通报/产品整改。

Q172：SLA（服务承诺）写不写？

A172：建议写但要可实现，尤其是：提现处理时限、系统故障公告、重大事件通知时限、以及客服响应时限；避免夸大承诺引发投诉与监管质疑。

Q173：客户教育（教育页面/风险提示）是否有必要？

A173：非常建议。监管与消费者保护趋势下，“充分告知 + 可理解”会成为争议时的关键证据。

Q174：客户账户被盗（ATO）怎么处理？

A174：必须有：冻结/止付流程、身份复核、取证留痕、资金追踪、客户通知模板、以及事后复盘与控制加固。

Q175：客户争议交易（chargeback/纠纷）如何处理？

A175：若涉及法币通道，按通道规则处理；内部要有：证据包（日志/确认记录/风险提示确认）、争议处理 SOP、以及监管或仲裁应对模板。

Q176：客户适当性问卷一定要“考试式”吗？

A176：不必，但要能区分风险承受能力与经验；并能把结果映射到权限（限额、产品可见性、复杂功能开关）。

Q177：零售客户是否需要提供“风险等级标签”？

A177：强烈建议对资产/产品做风险分级标签，并在下单前提示；同时保留客户确认留痕。

Q178：费用变更可以立即生效吗？

A178：不建议。应提供提前通知期、版本对比、客户拒绝/关户权利说明，并保留通知证据。

Q179：如何处理“误导性营销/夸大收益”的合规风险？

A179：建立 Marketing Approval 流程、话术库、禁用词清单、抽查机制与渠道违规处罚；保留审批与发布记录。

Q180：KOL/代理推广是否需要纳入合规？

A180：必须纳入。要做渠道尽调、合同约束（合规话术/禁用承诺）、培训、抽查、以及违规下架与追责机制。

Q181：客户资料与交易数据要保密到什么程度？

A181：GDPR 与安全要求叠加：最小化、加密、访问控制、日志审计、数据留存策略、以及数据主体权利流程。

Q182：是否需要多语言条款（英文/荷兰语）？

A182：建议面向荷兰零售客户至少提供可理解语言版本；对外营销语言与披露语言要一致，避免“英文条款+荷兰语营销”的纠纷风险。

Q183：客户终止服务/关户要做什么？

A183：关户前清算、资产返还路径、未完成订单处理、冻结资金处置、以及数据保留与删除规则（符合法律留存）。

Q184：客户资产返还（退出）时限如何设置？

A184：以可实现为原则，明确“正常/异常/风控冻结”不同场景；并在 BCP/Wind-down 计划中一致化。

Q185：客户资产丢失/被盗，是否必须赔付？

A185：取决于责任归属与条款、保险覆盖、以及事件调查结论。关键是：事前披露清楚 + 事中证据链完整 + 事后处置透明。

Q186：如何处理“系统故障导致错价成交”？

A186：必须预设“明显错误交易”规则、回滚/撤单机制、公告与客户沟通模板、以及审计与复盘机制。

Q187：客户保护与 AML 冲突（例如冻结与客户权利）怎么办？

A187：以法律义务优先：制裁/AML 冻结时需要限制客户操作；但应在条款中写明触发条件与客户申诉路径，并保留证据链。

Q188：客户资产是否需要第三方独立审计？

A188：强烈建议至少年度审计或独立鉴证，尤其托管/平台型；并在审计发现后形成整改闭环。

Q189：客户保护最常见补件点是什么？

A189：条款与实际流程不一致、费用披露不清、资产隔离不可证明、投诉机制不闭环、以及营销合规缺审批证据。

Q190：客户保护材料如何做成“可递交索引”？

A190：把 H 类做成：H1 条款与披露清单、H2 风险披露、H3 费用披露表、H4 投诉 SOP 与模板、H5 利益冲突政策、H6 资产隔离与对账包、H7 营销审批机制与话术库。

