BaFin 300 条 Q&A（填充版）｜（适用于德国 MiCA-CASP）

德国 MiCA 加密资产服务提供商（CASP）牌照申请注册所需

本文内容由仁港永胜（香港）有限公司拟定，并由唐生提供讲解。

仁港永胜唐生根据历次德国补件，整理出《300 条常见 RFI》：

- 商业模式类（30 条）
- 治理结构类（30 条）
- AML 类（50 条）
- IT 安全类（40 条）
- Safeguarding 类（40 条）
- 风控 + 内部控制类（40 条）
- 交易监测类（20 条）
- 链上 AML 类（20 条）
- 审计/报告类（10 条）
- 市场行为类（10 条）
- 法律分类（CASP 服务范围）20 条

此表格是德国申请必须掌握的知识库。

✅ **点击这里可以下载PDF文件：300 条 RFI 全部 Q&A 填充版**（适合直接提交 BaFin），由仁港永胜唐生根据实战经验填充。

本文件为申请 **德国 MiCA 加密资产服务提供商（CASP）牌照** 的监管补件（RFI）正式回复集。

该文档由：

仁港永胜（香港）有限公司（Rengang Yongsheng）拟定
唐上永（唐生）作为项目主负责人、文档主要撰写人

为了确保符合 *Regulation (EU) 2023/1114 (MiCA)* 及德国本地监管要求（包括：

- **KWG（德国银行法）**
- **GwG（反洗钱法）**
- **BAIT（IT 要求）**
- **ZAG（支付服务监督法）**
- **MaRisk（风险管理最低要求）**

我们对 BaFin 补件要求进行了系统化结构整理，并逐条提供完整回答。

文件目的（Purpose）

本文件旨在为 BaFin 提供：

- 申请人完整的业务与合规架构说明
- 对所有 **300 条补件问题（RFI）** 的正式回答
- 明确展示申请人已符合 **MiCA CASP 授权要求**

Q1. 请详细阐述贵司在德国申请 CASP 牌照的商业模式、核心业务结构及各服务之间的衔接方式。

A1（监管版｜BaFin-ready Answer）

我司拟在德国提供的 CASP 服务，包括 MiCA 附件 I 规定之以下服务类型：
（1）接收与传送加密资产订单；
（2）执行订单；
（3）加密资产交易平台运营；
（4）加密资产托管与钱包管理；
（5）加密资产兑法币与兑加密资产服务。

商业模式核心架构如下：

一、业务拆分结构

- **前端（Front Office）**：负责客户注册、KYC、风险评级、交易下单。
- **中台（Middle Office）**：执行风控、价格撮合、订单路由、链上监控、反洗钱审查。
- **后台（Back Office）**：清算、对账、Safeguarding 客户资产、财务报表、报告提交 BaFin。

二、收入结构（符合 MiCA 对收入透明度要求）

收入来源包含：

1. **交易手续费（Maker/Taker）**
2. **托管费（Custody Fee）**
3. **法币入金/出金费用**
4. **机构 API 使用费**
5. **合规性服务费（与机构客户合作时）**

不包括 MiCA 禁止的收入来源，例如：
— 不涉 Staking-as-a-Service
— 不提供收益承诺
— 不提供保证回报产品

三、风险点与控制点（Risk Mapping）

1. **市场风险**：订单执行透明度 → 由内部撮合引擎记录。
2. **操作风险**：交易系统故障 → 建立冗余节点 + BCP。
3. **AML 风险**：高风险地址 → 链上监控工具自动识别。
4. **技术风险**：私钥泄露 → 多签架构 + HSM。
5. **客户资金风险**：资金隔离 → MiCA Safeguarding 机制。

四、为什么选择德国作为主监管地?

- 德国金融监管制度成熟、可信性高
- 有利于与机构客户合作
- 容易获得欧洲多国大型金融机构信任
- MiCA 在德国执行更严格 → 提升公司监管信誉
- 获批后更便于在全欧 30 国开展业务

综上所述，本司商业模式完全符合 MiCA 之要求，风险可控、机制完备，并具备持续经营能力。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A1（内部解释版｜Internal Explanation）

这是典型的 BaFin 第一类问题：
他们想了解你的业务到底做什么、有没有违法风险、是否具备经营能力。

要点：

- 德国不喜欢"宽泛"、"Web3 化"的叙述
- 喜欢"银行式结构化"表达
- 要强调"无收益承诺，无投机产品"
- 强调风险可控、收入来源合法、无监管灰区
- 强调德国是公司战略中心（不能让监管觉得你只是借德国护照做其他国家业务）

这一回答已经完全满足 BaFin 审查逻辑。

（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

Q2. 请提供贵司在德国市场的目标客户（Target Market）细分及风险等级划分方法。

A2（监管版｜BaFin-ready Answer）

本司的目标客户群体明确区分如下，并已通过风险基础方法论（Risk-Based Approach, RBA）进行分级：

第一类：普通零售客户（Retail Clients）

- 德国本地自然人
- 加密资产交易需求稳定
- 通过完整 KYC（ID+PoA+Liveness）
- 风险等级：低至中风险

第二类：专业投资者（Professional Clients）

- 德国/欧盟 MiFID 认证专业客户
- 机构交易者、资产管理人、家族办公室
- 风险等级：中风险

第三类：合格企业客户（Corporate Clients）

- 以德国 GmbH／欧盟法人身份开户
- 明确资金来源
- 公司架构透明
- 风险等级：中风险

风险等级计算方法（RBA）

采用以下参数：

指标	权重
客户类型	20%
资金来源透明度	20%
地区风险（FATF）	15%
交易行为复杂度	20%
使用链上地址风险评分	25%

最终得分后形成三类：

- **L1：低风险**（<40 分）
- **L2：中风险**（40–70 分）
- **L3：高风险**（>70 分）

高风险客户将进入 EDD（强化尽调）。

不服务的客户类型（Regulatory Exclusion）

- 高风险管辖区（FATF 黑名单）

- 无法提供资金来源证明
- 暗网相关地址
- Mixer/隐私币高度使用用户
- 政治敏感人物（PEPs）无商业合理性者

此分类完全符合 MiCA + AMLD6 要求。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A2（内部解释版）

监管主要想确认：

- 你是否乱做业务、是否敢接受高风险国家用户
- 你的客户分类是否满足 AML 基本要求
- 是否执行风险评估（RBA）
- 是否区分 Retail vs Pro Investor

德国监管不喜欢"所有客户都能用"的平台。
他们想听到的是 "我们会过滤掉高风险用户"。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

Q3. 请详细解释贵司的收入模式，并说明是否存在任何与 MiCA 冲突的高风险收入来源。

A3（监管版）

本司收入结构遵循 MiCA 透明度原则，并不包含任何收益承诺、利息类业务、或 MiCA 禁止的加密资产服务。
收入来源如下：

1. **交易手续费（交易量基础）**
2. **托管费（每月固定费 + 资产比例费）**
3. **法币出入金费用**
4. **企业 API 用户月费**
5. **机构交易接口费用（Market Access Fee）**

以下业务不开展：

- 保证收益类产品
- 借贷/衍生品高杠杆服务
- Staking-as-a-Service
- DeFi LP 收益分成
- 高风险衍生品交易
- 混币器服务
- 高风险流动性挖矿产品

因此收入模型完全符合 MiCA 的"透明、可审计、真实"原则。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A3（内部版）

监管最怕：

- 你靠"收益承诺"赚钱
- 你靠"拉人头/返佣"赚钱
- 你靠"代币价格"赚钱

- 你靠"DeFi 收益"盈利
- 你靠"美国禁止的业务"盈利

所以回答必须强调：

- 收入正规、透明
- 不涉及高风险产品

Q4. 请说明贵司为何选择在德国而非其他欧盟成员国申请 MiCA-CASP 牌照，并提供监管选择的合理性依据。

A4（监管版｜BaFin-ready Answer）

贵司选择德国作为 MiCA-CASP 主监管地的原因如下：

（一）监管透明度及可靠性强

德国 BaFin 监管成熟度高，拥有：

- 清晰的监管框架（MiCA + KWG + WpIG）
- 高度透明的执法标准
- 在欧洲范围内具备最高的监管信任度

这有利于本司未来在欧盟/EEA 的跨境业务。

（二）适合作为机构客户重点市场

德国是欧洲机构投资者最集中的地区之一：

- 银行
- 金融科技公司
- 资产管理公司
- 大型企业客户

本司未来主要目标为合规机构客户，因此德国最符合战略方向。

（三）德国适用于"高合规平台"的定位

德国监管标准高 → 有助于企业建立长期信誉，提升可信度。
本司商业模式更适合以**高合规、高控制、高治理**为核心，因此德国是最匹配的主监管地。

（四）德国 MiCA 实施严格 → 便于未来护照机制（Passporting）

由于德国执行 MiCA 细节更严格，获批后可：

- 更顺利覆盖其他 29 国
- 降低后续补件风险
- 提升集团在欧盟的监管地位

综上，本司选择德国作为 CASP 监管地，符合 MiCA 要求、经营需求与长期战略。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A4（内部版解释）

BaFin 想确认：

- 你不是"随便找一个欧盟国家"
- 你是真的想长久经营
- 你不是想拿牌照到处做高风险业务

- 你不是绕道监管较弱国家进入欧洲市场

因此回答必须：

- 强调"战略选择"
- 强调"机构客户群体"
- 强调"合规文化"
- 强调"德国是长期布局重点"

这类回答会让 BaFin 感觉公司更稳健。

Q5. 请解释贵司的产品/服务是否涉及 MiCA 中"加密资产发行""稳定币""电子代币"等其他监管类别。

A5（监管版）

本司的业务范围明确限定于 MiCA 附件 I 所列之 **CASP 服务类别**，不涉及 MiCA 第三章之发行人监管义务，具体如下：

（一）本司 *不从事* 以下活动：

- **不发行**加密资产（Crypto-asset Issuance）
- **不发行**资产参考代币（ART）
- **不发行**电子货币代币（EMT）
- **不进行**稳定币发行或清算
- 不为发行人提供推广代理
- **不做任何收益承诺类产品**

（二）本司的加密资产为"第三方发行之公开流通代币"

我们仅处理已上市、已发行之代币，不承担发行人责任，不涉 WP、Whitepaper 审批等 MiCA 额外监管模块。

（三）不提供高风险金融服务

- 不提供杠杆
- 不提供借贷
- 不提供衍生品
- 不提供收益型代币

综上，本司完全属于 MiCA 第三编 "CASP 特许经营"范围内，不触发发行人监管、稳定币监管或电子代币发行监管要求。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A5（内部版解释）

监管最怕：

- 项目方"假装 CASP，实际发币"
- 涉及稳定币业务
- 涉及 MiCA 中第二大高风险类别

所以必须：

- 清晰锁定业务
- 表明"不发币、不做任何收益承诺、不涉稳定币、不涉 ART/EMT"

这是保护申请成功率的绝对关键。

Q6. 贵司是否提供 DeFi、Staking、收益类产品或任何具备"回报承诺"的业务?

A6（监管版）

本司不提供任何具备收益承诺或潜在证券属性之产品，包括：

（一）不提供 DeFi 协议接入服务

- 不提供 AMM
- 不提供流动性池（Liquidity Pool）
- 不提供 Farming
- 不提供 Lending
- 不提供 Staking-as-a-Service

（二）不提供收益承诺类产品

包括：

❌ 固定回报
❌ 保证收益
❌ 收益分成
❌ 代币质押回报
❌ 挖矿回报
❌ 复利型产品

（三）所有服务均为"交易 + 托管"范围内活动

完全符合法规要求，不触发 MiCA 第四章可能涉及的"禁止性投资产品"监管标准。

本司所有收益结构均为 "使用费、服务费、手续费" 三大类。

（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A6（内部版解释）

德国监管极度排斥：

- Staking
- DeFi
- Lending
- 任何收益承诺

原因：

这些业务容易触发"金融工具"监管（证券法），会直接导致：

⚠ 申请失败
⚠ 执照转为 WpIG / KWG（难度 10 倍）
⚠ 被认定为非法吸收存款

所以回答越干净越好：

"我们只做交易 + 托管。"

Q7. 请说明贵司计划提供的服务是否包含"算法定价机制"、"流动性提供者"、"演算法撮合"等高风险元素。

A7（监管版）

本司交易系统采用 **集中式订单簿（CLOB）** 模型，并不使用任何高风险的：

- 算法定价机制
- 自动做市（AMM）
- DeFi 算法撮合
- 外部匿名流动性池
- 隐性流动性来源

系统设计如下：

1. **订单簿价格来源**：
   来自多个公开交易所 + 合规机构 LP。
2. **价格机制**：
   以 VWAP/TWAP 模型为价格参考，完全透明。
3. **撮合逻辑**：
   遵循"价格优先 + 时间优先"，固定规则，不依赖黑箱算法。
4. **流动性提供者（LP）要求**：
   全部为受监管机构（欧盟或英国牌照 LP）。

因此业务不含 MiCA 所定义的"高风险市场结构机制"，亦不涉及复杂算法引擎。

（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A7（内部版解释）

监管怕：

- 隐性 AMM
- 黑箱定价
- 抽水或不透明价格机制
- 引发市场操纵风险

要点：

- 强调"集中式撮合"
- 强调"透明定价"
- 强调"无 DeFi 或算法黑箱结构"

Q8. 请解释贵司在德国市场的竞争优势与差异化定位。

A8（监管版）

本司在德国市场的竞争定位如下：

（一）安全性与合规优先

本司采用：

- 多签 + HSM
- 链上 AML 风控
- 全面 Safeguarding 模型
- 完整内部审计 + 年度合规报告

此机制较行业平均水平更高。

（二）机构级市场定位

本司主要目标客户为：

- 机构投资者
- 家族办公室

- 专业交易者

此客户群对合规要求高，可提升平台稳定性。

（三）透明费用架构

- 无隐性收费
- 无收益分成
- 无复杂金融产品

（四）强治理架构

- 具德国本地 RO
- 具备合规委员会
- 定期进行风险审查

因此本司将成为德国市场的"高合规标准平台"。

（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A8（内部版解释）

德国监管喜欢：

- 强调安全
- 强调合规
- 强调透明
- 强调治理
- 强调机构客户为主

不喜欢：

- "我们做 Web3 创新"
- "我们做颠覆性业务"

保持稳健语调是关键。

Q9. 请说明贵司在德国的商业模式是否依赖单一收入来源，并说明如何确保业务持续性。

A9（监管版）

本司收入结构具有多元性，不存在单一来源依赖风险。

收入结构包括：

- 交易手续费（约 40–50%）
- 托管费（约 20–30%）
- 企业服务费（约 10–20%）
- 法币出入金费用（约 5–10%）
- API 使用费（少于 5%）

持续经营能力（Going Concern）

企业设立了：

- 12–18 个月运营资金储备
- 风险资本储备
- 可持续费用模型（工资、系统、审计、合规）

- 连续性计划（BCP/DRP）

以上均符合 MiCA 第 62 条对 CASP 经营可持续性的要求。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A9（内部版解释）

监管最怕：

- "只有交易手续费收入"
- "收入波动会导致平台倒闭"

所以回答要强调：

- 收入来源多元
- 有足够运营资金
- 有财务持续性
- 不依赖市场行情

Q10. 请说明贵司是否采用外包模式，并解释外包服务是否影响商业模式的核心合规性。

A10（监管版）

本司采用外包模式之原则为 **"核心功能不外包（No Outsourcing of Core Functions）"**，即：

以下功能均不外包：

- AML/CTF 审查
- 交易监测
- Safeguarding 客户资金管理
- 风险管理
- 系统关键模块
- 审计
- 合规委员会决策

允许外包的非核心服务：

- 云端服务器（合规地区）
- 客服（非关键 AML 部分）
- 市场营销
- 部分非关键 IT 开发

外包监管控制措施：

1. 供应商尽职调查（Vendor Due Diligence）
2. 外包风险评估矩阵
3. 外包 SLA
4. 年度审查
5. 退出策略（Exit Strategy）
6. 外包登记册（Outsourcing Register）

本司外包模型完全符合 MiCA 第 61 条及 EBA Outsourcing Guidelines。
（本回答由仁港永胜（香港）有限公司编制，并由唐上永（唐生）业务经理提供专业讲解。）

A10（内部版解释）

监管重点：

- 不允许"关键功能外包"
- 不允许"合规外包"
- 必须要有外包治理结构

德国监管对 Outsourcing 极度敏感，因此回答必须谨慎。

Q11. 贵司的商业模式是否依赖单一交易所、单一流动性来源或单一市场环境？请说明去中心化风险如何缓解。

A11（监管版｜BaFin-ready）

本司的商业模式不存在对单一交易所、单一流动性提供者或单一市场的依赖。本司采用多源头、多地域、多机构的分散式业务结构：

（一）流动性来源多元化

- 欧洲受监管 LP（MiFID 投资机构）
- 英国 FCA 受监管 LP
- 美国 FinCEN 注册机构
- 多家国际加密资产流动性提供者

任何单一 LP 下线不会影响整体运营。

（二）交易对接为"多节点模型"

本司技术系统支持：

- 多交易所报价
- 多节点比价
- 自动容灾切换（Failover）
- 集中撮合引擎保证连续报价

（三）市场环境依赖度低

我们收入不依赖代币行情，而来自：

- 交易手续费
- 托管费
- 入金/出金费用
- 企业服务费
- API 使用费

波动行情不会导致业务不可持续。

结论：
本司不存在单点依赖（Single Point of Failure），整体架构符合 MiCA 对风险分散的要求。
（由仁港永胜（香港）有限公司编制，唐上永（唐生）业务经理提供专业讲解。）

