波兰 Poland（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 Polish (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（Tang Shangyong）** 提供专业讲解。

适用对象：拟以**波兰**为 MiCA 申请国（Home Member State），申请并运营 **CASP（Crypto-Asset Service Provider）**，并通过 **MiCA 护照机制**向全欧盟跨境展业的机构。

法律底座：MiCA（EU 2023/1114）统一授权与持续监管框架。

交付提示（PDF/附件索取）：本指南由仁港永胜唐生拟定讲解，可提供可编辑的 **Master Checklist（A–I）**、BP 模板、AML 手册、ICT/DORA 外包治理制度、RFI（补件）应答包、面谈题库与"护照通报包"等（可向仁港永胜唐生有偿索取）。

✅ 点击这里可以下载 PDF 文件：波兰 Poland（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：MiCA 的实践：缺乏国家法规阻碍在波兰获得 CASP 授权

✅ 点击这里可以下载 PDF 文件：关于仁港永胜

牌照名称

- **牌照名称**：MiCA 体系下 **Crypto-Asset Service Provider（CASP）授权**（以波兰为申请地/主管机关）。
- **主管机关（拟）**：波兰拟制定的《加密资产市场法》草案中明确由 **Komisja Nadzoru Finansowego（KNF，波兰金融监管局）**承担加密资产市场监管与监督框架。
- **文档定位**：以"**可递交、可审计、可补件**"为写作标准，直接对齐 MiCA、ESMA 技术标准（RTS/ITS）、DORA 与波兰本地 AML 义务。
- **服务商**：仁港永胜（香港）有限公司｜Rengangyongsheng (Hong Kong) Limited

常见问题（FAQ）（Q1–Q400）—波兰版

波兰 Poland（MiCA）加密资产服务提供商（CASP）牌照常见问题（FAQ 大全）

模块结构：

A 牌照与范围｜B 实体与实质｜C 股东/UBO｜D 董事适任性｜E 资本/保障｜F AML/制裁/STR｜G ICT/DORA/外包｜H 客户保护｜I 护照与跨境｜J 运营与持续合规

（唐生说明：MiCA 主法源为 Regulation (EU) 2023/1114；DORA 为 Regulation (EU) 2022/2554 且自 **2025-01-17** 起适用。波兰本地落地与主管机关指定以最终实施法与官方公告为准；业界信息普遍指向由 **KNF** 承担主管机关角色，但仍应以最终颁布文本/公告核验。）

（说明：MiCA 主法源为 Regulation (EU) 2023/1114 EUR-Lex；DORA 为 Regulation (EU) 2022/2554 且自 **2025-01-17** 起适用 EUR-Lex。波兰本地落地与主管机关指定以最终实施法与官方公告为准；业界信息普遍指向由 **KNF** 承担主管机关角色，但仍应以最终颁布文本/公告核验。）

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。

A｜牌照与范围（Q1–Q20）

Q1：MiCA 下 CASP 牌照是什么？在波兰获批后意味着什么？

A：CASP 是欧盟统一框架下的"加密资产服务提供商"授权。获批后，你在波兰成为受监管实体，可在获授权服务范围内向客户提供 MiCA 列举的加密资产服务，并在满足护照程序后扩展到其他欧盟/欧洲经济区市场。重点是：**服务范围"以授权为准"**，不能用"我们是加密公司"泛化替代具体服务类别。

Q2：CASP 能覆盖哪些服务？是否"一个牌照通吃交易所+托管+经纪+撮合"？

A：MiCA 将服务拆分为多个类别（例如：托管与管理、交易平台运营、兑换法币/加密、兑换加密/加密、执行订单、接收与传递订单、提供

建议、投资组合管理、转移服务等）。可以多项同时申请，但监管会看：

- 你是否具备对应的**系统能力、风控能力、人员能力**；
- 业务是否存在**利益冲突与隔离机制**；
- 同时申请会提高审查深度与材料体量。并非“一次申请越多越好”。

Q3：我们做 OTC（场外）算哪类服务？
A：通常落在“加密资产兑换服务”（法币↔加密、加密↔加密）和/或“执行订单/接收传递订单”。如果你以自营对手盘报价、赚取点差，监管会重点问：

- 定价机制与披露；
- 对手盘风险与库存风险；
- 客户是否理解你是“做市/自营对手方”。
  若你只是撮合第三方，可能涉及“订单接收与传递/执行”或“平台运营”性质（视交易组织方式而定）。

Q4：我们只做“钱包”算 CASP 吗？
A：若提供托管钱包（你掌握私钥或可影响客户资产转移），通常属于“托管与管理”。若是纯非托管软件（客户自持私钥、你不接触资产），可能不构成该项服务，但仍可能触发其他监管（营销、数据安全、消费者保护等）。监管会以**实际控制权**判断，而不是你自称“非托管”。

Q5：做“交易平台”与做“经纪/兑换”在监管上差别在哪里？
A：平台运营的关键在于：

- 交易规则与市场秩序（撮合、挂单、撤单、异常处理）；
- 市场滥用防控（操纵、刷量、抢跑等）；
- 透明度与披露（撮合优先级、费用、冲突）；
- 系统韧性、容量、灾备。
  经纪/兑换更强调：报价透明、客户适当性、执行质量、库存与对手风险、投诉与纠纷处理。

Q6：CASP 能否经营“稳定币”？
A：能否经营取决于你提供的服务类别以及稳定币本身是否合规（例如符合 MiCA 下 ART/EMT 的发行与流通要求）。监管会要求你对：

- 稳定币合规属性与风险；
- 赎回、流动性、脱锚风险披露；
- 交易与托管的操作控制
  建立清晰制度。很多项目卡在“把不合规稳定币当作普通币”处理。

Q7：CASP 是否等同于 VASP（FATF 口径）？
A：概念有交集但不等同。VASP 是国际反洗钱框架用语；CASP 是 MiCA 的监管授权主体。你作为 CASP，仍必须满足 AML 法项下义务（通常会被视为 AML 义务主体），并在 Travel Rule、制裁、STR 等方面满足要求。

Q8：我们可否先申请最小范围（例如仅兑换），后续再扩项？
A：可以，且是常见策略。优点：缩小审查面、降低首次材料与系统复杂度；缺点：未来扩项仍需“重大变更/再授权”流程，需再做系统与制度升级、可能触发再审。建议用“三阶段路线图”写进 PoO：**首期可监管落地、二期扩项、三期跨境护照**。

Q9：广告宣传能否写“欧盟牌照/全欧通行”？
A：宣传必须准确、可核验。通常需要：

- 清晰写明授权国家、授权主体名称；
- 列明授权服务范围（不夸大）；
- 披露关键风险。
  “全欧通行”应表述为“可依法定程序申请跨境护照提供服务”，并且在护照未完成前不得暗示已在他国被允许展业。

Q10：CASP 是否能帮我们开银行账户更容易？
A：一般会改善银行尽调的可解释性，但不是保证。银行还会看：

- 业务模式风险（高风险客户/OTC/跨境）；
- AML 与制裁成熟度；
- 技术安全与审计；
- UBO 背景与资金来源。
  建议准备“银行尽调包”：牌照进度、制度摘要、风险评估、交易监测说明、审计计划、治理架构。

Q11：MiCA 对“加密资产”定义是什么？我们做的是不是“加密资产”？
A：监管会看是否属于可转让、可存储、使用 DLT 或类似技术的数字表示价值/权利。若是证券型代币/金融工具，则可能落入 MiFID/MiFIR 体系而非 MiCA。你需要做“分类备忘录”：Token 分类、权利属性、是否金融工具、是否 EMT/ART、是否 utility。

Q12：NFT 业务需要 CASP 吗?
A：需看 NFT 是否“唯一且不可替代”并且是否具备金融化特征（分割、集合、可替代化、类证券化）。很多“看似 NFT 实为可替代系列”可能被纳入监管关注。建议对 NFT 产品做：结构说明、流通机制、可替代性分析、营销与风险披露。

Q13：我们提供“质押/借贷/收益产品”是否在 CASP 范围?
A：MiCA 的 CASP 服务清单并不直接等同于所有收益型业务。收益、借贷、质押可能触发其他金融监管框架或消费者保护规则。监管会重点问：收益来源、对手风险、资产再质押、是否形成存款类或集合投资性质。务必先做“监管映射（Regulatory Mapping）”。

Q14：我们能否向零售客户提供服务?
A：通常可以，但零售面向意味着更强的客户保护义务：风险披露、费用透明、投诉机制、适当性/适配性、营销合规、冷静期/撤销权（如适用）、以及更高强度的运营控制。

Q15：专业客户与零售客户的差别有哪些?
A：差别通常体现在：

- 披露深度（零售更详细）；
- 适当性评估要求（零售更严格）；
- 风险承受能力与杠杆/复杂产品限制（若涉及）；
- 投诉处理与争议解决路径。
  建议建立分层客户政策：零售/专业/机构/合格对手方（如适用），并在开户流程固化。

Q16：我们是否必须在波兰本地雇人？可否全部远程?
A：可以有跨境团队，但监管关注“实质经营”。关键职能（合规、MLRO、风控、ICT安全、管理层）需要能有效履职、可被监管联系、能在波兰形成可解释的治理中枢。完全“空壳+海外遥控”是高风险。

Q17：申请前可以先试运营/内测吗?
A：内部测试可以，但对公众提供服务、收取费用、对外营销可能被视为未授权经营。建议：

- 沙盒/试点（如主管机关提供）；
- 封闭测试：不对外、无真实客户资产；
- 预营销材料必须谨慎：不得暗示已获批。

Q18：是否需要保险?
A：多国主管机关在客户资产风险、网络安全风险方面会期待适度保险配置（职业责任险、网络险、犯罪险等），尤其当你托管客户资产、处理法币资金或大规模零售客户时。保险不是万能，但能体现风险管理成熟度。

Q19：CASP 与 DORA 有什么关系?
A：DORA 是欧盟数字运营韧性框架，适用于金融实体及其 ICT 第三方风险管理。CASP 在欧盟体系下与 DORA 的技术治理要求高度耦合：外包治理、渗透测试、事件报告、BCP/DR、访问控制、日志留存等都需要对齐。

Q20：波兰主管机关会最关注什么?
A：通常是“可控性”四件事：

1. 股东/UBO 资金来源闭环；
2. 管理层与关键岗位适当人选；
3. AML/制裁/交易监测与 STR 决策留痕；
4. ICT 安全与外包可控（含退出迁移）。

B｜实体与实质（Q21–Q40）

Q21：在波兰设立什么实体形态更常见?
A：常见为 Sp. z o.o.（有限责任公司）或其他符合本国公司法的形式。监管更关心：公司治理结构是否清晰、章程是否支持合规要求（例如董事权限、合规否决权、股权变更门禁、审计权、外包审批机制）。

Q22：MiCA 申请前公司必须先设立吗?
A：多数情况下需要：申请主体必须是可承担监管义务的法人实体。可以先设立，再启动申请；若你用欧盟其他国实体在波兰申请，涉及跨境结构解释、实质安排与监管协调，材料更复杂。

Q23：什么叫“实质经营（Substance）”?
A：不是办公室摆设，而是：

- 关键决策与治理在波兰有落点；
- 关键岗位能履职、可被监管接触；
- 运营活动（开户、监测、客服、投诉、事件响应）有明确责任人；
- 记录留存、审计、报表能在本地调取或可控。

Q24：需要实体办公室吗？
A：通常建议有。即便你采用混合办公，也应具备：注册地址、合规档案存放安排、受监管沟通机制、数据与记录访问控制。监管会问：如果突击检查，你在哪里展示记录？

Q25：董事是否必须常驻波兰？
A：未必，但需要可解释的时间投入、沟通机制、会议安排、签署权限。若董事都在境外，需证明：治理仍有效、关键决策记录完整、监管联络顺畅。

Q26：可以用集团共享服务中心吗？
A：可以，但必须：

- 明确服务边界（哪些职能共享）；
- 具备外包/内部服务协议；
- 保证监管可穿透、可审计；
- 数据安全与访问控制符合要求；
- 退出迁移计划明确。
  共享服务中心本质上也会被监管按“外包风险”审视。