I | 持续合规、报告、审计、变更报备（Q191-Q230）

Q191：拿到 CASP 牌照后，最重要的持续义务是什么？

A191：持续满足治理与资源、AML/制裁有效运行、ICT 安全与外包治理、客户保护与披露、以及“重大事项变更”及时报备。

Q192：续牌/年审一定会有吗？

A192：各国监管实务不同，但一般会有持续监管、年度费用、信息更新与抽查/检查；应把“监管年费 + 审计/合规审查成本”列入预算。

Q193：需要定期向监管提交哪些报告？

A193：通常包括：经营与财务信息、合规与风险报告、重大事件报告、外包/ICT 事件相关报告等；建议建立“监管报送日历 + 模板库”。

Q194：是否需要年度合规报告（Compliance Report）？

A194：强烈建议：年度合规计划执行情况、合规监控结果、投诉与事件统计、整改闭环、培训记录、以及下一年度计划。

Q195：AML 年度风险评估必须更新吗？

A195：必须定期更新，至少年度复核；发生重大事件或新增产品/市场/渠道时应即时更新并上会。

Q196：需要做独立审查（independent review）吗？

A196：强烈建议对 AML、ICT、外包治理、以及客户资产隔离做年度独立审查（内审或外部），形成整改闭环证据。

Q197：审计师/外部鉴证机构要具备什么条件？

A197：要独立、具备相关行业经验、能提供可被监管理解的报告格式；合同需明确工作范围、时间表、以及报告交付与跟踪。

Q198：哪些变更属于“重大变更”需要报备？

A198：通常包括：股东/控制权变化、董事/高管/MLRO 等关键岗位变化、服务范围新增/变化、关键外包变更、核心系统架构变更、以及重大事件。

Q199：更换 MLRO 要怎么做？

A199：准备“离任原因说明 + 继任者 Fit&Proper 包 + 交接清单 + 过渡期安排 + 董事会决议 + 报备信模板”，并保留交接证据。

Q200：更换董事/CEO 要怎么做？

A200：同样需 Fit&Proper 包、时间投入声明、冲突披露、以及治理连续性说明；建议准备面谈 Q&A 包。

Q201：新增服务项（例如从兑换扩展到托管）怎么做？

A201：先做差距评估（资本/岗位/系统/条款/AML 场景），更新 Programme of Operations 与相关制度，必要时走许可范围变更/监管沟通流程。

Q202：新增币种/代币上架需要审批吗？

A202：建议建立 Token Listing 框架：法律属性评估、市场/操纵风险、链上风险、制裁暴露、技术安全、披露与限额；并留存委员会决议与评估表。

Q203：投诉激增是否需要通报监管？

A203：若反映系统性问题或客户损害事件，建议按重大事件机制评估并通报；至少应形成上会记录与整改计划。

Q204：安全事件一定要通报监管吗？

A204：通常重大 ICT 事件需按制度分级并通报；关键是“事件分级标准 + 通报时限 + 证据链 + 复盘整改”。(与 DORA 化框架一致更稳。)