A11（内部解释版）

BaFin 要确认：

- 你不会因为"某一交易所停售"而倒闭
- 你不是挂靠某个大交易所的"马甲平台"
- 你有完整的 LP & 报价体系

越强调"多元"，越安全。

Q12. 贵司是否支持与第三方钱包或第三方交易所的外部对接？请说明风险控制措施。

A12（监管版）

本司允许客户将资产：

- 从第三方钱包转入
- 提至客户自有钱包
- 从合规交易所充值
- 转向合规交易所提款

前提是：全部对接均经过 AML 风险评估。

风险控制措施包括：

（一）链上监测（On-chain AML）

所有收付均通过：

- 地址风险评级
- 风险标签（Sanctioned / Mixer / Darknet）
- 资金路径回溯（Fund Flow Tracing）
- 风险打分模型（Scorecard）

（二）合规白名单机制

- 仅允许受监管交易所
- 仅允许客户实名钱包
- 禁止匿名高风险钱包
- 禁止高风险国家地址

（三）提款绑定机制（Withdrawal Binding）

- 客户提款必须绑定实名钱包
- 禁止提至临时地址或一次性钱包
- 提款前自动 AML 评估

本司所有对接均符合 MiCA + AMLD6 要求。
（由仁港永胜唐生提供专业讲解。）

A12（内部解释版）

监管最怕：

- 平台成为"洗币跳板"
- 和高风险钱包互通
- 匿名提款

所以必须强调：

- KYC + 链上 AML + 白名单
- 禁止匿名钱包
- 强制绑定机制

Q13. 贵司的目标客户群体是什么？是否涉及零售客户？

A13（监管版）

本司主要客户群体为 **专业及机构客户**，包括：

- 持牌金融机构
- 家族办公室（Family Office）
- 专业投资者
- 企业级客户（B2B）
- 专业交易者（符合 MiCA "Professional Client" 定义）

不以零售客户为主要市场。
若未来提供零售服务，将严格遵守：

- MiCA 投资者保护要求
- 风险标签
- 适当性评估（Suitability Assessment）
- 拟议服务测试（Appropriateness Test）

目前，本司的服务定位以机构为中心，符合 MiCA 第 55、56 条关于机构客户风险管理的要求。
（由仁港永胜唐生提供专业讲解。）

A13（内部解释版）

BaFin 对"零售客户"非常敏感。

如果说你以"散户为主"，
→ 难度会直接 ×3。

说"机构为主、零售不是主要市场"，
→ 审批速度更快。

Q14. 贵司是否提供加密资产与法币之间的兑换服务（on/off-ramp）？如有，请说明监管配套。

A14（监管版）

是，本司提供：

- Crypto → Fiat
- Fiat → Crypto

的受监管兑付服务（On/Off-Ramp）。

配套监管措施：

（一）支付伙伴全部为受监管机构

- 欧盟支付机构（PI/EMI）
- 英国 FCA EMI
- 美国持牌 MSP/Money Transmitter

（二）外汇结算透明

- 所有汇率可追溯
- 无"隐藏汇差"
- 由合作银行或支付机构提供结算

（三）全流程 AML 控制

- 入金前 KYC
- 入金后资金来源调查
- 全链路交易监测
- SAR/STR 上报机制

（四）客户资金全额隔离（Safeguarding）

法币资金存于受监管银行的隔离账户。
服务完全符合 MiCA 的"加密资产与法币交换服务"定义。
（由仁港永胜唐生提供专业讲解。）

A14（内部版解释版）

此题敏感，因为：

- 法币通道容易涉及银行审查
- 资金来源必须非常干净

回答要稳健：

- 强调受监管支付伙伴
- 强调 AML 强度
- 强调 Safeguarding

Q15. 贵司是否在商业模式中涉及"代币上架"（Listing）服务？请说明上架机制与审查流程。

A15（监管版）

是，本司提供代币上架（Token Listing）服务，但仅限：

- 公链主流代币
- 市场交易额稳定的代币
- 符合 MiCA 分类
- 已在主要合规交易平台上架
- 不涉及发行人代理职责

上架流程包括：

（一）合规审查

- MiCA 分类（Utility、ART、EMT、其他 Crypto-asset）
- 法律意见
- KYC/KYB
- 发行团队背景审查
- 风险评级（高、中、低）

（二）技术审查

- 智能合约安全
- 代码审计报告
- 链上风险报告

（三）市场风险审查

- 流动性状况
- 代币分配结构
- 市场操控风险

（四）Listing 委员会决策

- 多成员合规委员会
- 有记录、有投票、有档案

流程完全符合 MiCA 投资者保护及市场操控条款。
（由仁港永胜唐生提供专业讲解。）

A15（内部解释版）

BaFin 要确保你不是：

- "随便上币平台"
- "黑链项目入口"
- "洗黑钱代币入口"

必须展示：

- 严格筛选
- 委员会制度
- 合规审查
- 全套文件

Q16. 贵司是否允许匿名交易或未完成 KYC 的用户进行任何操作?

A16（监管版）

不允许。本司严格执行：

（一）交易前强制 KYC（Mandatory KYC-before-Trade）

- 未 KYC → 不允许入金
- 未 KYC → 不允许交易
- 未 KYC → 不允许出金
- 未 KYC → 不允许使用任何功能

（二）受限模式（Restricted Mode）

未完成 KYC 的客户仅能：

- 浏览界面
- 查看通用市场信息

不能参与任何涉及资产的活动。

（三）符合 AMLD6 + MiCA 第 63 条要求

所有客户均通过：

- 身份验证
- 地址验证
- 资金来源调查（必要时）
- 黑名单、制裁、PEP 检查

完全符合欧洲严格的 AML 要求。

（由仁港永胜唐生提供专业讲解。）

A16（内部解释版）

BaFin 最讨厌：

- 先让用户交易，后续才补 KYC
- KYC 不严格
- 可匿名充值

所以回答必须极端明确：
❗"未 KYC，一律禁止操作。"
这是提高成功率的关键。

Q17. 贵司是否支持跨境客户？是否对不同国家实行风险分类？

A17（监管版）

是，本司接受跨境客户（Cross-border Clients），但严格按国家风险分类管理。

（一）不接受高风险国家（High-risk Third Countries）

禁止地区包括：

- FATF 高风险国家
- 欧盟制裁国家
- 高腐败风险国家
- 战争冲突国家
- 洗钱高风险地区

名单随 FATF/EU 更新。

（二）中风险国家（Enhanced Due Diligence）

实施：

- 强化尽调（EDD）
- 资金来源调查
- 交易监控增强

（三）低风险国家（Standard Due Diligence）

执行：

- 标准 KYC
- 标准风险监测

本司跨境策略完全符合 MiCA + AMLD6 国家风险分类。
（由仁港永胜唐生提供专业讲解。）

A17（内部解释版）

关键是：

- 必须禁止高风险国家
- 必须展示"分级管理模型"
- 必须和 FATF 对齐

监管看到这一点会更放心。

Q18. 贵司的交易模式是否包含杠杆、保证金、合约或衍生品?

A18（监管版）

不包含。本司的商业模式完全不涉及：

- 杠杆交易
- 保证金交易
- 永续合约
- 期货
- 任何衍生品
- 任何可能落入 MiFID II/WpHG 的金融工具

本司仅提供：

- 现货（Spot）加密资产交易
- 资产托管
- 资金兑换
- 机构级结算
- API 服务

避免触发"金融工具（Financial Instrument）"监管，是本司的重要设计原则。
（由仁港永胜唐生提供专业讲解。）

A18（内部解释版）

BaFin 对衍生品监管非常严格。
只要涉及：

- 杠杆
- 合约
- 期货

→ 审批难度 ×10。
因此回答必须坚决：
❗"只做现货，不碰衍生品。"

Q19. 贵司是否允许用户之间进行点对点（P2P）交易?

A19（监管版）

不允许。本司平台完全不支持：

- P2P 自由交易
- 用户间私下转账
- 匿名撮合
- 外部钱包互转（非白名单）

原因：

P2P 会：

- 削弱 AML 监控
- 难以保障投资者保护
- 容易成为洗钱入口

- 不符合 MiCA 风控原则

平台仅允许：

- 用户与平台之间交易（平台作为中介）
- 委托撮合订单簿交易
- 受监管的资金清算流程

本司的交易模式完全符合 MiCA 对市场透明度及 AML 要求。
（由仁港永胜唐生提供专业讲解。）

A19（内部解释版）

BaFin 对 P2P 十分排斥，因为：

- 难监控
- 易洗钱
- 有监管套利嫌疑

所以要完全禁止。

Q20. 贵司是否提供"子账户""共享账户"或"代理交易服务"？如有，请说明控制措施。

A20（监管版）

本司不提供任何"共享账户""子账户"或"匿名代理交易"服务。

唯一允许的情况：企业账户（Corporate Account）

企业账户使用限制如下：

- 必须由公司法定代表人（或授权人）操作
- 需提供授权书（PoA）
- 所有操作均记录在案
- 资金来源需符合 AML 要求
- 不允许"多人共享密码"

本司严格禁止：

- 代理人替客户进行交易
- 无授权的"代客操作"
- 多人共享私人账户
- 私下转移资产

所有账户仅限实名客户本人操作。
（由仁港永胜唐生提供专业讲解。）

A20（内部解释版）

监管最怕：

- "代理炒币"
- "子账户用于洗钱"
- "共享密码"

因此必须强调：

- 只允许"公司账户 + 授权书"
- 严禁共享账户
- 严禁代理交易

Q21. 请说明贵司的收入模式是否存在"操纵价格""扩大点差""隐藏费用"等潜在利益冲突情形。

A21（监管版｜BaFin-ready）

本司收入模式透明、明确，不存在任何形式的价格操控或隐性收费。所有费用均在用户协议、收费表（Fee Schedule）及产品说明文件中公开披露。

本司收入来源如下：

（一）交易手续费（Trading Fee）

- 固定费率
- 已公开披露
- 不随市场波动任意调整
- 不针对特定代币设定差别费率

（二）托管费（Custody Fee）

- 基于托管余额的固定费率
- 无隐藏费用

（三）兑换费用（Conversion Fee）

- 透明报价
- LP 价格直接传递
- 无"暗点差补偿机制"

（四）技术与 API 服务费用

- 按月订阅
- 固定计费逻辑

利益冲突控制：

- 平台不参与自营交易
- 不与 LP 有利润共享
- 报价透明
- 交易记录可审计

上述机制确保本公司不存在任何形式的利益冲突。
（由仁港永胜唐生提供专业讲解。）

A21（内部解释版）

BaFin 很怕：

- "暗点差"
- "扩大 Spread"
- "隐藏费用"
- "操控价格"

因此必须强调：

- 收入来源固定、透明
- 不操控价格
- 不参加自营
- 不从 LP 回扣

越透明越安全。

Q22. 贵司是否运营自营交易（Proprietary Trading）？如否，请说明如何确保平台与客户利益不冲突。

A22（监管版）

本司 **完全不进行自营交易**。
为确保平台与客户之间无任何利益冲突，制定以下制度：

（一）平台与客户之间无对赌机制

- 无对赌
- 无做市角色
- 无内部撮合对手盘
- 所有交易通过订单簿撮合

（二）内部禁止代币交易政策

- 公司本身禁止持有交易型加密资产
- 员工禁止使用本平台进行交易
- 所有员工账户受监控

（三）公司收入不依赖价格波动

我们不依赖：

- 代币涨跌
- 流动性激励
- 交易对冲收益

（四）合规团队每月审查记录

确保没有任何利益冲突行为。
（由仁港永胜唐生提供专业讲解。）

A22（内部解释版）

BaFin 监管逻辑：

如果你"做市"或"自营"
→ 会产生利益冲突
→ 被认为是"有动机操控市场"

所以：

- 必须声明"绝不自营"
- 强调没有对赌机制

这是通关关键。

Q23. 贵司是否提供任何形式的"收益""理财产品""利息"或"锁仓奖励"?

A23（监管版）

本司不提供任何形式的：

- 收益产品
- 锁仓奖励
- 年化收益
- 质押利息
- DeFi 量化收益
- CEX 理财产品（Earn、Saving、Staking 等）

理由：

根据 MiCA + BaFin 指引，此类产品可能构成：

- Collective Investment Scheme（集体投资工具）
- CRR 信贷或存款业务
- MiFID II 金融工具
- 证券型代币募集
- 变相吸收公众存款

为避免触发上述监管，本司商业模式中完全不包含任何收益性产品。
（由仁港永胜唐生提供专业讲解。）

A23（内部解释版）

BaFin 会特别盯"收益产品"：

- Binance Earn
- OKX Earn
- 火币质押
- DeFi Staking

只要涉及收益，监管难度 = 无限大。
所以上策是：
❗"完全不做收益类产品"
并把原因讲得非常清楚。

Q24. 贵司是否涉及代币发行（ICO/IEO）或与发行方存在经济利益关系?

A24（监管版）

本司不参与任何形式的：

- ICO
- IEO
- 代币销售
- 发行代理
- 私募配售
- 做市奖励

- Token Allocation

与发行方无经济利益关系

- 不接受代币作为合作报酬
- 不参与项目方股权
- 不提供发行承销服务
- 不提供筹资类服务

唯一允许的合作方式

- 技术对接
- API 集成
- 法律合规咨询（非营销性质）

且所有合作均披露于利益冲突政策中。
（由仁港永胜唐生提供专业讲解。）

A24（内部解释版）

监管很怕：

- 平台帮项目方"上币集资"
- 与项目方共享收益
- 与项目方暗中合作

这些都可能被视为证券发行。
最安全做法：
→ "完全不参与任何代币发行行为"

Q25. 贵司是否向第三方提供"白标交易平台（White Label）"服务？如有，请说明如何管理风险敞口。

A25（监管版）

本司确实提供 White Label 服务，但严格限定于：

- 受监管的金融机构
- 需要合规技术的企业客户
- 仅提供技术框架（Tech Stack）
- 不参与运营、不参与交易

风险控制如下：

（一）White Label 客户必须通过 KYB

- 许可证核查
- 实际控制人核查
- AML 风险分析

（二）本司不持有其客户资产

- 客户资产受其自身监管机构监管
- 本司不接触客户资金

（三）White Label 明确划分职责

- 本司：技术
- 客户：运营、AML、KYC、风控
- 双方有 SLA 文件

此服务不影响本司的 CASP 核心业务。
（由仁港永胜唐生提供专业讲解。）

A25（内部解释版）

White Label 是敏感服务。
关键是强调：

- 你只提供技术
- 你不触碰他们的客户资产
- 风控由对方负责

这样 BaFin 才能接受。

Q26. 贵司是否提供跨链、跨资产或跨平台的聚合服务（Aggregator）？

A26（监管版）

否。本司没有提供任何跨链、跨平台的聚合服务，例如：

- DeFi 价格聚合
- DEX/AMM 聚合
- 跨链桥（Bridge）
- 多链互通协议

理由：

此类业务涉及：

- 技术攻击面扩大
- 资产跨链跳转 AML 风险极高
- 难以确认资金流向
- 涉及智能合约风险
- 监管不认可

为确保 MiCA 风险可控，我们不提供聚合类服务。
（由仁港永胜唐生提供专业讲解。）

A26（内部解释版）

一句话：
"聚合类 = 风险放大器"
BaFin 对跨链最排斥，因为没有办法做 AML。
回答必须坚决拒绝。

Q27. 贵司是否允许客户使用第三方 API 或程序化交易？如允许，请说明如何控制风险。

A27（监管版）

本司允许机构客户使用：

- REST API
- Websocket API
- FIX API

主要用于：

- 批量下单
- 算法交易
- 机构资产管理
- 做市服务（非自营）

风险控制措施如下：

（一）API Key 权限分级

- 读取权
- 下单权
- 转账权（默认关闭）

（二）频率限制（Rate Limit）

- 防止 DDoS
- 防止滥用
- 保护平台稳定性

（三）IP 白名单

客户可绑定 API 专用 IP。

（四）实时行为监控

- 异常交易检测
- 爆量下单检测
- 价格操纵监测

本司 API 使用流程符合 MiCA 对市场操控风险的要求。
（由仁港永胜唐生提供专业讲解。）

A27（内部解释版）

监管担心：

- API 高频操纵
- API 洗钱
- API 超频攻击

重点表达：

- 只给机构
- 权限分级
- 风控监测

这样即可。

Q28. 贵司是否允许客户使用机器人、量化模型或自动策略进行交易？

A28（监管版）

本司允许 **合规前提下的** 自动化策略交易，限于：

- 专业投资者
- 机构客户
- 算法交易公司

限制如下：

（一）禁止操纵市场

禁止：

- 拉高出货
- 刷量
- 虚假报价
- Market Spoofing
- Wash Trading

（二）算法需备案

- 算法类型
- 使用目的
- 风控机制

（三）可被系统自动限制

- 异常行为自动熔断
- 违规行为直接封禁

本司的算法交易政策符合 MiCA 第 76 条的市场行为要求。
（由仁港永胜唐生提供专业讲解。）

A28（内部解释版）

监管对 Algo Trading 担忧：

- 刷量
- Manipulation

所以要强调：

- 仅限机构
- 风控必须强
- 有自动熔断机制

Q29. 贵司是否向企业客户提供“托管 + 交易”一体化服务？请说明如何避免利益冲突。

A29（监管版）

本司确实为企业客户提供：

- 托管服务（Custody）
- 交易服务（Trading）

但通过严格结构分离来降低利益冲突。

（一）托管与交易完全分部门运行

- Custody 部门
- Trading 部门
- 运营分离
- 权限分离
- 数据隔离

（二）托管资产不参与交易流动性

- 托管资产不用于借贷
- 不用于做市
- 不用于任何用途
- 完全隔离保存

（三）通过内部控制政策降低冲突

- 利益冲突政策
- 职责划分制度
- 独立监督责任人

此结构符合 MiCA 对 Custody 服务的风险隔离要求。
（由仁港永胜唐生提供专业讲解。）

A29（内部解释版）

BaFin 很看重：

- 托管和交易是否"混在一起"
- 是否会挪用资产

必须强调：

- 部门分离
- 资产不挪用
- 全隔离

Q30. 贵司是否涉及 OTC 大宗交易（Block Trade）？如有，请说明风控流程。

A30（监管版）

是，本司提供 OTC Block Trade 服务，主要面向：

- 机构客户
- 高净值客户
- 资产管理机构

风控流程如下：

（一）强制 KYB/KYC

对企业及其最终受益人进行全套尽调。

（二）资金来源审查（SOF/SOW）

- 法币入金：银行回单 + 资金证明

- 加密资产：链上路径分析

（三）价格机制透明

- 采用 LP 全透明报价
- 无暗点差
- 无对赌

（四）反市场操控机制

- 大单拆单机制
- 稳定执行价格

（五）记录保存

所有 OTC 大宗交易保存 10 年。
服务符合 MiCA 第 68 条关于大宗交易透明度要求。
（由仁港永胜唐生提供专业讲解。）

A30（内部解释版）

OTC 是"高风险业务"，监管关注点：

- 价格透明度
- 资金来源
- 反洗钱
- 是否有对赌

越严谨越好。

Q31. 请提供贵司完整的治理架构（Governance Structure），包括董事会组成、管理层职责与监督机制。

A31（监管版｜BaFin-ready）

本司治理结构符合 MiCA、BaFin、《公司治理指引（BaFin MaRisk）》要求，由三层结构组成：

（一）董事会（Board of Directors）

- **董事会成员数量：3–5 名**
- **独立董事比例：≥1 名**
- 负责任务：
  - 制定公司战略
  - 审批政策、预算、风险框架
  - 任命高级管理人员
  - 监督管理层履职情况
  - 审查年度合规与风险报告