Q27：能否用“名义董事/挂名合规”降低成本？
A：高风险。监管会做真实性判断：履历、面谈问答、时间投入、实际工作产出（合规抽查、STR记录、培训记录等）。一旦被判断为“名义任职”，容易被拒或后续被处罚。

Q28：管理层需要设置哪些委员会？
A：视规模。常见做法：风险与合规委员会、审计委员会、ICT/安全委员会。小公司可合并，但必须明确职责、会议频率、议题模板、决议留痕、跟踪整改闭环。

Q29：公司章程/股东协议建议加入哪些监管友好条款？
A：建议加入：

- 股权变更触发监管通知的门禁（未完成报备不得过户）；
- 董事/关键岗位任免需合规审查；
- 合规否决权与升级路径；
- 外包需董事会批准并保留审计权；
- 数据与记录可访问条款；
- 重大事件（制裁命中、数据泄露、重大投诉）报告机制。

Q30：申请期间能不能对外签客户？
A：可签意向或框架协议，但不得开展受监管服务、不得收取客户资产/资金进行交易或托管。所有对外材料必须加清晰声明：尚未获批，不提供受监管服务。

Q31：实质要求会影响护照吗？
A：会。护照扩张本质上建立在“你被本国有效监管”。如果本国监管认为你实质薄弱，会在护照阶段更谨慎，或在后续检查中要求整改，甚至影响跨境扩张节奏。

Q32：是否需要本地审计师/会计师？
A：通常建议配置本地审计资源，特别是涉及法币账务、客户资金隔离、财务报表审计、监管报表支持。即便可用国际所，也要保证波兰本地可执行与沟通效率。

Q33：是否必须有本地法律顾问？
A：强烈建议。因为除了 MiCA，还涉及波兰本地 AML 法、雇佣法、数据法、消费者保护、广告法等。没有本地法律支持，制度落地与合同条款容易与本地强制性规定冲突。

Q34：集团控股结构复杂会增加审查吗？
A：会。尤其多层控股、离岸结构、代持、信托安排、跨境资金链，会显著提升 SoF/SoW 与穿透披露要求。建议尽量简化层级，或提前准备“穿透备忘录+证据链索引”。

Q35：是否允许同一集团多个 CASP？
A：允许但需解释：分工、冲突隔离、共享服务、客户迁移、数据流、品牌与营销边界。监管会问：是否存在监管套利、是否会混同客户资产与责任。

Q36：如何证明“关键管理在波兰”？
A：用证据说话：董事会会议安排与纪要、关键决策清单、审批流程、签署权限矩阵、系统后台权限日志、合规抽查报告的签署与跟进、事件响应演练记录等。

Q37：申请材料语言用什么？
A：通常需满足主管机关要求（可能是波兰语/英语）。实务上建议：核心制度与PoO可提供英文主版本，并准备关键章节的波兰语摘要或官方要求格式，避免翻译差错引发补件。

Q38：我们能否把运营放在其他欧盟国，波兰只做牌照?
A：风险极高。监管会认为你在波兰缺乏实质，可能拒批或要求重大整改。更合规的做法是：波兰作为真正的治理与控制中心，其他国家作为分支/营销据点在护照后逐步落地。

Q39：如何设计“最小合规团队”？
A：建议至少：合规负责人、MLRO、ICT安全/运维负责人、运营负责人、客户支持/投诉负责人。内审可外包但要有审计计划与整改跟踪责任人。团队最小化可以，但不能牺牲关键控制职能。

Q40：实质要求最常见补件是什么?
A：通常是：岗位是否真实、汇报线是否独立、资源是否足够、外包是否可控、记录留存是否可调取、决策留痕是否可审计。

C｜股东/UBO（Q41–Q60）

Q41：10% 持股为什么敏感?
A：10% 是 qualifying holding 起算线。达到或超过该比例的直接/间接股东通常需要做更深入的适当人选与资金来源审查，并触发后续变更通知义务。

Q42：UBO 的认定按什么原则?
A：以最终自然人控制为核心：直接/间接持股、投票权、控制安排（协议控制、一致行动、委托投票、信托受益）。必须披露至自然人终点，不能“停在公司”。

Q43：资金来源（SoF）与财富来源（SoW）有什么区别?
A：SoW 解释“你整体财富怎么来的”（长期路径）；SoF 解释“本次出资/收购/增资的钱具体从哪里来、怎么到位”。监管通常两者都要，并要求可核验的证据链。

Q44：哪些 SoW/SoF 证据最有说服力?
A：审计报表、纳税证明、股权出售协议与对价流水、分红决议与入账、工资与雇佣证明、房产处置合同与收款、银行对账单、交易所或经纪账户报表（视情况）等。关键是“结论能回指证据”。

Q45：如果资金来自加密资产收益怎么办?
A：必须更细：

- 资产形成路径（何时买入/挖矿/项目分配）；
- 交易平台/钱包地址证明；
- 链上可追溯性与对手风险；
- 兑换成法币的路径与合规性；
- 税务处理说明。
  监管会对“加密收益直接作为资本金”格外敏感。

Q46：股东有 PEP 或高风险背景能过吗?
A：不必然否定，但会显著提高EDD深度：资金来源、关联交易、制裁风险、声誉风险、治理隔离机制、额外监控与披露。若涉及制裁命中或重大负面事件，风险极高。

Q47：股东在其他国家曾被监管处罚会怎样?
A：必须披露并解释：处罚原因、整改措施、现状（是否已解除/是否持续影响）。隐瞒通常比处罚本身更致命。监管更看重透明度与整改能力。

Q48：多层离岸架构是否一定不行?
A：不是一定不行，但一定更难：穿透、文件公证/认证、税务与资金链解释、代持/信托安排披露、真实控制权证明。建议能简化就简化；不能简化就提前做“穿透说明书”。

Q49：是否需要提供股东的银行推荐信?
A：有时可作为辅助，但不是核心。核心仍是可验证的 SoF/SoW、合规与声誉证明、以及资金到位路径。

Q50：股东出资是否必须实缴?
A：取决于公司法与监管要求。监管更在意：你是否具备满足资本与稳健经营的资金实力、资本是否可用、是否存在抽逃或短期过桥资金。

Q51：股东借款给公司算资本吗?
A：通常不等同资本金。可作为营运资金来源，但监管会问：期限、利率、从属安排、是否影响偿付能力、是否可随时抽走导致风险。若用借款“伪装资本”，风险很大。

Q52：关联方注资/往来需要披露吗?
A：需要。关联交易是监管重点：定价、公允性、利益冲突、资金回流、是否输送利益。建议建立关联交易政策与董事会审批流程。

Q53：股权变更后多久必须通知?
A：一般要求在法定触发下“事前/事后及时通知”。实务上建议：**交易前先做监管沟通**，在 SPA 里设定“监管不反对/批准”为先决条件，避免交易完成后被认定违规。

Q54：股东是否必须提供个人无犯罪记录?
A：通常需要对关键股东/UBO提供相应的声明与证明（视国家要求）。即便不强制出具纸质证明，也应至少提供宣誓声明、背景调查报告与可核验信息。

Q55：如果股东是法人，董事也要审查吗？
A：会审查法人股东的控制人、董事、实际管理层以及最终自然人UBO，尤其当法人股东本身是受监管实体或跨境集团时，审查会更深入。

Q56：股东的“声誉”怎么评估？
A：综合：刑事/行政记录、监管处分、破产与失信、重大诉讼、制裁名单、负面媒体、业务道德争议等。关键是：是否影响稳健经营、是否引入 AML/制裁风险。

Q57：股东是否要承诺不干预合规？
A：建议。监管不喜欢“股东直接指挥合规/风控”。可通过治理文件：明确管理层独立履职、合规否决权、董事会监督机制、股东不当干预的举报与升级机制。

Q58：UBO 信息需要持续更新吗？
A：需要。建议制度化：季度 cap table 核对、年度UBO确认、重大事件触发更新（新增代持、投票委托、一致行动等）。

Q59：监管最常问的 SoF/SoW 细节有哪些？
A：

- 钱从哪来、哪一年赚到、凭什么赚到；
- 资金链是否完整、是否有第三方代付；
- 是否涉及高风险司法区、现金密集行业；
- 是否有税务合规证明；
- 是否存在循环交易或“短期过桥”。

Q60：我们怎样把 SoF/SoW 做成“可审计交付版”？
A：建议三件套：

1. 结构图（穿透到自然人）；
2. 叙事备忘录（SoW/SoF逻辑）；
3. 证据索引表（每条结论对应文件编号、日期、页码、流水号）。

D｜董事适任性（Q61–Q80）

Q61：董事/管理层“适当人选”核心看什么？
A：四个维度：诚信与声誉、能力与经验、时间投入、治理有效性（独立性、冲突管理、决策留痕）。

Q62：董事必须有金融牌照经验吗？
A：不一定，但必须具备与业务匹配的综合能力。若没有直接监管经验，应通过：顾问支持、培训体系、合规与风险控制机制、面谈准备来补足，并证明“能理解并执行监管要求”。

Q63：技术型创始人可以当董事吗？
A：可以。但监管会问：谁负责合规、谁负责风险、谁负责财务稳健、谁负责客户保护。技术型董事需能解释：钱包治理、权限分层、事故响应、外包管理与安全控制。

Q64：董事是否要通过考试？
A：MiCA 不以“统一考试”为核心，但波兰本地可能要求声明、履历、无犯罪、以及面谈。关键是**面谈表现**与**证据化履历**：你做过什么、如何做、如何管理风险。

Q65：董事兼职太多会怎样？
A：可能被质疑时间投入。需要：时间承诺说明、会议安排、授权机制、替代安排、关键决策参与证据。监管担心“挂名董事”。

Q66：董事的利益冲突如何管理？
A：必须有制度：关联交易审批、持仓与交易限制、内幕信息管理、礼品与招待政策、外部任职披露、与供应商/代币项目方关系披露。

Q67：董事能否兼任 CEO 与合规负责人？
A：小公司可能出现兼任，但必须解释独立性与防火墙：

- 合规否决权如何实现；
- STR 决策如何独立；
- 内审如何独立（通常建议外包）；
- 董事会如何监督。
  兼任越多，监管越谨慎。

Q68：管理层需要哪些关键政策必须“亲自批准”？
A：通常包括：风险偏好声明、AML政策、制裁政策、外包政策、客户资产保护政策、事件响应与BCP/DR、投诉与纠纷处理政策、利益冲突政策。

Q69：董事会会议与纪要要写到什么程度？
A：要能证明“真正治理”。建议纪要包含：议题、风险讨论、决策依据、反对意见、整改事项、责任人与截止日期。监管抽查会看“是否走

形式”。

Q70：董事是否要对客户投诉负责？
A：董事会需监督投诉机制有效性，重大投诉与系统性问题应上升到董事会层面，并形成整改闭环。投诉不是客服问题，是合规与声誉风险。

Q71：董事对 AML 的责任边界是什么？
A：董事会负责设定风险偏好、批准 AML 框架、确保资源充分、监督 MLRO 的独立性与有效性。MLRO负责具体执行与 STR 决策，但董事会对体系有效性负最终责任。

Q72：董事对 ICT 安全的责任边界是什么？
A：董事会需监督 ICT 风险管理：外包、渗透测试、事件报告、BCP/DR、权限治理、关键系统变更。不能把“安全”完全甩给技术团队。

Q73：董事是否必须懂区块链？
A：不必人人都懂，但必须确保治理层具备足够知识覆盖关键风险。建议至少一名董事或高管具备加密/ICT安全实战背景，并通过定期培训提升整体治理能力。

Q74：董事背景调查通常包括什么？
A：身份与地址、无犯罪记录、破产与失信、监管处分、重大诉讼、制裁与PEP筛查、负面媒体、学历与工作经历核验、利益冲突与关联方披露。