Q205：发生资金被盗，第一时间做什么？

A205：冻结/止付、隔离系统、取证留痕、评估影响范围、通报路径启动、客户沟通模板、以及保险理赔路径同步启动。

Q206：合规培训频率怎么安排？

A206：入职必训 + 年度全员复训 + 岗位专项（客服/交易/风控/技术/高管）+ 事件复盘培训；每次培训留存签到、课件、测验与整改。

Q207：需要做演练（table-top exercise）吗？

A207：强烈建议做：DR 演练、安全事件演练、制裁命中冻结演练、挤兑/提现潮演练、以及媒体危机演练；保留演练报告。

Q208：如何建立合规监控（Compliance Monitoring Plan）？

A208：按季度/月份列测试项：KYC 抽样、制裁筛查抽样、交易监控处置抽样、渠道营销抽查、外包 SLA 抽查、权限复核、对账复核。

Q209：哪些 KPI 最能证明“持续合规有效”？

A209：KYC 完整率、复核逾期率、报警处置时效、STR 决策留痕率、制裁命中处置时效、投诉处理时效、对账差异率、以及外包 SLA 达成率。

Q210：外包登记册（Outsourcing Register）要写什么？

A210：供应商信息、服务描述、关键性评级、数据处理与所在地、分包情况、SLA/KPI、审计权、退出计划、以及最近一次评估与抽查结果。

Q211：外包供应商更换要不要报备？

A211：若属于关键外包，通常需要事前评估并可能触发报备；至少要更新登记册、尽调报告、合同条款与退出计划。

Q212：内部权限复核多久做一次？

A212：建议至少季度复核；关键系统（钱包签名、提现审批、生产环境访问）可月度复核；离职/调岗即时撤权。

Q213：是否需要年度董事会自评/治理评估？

A213：建议做。监管越来越关注董事会有效性；自评记录可作为“有效管理”证据。

Q214：记录保存（Record Keeping）怎么做才稳？

A214：统一留存策略：AML/交易/日志/投诉/审批/外包/培训等分类，定义留存年限、访问权限、导出格式、不可篡改措施与备份。

Q215：监管检查（on-site/desk-based）通常怎么来？

A215：常见：先 desk-based 要求材料 → 抽样客户档案与交易 → 访谈关键岗位 → 现场查看系统与日志 → 出整改清单 → 跟踪复核。

Q216：监管抽查最喜欢“抽哪类客户”？

A216：高风险国家/PEP、异常交易频繁、第三方付款、OTC 大额、制裁命中边缘案例、以及频繁提现到高风险地址。

Q217：如何准备“随时可查”的审计包？

A217：建立“监管数据室”：索引清单 + 最新版本制度 + 抽样数据导出脚本 + 关键报表一键生成 + 最近一次独立审查报告与整改闭环证据。

Q218：重大事项通报的“阈值”怎么设定？

A218：按影响面：客户资金/资产损失、系统不可用时长、数据泄露规模、制裁/AML 高风险事件、媒体重大负面、以及治理重大变更。

Q219：客户资金/资产差异对账出现缺口怎么办？

A219：立即冻结相关操作、启动调查与取证、上报管理层与合规、评估是否构成重大事件、并形成根因分析与补救计划。

Q220：如何管理版本（policy version control）？

A220：每个制度有版本号、变更记录、批准人、发布日期、生效日；重大变更要培训并收集确认回执。

Q221：是否要设立合规热线/举报机制？

A221：建议设立。内部举报机制与反报复政策，能提升治理可信度并满足审计/监管对“文化与控制环境”的期待。

Q222：如果业务停止/退出市场，需要做什么？

A222：启动 Wind-down Plan：客户通知、资产返还、未完成订单清算、外包退出与数据迁移、员工撤权、监管通报与最终报告。

Q223：是否需要定期更新商业计划与财务预测？

A223：建议至少年度更新，重大市场变化或业务扩张时更新；并把合规与安全投入真实反映在预算中。

Q224：如何证明“合规资源充足”？

A224：岗位说明书、组织架构、预算、培训、监控计划执行证据、以及独立审查与整改闭环成果。

Q225：持续合规中“最致命”的红线是什么？

A225：无证超范围展业、故意隐瞒重大事项、客户资产隔离失效、制裁/AML 严重缺陷、以及系统安全事故处理不当。

Q226：监管沟通有哪些“正确姿势”？

A226：信息一致、证据充分、答复可核验；不要在不同文件里给出矛盾口径；补件要用“问题一回答一证据一附件索引”格式。

Q227：是否需要年度“合规演练报告”上会？

A227：建议上会，尤其是 DR/安全/制裁/挤兑演练；形成董事会决议与整改资源投入记录。

Q228：如何做“监管整改闭环”？

A228：整改清单→责任人→期限→验收标准→证据附件→复测/复审→上会确认→归档。

Q229：续期/持续监管的“资料一键包”怎么做？

A229：年度：治理与人员变化、财务与资本/保险、AML 年度风险评估与独立审查、ICT 演练与测试、外包登记册、投诉与事件统计、以及下一年度计划。

Q230：持续合规最常见“被点名”的问题？

A230：培训与监控走过场、外包不可审计、日志与对账不可追溯、重大事件未及时通报、以及营销话术失控。

J | 税务与法律配套 (CIT/VAT/预提税/雇佣/架构) (Q231-Q260)