董事会每季度召开一次会议，并保留完整会议记录（Minutes）。

（二）高级管理层（Senior Management）

包括以下核心岗位：

1. CEO（首席执行官）

- 负责战略执行与日常运营
- 对董事会负责

2. COO（首席运营官）

- 负责运营框架、SOP、服务交付

3. CFO（首席财务官）

- 负责财务管理、Safeguarding、账目监督

4. CTO（首席技术官）

- 负责系统安全、DORA 合规、网络安全

5. CCO（首席合规官）

- 负责 MiCA、BaFin、AMLD6、GDPR 合规
- 每季度提交合规报告

6. MLRO（反洗钱报告官）

- 独立于业务部门
- STR/SAR 报告
- AML 政策执行监督

（三）三道防线（Three Lines of Defense）

第一道防线：业务部门

- 负责日常操作与风险识别

第二道防线：合规 + 风控

- 独立风险团队
- 监控市场风险、运营风险、AML 风险

第三道防线：内部审计（Internal Audit）

- 每年 1 次独立审计
- 向董事会直接汇报

结论：

治理架构透明、职责分明、监督链条完整，符合 BaFin 对 MiCA CASP 的治理强度要求。
（由仁港永胜唐生亲自整理与撰写。）

A31（内部解释版）

这一题必须展现：

- 三道防线
- 董事会与管理层分工
- 合规独立性
- 监督链条

BaFin 对"治理结构不清晰"的机构一律驳回。

Q32. 请解释董事会成员是否具备充分的胜任能力（Fit & Proper），并说明其资质及经验。

A32（监管版）

本司所有董事均符合 BaFin 的“Fit & Proper”要求（§ 25c KWG、MiCA 第 63 条）。

（一）资质要求

所有董事均至少具备：

- 金融、法律、会计或风险管理专业背景
- 5–10 年金融行业经验
- 熟悉欧盟监管框架
- 无任何金融犯罪记录

（二）背景审查（Background Check）

已完成：

- 犯罪记录证明
- 破产记录查询
- 监管处罚记录查询
- 信用记录检查
- PEP 检查

（三）董事履职能力体现：

- 具备审阅审计报告能力
- 理解 IT 风控架构
- 理解 AMLD6 要求
- 能监督预算、战略实施
- 参与年度治理审查

所有记录已整理成《Fit & Proper 文件包（Board Edition）》用于监管提交。
（由仁港永胜唐生提供专业讲解。）

A32（内部解释版）

考核点：

- 董事 ≠ 挂名
- 必须展示真实履职能力
- 必须展示无瑕疵记录

BaFin 很重视“能否真正监督”。

Q33. 请说明 MLRO（反洗钱报告官）的独立性与职责范围。

A33（监管版）

（一）MLRO 完全独立于业务部门

- 不参与销售
- 不参与市场活动
- 不参与运营决策

- 直接向董事会负责（而非管理层）

（二）MLRO 核心职责：

1. STR/SAR（可疑交易报告）
2. AML 政策制定与执行监督
3. 交易监测框架维护
4. 链上 AML 分析
5. 高风险客户审批
6. 员工 AML 培训
7. 每季度提交 AML 报告

（三）MLRO 背景要求：

- 至少 5 年 AML 经验
- 持有 AML 相关证书（如 CAMS）
- 熟悉链上 AML 工具（Chainalysis、Elliptic）

（由仁港永胜唐生提供专业讲解。）

A33（内部解释版）

强制表达：

- MLRO 独立
- MLRO 权限高
- MLRO 对董事会负责

这是 AML 体系的关键。

Q34. 请解释贵司是否设立独立的风险管理职能（Risk Management Function）。

A34（监管版）

是，本司设立 **独立的风险管理部门**（Risk Management Function），并符合 MaRisk 与 MiCA 要求。

职责包括：

- 市场风险监测
- 操作风险监测
- 交易异常监测
- 价格风险控制
- 流动性风险管理
- IT 风险评估（DORA）
- 压力测试（Stress Test）
- 供应商风险管理（Vendor Risk）

运营方式：

- 独立于业务、合规部门
- 每月向管理层汇报
- 每季度向董事会汇报
- 具备独立调查与阻断权限

本部门由具备金融风险管理经验 10 年以上人员负责。

（由仁港永胜唐生提供专业讲解。）

A34（内部解释版）

核心逻辑：

- 风险部门必须独立
- 有阻断权
- 有直达董事会权

否则 BaFin 会说"治理结构不充分"。

Q35. 请说明内部审计（Internal Audit）功能是否独立，其报告线为何？

A35（监管版）

本司内部审计为 **完全独立的职能**，符合 MiCA 治理要求与 BaFin MaRisk 要求。

（一）独立性体现：

- 不参与业务
- 不受管理层控制
- 不与风险或合规共享人员
- 拥有独立预算

（二）报告线：

- 内部审计直接向董事会审计委员会报告
- 不向 CEO 或 COO 汇报
- 涉及重大发现时可直接向全体董事报告

（三）工作范围：

- 年度内部审计计划
- 执行 AML 程序检查
- 审查 Safeguarding
- 审查 IT 安全
- 审查风险管理
- AAF 01/20 审计配合
- 年度合规度检查

（四）审计频率：

至少每年 1 次全范围审计。

（由仁港永胜唐生提供专业讲解。）

A35（内部解释版）

监管要的重点是：

- 内审不受管理层支配
- 直接向董事会汇报

这是"公司治理成熟度"的关键指标。

Q36. 请说明贵司是否设立利益冲突管理政策（Conflict of Interest Policy）。

A36（监管版）

是，本司制定并实施严格的 **利益冲突管理政策**，涵盖以下内容：

（一）潜在冲突识别：

- 平台 vs 客户
- 员工 vs 公司
- 自营 vs 客户
- 上币委员会 vs 项目方
- LP vs 平台
- 白标客户 vs 主平台

（二）管理措施：

- 禁止员工内部交易
- 交易数据隔离
- 独立定价模块
- 上币流程需委员会投票
- 禁止接受项目方代币奖励

（三）披露机制：

任何潜在冲突将：

- 报告 CCO
- 记录在利益冲突登记册（Conflict Register）
- 必要时披露给客户

政策执行由合规部门监督。

（由仁港永胜唐生提供专业讲解。）

A36（内部解释版）

利益冲突 = BaFin 最敏感领域之一。

一定要强调：

- 员工不得交易
- 公司不得自营
- 不能与项目方利益绑定

越严越好。

Q37. 请说明贵司是否设立独立的上币委员会（Token Listing Committee）。

A37（监管版）

是，本司设立独立的 **Token Listing Committee（TLC）**，完全符合 MiCA 投资者保护要求。

（一）委员会组成：

- 法律顾问
- 合规官（CCO）
- 技术主管（CTO）
- 风控主管
- 市场情报分析员

（二）职责：

- 审查代币法律分类
- 审查项目资料真实性
- 评估市场操控风险
- 审查智能合约安全报告
- 进行 AML 发行主体尽调
- 投票是否批准上币

（三）流程：

1. 风险预审
2. 项目方资料提交
3. 法律与合规审查
4. 技术安全审查
5. 在 TLC 会议上投票
6. 记录决议与理由

所有会议均记录在案。

（由仁港永胜唐生提供专业讲解。）

A37（内部解释版）

上币委员会是必须要有的结构，因为：

- 可以证明平台不会"乱上币"
- 表明有治理程序
- 有透明决策过程

BaFin 很认可这种结构。

Q38. 请说明贵司是否设立政策管理框架（Policy Framework）并保持定期审查。

A38（监管版）

是，本司建立全面的政策管理框架，包括：

（一）核心政策文件（至少 30+ 项）

如：

- AML/KYC 政策
- 风险管理政策
- IT 安全政策
- 数据保护政策
- Safeguarding 政策
- Incident Response
- Business Continuity

- Conflict of Interest
- Outsourcing Policy
- Token Listing Policy

全部与 MiCA、DORA、GDPR 和 BaFin 指引对齐。

（二）年度审查机制

所有政策每年进行：

- 更新
- 董事会批准
- 合规部门记录

（三）政策版本管理

采用版本号（Version Control），并保留历史记录。
（由仁港永胜唐生提供专业讲解。）

A38（内部解释版）

政策管理是最容易出问题的环节。
必须强调：

- 文件多
- 每年更新
- 董事会批准

这是监管想看到的成熟度。

Q39. 请说明贵司是否存在管理层重叠、角色冲突或人员权责不清的问题。

A39（监管版）

无。本司采用严格的职权分离制度（Segregation of Duties），所有管理层职责明确：

CEO

- 战略与整体管理
- 不参与技术、不参与合规

COO

- 日常运营
- 不参与AML决策

CFO

- 财务、Safeguarding
- 不参与交易

CTO

- 技术安全
- 不参与业务决策

CCO

- 合规

- 不受业务干预

MLRO

- AML
- 不受管理层干预
- 对董事会负责

所有职责以 RACI Matrix 形式记录。
（由仁港永胜唐生提供专业讲解。）

A39（内部解释版）

监管要确认：

- 人员不冲突
- 不一人多岗
- 不会因为角色混乱导致风险

必须强调"分工明确"。

Q40. 请说明贵司是否对董事、高管及核心员工进行持续合规培训。

A40（监管版）

是，本司实施年度与季度的合规培训体系：

（一）培训对象：

- 董事
- 高级管理层
- AML 团队
- 风控团队
- 客服及运营团队
- 技术团队

（二）培训内容包括：

- MiCA 最新规则更新
- AMLD6
- 链上 AML
- DORA 网络安全法规
- GDPR 数据保护
- 市场操控风险
- 客户适当性
- 交易监测框架

（三）培训记录：

- 保留 10 年
- 包含出勤、内容、测验结果
- 由合规部门归档

本体系符合 BaFin 对"持续性合规文化"的要求。
（由仁港永胜唐生提供专业讲解。）

A40（内部解释版）

BaFin 非常看重"培训文化"，因为：

- 证明管理层重视合规
- 能证明内部不是"挂名部门"
- 能展示组织成熟度

培训越多越好。

Q41. 贵司董事会是否定期审查风险管理框架，并如何记录审查结论？

A41（监管版｜BaFin-ready）

是，本司董事会每季度审查一次《风险管理框架（Risk Management Framework）》，并在以下会议文件中留存可审计记录：

（一）会议形式

- 每季度举行正式董事会会议
- 线下 / 视频会议均有记录
- 会议召集程序符合公司章程

（二）董事会审查内容

1. 市场风险报告
2. 操作风险报告
3. 流动性风险报告
4. AML 风险趋势
5. 新兴风险（如链上攻击、Bridge 风险）
6. 关键供应商风险（DORA 要求）
7. 上季度风险事件及整改

（三）记录方式

- 董事会会议纪要（Board Minutes）
- 风险委员会附议意见（如适用）
- 决议文件（Board Resolution）
- 行动清单（Action Points）

所有文件均保留 10 年。
（由仁港永胜唐生提供专业讲解。）

A41（内部解释版）

监管想确认：

- 董事会不是橡皮图章
- 风险管理是"真正被审查"
- 所有行动都有记录

务必强调"每季度审查 + 有记录"。

Q42. 贵司是否有独立于 CEO 的合规负责人（CCO），其汇报线如何体现独立性？

A42（监管版）

是，本司设立独立合规负责人（Chief Compliance Officer，CCO），其独立性体现在：

（一）汇报线

- CCO **直接向董事会合规委员会**汇报
- 不向 CEO 或 COO 汇报
- CCO 的 KPI 不与业务指标挂钩

（二）职责

- 监管沟通（BaFin）
- 政策制定与更新
- 合规审查（包括 Token Listing 审查）
- 年度合规报告
- 负责内部监测和合规文化建设

（三）职业保护（Regulatory Safeguard）

- 董事会批准聘任与解聘
- 合规预算由董事会控制
- 保证 CCO 可独立履行职责

本架构完全符合法规要求（MiCA 第 62 条、BaFin MaRisk）。
（由仁港永胜唐生提供专业讲解。）

A42（内部解释版）

BaFin 最怕"CCO是客服主管兼的"。
必须强调：

- CCO 不受 CEO 控制
- 不受业务指标绑架
- 汇报线到董事会

这是合规体系的灵魂。

Q43. 贵司董事会是否定期接收 AML 报告？报告包含哪些内容？

A43（监管版）

是，本司董事会每季度接收一份《董事会反洗钱报告（Quarterly AML Report to Board）》。

报告内容包括：

（一）KYC/KYB 数据

- 新增客户数
- 高风险客户数
- 触发 EDD（强化尽调）情况

（二）链上 AML 分析

- 高风险地址识别数
- 危险标签（Sanction/Mixer/Darknet）
- 资金流向监测报告

（三）可疑交易报告（STR/SAR）

- 本季度 STR 数
- 触发原因
- 调查时间
- 是否上报 FIU

（四）案例分析（Case Studies）

- AML 风险案例
- 风险场景模拟
- 改进措施

（五）系统与技术更新

- Chainalysis/Elliptic 风险参数更新
- AML 引擎新功能

报告经董事会全体成员阅签。

（由仁港永胜唐生提供专业讲解。）

A43（内部解释版）

关键点：

- 必须有"季度 AML 报告"
- 内容越详细越好
- 监管特别关注"链上 AML 指标"

这是加密业务与传统金融的最大不同。

Q44. 贵司是否设立风险委员会（Risk Committee），其职能为何?

A44（监管版）

是，本司设立独立的 **风险委员会（Risk Committee）**，由董事会成员组成。

（一）组成

- 独立董事（Chair）
- CEO
- CFO
- 风控主管
- CCO（观察员）

（二）职能

1. 确定风险偏好（Risk Appetite）
2. 监督风险管理框架
3. 审查季度风险报告
4. 批准重大风险项目（如新产品引入）
5. 监督 stress test 结果
6. 监督第三方供应商风险

（三）会议频率：

每季度召开一次。

（由仁港永胜唐生提供专业讲解。）

A44（内部解释版）

风险委员会不是必须项，但有助于：

- 提升治理评级
- 强化董事会形象
- 展现成熟的风险文化

监管会极大加分。

Q45. 请说明贵司是否为重大岗位（如MLRO、CCO、CTO）制定接班计划（Succession Plan）。

A45（监管版）

是，本司已为关键岗位制定《关键岗位接班计划（Succession Planning For Key Functions）》，符合 BaFin 要求。

（一）适用岗位：

- MLRO
- Deputy MLRO
- CCO
- CTO
- 风控主管
- 内审主管

（二）接班内容包括：

1. 候选人条件要求
2. 候选人资格文件
3. 必要培训计划
4. 潜在冲突评估
5. 过渡安排流程
6. 在岗期间 shadow 机制

（三）目的：

- 防止关键岗位空缺
- 防止 AML 和 IT 出现监管断层
- 保证 MiCA 许可条件持续符合

所有流程均可审计。

（由仁港永胜唐生提供专业讲解。）

A45（内部解释版）

监管害怕：

- AML 官离职无人替补
- CTO 离职系统瘫痪

所以必须有接班人机制。

Q46. 贵司是否设立文件留存制度（Record Keeping），保存期限为何?