Q75：董事曾经创业失败或破产是否必然被拒？
A：不必然，但需解释原因、是否存在诚信问题、是否对稳健经营产生重大疑虑，并展示改进与治理能力。关键在透明披露与可解释性。

Q76：董事需提交哪些声明类文件？
A：常见包括：适当人选声明、无利益冲突声明、时间投入声明、无刑事定罪声明、遵守监管义务承诺、信息真实完整承诺等。

Q77：董事能否由集团母公司委派？
A：可以，但需防止母公司利益凌驾于客户保护与合规之上。需明确：本地实体董事对本地实体负信义责任，关键决策不得被母公司不当干预。

Q78：董事更换后需要报备吗？
A：通常属于重大变更事项，需要及时通知主管机关，并提供新任董事的完整适当人选材料包与过渡安排。

Q79：如何准备监管面谈？
A：建议准备“面谈题库+证据包”：业务模式、收入来源、客户类型、AML风险、制裁处置、钱包治理、外包与退出、投诉机制、资产隔离、事件响应演练。

Q80：最常见的董事适任性补件是什么？
A：履历与业务不匹配、时间投入不足、利益冲突未披露、对 AML/ICT/客户保护理解不清、治理证据不足（纪要、审批、整改闭环缺失）。

E｜资本/保障（Q81–Q100）

Q81：MiCA 对资本金怎么要求？
A：按服务类型与风险，存在最低资本要求与持续稳健经营要求。你需要把：服务范围、客户资产规模、运营成本、风险暴露映射到资本规划，并写入资本充足性评估（ICAAP类思路）。

Q82：资本是否需要一次性到位？
A：通常申请阶段需要证明可满足最低资本并支撑启动期运营（含技术、合规、人员、审计、保险）。若计划分期注资，必须有可执行的资金承诺与时间表，并解释启动期如何满足稳健经营。

Q83：资本来源可以是股东贷款吗？
A：贷款不等同资本。可作为营运资金，但监管会担心随时抽走。若你用贷款支撑关键控制职能，监管可能要求更稳健的资本结构或从属安排。

Q84：是否需要准备“资本与财务预测模型”？
A：强烈建议。至少3年预测：收入、成本、人员、技术、审计、保险、外包费用、合规成本、市场扩张成本。并做压力测试：币价波动、交易量下滑、制裁事件、系统事故。

Q85：客户资产是否必须隔离？
A：客户保护是 MiCA 核心之一。若你托管或可控制客户资产，必须有隔离机制：账务隔离、钱包隔离、权限隔离、以及破产隔离的法律安排说明。

Q86：需要设立保证金或储备吗？
A：具体取决于服务类型与主管机关要求。即便无明确保证金要求，监管也会期待：运营储备、事故应对资金、赔付能力安排（含保险）。

Q87：是否要做外部审计？
A：通常需要年度财务审计，且关键控制领域（客户资产隔离、AML有效性、ICT安全）也可能被要求独立评估或专项审计。建议提前选定审计师与审计计划。

Q88：资金与资产如何估值？
A：资本认定通常以法币计量；加密资产作为资本或储备需要谨慎，监管会关注波动性与可用性。建议核心资本以稳定法币资产为主。

Q89：如果我们只做“非托管软件”，资本要求会更低吗？
A：风险可能更低，但仍需支撑合规、客户保护、ICT安全与运营韧性。监管不会因为你“轻资产”就接受“零治理”。

Q90：如何证明公司不会挪用客户资产？
A：制度+技术+审计三位一体：

- 权限分层、多签、冷存储策略；
- 资产变动审批与日志；
- 定期对账与审计；
- 关联方交易限制；
- 员工行为与访问控制。

Q91：资本不足会怎样？
A：可能导致拒批或附条件批准并要求补足资本、限制业务规模、限制扩张。持牌后资本不足可能触发监管介入、整改命令甚至暂停业务。

Q92：是否需要建立“资金管理政策（Treasury Policy）”？
A：建议建立：资金头寸管理、银行账户权限、支付审批、法币与加密头寸限额、对手方管理、收益与成本核算、异常交易监测等。

Q93：我们做做市/自营库存，资本怎么考虑？
A：做市会带来市场风险与流动性风险。资本规划需考虑：库存限额、对冲策略、极端行情压力测试、交易对手风险、资金占用与保证金安排。

Q94：是否要设立客户赔付机制？
A：建议在客户条款与投诉机制中明确赔付原则、责任边界、争议解决与仲裁/法院管辖，并结合保险与事故响应计划形成闭环。

Q95：能否以集团担保代替资本？
A：担保可作为补充，但不应替代最低资本要求。监管更偏好实体具备可持续的自有资本与稳健经营能力。

Q96：我们需要准备“破产处置计划（wind-down plan）”吗？
A：非常建议。说明：若停止经营，如何安全退出、如何返还客户资产、如何通知客户与监管、如何迁移系统与数据、如何处理未完成交易与投诉。

Q97：审查时监管会问哪些财务细节？
A：收入来源是否真实、费用结构是否合理、合规与安全预算是否足够、外包费用是否低估、是否存在不合理关联交易、是否有资金挪用风险。

Q98：税务会影响资本吗？
A：会。税负会影响利润与净资产。财务预测应纳入 CIT/VAT/预提税、雇佣成本与社保、公允价值会计处理等。

Q99：客户法币资金如何处理最合规？
A：通常建议：客户资金专户、受信安排或等效隔离机制；支付流程审批；对账与异常识别；清晰披露资金性质与可用性；避免混同公司营运资金。

Q100：资本/保障模块最常见补件是什么？
A：财务预测过于乐观、没有压力测试、未解释做市/库存风险、客户资产隔离描述过于概念化、缺少退出计划与对账审计安排。

F｜AML/制裁/STR（Q101–Q120）

Q101：CASP 在波兰一定属于 AML 义务主体吗？
A：实务上大概率是。你必须满足本国 AML 法要求（客户尽调、持续监控、STR、记录保存、培训、独立审查等），并与 MiCA 的客户保护与治理要求一起形成统一合规体系。

Q102：我们需要 MLRO 吗？
A：强烈建议必须设置（或等效职责负责人），并且具备独立性、资源与直接升级路径。没有 MLRO 的体系很难通过审查。

Q103：KYC 的最低要做到什么程度？
A：至少包括：身份核验、受益人识别（法人）、风险评级、PEP/制裁筛查、资金来源信息收集（视风险）、持续监控与定期复核。

Q104：EDD 什么时候触发？
A：高风险客户/国家、PEP、制裁相关、异常交易、复杂结构、加密资产来源不明、频繁跨境、与混币/暗网风险相关等，均触发增强尽调：更多文件、更多验证、管理层批准、降低限额或拒绝。

Q105：制裁筛查要筛哪些？
A：至少：EU 制裁名单 + UN + 本地要求；很多项目还会加 UK/US OFAC 等（取决于业务风险与银行通道要求）。筛查对象包括：客户、UBO、收款/付款对手、受益人、地址、设备指纹（可选）。

Q106：链上监控必须做吗？
A：如果你处理链上转账、托管或兑换，强烈建议使用链上分析工具与规则体系：高风险地址识别、混币器/暗网关联、制裁地址、跳转路径、风险评分与处置SOP。

Q107：Travel Rule 怎么做？
A：建立信息收集、传递、验证机制：发送方/接收方信息字段、阈值规则、与对手机构的互通方式、失败处理（缺字段/对手不支持）、留痕与审计。对 OTC/自托管钱包交互要特别设计。

Q108：什么是 STR？谁决定报不报？
A：STR 是可疑交易报告。通常由一线触发警报→合规/AML团队调查→MLRO 决策→必要时报送→留痕保存。必须有**决策树**与**记录模板**，证明“为什么报/为什么不报”。

Q109：STR 不报会怎样？
A：风险极高：监管处罚、刑事风险、银行通道终止、牌照风险。最常见问题不是“漏报一次”，而是“没有可解释的决策与留痕”。

Q110：我们可以因为“商业原因”不报 STR 吗？
A：不可以。STR 决策必须以风险与法律义务为准，不得被营收压力或客户关系左右。MLRO 的独立性就是为防这种情况。

Q111：交易监测规则如何设计？
A：建议分三层：

- 基础规则（频次、金额、地域、设备、账户行为）；
- 场景规则（分散/聚合、快速进出、跨链跳转、混币、异常对手）；
- 风险自适应（高风险客户更严阈值）。
  并做回溯测试、误报率评估、规则变更管理。

Q112：如何处理“自托管钱包”出入金？
A：关键是证明你对风险有控制：地址归属证明（签名验证/小额验证）、链上风险评分、限额、冷却期、异常触发人工复核、必要时拒绝或冻结并升级 MLRO。

Q113：可以把 AML 外包吗？
A：部分可外包（例如工具、部分调查支持），但 MLRO 决策与体系责任不能外包掉。必须保留审计权、监督权、数据控制、退出迁移计划。

Q114：培训要怎么做才算“可审计”？
A：要有：年度培训计划、课件、签到、测验、通过率、补训记录、培训覆盖矩阵（岗位→课程），并与真实案例/STR复盘结合。

Q115：记录保存要多久？保存什么？
A：按本国 AML 法要求（通常多年）。保存内容包括：KYC文件、风险评级、筛查结果、交易监测警报与处置、STR 决策记录、客户沟通、投诉、培训、审计与整改等。关键是：可检索、可调取、不可篡改。

Q116：如何管理“黑名单/拒绝客户”？
A：建立拒绝与退出政策：触发条件（制裁、欺诈、虚假信息、拒绝提供资料、链上高风险等）、审批流程、通知策略、资金处理、STR评估与留痕。

Q117：我们发现制裁命中怎么办？
A：立即冻结/停止服务（按法律与银行通道要求）、升级 MLRO 与管理层、评估是否必须报告、记录所有动作、与监管/执法沟通（如适用）。

Q118：如何避免员工内鬼/合规绕过？
A：权限最小化、四眼原则、多签、关键操作录像/日志、异常行为监控、强制休假、轮岗、背景调查、举报机制、内审抽查。

Q119：AML 体系最常见被问穿的点是什么？
A：

- STR 决策没有留痕；
- 规则过于模板化、不贴合业务；
- 高风险客户照样放行但没管理层批准；
- 没有链上监控或不会用；
- Travel Rule 无落地流程。

Q120：如果我们只服务机构客户，AML 可以简化吗？
A：可相对简化，但不能缺失。机构客户也可能高风险（OTC商、做市商、跨境支付商）。你仍要做 UBO 穿透、交易监测、制裁筛查、持续复核与STR机制。

G｜ICT / DORA / 外包（Q121–Q140）

Q121：监管眼里“合规的系统”要具备哪些最小能力？
A：至少：身份与权限管理、交易与资金流记录、日志不可篡改、报警与工单、对账、冷/热钱包治理、密钥管理、多签审批、BCP/DR、事件响应与报告流程。

Q122：冷热钱包怎么设计更容易过审？
A：常见“监管友好”结构：

- 绝大部分资产冷存储；
- 热钱包限额与自动补给机制；
- 冷钱包多签（不同角色分持、地理隔离）；

- 提币风控（白名单、延迟、人工复核）；
- 全流程日志与定期对账审计。

Q123：多签签名人如何配置？
A：建议分散在不同职能：运营、合规/风控、技术安全，并设置替代人机制与紧急流程。避免单点或同一部门掌控所有签名。签名权限与变更必须有董事会级审批与记录。

Q124：权限管理（RBAC）要做到多细？
A：越细越好，至少到：

- 查看/操作/审批分离；
- 关键操作双人复核；
- 管理员权限审计；
- 临时权限（Just-in-time）与到期回收；
- 定期权限复核（Access Review）。

Q125：渗透测试必须做吗？
A：强烈建议做，并形成报告与整改闭环。监管更看重“发现问题后怎么修、多久修、谁负责、是否复测”。

Q126：BCP/DR 要写到什么程度？
A：要能执行：

- RTO/RPO 指标；
- 关键系统与数据备份策略；
- 备援演练计划与记录；
- 第三方依赖与替代方案；
- 客户沟通与公告机制。

Q127：安全事件发生时的流程？
A：必须有：检测→分级→隔离→调查→修复→通报→复盘。并明确：谁是事件指挥官、谁对接监管、谁对接客户、谁保全证据。事件日志要可审计。