Q231：CASP 在荷兰一般会涉及哪些税种关注？

A231：常见关注：公司所得税 (CIT)、增值税 (VAT，尤其服务性质与地点规则)、雇佣相关税费、以及跨境服务/分支的税务常设机构风险。

Q232：加密资产交易收入如何分类（交易费/点差/托管费）？

A232：应在会计政策中明确：收入确认时点、净额/总额口径、点差计量方法、以及退款/争议处理；并与客户条款与报表一致。

Q233：托管资产是否计入公司资产负债表？

A233：通常客户托管资产属于表外或代管属性（取决于会计准则与具体结构），关键是：客户资产隔离、对账机制与披露清晰，避免混同。

Q234：VAT 是否一定适用？

A234：取决于服务类型与交易性质；某些金融服务可能有特殊 VAT 处理，但必须由税务顾问结合具体模式判断，建议在 BP 中列税务假设与风险点。

Q235：跨境向欧盟其他国家客户提供服务，税务上要注意什么？

A235：关注：服务发生地、VAT 规则、是否形成常设机构 (PE)、以及跨境雇佣与远程团队的税务/社保合规。

Q236：在荷兰设分支 vs 子公司，差别是什么？

A236：子公司治理更清晰但成本较高；分支可能在税务与监管责任边界上更复杂。建议结合护照策略、团队配置与银行开户难度评估。

Q237：雇佣合规要写到申请包吗？

A237：至少要证明关键岗位已到位或可招聘落地，包含岗位说明书、薪酬预算、KPI、以及独立性（合规/MLRO）。

Q238：关键岗位外包会影响雇佣与治理评估吗？

A238：会。外包不等于没有雇佣义务，但会增加独立性与问责的审查强度；建议关键岗位尽量内部化或至少设内部责任人。

Q239：员工激励（期权/代币激励）会影响监管吗？

A239：可能影响利益冲突与行为风险；需要披露激励结构与合规限制（交易窗口期、内幕信息隔离、违规处罚）。

Q240：是否需要法律意见书 (Legal Opinion)？

A240：常见需要：业务定性 (MiCA 服务项映射)、产品条款与风险披露、外包与数据保护、以及代币法律属性（上架评估）。

Q241：合同体系最少要准备哪些？

A241：客户条款、隐私政策、外包合同（含审计权/退出）、渠道代理协议、做市/流动性提供协议（如有）、以及银行/EMI 合作协议摘要与责任边界。

Q242：争议解决条款怎么写？

A242：明确法律适用、管辖或仲裁、语言、以及投诉前置程序；对零售客户要避免不公平条款带来消费者保护风险。

Q243：数据跨境传输怎么处理？

A243：GDPR 框架下做：数据映射、DPA、跨境传输机制（如标准合同条款 SCC）、安全措施与审计；并与外包登记册一致。

Q244：是否需要“知识产权与代码归属”条款？

A244：需要，尤其是核心系统外包开发：源代码托管、交付物归属、访问权限、退出时可迁移性，直接关系到可持续经营与监管认可。

Q245：反欺诈与消费者保护法律要考虑吗？

A245：要。即便 MiCA 统一，荷兰本地消费者保护与广告规范仍会影响营销与合同公平性，建议建立审查清单。

Q246：客户资产的法律关系（信托/保管/委托）要写清吗？

A246：必须写清。客户资产归属、托管责任、风险边界、赔付与保险关系，都是纠纷与监管检查的核心点。

Q247：如果提供利息/收益产品，税务与法律风险会增加吗？

A247：会。收益属性可能触发额外监管分类、消费者保护与税务处理复杂度；必须先做法律定性与披露框架。

Q248：把集团共享服务写进申请包会影响税务吗？

A248：可能影响转让定价与成本分摊；应明确服务内容、计费方式、合同、以及可审计的费用分摊机制。

Q249：如何降低银行开户的合规阻力？

A249：准备完整的 AML/制裁体系、业务流程图、资金流说明、客户来源与风险控制、审计与对账机制；并尽量减少高风险业务（现金/匿名/高风险地区）。