A46（监管版）

是，本司设立全面的文件留存政策，符合 MiCA、GDPR、AMLD6 与 BaFin 要求。

（一）保存期限：

- 客户 KYC/KYB 文件：**10 年**
- 交易记录：**10 年**
- AML 档案：**10 年**
- 董事会文件：**10 年**
- 系统日志：**5-10 年**（依据数据类型）
- 外包供应商文件：**10 年**

（二）保存方式：

- 加密存储
- 多副本
- 权限分级
- 不可更改（immutable log）
- 有访问审计（audit trail）

符合 GDPR 数据最小化原则。
（由仁港永胜唐生专业整理。）

A46（内部解释版）

保存期限必须 ≥5 年，最好 ≥10 年。
因为：

- AMLD6 要求高
- 加密业务风险高

监管非常喜欢"严格留档"。

Q47. 贵司是否有年度治理审查（Annual Governance Review）？请说明审查内容。

A47（监管版）

是，本司每年进行一次《年度治理审查（Annual Governance Review）》。

（一）审查内容：

1. 董事会结构
2. 高管胜任能力（Fit & Proper）
3. 三道防线独立性
4. 合规运作情况
5. 风险管理有效性
6. 关键风险指标（KRI）
7. 上一年度治理整改情况
8. 内部审计发现
9. 外包管理（DORA）
10. Token Listing 治理流程

（二）审查参与方：

- 董事会
- 内部审计
- 风控
- 合规

（三）输出文件：

- Annual Governance Review
- 改进建议报告
- 行动计划（Action Plan）

符合 EU Corporate Governance 指南。

（由仁港永胜唐生提供专业讲解。）

A47（内部解释版）

重点：

- 必须每年做
- 必须有报告
- 必须包括治理、合规、风险

这可以体现公司"成熟度"。

Q48. 贵司是否制定 Outsourcing Policy（外包政策），并符合 BaFin 外包指引？

A48（监管版）

是，本司制定《外包管理政策（Outsourcing Policy）》并完全符合：

- BaFin Circular 10/2017
- EBA Outsourcing Guidelines
- DORA（ICT 第三方风险）

（一）适用范围

包括但不限于：

- 云服务（AWS、GCP）
- KYC 提供商
- AML 工具
- 数据存储
- 技术供应商
- 清算伙伴
- 外包客服

（二）核心原则

- 供应商风险分类
- 尽调（Vendor Due Diligence）
- 合同条款
- 退出机制（Exit Plan）
- 服务连续性要求（BCP）
- 数据处理协议（GDPR）

（三）监督机制

- 季度 KPI 评估
- SLA 绩效监控
- 年度外包审计

（由仁港永胜唐生提供专业讲解。）

A48（内部解释版）

监管怕：

- 把关键业务外包
- 风险不可控
- 云服务不符合 DORA

所以必须：

- 风险分级
- 尽调
- SLA
- 年度审计

Q49. 贵司是否建立明确的职责划分矩阵（RACI Matrix）？请说明其内容。

A49（监管版）

是，本司建立并实施 **RACI 职责划分矩阵**，覆盖所有关键流程。

（一）RACI 定义：

- **R（Responsible）负责执行**
- **A（Accountable）最终负责**
- **C（Consulted）需咨询**
- **I（Informed）需知会**

（二）适用流程包括：

- 上币流程
- 开户流程
- 风险事件响应
- 安全事件处理
- AML 客户审查
- 升级审批
- 产品上线
- 外包供应商管理
- 政策更新流程

（三）文件管理

- 每年更新
- 董事会批准
- 内审检查

可审计、透明、分工清晰。

（由仁港永胜唐生提供专业讲解。）

A49（内部解释版）

RACI = 治理结构最重要证明材料。
显示：

- 不是"人人都管 / 人人不管"
- 职责清晰

监管非常看重。

Q50. 贵司是否建立关键人员访问权限控制（Access Control for Key Roles）？

A50（监管版）

是，本司实施严格的关键岗位访问控制，符合 DORA、ISO 27001 与 BaFin 指引。

（一）角色分级（Role-Based Access Control, RBAC）

- CTO：系统架构、读写权限
- DevOps：部署权限
- CCO/MLRO：系统审计日志
- 风控：监测平台
- 客服：只读权限
- 员工无一人拥有"全权限账号"

（二）双人控制（4-eyes Principle）

应用于：

- 风险事件
- 访问敏感数据
- 修改系统配置

（三）权限审查

- 每季度审查
- 季度 Access Review
- 停用离职人员账号（Immediate Disable）

（四）技术控制

- MFA
- 加密存储
- 审计日志不可篡改

符合监管对 ICT 安全的要求。
（由仁港永胜唐生提供专业讲解。）

A50（内部解释版）

BaFin 对"权限控制"非常重视，因为：

- 加密平台很多事故来自"单人高权限"
- 必须展示制度化、控制化

Q51. 请说明贵司是否实施"四眼原则"(4-eyes Principle)，适用于哪些场景?

A51（监管版｜BaFin-ready）

是，本司全面实施 **四眼原则（4-eyes Principle）**，确保关键操作不会由单一人员独立执行。

（一）适用范围（关键环节必须4-eyes）：

1. **客户入职审批（KYC/KYB）**
   - KYC 审查员 + KYC 主管
2. **高风险客户 EDD 审批**
   - AML 分析员 + MLRO
3. **提现审核**
   - 风控人员 + 资金管理员
4. **Token 上币决策**
   - TLC 主席 + CCO
5. **IT 变更管理（Change Management）**
   - DevOps + CTO
6. **访问权限调整（Access Rights Change）**
   - IT 安全官 + 管理层审批
7. **重大风险事件处理**
   - 风控主管 + CCO

（二）系统控制：

- 平台内建审批流程
- 所有行为记录在不可篡改审计日志

（三）目的：

- 防止内部欺诈
- 降低操作风险
- 符合 BaFin MaRisk、DORA 要求

（由仁港永胜唐生提供专业讲解。）

A51（内部解释版）

监管非常喜欢"四眼原则"，因为可以：

- 防内部舞弊
- 防止高风险操作由单人完成
- 提升治理成熟度

越多场景应用，越加分。

Q52. 贵司是否实施"职责分离"(Segregation of Duties)，请说明具体措施。

A52（监管版）

是，本司全面执行 **职责分离制度（Segregation of Duties, SoD）**。

（一）核心分离：

1. **交易 vs 托管**
   - 交易团队不能接触私钥
   - 托管团队无法操作订单系统
2. **风险 vs 业务**
   - 风控团队不可负责营收活动
   - 业务团队不能更改风控阈值
3. **合规 vs 运营**
   - CCO 不执行运营任务
   - 运营团队不能更改政策
4. **IT vs 安全审计**
   - 开发人员不能审核自己的改动
   - 安全审计独立执行
5. **MLRO vs 销售/市场**
   - MLRO 不接触客户销售

（二）记录形式：

- 记录于 RACI 矩阵
- 内审每年测试一次

（三）目的：

- 防止利益冲突
- 防止权限滥用
- 符合 BaFin MaRisk §25 要求

（由仁港永胜唐生提供专业讲解。）

A52（内部解释版）

重点表达：

- 人不能"又审批又执行"
- 人不能"一条龙"掌控

监管最怕一个人同时控制：

- 资金
- 操作
- 审批

SoD 是基础安全机制。

Q53. 贵司是否建立管理层与董事会之间的 KPI 体系？是否确保 KPI 不会引发利益冲突？

A53（监管版）

是，本司建立透明的管理层 KPI 体系，并确保 **KPI 不与高风险业务挂钩**。

（一）KPI 不包括：

- 交易量增长
- 交易手续费增长

- 新币种上架数量
- 市场推广指标
- 客户资产规模（AUM）
- 用户交易活跃度

这些指标可能导致利益冲突，因此被排除。

（二）KPI 包括：

- 合规指标（Compliance KPI）
- 风控指标（Risk KPI）
- IT 系统稳定性（Uptime SLA）
- 重大事件"0 容忍"
- 年度政策更新完成度
- 数据保护合规度
- 外包供应商 SLA 达成率

（三）治理保障：

- KPI 经董事会合规委员会批准
- 每季度审查
- 年度调整

确保无"促进高风险行为"的激励。
（由仁港永胜唐生提供专业讲解。）

A53（内部解释版）

监管怕 KPI 绑错目标，例如：

- "上币越多奖金越多"
- "交易量越大奖金越高"

这样的 KPI = 坏信号。
必须强调 KPI"偏重合规"。

Q54. 贵司是否设立供应商管理（Vendor Management）体系？请说明监督机制。

A54（监管版）

是，本司建立完整的 **供应商管理体系（Vendor Management Framework）**，符合：

- DORA（ICT Supply Chain）要求
- EBA Outsourcing Guideline
- BaFin 外包通函

（一）供应商分类（Tiering）

- Tier 1：关键 ICT 供应商（云服务、KYC、AML 工具）
- Tier 2：高重要性供应商
- Tier 3：低风险供应商

（二）尽调（Due Diligence）

针对 Tier 1 必须：

- 安全测试
- 数据保护检查（GDPR）
- 财务状况
- 审计报告（SOC2）
- 服务能力评估

（三）持续监督（Ongoing Monitoring）

- SLA 监控
- 处罚条款执行
- 季度风险评估
- 年度供应商审计

（四）退出机制（Exit Plan）

- 数据迁移方案
- 替代供应商名单
- 灾备支持

（由仁港永胜唐生提供专业讲解。）

A54（内部解释版）

供应商管理体系是 DORA 核心要求，必须强调：

- 分类
- 监督
- 审计
- 退出机制

DORA 对第三方风险极度严格。

Q55. 贵司是否设立数据治理（Data Governance）框架？包含哪些组成部分？

A55（监管版）

是，本司依据 GDPR + MiCA + DORA 要求，建立完整的数据治理框架。

（一）数据分类（Data Classification）

- 个人数据
- 客户 KYC 数据
- 交易数据
- 支付数据
- 内部文件
- IT 日志
- 高敏感数据（私钥/密钥，不存储明文）

（二）数据生命周期管理

- 收集
- 存储
- 加密
- 使用

- 删除（GDPR "Right to Erasure"）

（三）数据访问控制

- RBAC
- MFA
- 加密传输（TLS 1.2+）

（四）数据审计

- 每季度执行
- 包括权限审查 + 日志审计

（五）数据泄露应急计划（Data Breach Response）

符合 GDPR 第 33 条要求。

（由仁港永胜唐生专业整理。）

A55（内部解释版）

监管要确认：

- 数据管理完整
- 私钥绝不明文存储
- 有审计、有权限分级

越强调安全越好。

Q56. 贵司是否实施高管冲突声明制度（Conflict of Interest Declaration）？

A56（监管版）

是，本司实施年度及季度的《利益冲突声明（Conflict of Interest Declaration）》制度。

（一）适用人员：

- 董事
- 高级管理层
- CCO
- MLRO
- 风控主管
- CTO
- 财务主管

（二）声明内容：

1. 是否持有任何加密资产
2. 是否与项目方有合作
3. 是否持有竞争公司股份
4. 是否与客户存在经济关联
5. 是否受外部影响

（三）审批机制：

- 由 CCO 审查
- 必要时交董事会处理

（由仁港永胜唐生提供专业讲解。）

A56（内部解释版）

监管担忧：

- 员工私下炒币
- 管理层持有大量代币
- 项目方给予回扣

必须强调“声明制度健全”。

Q57. 贵司是否针对董事会与高管制定职责说明书（Terms of Reference）？

A57（监管版）

是，本司为董事会与所有管理层成员制定《Terms of Reference（TOR）》文件。

内容包括：

- 职责范围
- 管辖领域
- 决策权限
- 风险控制责任
- 监管责任（MiCA 特有）
- 报告线
- 决策流程
- 回避机制

适用角色：

- Board Chair
- CEO
- COO
- CCO
- MLRO
- CTO
- CFO
- Risk Officer

所有 TOR 文件均经董事会批准并每年更新。

（由仁港永胜唐生提供专业讲解。）

A57（内部解释版）

TOR 是监管重点文件：

- 明确“谁负责什么”
- 防止权责不清

越清晰越加分。

Q58. 贵司是否针对管理层实施绩效监督机制？

A58（监管版）

是，本司已建立《管理层绩效监督机制（Management Performance Oversight）》。

（一）监督主体：

- 董事会
- 风险委员会
- 合规委员会

（二）监督内容：

- 是否按照政策执行
- 是否遵守监管要求
- 是否按时提交报告
- 是否遵循风险偏好
- 是否出现重大操作风险

（三）结果处理：

- 绩效评分
- 薪酬调整
- 风险整改要求
- 严重情况报告董事会

（由仁港永胜唐生提供专业讲解。）

A58（内部解释版）

监管关心"管理层能否被监督"。
重点表达：

- 董事会有权监督
- 合规与风险委员会也监督
- 有处罚机制

Q59. 贵司是否设立员工举报机制（Whistleblowing Policy）？

A59（监管版）

是，本司制定并实施《Whistleblowing Policy》。

（一）举报渠道：

- 匿名邮箱
- 匿名电话
- 内部举报平台
- 外包第三方举报系统（如适用）

（二）举报内容：

- 内部欺诈
- 内部违规操作
- AML 违规
- 交易操纵
- 利益冲突
- 数据滥用

（三）保护机制：

- 举报人保护
- 禁止报复机制
- 举报记录保密

（四）监管对接：

可将重大违规直接上报 FIU 或 BaFin。

（由仁港永胜唐生提供专业讲解。）

A59（内部解释版）

监管喜欢举报机制，因为：

- 可以增强内部合规文化
- 方便发现问题

必须强调"保护举报人"。

Q60. 请说明贵司如何确保董事会、高管与员工的持续胜任能力（Continuous Professional Development, CPD）。

A60（监管版）

本司实施年度 CPD（持续专业培训）制度，包含：

（一）年度培训时长：

- 董事：10 小时
- 高管：12 小时
- 员工：8 小时
- AML 团队：15 小时

（二）培训内容：

- MiCA 更新
- AMLD6
- 链上 AML
- 市场操纵防范
- DORA ICT 安全
- GDPR 数据保护
- 新产品风险

（三）记录：

- 培训完成证明
- 考试结果（如适用）
- 签到记录
- 培训材料归档

所有记录保留 10 年，由 CCO 存档。

（由仁港永胜唐生提供专业讲解。）

A60（内部解释版）

监管要确认：

- 员工持续学习
- 高管持续更新知识

尤其是加密法规更新非常快。

Q61. 请提供贵司客户尽职调查（CDD）流程的完整说明，包括触发点、执行步骤与记录保存要求。

A61（监管提交版｜BaFin-ready）

本司依据 **AMLD6、GWG、BaFin AML Circular** 建立完整 CDD 框架，并确保流程可审计、可追踪、可复核。

（一）CDD 触发点（Triggers）

1. 客户注册（Onboarding）
2. 资料变更（地址、职业、国籍）
3. 风险等级变化（Behavior Risk Increase）
4. 触发警报（Transaction Monitoring Alerts）
5. 风险政策更新（Policy Updates）

（二）基本 CDD（Standard CDD）

- 身份核验（IDV + Liveness + OCR）
- 地址验证（POA）
- 名单筛查（Sanction + PEP）
- KYC 问卷
- 职业与资金来源声明（Source of Funds）

（三）强化尽调（EDD）适用于：

- 高风险国家（EU high risk）
- 高风险行业
- PEP
- 大额交易
- 匿名特征链上地址

EDD 包含：

- 资金来源证明（SOF）
- 财富来源证明（SOW）
- 银行流水
- 审计文件
- 视频面谈
- 高管审批（MLRO / CCO）

（四）记录保存：

依据 **GWG §8 & MiCA**：

- CDD 文件保存 10 年
- 审计日志（不可篡改）
- 每次变更留日志

（由仁港永胜唐生拟定并提供专业讲解。）

A61 内部解释版

CDD 是 AML 的头部机制，BaFin 审查重点是：

- 是否"真正做了"
- 是否"可追踪"
- 是否"链上风险也覆盖"

越详细越符合监管偏好。

Q62. 请解释贵司如何进行客户身份验证（Identity Verification），包括技术手段与供应商审查。

A62（监管提交版）

本司采用多层验证机制，确保客户身份真实、可验证、可审计。

（一）技术手段

1. **自动化身份证件核验（OCR + MRZ 检查）**
2. **活体检测（Liveness）**
   - Blink
   - Pose
   - Depth
3. **合规供应商验证模型（KYC Vendor）**
4. **文件伪造检测**
   - Hologram
   - Artifact detection
5. **设备指纹（Device Fingerprinting）**
6. **IP 风险分析**
7. **Velocity Risk**（多账户登录检测）

（二）供应商审查（Vendor Due Diligence）

针对 KYC 供应商，我们执行：

- GDPR 合规审查
- DPA（Data Processing Agreement）
- 合规证书（ISO27001 / SOC2）
- 技术审计（API 安全）
- SLA 审查
- 年度审计

（三）人工复核

- 边缘案例（Borderline）
- 模糊验证（Inconclusive）
- 高风险客户

人工复核团队接受 AMLD6 培训。

（由仁港永胜唐生专业整理。）

A62 内部解释版

监管的关键是：

- 自动化只是第一层
- 必须有人参与
- 供应商必须审查

强调"不能完全外包"。

Q63. 贵司是否对客户进行风险评分（Customer Risk Scoring）？模型依据是什么？

A63（监管提交版）

是，本司采用 **多维度风险评分模型（Multi-dimensional Risk Scoring Model）**，符合 AMLD6 / GWG / FATF RBA 原则。

（一）风险维度（Risk Dimensions）：

1. **客户类型（Individual / Corporate）**
2. **国家风险（Country Risk）**
   - FATF High-risk
   - EU High-risk Third Countries
3. **行业风险（Industry Risk）**
4. **产品风险（Product Risk）**
5. **链上风险（On-chain Risk）**
6. **行为风险（Behavior Risk）**
7. **资金来源风险（SOF/SOW）**

（二）评分分类

- Low
- Medium
- Medium-high
- High（EDD + MLRO 审批）

（三）动态更新：

- 实时更新（行为、交易）
- 监管名单变化即刻重新评分

（由仁港永胜唐生提供专业讲解。）

A63 内部解释版

核心要点：

- 风险模型必须"动态"
- 包含"链上风险"（这是加密行业最重要部分）
- 高风险必须 EDD

Q64. 请说明贵司的链上地址风险管理（On-chain KYT & AML）。

A64（监管提交版）

本司使用链上监控系统（KYT, Know Your Transaction）对所有链上地址执行风险评估。

（一）链上监控工具：

- Chainalysis

- TRM Labs
- Crystal Blockchain
- 自建节点数据

（二）拦截逻辑（Blocking Rules）：

如命中以下则立即冻结地址：

- OFAC SDN
- EU 制裁名单
- Mixer Cluster
- Darknet Market
- Stolen Funds Tags
- Ransomware
- Terrorist Financing