Q128：我们用云服务可以吗？
A：可以，但监管会看：数据位置、访问控制、加密、密钥管理、供应商尽调、审计权、分包控制、退出迁移、SLA、事故通报与协作机制。

Q129：外包哪些属于“关键或重要职能”？
A：通常包括：托管与密钥管理、核心交易系统、客户身份核验、交易监测、制裁筛查、云基础设施、数据存储等。关键外包的治理要求更严：审批、尽调、合同条款、持续监控、退出计划。

Q130：外包合同必须写哪些条款才算合规？
A：至少包括：

- 审计权与访问权（含第三方审计）；
- 数据安全与保密、加密、访问控制；
- 分包限制与审批；
- 事件通报时限与协作；
- SLA/可用性/灾备；
- 退出与迁移（Exit plan）与数据返还/销毁；
- 监管可接触条款（监管要求时可提供信息）。

Q131：如何做供应商尽调？
A：从五类证据：公司资质与财务稳健、信息安全认证与报告（ISO/SOC等）、人员与流程、过往事件与整改、服务连续性与退出能力。并建立供应商评分与年度复评。

Q132：可以把合规系统外包给 SaaS 吗？
A：可以，但要证明：

- 数据可控；
- 规则可配置、可解释；
- 记录可导出、可审计；
- 供应商不会成为单点；
- 退出迁移可执行。

Q133：日志保存怎么做才“不可抵赖”？
A：建议：集中日志、时间同步、访问控制、不可篡改存储（WORM/等效）、日志审计与定期抽查、日志保留期限与检索能力。尤其是密钥操作、提币审批、权限变更、风控豁免。

Q134：代码变更与上线需要合规参与吗？
A：需要。建立变更管理：需求→评审→测试→安全扫描→上线审批→回滚方案→上线后监控。合规/风控需对影响客户保护与 AML 的变更有审阅权。

Q135：如何证明系统容量能扛高峰？
A：提供容量规划、压力测试报告、扩容策略、限流熔断、关键指标监控。监管担心高峰宕机导致客户损失与市场秩序风险。

Q136：私钥如何生成、存储、备份？
A：建议采用 HSM/硬件隔离、密钥分片或多签、离线备份、访问控制、密钥轮换、应急恢复流程，并做演练与记录。监管会问“如果签名人失联怎么办”。

Q137：第三方托管是否更容易过审？
A：不一定。第三方托管降低自建难度，但引入外包风险。你仍需证明：选择理由、尽调充分、合同可审计、退出可迁移、客户条款披露清晰。

Q138：DORA 会要求我们做什么额外工作？
A：核心是 ICT 风险治理体系化：外包治理、韧性测试、事件管理、第三方风险、持续改进。即使你还未完全纳入某些细项，监管也会期待你“对齐方向与落地计划”。

Q139：系统最常见补件是什么？
A：外包合同缺审计权/退出条款、钱包治理描述泛泛、权限分层不清、BCP/DR没有演练证据、事件报告流程不完整、日志与对账机制不清晰。

Q140：如何把 ICT 模块做成“交付版”材料？
A：建议交付包：系统架构图、数据流图、权限矩阵、钱包与签名流程图、变更管理SOP、BCP/DR手册、渗透测试报告与整改、外包尽调与合同条款库、事件响应演练记录模板。

H｜客户保护（Q141–Q160）

Q141：MiCA 客户保护最核心三件事？
A：透明披露（费用/风险/执行/冲突）、客户资产保护（隔离/控制/返还）、投诉与纠纷机制（可用、可追踪、可整改）。

Q142：费用披露要披露到什么程度？
A：不仅是“手续费多少”，还应包括：点差、滑点、提币费、托管费、换汇费、网络费、第三方费用、返佣、隐藏成本。并说明费用触发条件、计费方式与示例。

Q143：定价与执行质量如何披露？
A：如果你是对手盘（OTC/做市），必须披露你如何报价、是否可能与客户利益冲突、如何确保执行公平。若是撮合平台，要披露撮合规则、优先级、异常处理、停牌机制。

Q144：客户风险披露要覆盖哪些？
A：至少：价格波动、流动性、技术风险、托管风险、链上风险（地址错误不可逆）、制裁与冻结风险、稳定币脱锚风险、第三方依赖风险、监管变化风险。

Q145：适当性/适配性怎么做？
A：建议对零售客户做：知识与经验问卷、风险承受能力评估、产品分级（高风险/复杂）、风险提示与确认、必要时限制某些产品或提高门槛。

Q146：客户资产隔离怎么向客户解释？
A：条款里要写清：资产是否托管、谁控制私钥、是否使用第三方托管、是否会再质押/借出、破产情况下的处理原则、对账频率与客户查询权。

Q147：我们能否在条款里写“任何损失不负责”？
A：不建议。过度免责可能被认定不公平条款。更合规做法是：明确责任边界、合理免责（例如客户自身错误地址）、同时提供事故处理与赔付原则。

Q148：投诉机制要怎么设计？
A：必须可用：线上入口、工单编号、处理时限、升级路径、证据收集、赔付/纠正、复盘与整改。并明确：监管投诉渠道与争议解决方式。

Q149：客户资金进出金要注意什么？
A：要防洗钱与欺诈：同名校验、第三方代付限制、异常频次与金额监控、提现白名单、冷却期、可疑情况冻结与升级 MLRO。

Q150：账户冻结条件如何设定才不引发纠纷？
A：条款中明确冻结触发（制裁命中、欺诈、虚假信息、监管要求、司法协助）、冻结期间客户通知策略、资金处理、申诉机制与时间预期。

Q151：如何防止市场操纵与不公平交易？
A：建立市场监控：异常挂单撤单、刷量、对敲、抢跑、内幕信息滥用等检测规则。平台应具备暂停交易、限制账户、调查与报告机制。

Q152：利益冲突政策应包含哪些？
A：公司自营交易、做市与客户交易冲突、员工持仓与交易限制、返佣与佣金安排、关联方项目上线、供应商关系、信息隔离与“优先执行”

承诺等。

Q153：客户数据与隐私怎么保护？
A：GDPR 合规：合法性基础、最小化、保留期限、数据主体权利、跨境传输、数据泄露通报、第三方处理协议、访问控制与审计。

Q154：客户教育是否必要？
A：强烈建议，尤其零售。提供风险教育、常见骗局提示、地址安全、2FA、钓鱼防范、冷钱包基础。教育材料也可作为监管证据：你在降低客户风险。

Q155：如何处理“误转账/误提币”？
A：流程要写清：能否追回取决于链上特性与对手合作；你能提供的协助范围；收费；证据收集；冻结窗口（如有）；以及客户需承担的不可逆风险提示。

Q156：客户条款需要本地语言吗？
A：通常建议提供客户能理解的语言版本（波兰语/英语视市场）。语言不清晰会直接影响客户保护评估与投诉风险。

Q157：如果我们提供杠杆或衍生品相关服务呢？
A：这可能触发 MiFID 等其他监管体系。MiCA 不是万能牌照。若涉及杠杆、期货、差价合约等，必须做监管映射并可能需要额外授权。

Q158：如何处理“代币上线/下架”对客户影响？
A：要有透明政策：上线评估标准、风险披露、下架触发、客户通知、资产处置窗口、异常情况应急。尤其下架时要避免客户被动损失扩大。

Q159：客户保护模块最常见补件是什么？
A：费用披露不够细、对手盘冲突未披露、投诉机制无时限与升级、资产隔离描述缺技术与法律支撑、冻结条款过于宽泛或过度免责。

Q160：如何把客户保护做成“交付版”材料？
A：建议交付包：客户条款（T&C）、风险披露书、费用表与示例、投诉SOP与工单模板、利益冲突政策、资产隔离说明书、冻结/退出政策、客户教育材料清单。

I｜护照与跨境（Q161–Q180）

Q161：什么是 MiCA 护照？
A：在一国获授权后，通过通知程序向其他成员国提供跨境服务或设立分支。关键是：必须先在本国被有效监管，且跨境营销与客户保护要逐国合规落地。

Q162：护照是否“自动生效”？
A：不是“你想去就去”。需要按程序通知、等待窗口期，并满足目标国的消费者保护、营销与语言等本地要求（即使 MiCA 统一，也仍有本地规则差异）。

Q163：护照前必须准备哪些材料？
A：建议准备：目标国清单、服务范围、营销计划、客户支持与投诉安排、语言与披露适配、税务与VAT影响评估、数据跨境与本地存储要求评估、当地合作伙伴/外包安排说明。

Q164：跨境提供服务时 AML 怎么做？
A：通常由本国 AML 体系承担主体责任，但你必须识别目标国风险差异（高风险国家、当地制裁与执法合作），并确保客户尽调与交易监测能覆盖跨境行为。

Q165：我们能否在目标国找代理做营销？
A：可以，但营销外包也要治理：合规审批、话术与材料审查、禁止误导宣传、客户引流数据保护、投诉转交机制、佣金与利益冲突披露。

Q166：护照是否允许我们“先在目标国做业务再补手续”？
A：不建议。被认定为未授权跨境展业会带来严重后果：监管处罚、护照受阻、银行通道中断、声誉受损。

Q167：如果目标国对某类代币更敏感怎么办？
A：要做逐国“产品可售清单”与限制策略。例如某些国家对高波动或特定结构代币的营销更严格，你需要有地理围栏、风险提示增强、产品限制等。

Q168：跨境客户支持要如何配置？
A：至少：多语言支持、时区覆盖、投诉与纠纷处理机制、重大事件通知机制。监管会问：目标国客户遇到问题找谁、多久回应、谁负责。

Q169：护照会影响税务吗？
A：可能影响 VAT、常设机构风险、预提税、雇佣与社保、以及转移定价。建议在护照路线图中加入税务评估与合规安排。

Q170：我们能否在目标国设分支机构？
A：可以，通常需要更充分的计划：人员、办公室、治理、合规联络、记录可访问。分支比纯跨境服务的实质要求更高。

Q171：跨境数据流（客户数据、交易数据）需要披露吗？
A：需要。尤其涉及云与第三方处理。要说明数据存储地点、访问控制、跨境传输机制、DPA、以及客户告知与同意（如适用）。

Q172：跨境扩张时最常踩雷是什么？
A：营销误导（“已在当地获批”）、语言与披露不足、投诉机制无法覆盖、税务未评估、代理乱承诺、目标国高风险客户与资金路径未被 AML 体系覆盖。

Q173：护照扩张要不要做“国家级时间轴”？
A：建议必须做。每个国家：通知→材料适配→营销合规→客服配置→税务评估→上线。把里程碑写清可控，避免同时铺开导致失控。

Q174：护照后，目标国监管会来查我们吗？
A：可能。尽管主要监管在本国，但目标国可以就消费者保护、营销、投诉等问题提出要求或协助检查。你需要准备跨境监管协作机制。

Q175：我们做机构业务跨境是不是更容易？
A：相对容易，但仍需合规。机构客户也要 KYC/UBO、制裁筛查、交易监测。营销与披露可相对简化，但不能缺失。

Q176：跨境业务是否要求本地银行账户？
A：不必然，但业务上可能需要。若涉及本地法币通道，银行尽调会看你是否在当地有合规落点、是否能处理当地投诉与争议。

Q177：跨境合作伙伴如何选择？
A：做尽调：合规记录、资金路径、客户质量、技术安全、合同条款（审计权、分包控制、退出）。并把合作伙伴纳入持续监控。

Q178：护照扩张是否影响我们申请更多服务类别？
A：会增加复杂度。建议策略：先把核心服务在波兰稳健运营并形成证据，再扩张护照，再在稳定基础上扩项服务类别。

Q179：护照扩张对“品牌宣传”有什么限制？
A：不能夸大授权范围、不能暗示在目标国被许可超出事实、必须披露风险与服务提供主体。所有广告素材需有合规审批与版本管理。