Q250：若团队在多国远程办公，雇佣税务如何处理？

A250：需评估各国雇佣税与社保、以及是否构成常设机构风险；建议把关键管理与控制职能集中在欧盟可触达地点。

Q251：税务假设与财务预测要一致吗？

A251：必须一致。税务假设（VAT、税率、费用可抵扣）要在 BP 注明，避免监管认为预测不可信。

Q252：是否要为客户提供税务提示（Tax Disclaimer）？

A252：建议提供一般提示：客户对其税务申报负责；平台不提供个税建议；并给出信息披露与交易记录导出功能。

Q253：交易记录导出要满足什么标准？

A253：可读、可核验、包含时间戳/币种/数量/价格/费用/钱包地址（如适用）、并与后台对账一致；方便客户税务与审计。

Q254：需要雇佣背景调查（screening）吗？

A254：强烈建议对关键岗位做背景调查与不利媒体筛查；并建立员工行为准则与利益冲突申报机制。

Q255：员工个人交易（personal dealing）怎么管？

A255：设：申报制度、黑窗期、限制币种/额度、预先批准、以及违规处罚；尤其涉及上市信息与市场敏感信息。

Q256：合同与制度需要董事会批准吗？

A256：关键制度（AML、风险、外包、信息安全、投诉、利益冲突、风控）建议董事会或高管层正式批准并留痕。

Q257：是否需要购买责任保险（D&O/PI/Cyber）？

A257：通常强烈建议；尤其网络安全、专业责任与董事责任保险，可作为风险覆盖的一部分并提升合作方信心。

Q258：预提税（WHT）会影响吗？

A258：视跨境支付（服务费、分红、特许权使用费）结构而定；建议在集团架构与合同中提前规划。

Q259：税务与监管冲突如何避免？

A259：以事实为基础：业务模式、资金流、合同与账务一致；不要为了税务“优化”做出与监管披露矛盾的结构。

Q260：税务与法律配套最常见补件点？

A260：客户资产法律关系不清、外包合同审计权不足、跨境数据合规缺证据、以及财务预测与税务假设不一致。

K | 监管趋势：ESMA Level 2/3、AMLA、DAC8 等（Q261–Q285）

Q261：什么是 ESMA Level 2/3？

A261：Level 2/3 通常指技术标准、指南、Q&A 等“细化执行口径”；会直接影响申请材料写法与持续合规颗粒度。

Q262：为什么我现在写申请包要“预埋可升级空间”？

A262：因为细则会持续更新，若文件与系统没有版本治理与参数化（规则引擎、阈值、报表字段），后续改造成本高、也容易被监管质疑持续合规能力。

Q263：AMLA（欧盟反洗钱局）会带来什么影响？

A263：AML 统一趋强，跨境一致性要求更高；你需要把 AML 做成“可审计标准件”，便于未来统一口径与跨境检查。

Q264：DAC8 对 CASP 意味着什么？

A264：税务信息交换与报告要求趋严，尤其客户身份数据与交易数据质量要求更高；建议提前做数据治理与可导出报表能力。

Q265：监管趋势对数据治理提出哪些要求？

A265：数据字典、字段来源（lineage）、报表一致性、留存与可追溯、以及数据质量监控（缺失率、异常值、重复率）。

Q266：跨境护照后，目标国还会查我吗？

A266：会。护照不等于“无人管”；目标国仍会关注消费者保护、营销合规与 AML 风险，并可能要求解释与配合。

Q267：未来更可能加强哪类检查？

A267：托管安全、外包与云集中度、制裁执行与链上监控、营销误导、以及客户资产隔离与对账。

Q268：稳定币与支付通道监管会如何影响 CASP？

A268：会影响出入金、结算与客户预期；你需要在合作结构与披露中明确通道风险与应急方案。

Q269：Travel Rule 会影响我吗？