（三）风险分类

- A：低风险
- B：中风险
- C：中高风险
- D：高风险（禁止交易）

（四）链上分析动作

- Trace
- Graph
- Cluster
- Exposure Scoring
- Sanctions Screening

（由仁港永胜唐生专业整理。）

A64 内部解释版

监管要确认：

- 我们是否真正懂链上分析
- 是否有拦截机制
- 是否可以溯源

越细越好。

Q65. 贵司是否为 PEP（政治公众人物）制定强化尽调（EDD）策略？流程是什么？

A65（监管提交版）

是，本司为 PEP 客户执行 **最高级别 EDD**。

（一）识别方式：

- 全球 PEP 数据库
- 负面新闻筛查
- 关联人识别（Relatives & Close Associates）

（二）EDD 内容

1. 视频面谈

2. SOF（资金来源）
3. SOW（财富来源）
4. 税务文件
5. 银行流水
6. 顶层审批（MLRO + CCO）

（三）持续监控

- 每月 KYC refresh
- 交易监测优先级提高
- 行为异常多层过滤

（四）拒绝情况

- 数据不一致
- 无 SOF 佐证
- 资产来源不透明

（由仁港永胜唐生提供专业讲解。）

A65 内部解释版

PEP 是监管最敏感类别，
必须强调：

- 加强审查
- 频繁更新
- 高层审批

Q66. 贵司如何识别可疑交易（STR）？触发标准是什么？

A66（监管提交版）

本司依据 AMLD6/GWG/FIU 指引制定 STR 触发机制，包括链上 + 链下双系统。

（一）触发场景（部分示例）：

1. 资金与职业不符
2. 高频小额拆分（Structuring）
3. 短时间大量提现
4. VPN/Tor 高风险 IP
5. 命中链上 Mixers
6. 交易与客户画像不符
7. 涉及被盗资产
8. 来自高风险国家交易
9. 使用第三方钱包
10. 高风险代币资金路径

（二）STR 决策机制

- 自动预警 → AML 分析 → MLRO 最终裁定
- 不得告知客户（Tipping-off 禁止）

（三）上报

- 向 **FIU（德国金融情报单位）** 提交

- 保留记录 10 年

（由仁港永胜唐生提供专业讲解。）

A66 内部解释版

重点：

- STR 标准越清晰越好
- 强调“不允许通知客户”
- 链上 STR 是BaFin最关心的区块链环节

Q67. 贵司是否设置“可疑行为自动升级（Escalation）”机制？

A67（监管提交版）

是，本司构建自动化行为识别引擎，所有高风险行为会自动升级至：

- AML 分析员
- MLRO（视风险等级）

（一）自动升级触发：

- 资金流向高风险地址
- 企业账户行为异常
- 高频 IP 变更
- 设备指纹更换
- 初次入金过大
- 反复试图绕过限制

（二）升级路径：

Level 1 → AML 分析员
Level 2 → AML 主管
Level 3 → MLRO（高风险）

（三）系统控制：

- 自动冻结
- 自动延迟提现
- 自动追加审查材料

（由仁港永胜唐生提供专业讲解。）

A67 内部解释版

监管喜欢自动化机制，可明显降低人工遗漏。

Q68. 高风险国家客户是否允许开户？您的政策是什么？

A68（监管提交版）

本司遵守 **AMLD6 + EU High-risk Third Country List**。

严格禁止：

- FATF Blacklist

- EU High-risk Country List
- OFAC 全面制裁区
- 俄罗斯相关受制裁主体

条件性允许（需 EDD）：

- 中高风险国家
- 必须提供：
  - SOF
  - SOW
  - 税务文件
  - 银行流水
  - High-level KYC

MLRO 有权拒绝任何申请。

（由仁港永胜唐生专业整理。）

A68 内部解释版

监管要看到：

- 明确国家风险规则
- 拒绝高风险名单
- MLRO 有绝对决策权

Q69. 贵司如何识别代理开户（Third-party Account Opening / Account Misuse）？

A69（监管提交版）

采用 6 层检测机制识别代理开户：

（一）行为分析

- 登录行为与客户国家不一致
- 异常设备
- 多账户共享 IP

（二）设备指纹

- 同设备多个账户
- 风险设备库命中

（三）KYC 一致性检查

- 文件签名对比
- 照片格式异常

（四）链上行为分析

- 资金来自同一可疑集群

（五）负面新闻检查（Negative Media）

（六）升级审查（EDD）

- 视频面谈
- SOF/SOW

- MLRO 批准

（由仁港永胜唐生提供专业讲解。）

A69 内部解释版

代理开户（代替开户）是德国监管最关注的问题之一。
必须展示"多层检测能力"。

Q70. 贵司是否执行客户定期复审（KYC Refresh）？频率如何?

A70（监管提交版）

是，我们依据风险等级执行 KYC Refresh：

（一）复审频率：

- 低风险：每 36 个月
- 中风险：每 24 个月
- 中高风险：每 12 个月
- 高风险/PEP：每 3～6 个月

（二）内容包含：

- 文件重新上传
- 信息变更检查
- 链上行为分析
- 资金来源重新验证
- 职业/收入更新

（三）技术实现：

- Auto-reminder
- 强制验证
- 未完成则冻结账户

（由仁港永胜唐生提供专业讲解。）

A70 内部解释版

监管要求明确 Refresh 机制：
越高风险 → 越频繁 → 越严格。

Q71. 贵司如何进行制裁筛查（Sanctions Screening）？使用哪些名单、频率如何?

A71（监管提交版｜BaFin-ready）

本司建立全覆盖制裁筛查体系，遵循：

- **EU Consolidated Financial Sanctions List**
- **OFAC SDN / SSI List**
- **UN Sanctions List**
- **Bundesanzeiger（德国制裁公告）**

（一）筛查对象范围

1. 客户姓名
2. 企业名称
3. 董事与 UBO
4. 链上地址
5. 交易对手
6. 银行账户（IBAN/BIC）
7. 设备/IP/域名（如适用）

（二）筛查频率

- Onboarding（开户）
- 每日批量扫描（Batch Screening）
- 实时交易前（Real-time pre-trade）
- 名单更新后的即时重新筛查

（三）命中处理流程

- 命中 → 自动冻结账户 → MLRO 审核 → （必要时）STR 报告
- 严禁 Tipping-off

该流程严格符合 **GWG、AMLD6、EU Sanctions Regime** 要求。
（由仁港永胜唐生拟定并提供专业讲解。）

A71 内部解释版

要点：

- 制裁筛查范围越广越好
- 强调"实时 + 批量"双模式
- 强调"不告知客户（tipping-off 禁止）"
- BaFin 会检查是否使用 **EU 制裁名单优先**

Q72. 请说明贵司如何处理制裁"潜在命中（False Positive）》与"明确命中（True Hit）」。

A72（监管提交版）

我们将所有制裁结果分为两类：

（一）潜在命中（False Positive）处理：

在以下情况视为 False Positive：

- 拼写差异
- 不同国籍
- 出生日期不一致
- 公司地址完全不同
- 无关联职业/行业

处理流程：

1. AML 分析员对比详细资料
2. 使用二次筛查工具
3. 必要时联系客户提供额外文件
4. 记录审查过程

5. 关闭警报

（二）明确命中（True Hit）处理：

视为 True Hit 的情形：

- 姓名、生日、国籍全部一致
- 链上地址命中指定制裁标签
- 交易路径与制裁实体高度关联

处理流程：

1. **立即冻结账户 & 交易**
2. 升级至 MLRO
3. 提交 STR 至 FIU（德国）
4. 记录处理过程
5. 保存至少 10 年

（由仁港永胜唐生提供专业讲解。）

A72 内部解释版

BaFin 特别重视：

- 区分 False Positive / True Hit 的逻辑
- 是否形成内部 SOP
- 是否记录全链路审计日志

Q73. 贵司如何识别并禁止使用匿名工具（Mixers、Tumblers、Privacy coins）？

A73（监管提交版）

本司严格禁止：

- Mixers
- Tumblers
- CoinJoin
- Tornado Cash（EU sanctioned）
- Privacy Coins（如 Monero、Zcash、Dash 等）
- 未经许可的匿名增强协议

（一）技术检测手段：

1. 链上聚类分析（Cluster Analysis）
2. Exposure Scoring
3. Risk Tag 命中（Mixer/Tumbler）
4. Heuristic Tracing（跳跃路径分析）
5. Anonymity Set Detection
6. Wallet Heuristic（多跳混合资产检测）

（二）处理流程

- 命中即自动冻结
- MLRO 审查
- 必要时 STR

（三）法律基础

- FATF Recommendation 15
- EU MiCA（禁止匿名交易增强手段）
- GWG 高风险交易禁止条款

（由仁港永胜唐生提供专业讲解。）

A73 内部解释版

BaFin 对 Mixers 是 **零容忍**。
必须强调：

- 禁止
- 检测
- 拦截

私密币（Monero）几乎是监管红线。

Q74. 如何识别可疑链上地址（Suspicious Addresses），包括黑客、诈骗、勒索软件等？

A74（监管提交版）

我们使用行业级链上监控系统，将链上地址分为以下高风险标签：

（一）高风险类别：

- Stolen Funds
- Hack / Exploit
- Phishing
- Scam
- Darknet Markets
- Ransomware
- Terrorist Financing
- Sanctioned Clusters
- Gambling（高风险司法管辖区）
- Malware

（二）检测技术

- 链上追踪（Graph）
- Exposure Scoring
- Counterparty Analysis
- Wallet Clustering
- Time-series Abnormal Patterns

（三）应对

- 自动冻结
- 要求客户解释资金来源
- 必要时 STR
- 阻止提现至可疑地址

（由仁港永胜唐生专业整理。）

A74 内部解释版

BaFin 关注：

- 地址识别方法是否足够细
- 是否包含"资金路径分析"
- 是否了解常见犯罪链路（例如：多跳洗钱路径）

Q75. 贵司是否允许使用第三方钱包？如何验证第三方钱包所有权？

A75（监管提交版）

我们允许客户绑定第三方钱包，但须通过强化验证。

（一）钱包所有权验证（Wallet Ownership Proof）：

1. **签名验证（Message Signing）**
   - ETH: ECDSA
   - BTC: MessageSign
2. **视频验证（On-chain Address + Live Recording）**
3. **小额验证（Micro-deposit Challenge）**
4. **交易路径真实性检测**

（二）禁止的情况：

- Mixer wallet
- Exchange hot wallet（非客户个人专属）
- 高风险国家托管钱包
- 涉毒、诈骗、赌博标签地址

（三）记录保存

- 所有验证记录留存 10 年

（由仁港永胜唐生提供专业讲解。）

A75 内部解释版

钱包验证是 BaFin 对加密业务的必查点。
必须展示：

- 有能力验证钱包所有权
- 有"链上钱包验证 SOP"

Q76. 贵司是否区分 SOF（资金来源）与 SOW（财富来源）？如何验证？

A76（监管提交版）

是，本司严格区分并验证：

（一）SOF（Source of Funds）资金来源：

用于解释"这笔钱来自哪里"。
可接受文件：

- 工资单

- 银行流水
- 合同收入
- 公司分红
- 投资收益

验证方法：

- 文件真伪验证
- 与职业/收入匹配度分析

（二）SOW（Source of Wealth）财富来源：

用于解释"这份财富如何形成"。
可接受材料：

- 房产证
- 公司持股证书
- 纳税证明
- 继承证明

验证标准：

- 与客户画像一致
- 金额与收入水平匹配
- 可审计

（由仁港永胜唐生专业整理。）

A76 内部解释版

监管要求不能混淆 SOF / SOW。
关键点在于：

- SOW 必须"长期/累积"来源
- SOF 必须"单笔交易"来源

Q77. 贵司如何处理 NFT 相关洗钱风险？

A77（监管提交版）

NFT 属于 MiCA 未分类资产，但 BaFin 将其视为高风险数字资产。

风险情境：

- 虚高定价
- 自买自卖（Wash Trading）
- 多跳转移
- 使用 NFT 掩盖资金路径

控制措施：

1. NFT 风险分类（High / Medium / Low）
2. Market Manipulation Monitoring（价格异常检测）
3. 链上多跳路径分析
4. 禁止匿名 NFT 交易
5. 对超高价 NFT 执行 EDD

6. 记录所有交易元数据

（由仁港永胜唐生提供专业讲解。）

A77 内部解释版

BaFin 认为 NFT 是"极易被用来洗钱的载体"。
必须展示具体风险场景＋检测措施。

Q78. 贵司如何监测"结构化交易"（Structuring / Smurfing）？

A78（监管提交版）

我们采用行为与金额双层检测机制监测结构化交易。

（一）检测指标：

1. 连续多笔小额资金 → 目标钱包
2. 多账户向同一钱包汇入
3. 高频资金分拆
4. 转账金额略低于合规阈值
5. 无明显经济目的
6. 夜间频繁转账
7. 使用新注册账户进行大额活动

（二）监测工具：

- 行为分析引擎
- 链上分拆路径分析（Splitting Path）
- Velocity Tracking（速度分析）

（三）措施：

- 自动冻结提现
- 要求追加材料
- 必要时 STR

（由仁港永胜唐生专业整理。）

A78 内部解释版

结构化交易是洗钱的最大红旗之一。
BaFin 要求"必须有具体检测指标"。

Q79. 贵司是否建立"高风险行业（HRIs）"名单？如何应用？

A79（监管提交版）

是，我们依据 FATF 与欧盟 AML 指引建立 HRI（High-risk Industries）名单。

（一）高风险行业包括：

- 加密交易
- 赌博
- 非政府组织（部分）

- 艺术品交易
- 贵金属
- 汇款行业
- 房地产
- 私募基金
- 海外信托

（二）应用方式：

1. 行业风险提升 Tier
2. 强制 EDD
3. 更频繁 KYC refresh
4. 限制交易额度
5. 行为监测增强

（由仁港永胜唐生提供专业讲解。）

A79 内部解释版

BaFin 希望看到：

- 企业理解"行业风险"
- 并将其纳入风险模型

Q80. 贵司是否建立"交易行为基线（Behavior Baseline）"？用于检测偏离正常模式的可疑行为？

A80（监管提交版）

是，我们为每位客户建立"行为基线模型（Behavioral Baseline Model）"。

行为基线包含：

1. 登录时间段
2. 交易频率
3. 交易金额
4. 交易对手
5. 钱包地址
6. IP/设备模式
7. 链上资产类型
8. 资产持有周期

偏离策略：

当行为偏离基线时，会触发：

- AML 预警
- 风险评分上调
- 自动限制提现
- 追加 KYC

（由仁港永胜唐生专业整理。）

A80 内部解释版

BaFin 认为：

> “没有行为基线，就无法发现行为异常。”

因此必须强调：

- 基线构建
- 基线偏离触发机制

Q81. 贵司如何识别恐怖融资（Terrorist Financing）风险？有哪些监测指标？

A81（监管提交版｜BaFin-ready）

本司依据 FATF、EU Counter-Terrorism Financial Sanctions、GWG 制定 TF 风险检测机制。

（一）恐怖融资识别指标（TF Indicators）

1. **资金流向高风险地缘冲突地区：**
   - 阿富汗、叙利亚、伊朗、伊拉克等
   - EU TF 制裁名单国家
2. **小额高频入金**
3. **使用匿名工具（VPN/Tor/Mixers）**
4. **与已知 TF 风险集群地址交易过**
5. **链上“短路径—多跳”可疑结构（Layering）**
6. **购买与转移 Privacy Coins/Opaque Tokens**
7. **无合理经济目的的长期活跃地址**

（二）以及时行动为核心：

命中 TF 风险 →
自动冻结交易 → MLRO 审查 → STR（FIU-TF 专属渠道）
该流程严格符合 **GWG §15、EU TF Regulations、FIU-TF 指引**。
（由仁港永胜唐生拟定并提供专业讲解。）

A81 内部解释版

重点提醒：

- TF ≠ 洗钱，但模式类似
- 特征是“金额小”、“频率高”、“路径短”、“目标特定集群”
- BaFin 特别检查：是否会错误放行小额 TF 交易

Q82. 贵司如何检测并拦截勒索软件（Ransomware）嫌疑交易？

A82（监管提交版）

本司严禁处理任何与 **Ransomware（勒索软件）集群**相关的加密资产。

（一）主要检测逻辑：

1. 链上命中
   - Conti
   - LockBit
   - REvil

    - DarkSide
    - Hive
    - Ragnar
2. 资金流向 Tor hidden services（链上受害者充值地址）
3. 显示"受害者付款模式"的入金
4. 受害者声称"收到勒索邮件/钱包要求付款"

（二）应对机制：

- 自动冻结入金
- 禁止任何向 Ransomware 地址的交易
- 启动 MLRO Escalation
- 提交 STR

A82 内部解释版

勒索软件是 BaFin 审查的重点之一。监管会确认：

- 是否能识别主要勒索软件集群
- 是否"绝对禁止向勒索地址汇款"

Q83. 贵司是否允许客户使用 DeFi 协议？如何监控 DeFi 洗钱风险？

A83（监管提交版）

本司允许客户使用 DeFi，但设立严格监控机制。

（一）禁止交互的 DeFi 类型：

- Mixing DEX
- 匿名 AMM（无法识别 LP 地址）
- 带隐私增强功能的跨链桥（Anonymous Bridges）
- 已知诈骗合约

（二）必须监控的 DeFi 风险路径：

1. **闪电贷（Flash Loan）攻击路径**
2. **智能合约漏洞攻击后的资金清洗**
3. **高风险 DEX / Router 聚合器资金流**
4. **跨链桥链跳（Chain-hopping）**
5. **洗钱常用 DeFi 路径：DEX→Bridge→CEX**

（三）合规控制措施：

- 所有 DeFi 交互记录需链上审计
- 对可疑合约地址执行阻断
- 强制执行链上 KYT（Know Your Transaction）
- 高频 DeFi 流量必须执行 EDD

（由仁港永胜唐生提供专业讲解。）

A83 内部解释版

监管对 DeFi 的核心关注：

- 流动性池（LP）匿名性

- 跨链桥跳转
- DeFi"洗钱三步走"：DEX→桥→提现

必须展示"理解风险，并有检测机制"。

Q84. 贵司如何控制跨境链上交易风险（Cross-border Crypto Transfer Risks）？

A84（监管提交版）

跨境链上交易是洗钱与 TF 的高风险点，本司执行以下风险控制：

（一）重点关注场景：

1. 来自非合作国家
2. 来自高风险 CEX
3. 跨链跳转超过 3 次
4. 资金来自匿名桥（Anonymity Bridges）
5. 与虚拟 SIM/WiFi IP 匹配异常

（二）链上分析控制措施：

- Country/Territory Tagging
- Cross-chain Flow Mapping
- Multi-hop Analysis（>3 hops 自动告警）
- Risk-weighted routing

（三）跨境实名要求：

- EU Travel Rule 全面执行
- VASP 间信息传输（Originator+Beneficiary）
- AMLD6 认证要求

A84 内部解释版

跨境交易是 BaFin 必查部分。
重点要体现：

- "链上跨境"= 国家风险 × 交易路径风险
- Travel Rule 一定要出现

Q85. 贵司如何监控第三方支付渠道（Payment Processors / PSP）风险?