Q180：护照模块最常见补件是什么？
A：目标国服务范围不清、营销材料不合规、客户支持不足、税务与数据跨境未评估、代理外包缺治理与审计权。

J｜运营与持续合规（Q181–Q200）

Q181：持牌后有哪些“必须持续做”的合规动作？
A：至少包括：持续 AML 监控与 STR 决策留痕、客户投诉处理与复盘、定期培训、风险评估更新、外包与供应商复评、系统安全测试与演练、财务审计与监管报表、重大变更报备。

Q182：需要提交哪些监管报表？
A：取决于主管机关要求与服务类型。通常会涉及：业务规模、客户数量、交易量、客户资产规模、事件与投诉、财务与资本状况、外包与ICT风险、AML活动指标（警报数量、STR数量等）。

Q183：重大变更需要报备什么？
A：典型包括：股权/控制权变化、董事与关键岗位更换、服务范围扩项、重大外包、核心系统迁移、客户资产托管方式变化、重大安全事件、重大合规事件、业务模式重大调整。

Q184：培训多久一次？培训对象有哪些？
A：建议年度计划+按事件触发补训。对象覆盖：董事会、全员、关键岗位、前线客服与运营、技术运维。要有签到、测验、通过率、补训与记录留存。

Q185：内部审计怎么安排？
A：可外包，但必须独立。要有年度审计计划、审计范围（AML、客户资产、ICT、外包、投诉等）、发现问题整改闭环（责任人+期限+复检）。

Q186：如何做“合规监测计划”？
A：按主题设定频率与抽样：开户KYC抽查、制裁筛查复核、交易监测警报质量、费用披露一致性、营销材料合规、投诉处理时效、权限与日志抽查等。输出“月报/季报”。

Q187：如何证明我们的 AML 有效？
A：用指标与证据：警报命中质量、误报率、调查时效、STR 决策记录、回溯测试、模型变更管理、培训覆盖、独立审计结论与整改。

Q188：如何做“事件响应演练”？
A：至少年度演练：数据泄露、钱包被盗、供应商宕机、制裁命中、异常挤兑、关键签名人失联等。每次演练要有：剧本、参与人、时间线、改进清单。

Q189：外包供应商复评多久一次？
A：建议至少年度复评，关键外包可更频繁。复评内容：SLA、事件记录、审计报告、分包变化、财务稳健、合规事件、退出可行性。

Q190：客户资产对账频率怎么设？
A：建议至少每日对账（系统对账+链上对账+银行对账），并对异常设定工单与升级机制。对账是托管业务的生命线。

Q191：如何处理监管问询（RFI）？
A：建立“RFI应答战情室”：合规牵头、法务/技术/运营联动；建立证据仓库；每一问都以“结论+证据引用+附件编号”回复；全程版本管理与留痕。

Q192：如何做记录管理（Recordkeeping）才符合审查？
A：建立记录清单与保留期限矩阵；集中存储；访问控制；不可篡改；可检索。并明确：谁负责、如何备份、如何应对监管抽查。

Q193：持牌后如果业务增长很快，监管会担心什么？
A：担心你控制失效：KYC质量下降、监测规则跟不上、客服与投诉积压、系统容量不足、外包失控。要准备“增长控制计划”：扩员、扩容、提高抽查与监测强度。

Q194：如果发生客户资金损失或被盗怎么办？
A：启动事件响应：冻结、隔离、调查、通知客户与监管（如需）、保全证据、评估赔付、复盘整改。并依据条款与保险安排处理赔付边界。

Q195：如何管理“新币上线/新产品上线”的持续合规？
A：建立产品治理委员会：评估风险、合规与客户保护；上线前审查披露材料与营销话术；上线后监控投诉与异常交易；必要时下架并通知

客户。

Q196：如何确保员工持续合规?
A：员工行为准则、交易限制、冲突披露、强制休假与轮岗、权限最小化、日志审计、举报机制、绩效不以“合规违规”为代价。

Q197：持牌后是否还需要法律顾问长期支持?
A：建议保留。监管变化（ESMA Level 2/3、AMLA、DAC8 等）、新产品、跨境扩张、重大合同外包、争议处理，都需要持续法律与合规协同。

Q198：持续合规最常见被罚点有哪些?
A：未及时报备重大变更、AML体系形式化、STR 决策无留痕、外包合同缺审计权与退出、客户投诉处理不当、营销误导、数据泄露处置不合规。

Q199：我们如何把“持续合规”做成可交付的运营体系?
A：用“证据仓库（Evidence Vault）”思想：每项合规活动都产出证据（培训、抽查、演练、会议纪要、对账报告、供应商复评、STR记录、投诉闭环），并可随时导出给监管/银行/审计。

Q200：这份FAQ如何直接用于申请与面谈?
A：建议把 FAQ 映射到你的 PoO 与制度目录：

- 每个问题对应制度章节/流程图/证据模板；
- 面谈按模块演练（AML/ICT/客户保护为重中之重）；
- 对高风险点（SoF/SoW、外包、钱包治理、STR）准备“附件包”随问随给。

K｜产品治理、上币/代币准入、市场滥用与透明度（Q201–Q250）

Q201：MiCA 下“产品治理/新产品审批（NPC）”为什么会被问?
A：监管要确认你不是“先上线后补制度”，而是：**立项→风险评估→合规评审→ICT评审→客户披露→上线验收→上线后监控**的闭环；并能提供会议纪要、审批记录与证据链（Evidence Vault）。

Q202：CASP 是否必须建立“上币委员会/Listing Committee”?
A：强烈建议。尤其平台/经纪/兑换类业务，上币影响：客户风险、市场操纵、制裁暴露、技术安全与声誉。建议：董事会授权、委员独立性、回避机制、外部专家机制（可选）。

Q203：上币评估的“最低维度”应包含哪些?
A：至少 8 类：①法律属性（是否可能为金融工具/衍生品/证券型代币风险）②发行与治理③链上可追溯与风险（黑产/混币）④流动性与操纵风险⑤技术安全（合约审计/节点安全）⑥客户适配与披露⑦制裁/地缘风险⑧利益冲突与收费透明。

Q204：如何把“上币评分模型”写得可审计?
A：用“指标→权重→阈值→结论→例外处理→复核周期”的结构；保留：数据来源、评估人、审批人、版本号、有效期、复核触发条件（重大事件/安全漏洞/监管警示）。

Q205：上币是否必须做“智能合约审计”?
A：对链上代币/合约交互强的资产，监管预期会问“你凭什么认为安全”。最佳做法：第三方审计报告 + 内部复核 + 漏洞赏金/监控策略 + 上线后异常告警。

Q206：平台是否需要“市场监控（Market Surveillance）”机制?
A：若运营交易平台/撮合/订单簿，强烈需要：刷量、对倒、拉盘砸盘、幌骗（spoofing）、自成交、关联账户操纵等规则库；并形成：报警→工单→处置→复盘。

Q207：MiCA 是否直接规定“市场滥用监控”细则?
A：MiCA 对 CASP 行为规范、利益冲突、透明披露与客户保护有统一框架，平台类业务会被要求证明“公平有序市场”能力。主法框架见 MiCA EUR-Lex；细化口径会叠加 ESMA 的 Level 2/3（RTS/ITS/Guidelines）。

Q208：OTC/经纪撮合也要做市场监控吗?
A：要，侧重点不同：价格偏离、异常点差、客户分层报价一致性、对手方集中度、做市返佣冲突、可疑对敲、异常大额等。

Q209：做市商/流动性提供者能否使用?
A：可，但必须披露：是否自营交易、是否影响价格形成、是否存在返佣/利益输送；合同需明确 KPI、禁止操纵条款、审计权、数据留存。

Q210：如何管理“内部交易/自营”与客户交易冲突?
A：最稳做法：**原则上隔离**（组织隔离+系统隔离+信息隔离）；若存在做市/库存管理：需有董事会批准、披露、定价与风控边界、交易日志可追溯。

Q211：是否必须披露“收费与点差”到什么程度?
A：建议做到“客户能理解 + 可对账”：交易费、点差、提现费、托管费、第三方费用、返佣、隐藏成本（滑点/优先路由）、费用变更通知机制。

Q212：上币收费（Listing Fee）能收吗?
A：可以，但监管关注：是否诱导上高风险资产、是否影响公正性。必须：披露、利益冲突管理、收费与上币结论分离、费用不等于通过。

Q213：上币后多久复核一次?
A：建议：常规每季度/半年；触发复核：重大安全事件、监管警示、制裁风险、流动性枯竭、集中度异常、重大投诉。

Q214：下架（Delisting）策略必须写吗?
A：必须。包括：触发条件、客户通知期、平仓/提现安排、异常资产处理、争议处理、公告模板与证据留存。

Q215：如何处理“硬分叉/空投/代币迁移”？
A：要有“事件分类→风险评估→支持或不支持→客户通知→操作流程→对账→争议处理”制度；并将支持范围写入 T&C。

Q216：能否上“匿名增强币/混币相关资产”？
A：极高监管敏感。即使不明文禁止，也会触发 AMLA 趋势下更严的 AML 预期；通常建议：原则性禁止或严格限制，并保留董事会风险声明。

Q217：如何处理“高风险链/桥/跨链协议”暴露?
A：用“资产—链—桥—地址”四层风险模型；设定：转入限制、额外核验、延迟提款、链上追踪、黑名单策略。

Q218：上币评估中如何体现“制裁合规”？
A：把制裁筛查扩展到：发行方/核心贡献者/主要持币地址/资金流向；并记录筛查工具与结果快照。

Q219：客户投诉经常指向“上币质量差”，怎么办?
A：投诉机制要可用：受理→调查→结论→补偿（如适用）→复盘；并把投诉数据纳入上币复核输入。

Q220：如何写“透明度与披露”最合规?
A：用清单化披露：资产风险、价格形成、撮合规则、费用、利益冲突、资产隔离、赎回/提现规则、错误转账、客户分类、争议解决。

Q221：平台是否需要“规则手册（Rulebook）”？
A：建议有：交易规则、订单类型、撮合优先级、熔断/异常处理、市场监控与处罚、公告与变更机制。

Q222：能否提供杠杆/合约/期权?
A：MiCA 主要覆盖加密资产服务，但衍生品往往触发 MiFID 等其他框架；建议在 PoO 中明确“不提供”或另行持牌路径。

Q223：如何控制“虚假宣传/误导性营销”？
A：建立 Marketing Approval Log：每一份宣传材料必须合规审查、留档；禁止“已获批/受监管等同银行”等表述；对“申请中”表述更要谨慎。

Q224：是否需要“客户适当性/适配性”问卷?
A：若提供投顾/组合管理/复杂产品分销，强烈需要；对平台/兑换类，建议至少做风险承受能力与知识测评（尤其零售）。

Q225：如何定义“专业客户/机构客户”？
A：建议采用明确标准 + 证明文件清单 + 复核周期；并在条款中明确不同保护水平（披露、限额、杠杆等）。

Q226：如何处理“员工或关联方提前知悉上币信息”导致交易?
A：建立 Insider Trading Policy：信息分级、知情名单、窗口期、交易申报、违规处罚；并与审计抽查联动。

Q227：价格异常/闪崩怎么处理?
A：预设：熔断/暂停、公告模板、客户工单、复盘报告；并记录“为何触发、谁批准、何时恢复”。

Q228：是否需要“撮合公平性证明”？
A：建议：撮合逻辑说明、订单优先级、延迟与队列管理、风控拦截规则；并留存系统日志用于审计。

Q229：上币是否要考虑税务与会计处理?
A：要，尤其手续费、返佣、空投、奖励类交易；建议税务备忘录与会计政策同步。

Q230：能否允许客户“多账户”操作?
A：监管往往不鼓励（洗钱与操纵风险），应设：同一客户唯一账户原则；例外需管理层批准并留档。

Q231：是否要对“高频/机器人交易”设限制?
A：建议设：API 限速、风控阈值、异常行为检测；并把机器人滥用纳入市场监控规则。

Q232：如何处理“黑客攻击导致市场异常”与客户索赔?
A：制度要写清：事件分级、通知、冻结、对账、赔付原则、保险索赔、法律程序；并与 DORA 的事件响应对齐。