A269：若你提供转移服务，跨境转账信息传输与对手方协作是重点；需准备数据字段、对接机制、拒绝/降级策略与留痕。

Q270：监管会关注“混币/隐私币”吗？

A270：高度关注。建议对高风险工具设限制/增强 EDD/更强链上分析；并在政策中明确接受与拒绝规则。

Q271：监管对 AI/自动化风控怎么看？

A271：可用但必须可解释、可审计、可回滚；模型治理、训练数据偏差与阈值调整记录要能出示。

Q272：平台市场操纵监管会更严吗？

A272：趋势上会更严。建议提前建设市场监控规则、关联账户识别、做市隔离、以及异常处置与公告机制。

Q273：未来对外包审计权会更硬吗？

A273：是。建议现在合同就写足：穿透审计、分包限制、监管可访问性、退出与迁移、以及事件通报时限。

Q274：加密资产会计与审计标准会不会收紧？

A274：趋势上会更规范；你应准备清晰的会计政策与审计接口（对账、估值、收入确认）。

Q275：监管对“储备证明”会趋于标准化吗？

A275：有可能。即使未统一，托管/平台型强烈建议建立内部 PoR 报告机制，便于未来对接标准化要求。

Q276：未来最容易被要求补强的治理点是什么？

A276：董事会有效性、关键岗位独立性、合规资源与预算、以及“系统化证据链”（日志、对账、报表、监控处置）。

Q277：跨境营销合规趋势是什么？

A277：更强调“准确、清晰、不误导”；且会关注 KOL、代理与返佣机制。建议建立渠道治理与话术库。

Q278：客户数据共享与隐私合规会更难吗？

A278：会。尤其 Travel Rule、税务报告与制裁筛查都需要更多数据处理；必须用 GDPR 框架做数据最小化与合规传输。

Q279：监管会要求更多“情景演练”吗？

A279：大概率会。建议把演练纳入年度计划，并形成可审计的报告与整改闭环。

Q280：监管对“第三国客户”会更敏感吗？

A280：会。高风险国家、跨境制裁暴露与欺诈风险会被重点审查；建议做国家风险政策与限额/EDD 机制。

Q281：监管趋势对费用披露有什么影响？

A281：更强调透明与公平定价，尤其点差与返佣；建议把费用拆解到可计算并能生成对账报表。

Q282：未来对链上监控与制裁执行会更严格吗？

A282：是。建议把链上监控作为核心能力，形成规则库、命中处置 SOP、以及审计证据链。

Q283：监管对“上市/下架”机制会怎么要求？

A283：更偏向制度化：评估、批准、监控、下架触发条件、客户通知与资产处置路径；并保留评估与决议。

Q284：AMLA/DAC8 会不会影响技术字段与报表格式？

A284：会影响数据字段与一致性要求；建议提前做数据字典、字段治理与可配置报表引擎。

Q285：监管趋势模块怎么写进申请包？

A285：建议做“Regulatory Change Management Policy”：法规扫描、影响评估、版本更新、培训、上线验收与记录留存。

L | 项目管理与实操落地（Preparation / Application / Post-Licence）（Q286-Q300）

Q286：三阶段法的核心是什么？

A286：Preparation 把“能力与证据链”建好；Application 把材料打包成可审计索引并控件；Post-Licence 把持续合规做成可运营体系。

Q287：Preparation 阶段最先做哪三件事？

A287：服务范围定性（MiCA mapping）→组织与岗位落地（合规/MLRO/ICT）→系统与外包边界确定（含日志/对账/DR）。

Q288：Preparation 阶段最关键交付物是什么？

A288：Programme of Operations（主索引）、A-I Master Checklist（文件索引）、以及差距评估报告（Gap + 里程碑 + 预算）。