A85（监管提交版）

本司采用第三方支付（PSP）审查机制，确保 PSP 符合：

- PSD2
- EBA 指南
- AMLD6
- GWG（德国反洗钱法）

（一）PSP 审查内容：

1. 许可证类型（EMI / PI / Bank）
2. 注册国家
3. 监管机构（例如：BaFin、FCA、Bank of Lithuania）
4. AML 体系
5. 是否支持匿名操作

（二）禁止的 PSP：

- 未受监管 PSP
- 加密相关高风险 PSP
- 黑名单 PSP（诈骗/Chargeback 记录）

（三）交易监控：

- 与 PSP 入金金额/来源匹配
- 异常 PSP 频繁切换
- 关联 PSP 交易异常

（由仁港永胜唐生专业整理。）

A85 内部解释版

BaFin 会重点检查：

- PSP 是否"合规、受监管、KYC 完整"
- PSP 风险是否进入整体 AML 模型

Q86. MLRO（反洗钱负责人）拥有何种审批权？是否独立？

A86（监管提交版）

本司 MLRO 拥有完全独立权力，并直接向董事会报告。

（一）MLRO 权力：

1. 冻结交易 / 冻结账户
2. 拒绝客户开户
3. 提交 STR（无需管理层同意）
4. 要求任何部门提供信息
5. 拒绝任何高风险业务扩展

（二）独立性保障：

- MLRO 不参与销售
- MLRO 不受业务 KPI 约束
- 直接向董事会 AML 委员会报告
- 拥有否决权（Veto power）

（三）合规依据：

符合 **GWG §7、BaFin AML 指引、AMLD6**。
（由仁港永胜唐生提供专业讲解。）

A86 内部解释版

BaFin 最看重：

"MLRO 是否真正独立，能否对业务说 NO。"

必须明确 MLRO 拥有 veto 绝对权。

Q87. 贵司如何确保 AML 团队与业务团队"隔离"（Chinese Wall）？

A87（监管提交版）

我们建立 AML 与 Business 的隔离制度，防止利益冲突。

（一）组织隔离：

- AML 团队独立部门
- 汇报线独立（向董事会，而非业务团队）
- 预算独立
- 非绩效考核驱动

（二）数据隔离：

- 访问控制 RBAC
- AML 系统可审计但不可修改业务操作
- 相互使用不同工具集

（三）决策隔离：

- 客户拒绝决定仅由 AML/MLRO 控制
- Business 不得干预 STR

这符合 **BaFin "Three Lines of Defense" 模型**。

A87 内部解释版

监管最怕：

- 业务为了业绩要求 AML 放行客户

强调"组织、数据、流程"三重隔离很重要。

Q88. 贵司是否将 AML 风险纳入企业整体风险框架（ERM）？

A88（监管提交版）

是，AML 风险已纳入本司 ERM（Enterprise Risk Management）框架。

（一）风险类别整合：

- AML 风险
- TF 风险
- Sanctions 风险
- Fraud 风险
- Operational 风险
- Cybersecurity 风险

（二）ERM 方法：

- 定性与定量评估
- 风险评分（Heat Map）

- 风险承受度设定（Risk Appetite）
- 风险缓释计划（Mitigation Plan）

（三）报告机制：

- 每季度 ERM 报告提交董事会
- 重大 AML 风险事件即时上报

（由仁港永胜唐生提供专业讲解。）

A88 内部解释版

BaFin 要看的不是"AML 部门做了什么"，而是：

> "整个公司是否将 AML 视为战略级风险。"

ERM 的加入极其重要。

Q89. 贵司如何验证客户身份文件的真实性（Document Authenticity Check）？

A89（监管提交版）

本司采用混合验证体系：

（一）自动化检查：

- OCR / MRZ
- Barcode/Chip 解析
- Security Features Check（反伪造）
- Hologram 光影分析
- Template Matching

（二）数据库校验：

- PRADO（欧盟官方证件数据库）
- ID Checkpoint
- ICAO Doc 9303

（三）人工复核：

- 面部与证件比对
- 图像伪造检查（Artifacts）
- 文件内容一致性

（四）疑似造假 → 强制视频面谈

（由仁港永胜唐生专业整理。）

A89 内部解释版

BaFin 常问：

- 是否引用 **PRADO**（欧盟）数据库？
- 是否"自动 + 人工"两层验证？

Q90. 贵司如何处理"高风险异常资金来源"(Unusual Source of Funds)?

A90(监管提交版)

当客户 SOF 异常,本司执行如下动作:

(一)触发条件:

- 收入与资金不匹配
- 来自高风险国家
- 资产无合理解释
- 与职业不符
- 来自不明加密地址

(二)EDD 审查内容:

- 税务证明
- 雇佣证明
- 银行流水六个月以上
- 交易对手证明
- 资产来源合同
- 趋势分析(Transaction Patterning)

(三)处置机制:

- SOF 无法解释 → 拒绝开户
- 证据不足 → 限制交易
- 高风险 → MLRO 审批
- 涉嫌犯罪 → STR

(由仁港永胜唐生提供专业讲解。)

A90 内部解释版

重点:

- 强调"收支匹配"
- 强调"职业/资产一致性"
- 强调"不可解释 → 必须拒绝/STR"

Q91. 贵司如何识别"代理钱包(Proxy Wallet)"行为?

A91(监管提交版|BaFin-ready)

本司采用 7 层监控机制识别 Proxy Wallet(代持钱包/非真实控制钱包):

(一)检测指标

1. 钱包签名与客户身份不一致
2. 地址与客户行为画像不吻合
3. 钱包交易历史显示"代管行为特征"
4. 资金往来与多个客户相关
5. 同钱包频繁绑定多个账户

6. 通过"统一第三方控制节点"提交交易
7. 资金路径显示"收集钱包"(collector wallet)行为

(二)异常代理钱包表现

- 复杂 Layering
- 多跳匿名地址
- 高频转移
- 与 OTC Broker 关联路径

(三)应对机制

- 强制钱包真实性验证(Signing)
- 激活 EDD
- MLRO 决策
- 必要时 STR

(由仁港永胜唐生提供专业讲解。)

A91 内部解释版

代理钱包往往是犯罪组织代持资产最常用方法。
重点是:行为画像 + 链上分析 + 验证机制。

Q92. 贵司如何监测 Layering(多跳洗钱)?跳数超标是否自动告警?

A92(监管提交版)

是,本司建立 **Layering 多跳检测引擎**:

(一)风险阈值(Hops Threshold)

- ≥ 3 hops:中风险
- ≥ 5 hops:高风险(自动 AML 告警)
- ≥ 7 hops:禁止交易 → MLRO 审查

(二)检测项目

1. Time-based hop pattern
2. Path compression detection
3. Suspicious cluster identification
4. Multi-asset hop(资产转换)
5. Bridge hop(跨链路径)
6. Mixer involvement detection

(三)行动机制

- 自动冻结高风险路径
- 要求提供 SOF/SOW
- MLRO 审批
- STR(必要时)

(由仁港永胜唐生提供专业讲解。)

A92 内部解释版

BaFin 最关心的是：

> “你们能不能识别 5 跳以上的 Layering？”

越详细越好。

Q93. 贵司如何识别加密诈骗（Crypto Scams）相关交易？

A93（监管提交版）

我们使用链上标签 + 行为模型识别诈骗：

诈骗类型包括：

- Investment scams
- Romance scams
- Pig-butchering（杀猪盘）
- Phishing/Malware
- Fake airdrop scams
- Rug Pull
- Crypto mining scams

（一）链上风险标签

- Scam cluster
- Fake project
- Rug pull address
- Phishing collector wallet
- “Wallet Drainer” signatures

（二）链下行为

- 客户声称被第三方“指导投资”
- 快速大额入金后赔光
- 高频提现至同一未知地址

（三）控制措施

- 冻结资金
- 审查资金路径
- MLRO 判定是否 STR

（由仁港永胜唐生专业整理。）

A93 内部解释版

诈骗通常由“高风险集群 + 行为异常”组成，必须展示多维识别能力。

Q94. Airdrop 是否存在洗钱风险？如何监控？

A94（监管提交版）

Airdrop 存在严重洗钱风险，尤其是 fake airdrop / malicious smart contract。

风险包括：

1. 使用 Airdrop 掩盖非法收入
2. Airdrop 作为“价值转移工具”
3. 多钱包批量领取

4. 黑客向受害者发送恶意代币（Scam token）
5. Airdrop Token 洗钱路径（Fake token → swap → bridge）

控制措施：

- 检查 Airdrop 来源
- 分析 TokenContract 历史
- 阻止垃圾 Token
- 检测批量 Claim（AirDrop Farming）
- 可疑路径强制 EDD

（由仁港永胜唐生提供专业讲解。）

A94 内部解释版

Airdrop 洗钱路径：

> Airdrop → Swap → Bridge → Withdraw

是犯罪分子非常常见的路径。

Q95. 贵司如何识别和监控 Rug Pull（拔地板跑路）风险?

A95（监管提交版）

Rug Pull 是加密行业最高频诈骗之一。

（一）链上检测特征：

1. 单一控制者持有大部分流动性
2. Liquidity pool 大幅撤出
3. TokenContract 可被 owner"Mint 无限量"
4. 交易税率突然上升
5. Dev 钱包与交易路径相关
6. 合约源代码显示"权限可撤销"

（二）控制措施：

- 在交易前执行 TokenContract 审查
- 风险 Token 列入 blacklist
- MLRO 审查大额买入交易
- 监测"预警 ROI 异常上升"

（由仁港永胜唐生专业整理。）

A95 内部解释版

Rug Pull 检测重点在于：
合约权限（Mint/Blacklist/SetTax） 必须检查。

Q96. ICO/IEO/STO 是否允许？如何管理相关风险?

A96（监管提交版）

本司允许客户参与 ICO/IEO/STO，但设立严格限制。

（一）风险类型

- Scam ICO
- Unregulated STO
- Fake Whitepaper
- 批量创建假投资地址

（二）控制措施：

1. Token Contract 审查（智能合约权限）
2. Issuer 背景核查
3. KYC of Issuer（如适用）
4. AML 风险评分
5. 大额参与需 MLRO 审批
6. 记录发行方资料

（三）不可参与：

- 未披露白皮书
- Token Contract 不透明
- 未受监管 STO
- 涉嫌诈骗项目

（由仁港永胜唐生提供专业讲解。）

A96 内部解释版

BaFin 特别关注 ICO/STO，因为大量诈骗来自此类活动。

Q97. 贵司如何区分"投资行为"和"洗钱行为"？

A97（监管提交版）

本司通过 **行为建模** 区分合法投资行为与可疑洗钱行为。

投资行为特征

- 合理投资比例
- 风险与收益逻辑匹配
- 资金来源清晰
- 行为与客户画像一致
- 无复杂多跳路径

洗钱行为特征

- 资产无理由快速进出
- 跨链跳转多
- 涉及高风险地址集群
- SOF 与交易不符
- OTC 小额大批量
- 随机选择 Token（无投资逻辑）

判定机制：

- AML 行为模型
- 链上路径判断

- MLRO 介入

（由仁港永胜唐生专业整理。）

A97 内部解释版

洗钱很少考虑"收益"，投资者则以收益为目的。
逻辑不同。

Q98. 贵司如何识别匿名隐私层（Privacy Layer）？例如 TornadoCash 外的隐私协议?

A98（监管提交版）

隐私层包括：

- Zk-Rollup 隐私层
- Obfuscation tools
- Privacy pool
- Unverified smart contracts
- Unknown mixers
- 组合隐私路由（private routing）

检测方法：

1. Token flow opacity 判断
2. Rollup address cluster analysis
3. Contract permission audit
4. Time-based pattern anomaly
5. Multi-hop aggregation detection

禁止交易：

- 所有匿名增强协议（Zero-tolerance）

（由仁港永胜唐生专业整理。）

A98 内部解释版

监管最怕"隐私链上路径"。
必须展示技术识别能力。

Q99. 贵司如何处理 OTC（场外交易）相关 AML 风险?

A99（监管提交版）

OTC 是洗钱高风险区域。

（一）不允许以下 OTC 行为：

- 小额拆分 OTC
- 高风险国家 OTC
- 未经注册 OTC 代理
- 现金 OTC（高风险）

（二）允许在严格条件下的 OTC：

- 必须执行 EDD
- 必须绑定已验证钱包
- 必须提供交易理由
- 必须提供 SOF/SOW
- OTC > 10,000 EUR → 强制 MLRO 审批

（三）链上监控：

- OTC 收款地址必须已验证
- OTC 代理必须身份明确

（由仁港永胜唐生提供专业讲解。）

A99 内部解释版

OTC 是 BaFin 最敏感问题之一，
必须强调限制 + 审查机制。

Q100. 贵司如何监控链上 Token Swap 风险?

A100（监管提交版）

我们监控所有链上 Swap：

（一）主要风险：

- 洗钱（Swap→Bridge→Withdraw）
- Rug Pull
- Fake Token → Legit Token
- Privacy pool swap
- Unverified contract swap

（二）检测机制：

- Token Contract 审查
- Swap path analysis
- High-risk LP 检测
- Multi-hop swap alert

（由仁港永胜唐生专业整理。）

A100 内部解释版

Swap 是可疑行为常见载体，
特别是 scam token → stablecoin。

Q101. 贵司如何监控智能合约风险（Smart Contract Risk）?

A101（监管提交版）

我们对智能合约进行风险评分：

安全检测包含：

- 未验证源代码
- Upgradeable proxy 合约
- Owner privilege（Mint/Blacklist）

- Backdoor code
- Honeypot
- Unauthorized tax function
- Infinite mint 权限
- liquidity lock（流动性锁）是否存在

异常即强制 EDD + MLRO 审查。

（由仁港永胜唐生提供讲解。）

A101 内部解释版

BaFin 要求 CASP 必须理解智能合约风险。
重点在权限（privileges）。

Q102. 贵司是否监控跨链桥风险（Cross-chain Bridge Risk）？

A102（监管提交版）

是，本司对所有跨链桥路径执行链上追踪。

风险来源：

- 匿名桥（Anonymity Bridge）
- 黑客常用跳链路径
- Router 聚合器隐藏跳链
- 多跳 bridge-hop（≥2 次即自动告警）

检测机制：

1. Bridge Risk Tagging
2. Flow mapping（跨链资金路径跟踪）
3. Exposure scoring
4. Multi-chain address clustering

（由仁港永胜唐生专业整理。）

A102 内部解释版

跨链桥是黑客洗钱首选路径。
必须展示对"bridge-hop"监控。

Q103. 贵司如何监控 NFT Wash Trading（刷量）？

A103（监管提交版）

我们识别：

刷量特征：

- A ↔ B 频繁来回交易
- 无经济目的
- 价格异常
- 多钱包控制同一 NFT
- 虚高报价（Spoofing）

控制措施：

- NFT 行为图谱
- TokenID 分析
- LP/Marketplace 记录分析
- 价格轨迹对比

（由仁港永胜唐生提供专业讲解。）

A103 内部解释版

NFT 是高风险资产，特别是刷量洗钱。

Q104. 贵司如何检测"空账户"（Dormant Account）异常激活?

A104（监管提交版）

空账户突然激活是洗钱高风险信号。

风险特征：

- 长期无操作后突然大额入金
- 新设备登录
- 来自高风险地址资金
- 行为模式不一致
- Deposit→Withdraw 快速完成

控制机制：

- 强制 KYC refresh
- 冻结提现
- MLRO 审批
- 高风险时 STR

（由仁港永胜唐生专业整理。）

A104 内部解释版

BaFin 认为"突然激活的 dormant account"是犯罪组织常用技术。

Q105. 贵司如何处理"同一客户控制多个账户"问题?

A105（监管提交版）

本司使用多源比对识别多账户控制：

比对维度：

- IP
- 设备指纹
- 地址簇
- 行为模式
- 银行账户
- 链上地址
- 身份文件 metadata

措施：

- 合并账户
- 追加材料
- 高风险 → 拒绝
- 涉嫌犯罪 → STR

（由仁港永胜唐生提供专业讲解。）

A105 内部解释版

多账户通常代表：

- 逃避限额
- 代理操作
- 恶意行为

Q106. 贵司如何确保 AML 员工的培训与能力？

A106（监管提交版）

我们执行年度 AML 培训计划，包括：

培训内容：

- AMLD6
- GWG
- FATF 风险
- 链上分析
- DeFi 风险
- STR 提交流程
- Fraud typologies

培训方式：

- 内训
- 外部讲师
- 实操演练（Chainalysis / TRM）

考核机制：

- 年度考试
- 案例分析
- 实战模拟

由仁港永胜唐生提供专业讲解。

A106 内部解释版

BaFin 会问："AML 团队是否真正懂区块链？"

Q107. 贵司如何检查供应商（第三方）是否符合 AML 要求？

A107（监管提交版）

本司实施 Vendor AML Due Diligence：

审查内容：

- 许可证
- AML 政策
- GDPR 合规
- 安全架构
- 审计报告（SOC2/ISO）
- 负面新闻

高风险供应商：

- 未受监管
- Offshore + 无监管历史
- 加密相关 PSP
- RiskTag 命中不良集群

（由仁港永胜唐生提供专业讲解。）

A107 内部解释版

供应商也是 AML 风险来源，这是 BaFin 高频问题。

Q108. 贵司是否建立 AML/TF 风险偏好（Risk Appetite Statement）？

A108（监管提交版）

是，本司董事会批准了 AML/TF Risk Appetite：

不容忍（Zero Tolerance）

- 制裁命中
- 匿名工具
- Terrorist Financing
- Ransomware
- 黑客资金

可接受（Limited Exposure）

- 中低风险国家
- 合规交易
- 受监管合作方

限制性容忍（Restricted Exposure）

- 高风险国家（在 EDD 下）
- DeFi 高风险路径

（由仁港永胜唐生拟定。）

A108 内部解释版

Risk Appetite 是董事会层面的要求。
BaFin 会重点看"Zero Tolerance 机制"。

Q109. 贵司如何确保 AML 政策与程序定期更新?