Q233：是否需要“资产证明（Proof of Reserves）”？
A：MiCA 强调客户资产保护，是否强制视服务类型与监管口径；实务上强烈建议：定期对账、审计支持、链上地址披露策略（平衡安全与透明）。

Q234：如何写“客户资产隔离”才算可审计?
A：明确：链上隔离（地址/子地址/标签）、链下隔离（法币账户/EMI合作方）、账务隔离（总账/客户分账）、每日对账与异常处理。

Q235：平台是否必须披露“订单执行质量/滑点”？
A：建议披露并做内部监控；若提供最佳执行类服务，应形成 Best Execution Policy 与可量化指标。

Q236：能否提供“复制交易/跟单”？
A：通常会触发投顾/组合管理的合规预期；需评估服务定性，至少要有适配性与风险披露。

Q237：如何处理“稳定币/ART/EMT”相关上架?
A：MiCA 对稳定币发行有专章与更严格要求；作为 CASP，上架与分销时要核验其合规状态与披露要求（以 MiCA 主法为依据 EUR-Lex）。

Q238：上币是否需要白名单链上地址?
A：对高风险资产/机构客户可采用；但要平衡用户体验与风险。可做分层：零售更严、专业客户可扩展。

Q239：如何管理“第三方发行方给的营销预算/补贴”？
A：这是典型利益冲突。必须：披露、审批、禁止与上币结论绑定、财务入账透明、审计可查。

Q240：上币/下架公告要保留多久？
A：建议按 AML 与监管记录保存要求设定统一留存策略（通常至少 5 年或更长，视本国 AML 法与监管口径）。

Q241：如何向监管证明“上币不是拍脑袋”？
A：给监管看 3 类证据：①流程（制度）②记录（会议纪要/评分表/审批链）③结果（上线后监控、投诉与复盘、下架执行）。

Q242：是否要为每个资产建立“风险披露卡（Risk Card）”？
A：强烈建议，便于客户理解与审查一致性：波动性、流动性、技术风险、监管风险、赎回/提现规则、费用与税务提示。

Q243：如何处理“代币回收/增发/黑名单冻结”等中心化权力？
A：必须披露并纳入上币评分，很多争议源于此；客户条款要写清风险与责任边界。

Q244：能否上“RWA/证券化代币”？
A：要非常谨慎，可能触发 MiFID/Prospectus 等；建议做业务定性备忘录，必要时走双合规路径。

Q245：如何把“产品退出计划（Wind-down）”写进产品治理？
A：对高风险服务（托管/平台）尤其重要：关停触发、客户资产返还、对账、通知、第三方依赖迁移、数据保全。

Q246：是否要对客户披露“重大事件历史”？
A：建议披露重大安全事件处置原则与客户权利；具体披露粒度以监管口径与安全策略平衡。

Q247：是否必须建立“费用变更治理”？
A：必须有：变更审批、客户通知期、拒绝权/退出权、历史版本留档；否则投诉与监管风险极高。

Q248：如何证明“客服与投诉”不是摆设？
A：用 KPI：受理时效、解决时效、升级比例、复发率；并保留工单与抽样审计记录。

Q249：如何管理“推荐机制/返佣”带来的误导风险？
A：披露返佣、禁止误导性表述、对渠道做尽调与监控、抽查录音/聊天记录（如适用）。

Q250：上币/市场监控体系与 AML 如何联动？
A：联动点：高风险资产/地址触发更严 AML、异常交易触发 STR 评估、做市/操纵与洗钱模式识别共享数据与工单闭环。

L｜数据治理、报表、审计、证据链与“可监管触达”（Q251–Q300）

Q251：监管为什么反复问“你能不能导出报表”？
A：MiCA 落地后，监管预期越来越“数据化模板化”。你必须证明：交易、客户、钱包、风控、投诉、外包、事件等数据可**一致导出、可追溯、可审计**。

Q252：什么是“Evidence Vault（证据仓库）”？
A：把合规变成“随时可抽查”：培训、抽查、面谈纪要、RFI 回复、系统日志、STR 决策记录、外包评估报告、渗透测试与演练记录、客户投诉工单等统一归档、版本控制。

Q253：证据仓库至少要有哪些目录？
A：建议 12 个：治理（Board）/人员（Fit&Proper）/股东（UBO）/PoO与BP/AML/ICT与DORA/外包/客户保护/财务与资本/审计与独立审查/事件与投诉/护照与跨境。

Q254：数据字典（Data Dictionary）为什么要做？
A：因为报表与抽查靠字段：客户税收居民、UBO、地址标签、交易类型、费用、风险评分、制裁命中、工单状态等；没有字典就无法证明一致性。

Q255：哪些系统日志最关键？
A：①权限与角色变更②关键操作（出金、密钥、白名单）③风控命中与处置④订单与撮合⑤对账与资金划转⑥外包调用与接口⑦异常与安全事件。

Q256：日志如何做到“不可篡改”？
A：采用 WORM 存储/集中 SIEM、严格访问控制、分离管理员权限、日志校验与定期审计抽查。

Q257：审计师/独立审查通常查什么？
A：AML 有效性（不是纸面）；客户资产隔离与对账；ICT 控制与变更管理；外包治理；财务与资本持续性；投诉与披露一致性。

Q258：是否必须年度审计？
A：通常需要公司层面法定审计；监管也可能要求专项独立审查。具体以本国公司法与监管口径为准。

Q259：如何组织“季度合规报告”？
A：用固定模板：业务概览、重大变更、KPI/KRI、STR统计、制裁命中、投诉统计、事件与演练、外包评估、整改跟踪。

Q260：如何证明“有效管理地在欧盟/波兰”？
A：证据：董事会决策留痕、关键岗位在岗、办公室与系统运维可触达、对外包的管理在本地完成、监管面谈能到场。

Q261：监管会要求展示“系统演示（demo）”吗？
A：经常会：KYC流程、风控拦截、钱包审批、多签签名、对账、投诉工单、报表导出、事件响应流程演练。

Q262：如何准备“抽查包（Inspection Pack）”？
A：随机抽 10–20 个客户：开户资料、风险评分、交易监控报警处置、制裁筛查快照、资金来源核验、沟通记录、关户记录；再抽 3 个事件演练与 3 个外包评估报告。

Q263：客户数据留存多久？
A：以本国 AML 法与监管要求为准；实务上通常至少 5 年（或更长）。要同时满足 GDPR 的合法留存基础与客户权利平衡。

Q264：GDPR 与 AML 留存冲突怎么办？
A：用“法定义务优先”的合法基础；在留存期内限制删除权，但要提供访问、更正与处理限制机制；期满后安全销毁并留痕。

Q265：如何做“版本管理（Document Control）”？
A：每份制度/流程：版本号、生效日、审批人、变更摘要、关联系统变更；保留历史版本，确保“制度—系统—执行记录”一致。

Q266：监管问“你们 KPI 怎么设定”该怎么答？
A：用合规 KPI（培训覆盖率、抽查完成率、RFI回复时效）+ 风险 KPI（误报率、STR时效、事件修复时效、对账差异率）+ 客服 KPI（投诉解决时效）。

Q267：如何证明“STR 决策链条可解释”？
A：每个 STR：触发规则→一线复核→MLRO结论→报送/不报送理由→证据链接→复盘；并对“未报送”保留理由记录。

Q268：财务预测必须到什么程度？
A：至少 3 年：P/L、BS、CF、压力测试；并把合规成本（工具、人、审计、保险、演练）单列，证明可持续经营。

Q269：如何把“资本/保障”与预算联动？
A：把资本与保险视为风险覆盖工具：安全事件、赔付、法律费用、客户索赔、运营中断成本；用情景压力测试证明足够。

Q270：监管会看“供应商尽调报告”吗？
A：会。尤其云、托管、链上分析、KYC、支付通道。必须：尽调问卷、SOC报告（如有）、SLA、审计权、退出计划、分包控制。

Q271：外包登记册（Outsourcing Register）要怎么做？
A：字段：服务、关键性、数据类型、所在地、分包、SLA、审计安排、退出方案、负责人、复核周期；对齐 DORA。

Q272：如何准备“RFI 补件战情室”？
A：设 RACI：合规牵头、法务把关、技术出证据、运营出流程；统一口径、统一编号、统一证据链接；每个问题给“结论+证据+附件索引”。

Q273：如何让材料“可复制交付”？
A：用索引化：PoO 索引、AML 索引、ICT 索引、外包索引、客户文件索引；每个条目对应模板与证据链接。

Q274：监管会要求“渗透测试报告”原件吗？
A：可能会。建议准备可对外版本（隐藏敏感细节）+ 内部完整版（受控披露）；并提供整改闭环证据。

Q275：如何证明“BCP/DR 演练有效”？
A：演练记录要量化：RTO/RPO 达成情况、问题清单、整改计划、复演结果；DORA 关注韧性测试体系。

Q276：如何管理“访问控制与最小权限”？
A：RBAC、强制 MFA、关键操作四眼原则、权限定期复核、离职即刻回收、特权账号监控与录屏（可选）。

Q277：审计追踪与客户争议有什么关系？
A：客户投诉/诉讼时，能否重构交易与指令链条决定胜负：订单、撮合、价格、费用、风控拦截、客服沟通、资金划转必须可回溯。

Q278：如何准备“管理层声明（Management Attestation）”？
A：管理层对 AML/ICT/客户资产隔离、外包、合规运行作年度声明，并列出已识别缺陷与整改计划（监管非常看重“自我识别与整改能力”）。

Q279：是否需要“内部审计职能”？
A：强烈建议具备；小机构可外包，但必须独立、可审计、向董事会汇报；外包不免除责任。

Q280：监管为何强调“会议纪要”？
A：因为这是证明治理与有效管理的核心证据：董事会/合规委员会/风险委员会/IT委员会的决策、挑战与结论必须留痕。

Q281：如何应对“数据跨境/云在非欧盟”的质询？
A：提供：数据分类、加密、访问控制、监管可触达、审计权、备份与退出、替代方案；但实务上优先 EU 区域部署更稳。

Q282：如何证明“客户资产没有被挪用”？
A：每日对账、独立对账人、异常阈值、链上地址隔离、法币账户隔离、资金划转审批链、多签、审计抽查与证明。

Q283：是否需要“客户资金流地图（Money Flow Map）”？
A：强烈建议：客户→支付渠道/EMI→公司→链上/托管→清算→客户；并标注每一步责任主体、对账点与风控点。

Q284：监管为什么会问“你们如何定价”？
A：防止不公平收费与误导；你需要说明点差形成、手续费、优惠与返佣、价格来源、异常行情处理。

Q285：如何准备“系统变更管理”证据？
A：变更单、审批、测试、回滚计划、上线窗口、上线后监控、版本记录；这与 DORA 的 ICT 风险控制一致。

Q286：如何证明“模型/规则不是随意改”？
A：对 AML 规则/风控阈值/市场监控规则建立版本管理：变更原因、数据验证、批准人、上线时间、效果评估。

Q287：监管会要求“组织架构与人数硬指标”吗？
A：通常不直接给硬指标，但会问“是否与业务规模匹配”。你要用岗位职责、值勤安排、替补计划证明足够。

Q288：如何应对“关键人风险”（人员离职）？
A：继任计划、交接清单、最小备岗人数、关键访问权限托管、文档化与演练。

Q289：如何管理“供应商锁定（vendor lock-in）”？
A：在外包合同加入：数据可携带、退出迁移、替代供应商预案、迁移演练；DORA 强调第三方集中度与退出。

Q290：监管抽查时最常见的“证据缺口”是什么？
A：制度有但没有执行记录；执行有但无审批；系统说能做但无法演示；外包合同缺审计权；STR 决策无留痕；对账无独立复核。