Q289：Application 阶段如何减少 RFI（补件）？

A289：用“问题—回答—证据—附件索引”的应答包；所有附件编号统一；交叉引用（BP↔AML↔ICT↔T&Cs↔财务）一致。

Q290：监管面谈最常问什么？

A290：服务范围边界、客户资产隔离、AML 规则与 STR 决策、外包审计权、钱包安全与权限、以及董事会如何有效管理风险。

Q291：Post-Licence 第一季度最容易出问题是什

A291：上线后流程与制度不一致、渠道营销失控、报警处置积压、对账差异没有闭环、以及外包 SLA 管控不足。

Q292：如何建立“上线验收（Go-Live Gate）”？

A292：资本/保险到位、关键岗位到岗、渗透测试与整改完成、DR 演练通过、日志与报表可导出、对账机制可跑通、客服与投诉 SOP 已培训。

Q293：如何做“监管数据室（Regulatory Data Room）”？

A293：一套索引：最新制度、组织与岗位、外包登记册、关键报表、抽样客户档案、培训记录、独立审查与整改闭环。

Q294：如果监管要求 2 周内交补件，怎么控节奏？

A294：设战情室：PM 统一口径、法务定性、合规证据链、技术导出报表、运营补充流程；每天站会 + 版本冻结 + 统一编号。

Q295：如何管理多供应商（KYC/链上分析/云/托管）？

A295：统一外包治理：关键性评级、SLA/KPI、审计权、事件通报、分包限制、退出计划、季度评估与抽查。

Q296：如何把制度写成“可执行”？

A296：每条制度必须对应系统控制点或工单节点（阈值、审批、日志字段、报表字段）；并做制度—系统一致性测试。

Q297：如果计划 EU 护照扩张，申请包需要预埋什么？

A297：跨境客户接入政策、语言与披露策略、目标国营销合规、跨境制裁/税务与数据合规、以及护照通报材料模板。

Q298：如何规划年度合规预算？

A298：监管年费、审计/独立审查、合规与 MLRO 人力、链上分析与制裁工具、渗透测试与演练、外包审计、以及法律/税务顾问。

Q299：如何衡量“拿牌后运营合规成熟度”？

A299：用指标：报警处置时效、对账差异率、投诉率与处理时效、培训覆盖率、独立审查通过率、以及重大事件数量与复盘质量。

Q300：一份合格的 CASP 合规体系最终长什么样？

A300：不是“厚文件”，而是：制度 + 系统 + 日志/报表 + 演练 + 审计 + 整改闭环，且能随时向监管“导出证据”。

仁港永胜建议（唐生结论 | 荷兰 CASP FAQ 使用方法）

- 先定服务范围，再定系统与文件深度：Programme of Operations 是全套申请的“主索引”，决定资本/岗位/ICT/外包/客户条款。
- 股东/UBO 资料要“闭环可核验”：SoW/SoF + 资金路径图 + 不利信息解释备忘录，是最常见补件点。
- ICT 直接按 DORA 思路写成“可审计”：日志、权限、外包审计权、DR 演练与事件响应证据链一次性建好。
- 把 AML 做成“制度+系统+证据链”：STR 决策留痕、制裁筛查覆盖链上地址、以及抽查包随时可出。
- 建立 RFI 补件战情室：合规+法务+技术+运营四方联动，补件速度与质量决定周期与通过率。

选择仁港永胜的好处优势

- 一体化交付：MiCA/CASP 申请包 + AML 手册 + ICT/DORA 外包治理 + 客户条款披露 + 面谈题库与 RFI 应答包。
- 强模板库：A-I Master Checklist、Risk Register、STR 决策树、外包尽调清单、系统权限矩阵、Go-Live 验收清单、护照通报包等可直接落地。
- “可审计写法”能力：把监管关心的问题（证据链、日志、责任边界、审计权）写进制度与系统，减少补件轮次。

关于仁港永胜

仁港永胜为专业的合规与金融咨询服务机构，我们专注全球金融牌照申请与持续合规：MiCA/CASP、VASP、EMI/PI、交易所/经纪牌照、AML/CFT 体系建设、DORA 外包与 ICT 合规、以及持牌后年度维护。我们在香港、深圳及多个司法辖区协同配置合规团队，可为客户提供从战略评估 → 申请文件编制 → 面谈辅导 → 监管沟通 → 持牌后持续合规的一站式服务支持。

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

官网：jrp-hk.com

香港：852-92984213 (WhatsApp)

深圳：15920002080 (微信同号)

电邮：tsy@cnjrp.com

办公地址：

- 香港湾仔轩尼诗道253-261号依时商业大厦18楼
- 深圳福田卓越世纪中心1号楼11楼
- 香港环球贸易广场86楼

注：本文涉及的模板/清单/电子档（如 Master Checklist、制度模板包、面谈题库等）可向仁港永胜唐生有偿索取。

免责声明

本文由仁港永胜（香港）有限公司拟定，并由唐生（Tang Shangyong）提供专业讲解。本文所载内容仅供一般信息与项目沟通之用，不构成法律、税务、审计或投资建议。具体监管要求、申请材料口径、费用及审查尺度以欧盟 MiCA 正式文本、ESMA/EBA 技术标准及荷兰 Netherlands 主管机关（AFM (Dutch Authority for the Financial Markets)）最新公布为准。仁港永胜保留对本文内容进行更新与修订的权利。如需针对贵司业务模式提供可落地的合规方案、文件编制与申请支持，请联系仁港永胜获取专业协助。

© 2025 仁港永胜（香港）有限公司 | Rengangyongsheng Compliance & Financial Licensing Solutions – 由仁港永胜唐生提供专业讲解。