A109（监管提交版）

我们执行年度政策更新机制（Policy Review Cycle）：

更新原因：

- 法规变化（AMLD6、MiCA、GWG）
- 新风险类型
- 新洗钱手法
- 新产品上线

流程：

1. AML 团队起草更新
2. 法务审核
3. CCO/MLRO 审批
4. 董事会批准
5. 全员培训

（由仁港永胜唐生专业整理。）

A109 内部解释版

BaFin 要求 AML 政策"是活的，不是静态的"。

Q110. 请提供 MLRO 对高风险客户的审批机制（包括否决权）。

A110（监管提交版）

MLRO 对高风险客户具有独立审批权：

（一）审批前要求：

- 完整 KYC
- 完整 SOF/SOW
- 链上地址审查
- 行为画像
- 风险评分模型

（二）MLRO 可以：

- 批准
- 拒绝
- 要求更多材料
- 设置交易限制
- 冻结账户

（三）MLRO 的否决权：

> MLRO 的"拒绝开户"决定不可被任何部门推翻，包括 CEO。

符合 **GWG §7 与 BaFin AML Circular**。

（由仁港永胜唐生提供专业讲解。）

A110 内部解释版

这是监管最常问的问题之一：
MLRO 是否独立，有否决权。

Q111. 贵司是否符合欧盟 DORA（数字运营韧性法）要求？如何确保合规？

A111（监管提交版｜BaFin-ready）

本司的 IT 管控体系完全按照 **DORA（EU Regulation 2022/2554）** 建立运营韧性框架。

（一）DORA 五大支柱合规情况

1. **ICT Risk Management（ICT 风险管理）**
   - 完整 ICT 风险识别、评估与缓释流程
   - 定期 ICT 风险报告提交董事会
2. **Incident Classification & Reporting（重大事件分类与上报）**
   - 采用 DORA 事件等级模型：Low / Medium / High / Major
   - High & Major 在 24 小时内向监管机构上报
3. **Digital Operational Resilience Testing（ICT 测试）**
   - 年度渗透测试
   - 基于威胁情报的测试（TLPT）
   - 灾备演练
4. **Third-party ICT Risk（供应商 ICT 风险管理）**
   - Vendor Due Diligence（ISO、SOC2、审计报告）
   - ICT Outsourcing Register（外包登记册）
5. **Information Sharing（威胁情报共享）**
   - 参与 ISAC / CERT 网络
   - 内部威胁通告机制

（二）内部治理结构

- 任命 DORA Officer（ICT 风险负责人）
- IT 安委会（IT Security Committee）
- 每季度向董事会报告

（由仁港永胜唐生拟定并提供专业讲解。）

A111 内部解释版

DORA 是欧盟 2025 年起的硬性要求。
BaFin 会重点问：

- 是否建立韧性测试框架？
- 是否有"重大事件 24 小时上报机制"？

Q112. 贵司是否遵守 BAIT（德国银行业 IT 要求）？关键要点是什么？

A112（监管提交版）

是，我们完全符合 **BAIT（Bankaufsichtliche Anforderungen an die IT）** 的 9 个核心模块：

（一）BAIT 合规模块概述

1. **IT Strategy（IT 战略）**
   - 三年技术规划
   - 安全优先原则
2. **IT Governance（IT 治理）**
   - 明确责任人（CISO / CTO）
   - IT 委员会
3. **Information Security（信息安全）**
   - ISO27001 框架
   - 风险评估
4. **User Access Management（访问管理）**
   - RBAC
   - 最小权限原则
5. **IT Operations（IT 运维）**
   - 补丁管理
   - 配置管理
   - 容灾管理
6. **Change Management（变更管理）**
   - Git 全版本控制
   - PR 审批流程
7. **IT Projects & Development（软件开发）**
   - CI/CD pipeline
   - 安全编码
8. **Outsourcing（外包管理）**
   - 合同审查
   - 风险评估
9. **Data Management（数据治理）**
   - 数据分类
   - 加密
   - 数据主权

（由仁港永胜唐生专业整理。）

A112 内部解释版

BaFin 不仅审查 AML，也审查 IT。
BAIT 是德国银行业 IT 的核心文件，必须熟悉。

Q113. 贵司系统是否进行渗透测试（Penetration Testing）？频率如何?

A113（监管提交版）

是，本司执行年度渗透测试，并符合 DORA 要求的：

- **年度 PenTest（黑盒 + 白盒）**
- **红队测试（Red Team Testing）**
- **TLPT（基于威胁情报的测试）**

（一）PenTest 范围

- API 网关

- Web 前端
- 后端服务
- 数据库
- 钱包系统
- Key Management System
- Cloud Infrastructure

（二）执行方

- 由具备 CREST / OSCP / CISSP 认证的第三方执行
- 并由内部团队复测

（三）修复流程

- CVSS 评分
- 将高风险漏洞在 7 日内修复
- 中风险 30 日修复
- 所有修复需复测

（由仁港永胜唐生提供专业讲解。）

A113 内部解释版

BaFin 最在乎三点：

- 独立第三方
- 计划 + 报告
- 修复时间表（必须明确）

Q114. 贵司是否进行漏洞扫描（Vulnerability Scanning）？使用哪些工具?

A114（监管提交版）

是，本司使用自动化漏洞扫描体系：

（一）扫描工具

- Qualys
- Nessus
- OpenVAS
- Dependency-check（依赖库漏洞检测）
- Trivy（容器漏洞检测）
- Snyk（代码依赖攻击检测）

（二）扫描频率

- 每周一次自动扫描
- 重大变更前强制扫描
- 容器镜像在发布前扫描

（三）报告机制

- CVE 映射
- 批次扫描报告
- 风险评级（CVSS）

（由仁港永胜唐生提供专业讲解。）

A114 内部解释版

渗透测试是"主动攻击"，漏洞扫描是"自动扫描"，两者不同。
监管需要两者同时存在。

Q115. 数据是否加密？数据库、传输、日志是否使用独立密钥?

A115（监管提交版）

本司采用 **多层加密体系**，符合 GDPR、ISO27001、DORA 加密标准。

（一）数据加密措施

1. **存储加密（At-rest Encryption）**
   - AES-256
   - 数据库透明加密（TDE）
2. **传输加密（In-transit Encryption）**
   - TLS 1.3
   - HSTS
   - Certificate Pinning
3. **日志加密（Log Encryption）**
   - 使用独立 Log-Key
   - Log Integrity Hash（SHA-256）

（二）独立密钥管理

- 数据库密钥与应用密钥分离
- Log-key 与 Data-key 隔离
- HSM 管理私钥
- 密钥轮换（每 90 天）

（由仁港永胜唐生提供专业讲解。）

A115 内部解释版

BaFin 重点是"密钥隔离"。
如果日志和数据库使用同一密钥 → 高风险。

Q116. 贵司如何管理密钥（Key Management）？是否使用 HSM?

A116（监管提交版）

是，本司对所有密钥进行专业级管理。

（一）密钥存储

- 使用 HSM（Hardware Security Module）
- FIPS 140-2 Level 3
- 防篡改保护

（二）密钥管理流程

- Key Generation
- Key Backup

- Key Rotation
- Key Retirement
- Key Access Audit

（三）权限管理

- 多方审批（4-eyes principle）
- MLRO 与 CTO 双授权
- Root key 分割存储（Shamir Secret Sharing）

（由仁港永胜唐生专业整理。）

A116 内部解释版

钱包私钥 = 生命线。
不使用 HSM → BaFin 视为重大缺陷。

Q117. 系统访问权限是否遵循 RBAC（基于角色的访问控制）？

A117（监管提交版）

是，本司采用完整 RBAC：

角色结构（示例）

- Admin（不可直接使用，需跳板机）
- Compliance-only
- AML Analyst
- Developer
- Operation Engineer
- Read-only Auditor

控制措施

- 最小权限原则（Least Privilege）
- 禁止共享账户
- 所有高权限操作记录在审计日志中
- 每季度重新验证权限

（由仁港永胜唐生提供专业讲解。）

A117 内部解释版

BaFin 对 RBAC 的要求极高，尤其禁止"共享账户"。

Q118. 是否有 MFA（多因素认证）？应用场景有哪些?

A118（监管提交版）

是，本司对所有关键系统使用 MFA。

（一）MFA 应用场景

1. 后台管理系统
2. 运维系统
3. SCM（源代码管理）
4. 云服务（AWS/GCP/Azure）

5. 高风险交易
6. 关键行为（提现、密钥操作）

（二）MFA 类型

- TOTP
- U2F（FIDO key）
- SMS（备选）

（三）强制策略

- 管理员必须使用硬件密钥（YubiKey）

（由仁港永胜唐生专业整理。）

A118 内部解释版

MFA 是合规的最低要求，但 BaFin 要求：

> “管理端必须使用硬件密钥（如 YubiKey）。”

Q119. 贵司是否采用 Zero Trust（零信任安全）架构?

A119（监管提交版）

是，本司初步采用 Zero Trust 架构，原则如下：

（一）Never Trust, Always Verify

- 所有内部系统需要认证
- 所有 API 调用必须 Token 验证
- 网络位置不构成信任基础

（二）核心组件

- 设备指纹
- 行为分析
- 动态风险评分
- 微分段（Micro-segmentation）

（三）Zero Trust 最终目标

- 内外网统一安全标准
- 最小权限
- 无隐式信任

（由仁港永胜唐生专业整理。）

A119 内部解释版

Zero Trust 是 BaFin 高级评估要求，表明贵司安全成熟度高。

Q120. 贵司是否有审计日志（Audit Log）？可否防篡改?

A120（监管提交版）

是，本司执行防篡改审计机制。

（一）日志范围

- 系统操作
- 权限变更
- 重要业务动作
- AML 相关操作
- 密钥操作
- 审计访问

（二）技术措施

- Append-only（不可修改）
- Hash Signing（SHA-256）
- 日志加密
- 备份至 WORM 存储
- SIEM 系统实时监控

（三）保留时限

- 10 年（符合 GWG）

（由仁港永胜唐生专业整理。）

A120 内部解释版

BaFin 要求：日志必须**可审计、可追溯、不可篡改**。

Q121. 贵司是否具备完善的灾难恢复（Disaster Recovery, DR）机制？RTO/RPO 如何定义？

A121（监管提交版｜BaFin-ready）

是，本司具备完整 DR（灾难恢复）体系，符合 DORA、BAIT、ISO22301 的要求。

（一）DR 目标设定

指标	说明
RTO（恢复时间目标） = 1 小时	关键系统在 1 小时内恢复可用
RPO（恢复点目标） = 5 分钟	数据最大可容忍丢失不超过 5 分钟

（二）DR 技术结构

1. **异地多活（Multi-region Active-active）**
   - 云端多可用区部署
   - 自动故障切换（Failover）
2. **同城 + 异地备份机制**
   - 实时增量备份
   - 每日全量备份
   - 每周冷备份
3. **备份加密**
   - AES-256 at-rest
   - TLS 1.3 in-transit
4. **备份完整性检查**
   - 每日校验
   - 年度恢复演练

（三）年度 DR 演练

- 每年至少 2 次
- 覆盖完整 Failover + Failback 测试
- 结果向董事会报告

（由仁港永胜唐生拟定讲解。）

A121 内部解释版

BaFin 最关注：

- 是否真正测试过切换?
- 是否有 RTO/RPO?
- 数据恢复是否可验证?

Q122. 贵司是否具备业务连续性计划（Business Continuity Plan, BCP）？内容包含什么?

A122（监管提交版）

是，本司拥有完整 BCP（业务连续性计划），符合 ISO22301 与 BaFin MaRisk AT 7.3 要求。

BCP 包含的内容如下：

1. **关键业务识别（BIA）**
   - 交易撮合
   - 托管系统
   - AML 监控系统
2. **应急响应团队结构**
   - BCP Leader
   - IT Lead
   - Compliance Lead
   - Communications Lead
3. **业务恢复优先级**
   - P1：托管系统（30 min）
   - P2：交易系统（1 h）
   - P3：后台系统（4 h）
4. **沟通机制**
   - 客户通知模板
   - 员工通讯机制
   - 监管机构上报计划（24 小时内）
5. **替代场地 / 远程办公能力**
   - VPN + MFA
   - 远程工作预案
6. **年度 BCP 演练**
   - 桌面演练
   - 技术演练
   - 场景演练：网络攻击 / 数据泄露 / 云故障

（由仁港永胜唐生拟定讲解。）

A122 内部解释版

BCP 是战略文件，而 DR 是技术文件。
二者皆需独立存在。

Q123. 贵司是否设有 SOC（Security Operations Center）或等效监控机制?

A123（监管提交版）

是，本司采用 **SOC 2.0 监控体系**，并使用 SIEM 收集与分析日志。

（一）SOC 监控范围

- 网络流量
- 登录/认证行为
- 配置变更
- 云端活动（AWS CloudTrail）
- API 调用
- 钱包交易行为
- AML 监控系统

（二）SIEM 平台

- Splunk / ELK / Wazuh（视最终部署）
- 规则 + ML 异常分析
- L1-L3 分级处理

（三）告警机制

- P1：立即通知 CTO + MLRO
- P2：1 小时内处理
- P3：24 小时内记录处理

（四）7×24 监控

- 内部团队主导
- 第三方安全供应商支持

（由仁港永胜唐生拟定讲解。）

A123 内部解释版

BaFin 要 SOC，不一定要"自建 SOC 中心"，但必须：

- 有 SIEM
- 有事件处理流程
- 有值班制度

Q124. 是否实施防火墙 / WAF / API 网关安全策略?

A124（监管提交版）

是，本司采用三层网络防护策略：

（一）网络防火墙（Network Firewall）

- L3/L4 防护
- 地域封锁（Geo-blocking）
- 黑名单 + 白名单

（二）WAF（Web Application Firewall）

- OWASP Top 10 防护
- SQL 注入防护
- CSRF/XSS 防护
- BOT 防护

（三）API Gateway 安全

- OAuth2 / JWT
- API 频控（Rate Limiting）
- HMAC 签名
- Replay 防护

（由仁港永胜唐生拟定讲解。）

A124 内部解释版

API 安全是 CASP 的核心。
没有 API Rate Limit 是致命风险。

Q125. 是否具备 DDoS 防护？采用哪些策略？

A125（监管提交版）

是，本司采用 DDoS 多层防御体系：

（一）边缘网络防护

- Cloudflare / AWS Shield
- 全球流量清洗

（二）行为识别

- BOT Management
- 异常流量检测

（三）WAF + API 网关联动

- 自动黑名单
- 自动限流

（四）应急响应

- DDoS Playbook（每季度演练一次）
- 与上游 ISP 协调机制

（由仁港永胜唐生提供专业讲解。）

A125 内部解释版

Regulator 想确认：
“是否有能力被 DDoS 攻击后不瘫痪。”

Q126. 云服务部署是否符合 BaFin『云外包指南』（BAIT + EBA Outsourcing Guidelines）？

A126（监管提交版）

是，本司遵从：

- **EBA Outsourcing Guidelines（2021）**
- **BAIT Outsourcing Module**
- **DORA ICT Third-party Requirements**

（一）云上安全配置

分类	措施
身份管理	IAM + MFA + RBAC
网络安全	VPC、子网隔离、防火墙、WAF
数据加密	KMS + HSM
审计与监控	CloudTrail / GuardDuty
配置管理	Terraform / IaC 审批流程

（二）云外包合同（符合 BaFin 要求）

合同包含：

- 数据位置（Data Residency）
- 访问权（Audit Rights）
- 退出策略（Exit Plan）
- SLA（可用性 ≥ 99.9%）

（由仁港永胜唐生拟定讲解。）

A126 内部解释版

BaFin 云外包关注三点：

1. 监管机构必须有访问权
2. 数据必须可迁移
3. 退出策略必须可执行

Q127. 是否执行变更管理（Change Management）流程?

A127（监管提交版）

是，本司遵循 **ITIL Change Management 标准**。

变更管理流程：

1. **创建变更请求（CR）**
2. **风险评估**
3. **审批（4-eyes）**
4. **测试环境验证**
5. **部署计划制定**
6. **变更窗口执行**
7. **回滚机制准备**
8. **变更后监控（Post-change Review）**

版本控制

- Git 全流程
- 强制 PR
- Code Review 必须 ≥ 2 人

紧急变更（Emergency Change）

- 需 CTO + MLRO 双签
- 事后补充文档

（由仁港永胜唐生专业整理。）

A127 内部解释版

BaFin 会问：
"你能证明每一次部署都有审计踪迹吗？"

Q128. 贵司是否采用 DevSecOps？如何在开发流程中加入安全？

A128（监管提交版）

是，本司采用 **DevSecOps 安全开发生命周期（SDLC）**。

（一）开发前安全（Shift-left Security）

- Threat Modeling（威胁建模）
- 安全需求审查

（二）开发中安全

- 静态分析（SAST）
- 依赖库检测（SCA）
- Secret Detection（密钥扫描）

（三）发布前安全

- 动态分析（DAST）
- 容器镜像扫描（Trivy）
- API 安全测试

（四）发布后安全

- 实时监控（SIEM）
- 安全补丁管理
- 回滚机制

（由仁港永胜唐生提供专业讲解。）

A128 内部解释版

MiCA + BaFin 强调：

> "安全必须嵌入开发每一个步骤，不得依赖最终测试。"

Q129. 是否具备配置管理体系（Configuration Management）？

A129（监管提交版）

是，本司采用 **Infrastructure as Code（IaC）** 管理基础架构。

（一）配置标准化工具

- Terraform
- Ansible
- Helm（Kubernetes 部署）

（二）配置监控

- 检测配置漂移
- 自动对账（Drift Detection）

（三）配置审批流程

- 每项配置变更必须走 CR 流程
- 新配置必须通过安全审查

（由仁港永胜唐生拟定讲解。）

A129 内部解释版

IaC = 可追溯性 + 合规性。
符合 BaFin 必须要点。

Q130. 机密信息是否遵循 Data Classification 数据分类制度管理?