Q291：如何让“客户条款/披露”与系统一致？
A：把条款字段映射到系统：费用、时限、限额、冻结条件、投诉时效；上线前做一致性测试并留档。

Q292：是否需要“年度训练与演练计划”？
A：必须要有：AML培训、网络安全演练、DR演练、事件响应桌面演练、客服/投诉演练；并保留签到与结果。

Q293：如何准备“监管面谈”时的数据型问题？
A：准备仪表盘：交易量、客户分布、风险等级、制裁命中、STR统计、投诉统计、系统可用性、事件响应时效、外包评估结论。

Q294：如何构建“合规日历（Compliance Calendar）”？
A：按月列：培训、抽查、内审、对账复核、外包复审、渗透测试、DR演练、董事会报告、税务申报与（未来）DAC8 数据准备。

Q295：监管为什么会关心“税务信息采集”？
A：DAC8 将强化加密资产信息交换与数据治理（成员国转化与执行时间节点以正式文本/官方口径为准；行业普遍按 2026 起采集/申报节奏规划）。建议提前做税务居民信息字段与变更触发。

Q296：如何做“客户税务居民自证（Self-Certification）”？
A：开户收集 + 变更触发（地址/国籍/控制人变化）+ 定期抽查；与 AML 的客户信息一致性校验。

Q297：如何处理“多钱包、多地址映射同一客户”？
A：建立 Address Book：客户ID—地址—标签—风险评分—用途；并把地址变更纳入审批与日志。

Q298：监管问“你们能否关停业务并把资产返还”怎么答？
A：提交 Wind-down Plan：触发条件、时间线、客户通知、对账与返还、第三方依赖迁移、数据保全与法律处理。

Q299：如何证明“投诉处理机制有效”？
A：工单系统截图/导出、时效统计、升级记录、补偿记录（如有）、复盘报告与制度改进记录。

Q300：总结：数据与证据链的三句话怎么写？
A：①我们所有关键流程均有“制度+系统+日志”三层证据；②所有监管问题均可“定位到附件与证据链接”；③我们按 DORA 框架建设 ICT 与外包治理，确保可审计可持续。

M｜护照跨境、第三国招揽边界、持续合规与监管趋势（Q301–Q400）

Q301：拿到波兰 CASP 后如何“护照”到其他成员国？
A：按 MiCA 护照机制进行跨境通报：明确服务类型、提供方式（跨境/分支）、目标国清单、客户保护与营销合规落地计划。MiCA 主法框架见 EUR-Lex。

Q302：护照后，目标国还能要求我再申请牌照吗？
A：原则上不应重复授权，但目标国可能关注消费者保护、营销、语言与投诉对接；你需逐国落地“本地化合规”而非重复许可。

Q303：护照扩张最常见踩雷是什么？
A：宣传用语误导（“已在全欧盟监管”）、未完成通报即招揽、条款未本地化、客服与投诉无法支持目标国、数据跨境不清晰。

Q304：第三国客户（非欧盟）可以服务吗？
A：可以，但要管理：制裁风险、地缘风险、数据跨境、第三国营销边界、交易对手风险；并明确不向高风险司法辖区提供服务或设置更严 EDD。

Q305：什么是“第三国反向招揽（reverse solicitation）”？
A：指客户主动发起而非你主动招揽。监管对其使用非常谨慎，不能把“反向招揽”当普遍营销策略。建议：记录客户发起证据与审查。

Q306：如何建立“跨境营销合规”体系？
A：每个国家一张表：允许/禁止渠道、语言要求、风险披露、客服时区、投诉对接、广告审查规则；并与 Marketing Approval Log 绑定。

Q307：是否要设“护照国别时间轴”？
A：必须。列：通报递交—生效—本地化条款上线—客服配置—数据与税务字段完备—监管沟通窗口。

Q308：MiCA 过渡期对波兰有什么影响？
A：取决于波兰最终实施法对既有主体的安排；若你是既有 VASP，应倒排关键节点，避免“窗口错过”。（具体以官方最终文本/公告为准。）

Q309：监管会如何审查“跨境客户保护”？
A：看你是否提供：本地语言披露、可达客服、投诉时效、争议解决与管辖条款合理性、客户资产隔离一致性。

Q310：护照后是否要在目标国设分支？
A：不一定。自由提供服务 vs 分支取决于业务规模、目标国预期、客户类型与银行合作；但无论如何都要可监管触达、可执行投诉与抽查。

Q311：跨境业务对 AML 有什么额外要求？
A：客户地域风险、资金来源核验难度、制裁筛查复杂度提升；需强化 EDD、交易监控与链上分析策略。

Q312：如何管理“跨境支付/法币通道”合规？
A：明确与银行/EMI/PI 的责任边界：谁持有法币、谁做对账、谁做退款、谁做拒付与欺诈；并把这写入 PoO 与客户条款。

Q313：持续合规最重要的“年度四件套”是什么？
A：①年度合规计划 ②年度 AML 报告（含 STR 统计与有效性评估）③年度 ICT 韧性与外包评估报告（DORA 对齐）④年度审计/独立审查与整改闭环。

Q314：重大变更需要报备哪些？
A：通常包括：股权与控制权、董事与关键岗位、服务范围、关键外包、核心系统、客户资产安排、定价与条款重大变化、重大事件与安全事故。以 MiCA 持续义务逻辑为准 EUR-Lex。

Q315：什么是“变更评估闭环”？
A：提出变更→合规/风险/ICT评估→董事会批准→必要时报备→实施→上线后验证→归档。

Q316：DORA 已适用后，监管对 ICT 的新预期是什么？
A：从“有没有制度”转向“是否韧性可验证”：事件分级、演练、第三方风险、退出计划、持续监测。DORA 生效见 EUR-Lex。

Q317：外包合规与 DORA 的关系是什么？
A：DORA 强化关键第三方风险管理：尽调、合同必备条款、审计权、分包控制、集中度风险、退出/迁移。

Q318：发生重大 ICT 事件要做什么？
A：按事件响应：识别→分级→隔离→取证→通报→恢复→复盘整改；并准备监管沟通模板（什么时候、什么影响、怎么修、怎么防再发）。

Q319：发生客户资产丢失/被盗怎么办？
A：立即冻结、对账、通知、索赔与保险路径、客户补偿政策（如适用）、根因分析、外部取证与执法协作；并记录每一步证据链。

Q320：如何管理“保险/等效保障”续保与变更？
A：建立保险台账：覆盖范围、免赔、索赔流程、承保人资质、续保节点；任何变更要做风险评估并必要时报备。

Q321：监管会要求“合规官/MLRO 独立性”到什么程度？
A：关键在“可直达董事会 + 不被业务线干预 + 预算与资源可保障”。若 MLRO 兼任业务岗位，需强解释与补偿性控制。

Q322：合规与 MLRO 可以外包吗？
A：可以有外包成分，但不应“空心化”。最好：内部设责任人（Owner），外包提供工具与执行支持；责任仍在持牌主体。

Q323：如何防止“合规被业务 KPI 绑架”？
A：把合规 KPI 纳入高管绩效；设合规否决权（对高风险客户/高风险资产/高风险外包）；董事会定期听取合规独立汇报。

Q324：监管趋势里“AMLA”对 CASP 意味着什么？
A：欧盟反洗钱体系趋向更强一致性与更强执法协同；CASP 的 AML 预期会从“有制度”升级为“可证明有效运行”（命中率、STR 时效、外包管理、数据治理）。

Q325：监管趋势里“ESMA Level 2/3”意味着什么？
A：更多模板化、格式化、可比性要求：披露、报送、数据字段与留痕会更统一；你的系统必须支持“按模板导出”。

Q326：监管趋势里“DAC8”意味着什么？
A：加密资产税务信息交换与数据采集更严格，要求你提前做客户税务居民信息、交易分类与可追溯数据治理（请以最终文本与本国转化法为准）。

Q327：如何把 DAC8 需求提前写进系统？
A：新增字段与流程：税务居民自证、TIN（如适用）、控制人信息、钱包/地址映射、交易类型分类、估值口径、报表导出与对账。

Q328：持续合规中“培训”要怎么做才不被认为走过场？
A：岗位化：一线（开户/客服）+ AML专项 + IT安全 + 管理层；每次培训要有测验与抽查，记录签到、成绩与整改。

Q329：持续合规中“演练”有哪些必须做？
A：至少：DR演练、事件响应桌面演练、反洗钱可疑交易处置演练、客户资产对账与异常演练、外包退出演练（选关键供应商）。

Q330：持续合规中“客户投诉复盘”怎么写？
A：按月/季：投诉类型分布、根因、整改措施、复发情况、条款/系统/流程改版记录。

Q331：监管会如何评价“合规文化”？
A：看：董事会是否挑战业务、是否愿意拒绝高风险客户、是否按制度处理投诉与事件、是否自我披露问题并整改。

Q332：如何设置“高风险客户拒绝与黑名单机制”？
A：风险触发→EDD→管理层批准/拒绝→记录→持续监控；黑名单来源包括：制裁、执法通报、链上黑产地址、欺诈账户、重复投诉欺诈。

Q333：如何应对“银行开户难”？
A：用“合规包”打银行：治理架构、AML制度、交易监控、客户资产隔离、审计计划、DORA对齐、外包治理、三年预算与资本保障。

Q334：监管问“你们如何盈利”该怎么答？
A：清晰列：交易费/点差/托管费/API费/上币费（如有）/机构服务费；并说明利益冲突控制与披露。

Q335：如何管理“集团内服务费/成本分摊”的合规与税务风险？
A：有转让定价逻辑、合同、定价依据、服务交付证据；避免被认为利润转移或缺乏实质。

Q336：如何设置“合规预算”才可信？
A：把工具、人力、审计、渗透测试、演练、保险、法律费用单列；并在三年预测中体现随着业务增长的可扩展性。

Q337：监管可能问“你们是否能承受黑天鹅事件”？
A：用压力测试回答：挤兑、价格暴跌、系统宕机、安全事件、银行通道中断；展示预案与资金/保险覆盖。

Q338：如何处理“客户要求删除数据”？
A：在 AML 留存期内只能限制处理/封存而非删除；期满后按安全销毁流程执行并留痕。

Q339：如何处理“执法机构冻结/调查请求”？
A：建立 LEA Request SOP：接收、验证、法律审查、冻结执行、记录、沟通、解冻与通知规则。

Q340：如何处理“错误转账/链上不可逆”争议?
A：条款披露 + 工单流程 + 链上追踪 + 对手方协作 + 风险提示；对可协助范围与不可协助范围写清。

Q341：跨境客户争议的管辖条款如何写更稳?
A：要兼顾目标国消费者保护要求；建议准备多语言版本与本地法律审查。

Q342：如何管理“客户资产证明与审计披露”的安全风险?
A：分层披露：对客户披露原则与摘要，对审计与监管提供完整证据；链上地址披露要评估被攻击与跟踪风险。

Q343：监管会要求“实体办公室”吗?
A：未必写死，但对“实质经营”会追问。建议有：注册地址、办公场地、可到场面谈能力、关键岗位在岗安排。

Q344：董事/高管的时间投入如何证明?
A：任命函、工作安排、会议出席记录、职责分工、KPI；对兼职与外部董事席位列清单并说明不冲突。

Q345：如何避免被认为“空壳+外包一切”？
A：保留核心控制：合规、MLRO决策、外包管理、风险偏好、客户资产治理、关键 ICT 风险所有权必须在内部。

Q346：持续监管中“最容易被罚”的点是什么?
A：误导性营销、未按授权范围经营、客户资产隔离缺陷、AML执行不到位（尤其STR与制裁）、外包无审计权、重大变更不报备。

Q347：如何准备年度监管沟通?
A：建立年度会议：提交年度报告、重大风险与整改清单、下一年度计划；把监管问答沉淀为 Q&A pack。

Q348：如何管理“新法规冲击”带来的整改?
A：做 Regulatory Radar：ESMA/EBA/本国公告跟踪→差距评估→改版计划→培训→上线→复盘。

Q349：如果监管要求限期整改怎么办?
A：用项目化方式：整改计划（milestone）、责任人、证据输出、复测与复报；并把沟通书面化。

Q350：如何维持“护照国的一致性监管预期”？
A：统一集团政策库 + 国别附录；任何变更做 impact assessment；多语言披露与客服一致性。

Q351：如何处理“制裁升级/地缘突发”事件?
A：制裁名单即时更新、风险国家策略、冻结与拒绝流程、存量客户复筛、对外包供应商同步要求。

Q352：如何管理“高风险行业客户”（赌博、成人、军民两用等）？
A：行业黑名单/灰名单、增强尽调、交易限额、持续监控；必要时拒绝服务。

Q353：是否需要发现并报告“规避制裁”的交易模式?
A：需要。将其纳入规则库与 STR 评估；并记录处置与不报送理由。

Q354：如何设置“合规热线/举报机制”？
A：匿名渠道、保护机制、调查流程、董事会通报；这是合规文化的重要证据。

Q355：如何管理“员工道德风险/内部作恶”？
A：最小权限、强审批、轮岗与强制休假、特权账号监控、审计抽查、行为告警。

Q356：持续合规下“新客户渠道/代理”怎么管?
A：渠道尽调、合同约束、培训、抽查、返佣披露、禁止误导性营销；渠道数据要可追溯。

Q357：如何证明“客户适当性”执行到位?
A：问卷记录、评分、拒绝或限制记录、客户确认、复核周期与例外审批。

Q358：如何在波兰本地化 AML 制度?
A：以波兰 AML 法与金融情报单位（FIU）要求为准，建立 STR/报告路径与时限；并与 MiCA 行为规范协同。MiCA 主法：EUR-Lex。

Q359：波兰监管更偏好英文还是波兰文材料?
A：实践上常采用英文以便国际团队准备，但最终语言与公证/认证要求以监管沟通结果为准；关键法律文件建议准备波兰文或认证译本。

Q360：如何处理“文件公证/认证链条”？
A：列清单：股东/董事/UBO 身份住址证明、无犯罪（如要求）、公司注册文件等；提前做时间管理，避免因认证拖延整体进度。

Q361：申请期间能否先运营/先上线?
A：非常敏感。应避免形成“事实展业”；可以做不构成受规管服务的准备与测试，但不得对外招揽、受理、撮合、托管。

Q362：如何写“申请中”的对外合规话术?
A：只能客观陈述状态，不得暗示已获批/受监管等同持牌；所有 PR/官网/APP 文案需合规审查留档。

Q363：获批后多久必须上线?
A：取决于监管批复条件与公司准备情况。通常监管更关心“上线条件是否满足”：资本/保险、系统验收、关键岗位到位、演练完成。

Q364：上线前的“Go-Live Checklist”必须有哪些?
A：注资与保险到位、权限矩阵与多签启用、对账跑通、渗透测试与整改完成、DR演练完成、客服与投诉工单上线、报表导出验证、培训完成。

Q365：如何应对“上线后第一年监管强度更高”？
A：准备 90 天稳态计划：每月合规报告、KPI监控、抽样审计、外包复核、客户反馈复盘；避免“上线即放松”。

Q366：如何设计“年度费用与预算更新机制”？
A：每季度滚动预测，遇重大变更（新国家、新产品、新外包）立即做预算与资本/保障重算。

Q367：如何处理“并购/股权变更”后的合规?
A：重大变更评估、股东/UBO 新尽调、资金来源闭环、治理与关键岗位重评估、必要时报备。

Q368：如何管理“集团共享系统”带来的监管问题?
A：清晰边界：数据隔离、访问控制、审计权、事故责任、变更管理；并证明本地实体对关键系统有控制权与监督权。

Q369：如何应对“监管现场检查（on-site inspection）”？
A：建立检查预案：检查联系人、资料清单、系统演示脚本、抽查样本包、会议室与权限开通流程、问答口径。

Q370：监管最爱问的“十个一句话”是什么?
A：你做什么服务？客户是谁？资产怎么隔离？钱怎么走？谁做 AML？STR 怎么报？谁管 IT 风险？外包怎么控？出了事怎么报？如何护照扩张?

Q371：如何把 FAQ 用作销售与投标材料?
A：把 Q&A pack 分为：对外简版（不泄露敏感）+ 对监管/银行详版（含证据索引）；统一口径、统一版本。

Q372：什么情况下需要补做法律意见书（Legal Opinion）？
A：业务定性不清（OTC/经纪/平台边界、稳定币、RWA）、跨境营销、税务结构、外包与数据跨境等。

Q373：如何与本地律师/审计/IT 安全团队协同?
A：仁港永胜作为总控：统一索引与证据链，律师出法律合规，审计出独立审查与财务，安全团队出渗透测试与韧性证据。

Q374：监管会不会要求“本地董事/本地 MLRO”？
A：未必硬性，但会追问可触达性与时间投入；实务上配备本地资源更利于通过与后续维护。

Q375：如何管理“客户资产借贷/质押/再利用”？
A：高度敏感。若存在，必须在条款中披露并获得明确同意，并评估是否触发额外监管框架；多数申请策略建议避免。

Q376：如何处理“客户资产与公司资产同链地址”的情况?
A：不建议；这会被直接质疑隔离。应使用独立地址体系与账务隔离，并证明对账机制。

Q377：如何应对“黑产资金流入”导致账户冻结?
A：链上追踪、资金冻结、执法协作、客户沟通模板、风险复盘；并优化规则避免同类事件复发。

Q378：如何处理“高风险自托管钱包（unhosted wallet）”？
A：地址评分、额外核验、限额、延迟提现、持续监控、可疑模式触发 STR 评估；条款披露责任边界。

Q379：如何保证“客户身份冒用/账户接管”风险可控?
A：强 MFA、设备指纹、异常登录检测、人工复核、提现冷静期、客服反欺诈脚本与取证流程。

Q380：如何应对“媒体负面/挤兑”事件?
A：危机公关预案 + 透明披露原则 + 客户资产证明与对账 + 客服扩容 + 银行/支付通道备援 + 监管沟通。

Q381：如何准备“年度管理层声明 + 董事会确认”？
A：将 AML/ICT/客户资产隔离/外包/投诉等核心控制纳入年度声明，董事会审阅并提出挑战，形成纪要与整改计划。

Q382：是否要做“合规成熟度评估”？
A：建议每年做一次：制度、系统、人员、证据链、外包、数据治理评分；形成提升路线图。

Q383：监管趋势下“低门槛套利”还可行吗?
A：趋势是不行。ESMA 口径收敛、DORA 强化 ICT、AMLA 强化 AML，一体化合规才可持续。

Q384：如何把“合规当成产品力”？
A：把合规输出成可展示能力：对账、报表、透明披露、事件响应、客户资产保护、审计可验证；这反而利于银行与机构合作。

Q385：如何做“跨国团队协作的文件一致性”？
A：统一模板与术语库、统一索引、统一版本控制、统一证据链接；每周例会对齐口径与风险。

Q386：如何设计“多语言客户支持”？
A：至少英文+目标国必要语言；设 SLA 与升级机制；并把客服脚本纳入合规培训与抽查。

Q387：如何证明“费用与披露没有误导”？
A：展示费用计算示例、历史版本、变更通知记录、客户确认记录、投诉数据与复盘。

Q388：如何处理“客户退款/撤单/冲正”？
A：建立退款 SOP：触发条件、审批、反洗钱复核、时限、费用、记录；并与资金流对账一致。

Q389：如何管理“系统容量与高峰期风险”？
A：容量规划、压力测试、降级策略、熔断策略、公告模板、事后复盘；将结果纳入 DORA 韧性体系。

Q390：是否需要“安全基线（baseline）”与配置管理?
A：需要：CMDB、基线配置、变更管理、漏洞管理；否则无法证明 ICT 控制有效。

Q391：如何管理“第三方 API 风险”（行情、链上服务）？
A：接口监控、超时与降级、数据一致性校验、供应商 SLA、替代供应商预案。

Q392：如何准备“监管问答（Q&A Log）”？
A：每个问题：日期、问题、结论、附件索引、负责人、提交时间、监管反馈、后续动作；这是项目成功关键。

Q393：为什么“补件速度”决定成败？
A：监管审查是迭代式，慢会导致窗口错过与资源消耗；建立战情室与证据仓库能显著提速。

Q394：获批后最容易忽视的持续义务是什么？
A：重大变更报备、外包复核、演练留档、投诉复盘、培训测验、对账独立复核——这些都需要证据。

Q395：如何把“合规成本”压到可控？
A：不是砍制度，而是“模板化+系统化+自动化+证据链一体化”；一次性对齐 DORA，避免反复整改。

Q396：如何选择落地国（波兰）对项目的意义？
A：波兰的关键在于：本地实施法节奏、监管沟通可预期性、人才与成本、以及后续护照扩张策略。最终仍以官方制度落地为准。

Q397：监管最认可的“项目方法论”是什么？
A：三阶段法：Preparation（定服务+搭班子+定外包+出蓝图）→ Application（索引化提交+补件战情室）→ Post-licence（证据链运营+报表+演练+变更闭环）。

Q398：如果我们想最快推进，第一周做什么？
A：定服务范围（MiCA服务映射）+ 股权结构与 UBO 穿透 + 外包清单 + 系统蓝图 + 关键岗位 JD；并建立索引与证据仓库框架。

Q399：如果只给一个“通过率最高”的建议是什么？
A：把申请包做成“可审计、可证据化、可演示”：监管看的是**真实可运行体系**，不是文字漂亮。

Q400：如果只给一个“后续合规不翻车”的建议是什么？
A：从第一天就运营 Evidence Vault：培训、抽查、演练、日志、STR 决策记录持续留档；持续合规不是文件，而是可验证的运行。

仁港永胜建议（唐生结论｜波兰 MiCA CASP）

1. **先定服务范围，再定系统与制度深度：PoO（Programme of Operations）是申请核心**（服务类型/地点/方式/外包/客户旅程必须可审计）。
2. **股东/UBO 的 SoF/SoW 必须闭环可核验：这是最高频补件点**（资金路径图 + 证据链 + 不利信息解释备忘录）。
3. **ICT/外包按 DORA 一次性建好：DORA 已自 2025-01-17 起适用**，越早对齐越省后期整改成本。

选择仁港永胜的好处优势（服务优势）

- **一体化交付**：MiCA 授权材料 + AML 手册 + ICT/DORA 外包治理 + 客户条款披露，一次性成体系。
- **强模板库**：BP/PoO、Risk Register、STR 决策树、外包尽调清单、面谈题库、RFI 应答包、护照通报包、证据仓库索引。
- **实操导向**：以“可审计、可证据化、可解释”的结构组织材料与演示脚本，提高审查效率与通过率。

关于仁港永胜｜联系方式

仁港永胜（香港）有限公司（Rengangyongsheng (Hong Kong) Limited）为专业的合规与金融咨询服务机构，专注于全球金融牌照申请、虚拟资产合规（MiCA/CASP、VASP）、支付与电子货币（EMI/PI）及持牌后持续合规维护。我们在香港、深圳及多个司法辖区协同配置合规团队，可为客户提供从战略评估 → 申请文件编制 → 面谈辅导 → 监管沟通 → 持牌后持续合规的一站式服务支持。

- 官网：jrp-hk.com
- 香港：852-92984213（WhatsApp）
- 深圳：15920002080（微信同号）
- 香港办公地址：香港湾仔轩尼诗道253-261号依时商业大厦18楼
- 深圳办公地址：深圳福田卓越世纪中心1号楼11楼
- 香港：香港环球贸易广场86楼

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

免责声明

本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐生** 提供专业讲解，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。MiCA 主法源为 Regulation (EU) 2023/1114 EUR-Lex；DORA 为 Regulation (EU) 2022/2554 且自 2025-01-17 起适用EUR-Lex。波兰本地实

施法、主管机关程序、费用与审查尺度以 **最终颁布文本及主管机关最新公告** 为准；关于波兰主管机关指定等本地落地信息，市场与业界材料虽有观点，但应以官方最终发布核验。仁港永胜保留对本文内容进行更新与修订的权利。