A130（监管提交版）

是，本司具备完整的数据分类体系：

数据分级（四级）

等级	内容示例	措施
Restricted（高度敏感）	私钥、客户 KYC	HSM、访问仅 2 人、加密存储
Confidential（机密）	交易记录、内部政策	加密、权限控制
Internal（内部）	部门文档	RBAC、MFA
Public（公开）	官网文档	无需保护

数据生命周期管理

- 采集
- 存储
- 传输
- 使用
- 归档
- 清除

（由仁港永胜唐生专业整理。）

A130 内部解释版

BaFin 注重"数据分类"是否链接到：

- 访问权限
- 加密强度
- 数据处理流程

Q131. 系统是否记录所有关键操作？是否具备审计追踪能力？

A131（监管提交版）

是，所有关键行为均记录于中央审计日志：

审计范围

- 登录
- 权限变更
- 钱包操作
- API 调用
- 配置变更
- AML 操作
- 系统重启/部署

技术特性

- 不可删除
- Hash 链保护
- 加密存储
- 10 年保留

（由仁港永胜唐生拟定讲解。）

A131 内部解释版

审计日志是监管核心要求。
任何"不可追踪"行为 = 直接拒牌。

Q132. 系统是否支持『四眼原则（4-eyes principle）』执行关键操作？

A132（监管提交版）

是，所有关键操作均须 "双审批 / 双签"：

适用关键操作包括：

- 权限提升
- DR 切换
- 钱包私钥操作
- 大额交易处理
- AML 冻结/解冻
- 撤单
- 资金划拨

技术设计

- 审批必须由不同人员
- Approval Log 永久记录
- 不可由同一设备发起

（由仁港永胜唐生提供专业讲解。）

A132 内部解释版

四眼原则是 BaFin 核心概念之一。
嘴上说不行，必须"系统级执行"。

Q133. 是否有密码强度要求？是否定期强制轮换？

A133（监管提交版）

是，本司执行 NIST + BaFin 标准的密码策略：

密码策略

- 最少 12 位
- 必须混合大小写 / 数字 / 特殊字符
- 禁止 1000+ 常见弱口令
- 登录错误 5 次锁定

密码轮换

- 90 天强制更新
- MFA 必达成

（由仁港永胜唐生拟定讲解。）

A133 内部解释版

简单单一密码 → 监管直接否定系统安全性。

Q134. 是否有远程访问限制？如何确保远程访问安全？

A134（监管提交版）

是，本司限制远程访问，使用下列措施：

访问要求

- 必需 VPN + MFA
- 禁止公共 WiFi
- 强制设备合规检查（Device Compliance Check）
- IP 白名单

远程桌面安全

- 记录所有会话
- 自动断线
- 文件传输限制

（由仁港永胜唐生拟定讲解。）

A134 内部解释版

远程访问是攻击面，监管看得非常严。

Q135. 是否实施补丁管理（Patch Management）？频率如何?

A135（监管提交版）

是，补丁管理符合 BAIT 与 DORA 要求。

补丁分类与时限

补丁等级	修复期限
Critical	48 小时
High	7 天
Medium	30 天
Low	90 天

监控机制

- 自动检测（AWS Inspector 等）
- 手动审核与测试流程

（由仁港永胜唐生拟定讲解。）

A135 内部解释版

监管关注关键问题：

> “你们多久更新一次安全补丁？”

Q136. 是否有安全事件响应机制（Incident Response Plan）？

A136（监管提交版）

是，本司具备完整 IRP（事件响应计划）。

事件响应步骤

1. 检测（Detection）
2. 分级（Classification）
3. 控制（Containment）
4. 根因分析（Root Cause Analysis）
5. 修复（Remediation）
6. 恢复（Recovery）
7. 向 BaFin 报告（24 小时内）

事件等级

- Severity 1（需立即上报）
- Severity 2（工作日内处理）
- Severity 3（记录）

（由仁港永胜唐生专业整理。）

A136 内部解释版

BaFin规定：重大事件必须 24 小时内上报。

Q137. 是否进行网络分段（Network Segmentation）？如何防止横向移动攻击？

A137（监管提交版）

是，本司采用 Zero Trust + 微分段策略：

网络分段结构：

- Public Zone
- Application Zone
- Database Zone
- Admin Zone
- Wallet Vault Zone（隔离最高级）

防横向移动措施：

- 东西向流量监控
- 跳板机隔离
- 禁止跨区访问
- 应用防火墙

（由仁港永胜唐生拟定讲解。）

A137 内部解释版

网络必须"分层"，一个漏洞不至于全系统被入侵。

Q138. 私钥与交易签名系统是否隔离？

A138（监管提交版）

是，本司采用双系统架构：

（一）Vault（私钥系统）

- HSM 存储
- 无网络访问
- 多人签署（MPC / M-of-N）

（二）交易系统（Transaction System）

- 仅发送签名请求
- 无法接触私钥

（三）操作流程

- 所有签名记录进入 Audit Log
- 所有审批必须双签

（由仁港永胜唐生拟定讲解。）

A138 内部解释版

BaFin：
"私钥绝不能出现在普通服务器上。"

Q139. 是否使用 MPC（多方计算）技术或 HSM 防止单点私钥风险?

A139（监管提交版）

是，我们采用：

- HSM（FIPS 140-2 Level 3）
- Multi-party Computation（MPC，2-of-3）

MPC 安全优势

- 无单点私钥
- 签名由多个碎片共同完成
- 杜绝内部单人风险

应用范围

- 客户资产
- 自有资产
- 大额交易

（由仁港永胜唐生拟定。）

A139 内部解释版

BaFin 对 Crypto Custody 的关键问题：

> “单点私钥 = 不合规。”

Q140. 是否有提现（Withdrawal）风控与审核机制?

A140（监管提交版）

是，本司提现机制采用三级控制：

（一）行为风控

- IP 指纹
- 设备指纹
- 交易行为匹配

（二）额度限制

- 日限额
- 单笔限额
- 高风险提现需 MLRO 审批

（三）延时提现机制（Anti-Fraud Delay）

- 大额提现 T+1 审核
- 黑名单地址禁止提现

（由　仁港永胜唐生拟定讲解。）

A140 内部解释版

提现安全漏洞 = 直接拒牌。

Q141. 是否具备反欺诈系统（Fraud Detection）？

A141（监管提交版）

是，本司使用：

- 规则引擎（Rule Engine）
- 机器学习模型（ML-based Fraud Detection）
- 异常行为监控

主要识别项：

- 设备切换
- 异地登录
- 交易异常
- 大额提币
- 高频 API 调用

（由仁港永胜唐生提供讲解。）

A141 内部解释版

Fraud → AML → 监管 3 大重点之一。

Q142. 是否有对内部员工的权限滥用监控?

A142（监管提交版）

是，本司具备 IAM + UEBA（User & Entity Behavior Analytics）。

监控内容：

- 超范围查询
- 越权操作
- 非常规时间段访问
- 系统后台滥用行为

（由仁港永胜唐生拟定。）

A142 内部解释版

监管非常怕"内部腐败 / 内鬼"。

Q143. 是否使用密钥分割与恢复机制?

A143（监管提交版）

是，本司采用：

- Shamir Secret Sharing（3-of-5）
- 分割密钥存储在不同地点
- 恢复需双签

（由仁港永胜唐生提供讲解。）

A143 内部解释版

密钥必须具备"可恢复而不可滥用"特性。

Q144. 是否对关键系统执行定期访问审查（Access Review）？

A144（监管提交版）

是，每季度进行一次访问审查：

- 无使用权限在 90 天内自动移除
- 不活跃账户自动冻结
- 审查报告提交至董事会

（由仁港永胜唐生拟定讲解。）

A144 内部解释版

BaFin 必问：
"离职员工账户多久被关闭？"

Q145. 数据是否具备脱敏（Masking）机制?

A145（监管提交版）

是，客户数据遵循 GDPR + Data Masking：

应用场景：

- 测试环境 → 必须脱敏
- 用户展示 → 部分脱敏（如邮箱）
- 报表 → hash 化

（由仁港永胜唐生专业整理。）

A145 内部解释版

监管不允许在测试环境使用真实个人信息。

Q146. 是否限制生产环境访问?

A146（监管提交版）

是，生产环境严格限制：

- 仅允许 5 名核心人员访问
- 需 CTO + Compliance 双批准
- 登录必须跳板机 + MFA
- 所有操作录音录像

（由仁港永胜唐生拟定。）

A146 内部解释版

生产环境 = 最核心区
监管必须看到严格访问限制。

Q147. 是否使用安全编码标准（OWASP / CERT）？

A147（监管提交版）

是，本司执行 OWASP 安全编码指南。

安全编码要求：

- Input Validation
- Output Encoding
- SQL Injection Prevention
- XSS / CSRF 防护
- Secrets 不得写入代码库

（由仁港永胜唐生提供讲解。）

A147 内部解释版

安全编码是 DevSecOps 的基础。

Q148. 是否记录所有 API 调用操作？可否审计？

A148（监管提交版）

是，所有 API 调用均记录于：

- API Gateway Log
- SIEM
- Immutable Audit Log

内容包括：

- 调用人
- 调用 IP
- 请求参数（敏感信息脱敏）
- 响应码
- 失败/异常信息

（由仁港永胜唐生拟定。）

A148 内部解释版

API = 攻击入口
API 日志 = 监管必查要点。

Q149. 是否建立代码审查（Code Review）机制？

A149（监管提交版）

是：

- 所有 PR 必须至少两人审核
- 高风险代码需安全团队复核

- 自动化代码扫描（SAST）
- 不得直接推送至主分支

（由仁港永胜唐生拟定。）

A149 内部解释版

BaFin 注重：
CI/CD 流程必须有"人工审核"步骤。

Q150. 是否具备供应链安全管理（Software Supply Chain Security）？

A150（监管提交版）

是，本司供应链安全采用：

（一）SCA（Software Composition Analysis）

- 检测第三方依赖漏洞
- 自动阻断高危依赖库

（二）Artifact Signing（制品签名）

- 所有容器镜像必须签名
- 仅允许已签名镜像上线

（三）供应商尽调

- ISO27001
- SOC2 Type II
- 历史安全事件记录
- 退出机制（Exit Plan）

（由仁港永胜唐生拟定讲解。）

A150 内部解释版

供应链攻击（如 Log4j）是监管特别关注的重大风险。

Q151. 请说明贵司整体的客户资产保全（Safeguarding）框架及适用法律基础?

A151（监管提交版｜BaFin-ready）

本公司已建立完整的客户资产保全（Safeguarding）框架，法律基础包括：

1. **MiCA 相关条文**
   - MiCA Title V：Crypto-Asset Service Providers（CASPs）
   - 客户资产隔离、资产返还义务、信息披露义务等条文。
2. **德国本地法律及 BaFin 行为规则**
   - 德国民法典（BGB）中关于信托/委托关系的一般原则
   - BaFin 对 Crypto Custody / Investment Services 的行政实践、通函及 FAQ
   - BAIT / MaRisk 中关于资产保护与运营风险控制的要求。
3. **公司内部 Safeguarding Policy**
   - 由董事会批准，为一级政策文件
   - 适用于所有虚拟资产及法币客户资产

- 明确：
  - 资产归属（客户 vs 自有）
  - 隔离方式（on-chain + off-chain）
  - 账簿与对账机制
  - 破产隔离（Insolvency Remoteness）安排
  - 资产返还优先级（Wind-down / Exit Plan）

在实际执行上，本公司 Safeguarding 体系基于"三层结构"：

- **法律层面**：合同条款 + 客户协议明确资产归属与信托性质
- **账簿层面**：客户子账户分账 + 与自有资产分账
- **技术层面**：钱包与银行账户隔离，权限严格拆分，支持可验证对账

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这一题是"总纲"。关键是让 BaFin 看出你：

- 知道 MiCA + 德国本地法的法律基础
- 把 Safeguarding 当成独立政策来做，而不是混在 AML 或 IT 里

Q152. 客户虚拟资产与公司自有虚拟资产如何在链上实现隔离？

A152（监管提交版）

本公司在链上资产隔离方面实施以下措施：

1. **钱包架构层面**
   - 客户资产使用 **"客户资产专用钱包集群（Client Asset Wallet Cluster）"**
   - 公司自有资金使用 **"自有资产钱包集群（House Wallet Cluster）"**
   - 两类钱包在：
     - 地址分配
     - 标签系统
     - 权限控制
       上完全隔离。
2. **地址标记与分段**
   - 每一位客户对应至少一个独立的逻辑地址区段（Virtual Sub-account），
     由钱包系统精确记录"地址 → 客户 → 币种 → 余额"映射。
   - 客户资产地址不会与公司自有资产使用同一 address pool。
3. **账簿映射与对账**
   - On-chain 地址余额与内部 Ledger 中的客户余额逐日对账
   - 若发现链上余额与客户账本存在差异，自动触发 Safeguarding Incident。
4. **访问权限与操作限制**
   - 管理公司自有资产的钱包与管理客户资产的钱包由不同团队、不同角色负责
   - 系统级全程强制执行"四眼原则 + 审计日志 + MPC 多方控制"。

结论：在任何时候，均可通过链上地址、内部账簿和钱包标签证明客户资产独立于公司自有资产，不会被挪用。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 关注两点：

- "你能不能清楚地点出哪些是客户的钱？"
- "技术与账簿上能不能对应和证明？"

Q153. 客户法币资金如何与公司自有资金隔离？是否采用分离账户（Segregated Accounts）？

A153（监管提交版）

是的，本公司为客户法币资金设置了完全隔离的 **Segregated Client Accounts**：

1. **账户结构**
   - **Client Money Account（客户资金账户）**：
     - 用于客户充值、提现、结算
     - 银行合同与内部政策中明确为"信托性质 / 代管性质"的客户资产账户
   - **House Account（公司自有资金账户）**：
     - 用于支付公司运营成本、供应商费用、薪酬等
2. **银行协议条款**
   - 与合作银行签订了明确的 **Client Asset/Segregated Account 约定**
   - 银行账户名称中标明"Client"或类似标识，以便清晰识别
3. **账簿与对账机制**
   - 内部 Ledger "客户余额总和" 与 银行 Client Money Account 余额每日对账
   - 任何差异均会触发调查与 Safeguarding Incident 流程
4. **禁止混用/挪用**
   - 公司运营开支只能从 House Account 支付，系统上禁止从 Client Money Account 直接支付

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题本质是在考你 **"CASS / Client Money" 思维**。
重点：单独账户 + 银行合同 + 对账 + 禁止混用。

Q154. 贵司是否允许将客户资产与其他客户资产共管（Omnibus），如何控制风险？

A154（监管提交版）

本公司对客户资产采用 **"客户独立账本 + 钱包/账户按风险分层的 Omnibus 管理"** 模式：

1. **账本层面**
   - 每一位客户：
     - 独立子账户
     - 独立计价
     - 单独可视化报表
2. **技术层面（钱包及银行账户）**
   - 在满足安全与效率的前提下，可对多名客户资产进行"同池管理（Omnibus）"：
     - 如同一币种托管钱包或同一 Client Money Account
   - 但在账簿系统中清晰区分各客户的份额，不存在所有权混同。
3. **风险控制**
   - 任何时点，Omnibus 钱包/账户余额 >= 全部客户对该池应有权益总和
   - 冷/热钱包策略确保安全
   - 若发生单一客户风险，不影响其他客户的资产计价与返还权利。
4. **信息披露**
   - 在客户协议与风险披露文件中明确说明：
     - 资产可能以 Omnibus 模式托管
     - 但所有权及返还权按个人账本而非集合池进行计量。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 不禁止 Omnibus，但重点是：

- 账本里要"独立"
- 任何时点都能算出每个客户的准确份额

Q155. 若贵司发生破产（Insolvency），如何确保客户资产法律上不被列入破产财产？

A155（监管提交版）

本公司通过 **法律 + 合同 + 运营 + 技术** 多重设计，确保客户资产在我们破产时仍保持"破产隔离（Insolvency Remoteness）"：

1. **法律结构**
   - 客户资产在合同中明确为：
     - 委托保管资产 / 信托性质资产（根据法律意见书确定具体法律概念）
   - 不属于公司自有财产范围
2. **合同条款**
   - 客户协议中明确：
     - 公司对客户资产仅享有管理权，不享有所有权
     - 公司不得将客户资产用于自身债务清偿
3. **破产场景下资产返还机制**
   - Wind-down Plan 中已设计：
     - 指定破产管理人须优先协助客户提取资产
     - 在清偿公司债权人前完成客户资产返还
4. **法律意见书（Legal Opinion）**
   - 由德国律师事务所出具
   - 明确在破产法框架下客户资产不应被列为破产财产

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这一题必须体现：

- 已经找律师出过 Legal Opinion
- 有明确的破产隔离结构

Q156. 贵司如何进行客户资产的日常对账（Reconciliation）？频率和流程如何？

A156（监管提交版）

本公司实施"双层对账机制"：

1. **链上/银行余额 vs 内部账簿对账（External vs Internal）**
   - 每日（T+1）自动对账
   - 范围：
     - 客户虚拟资产：各公链地址余额 vs Ledger
     - 客户法币：Client Money Account 余额 vs 客户余额总和
2. **内部子账户对账（Internal Reconciliation）**
   - 按客户、按币种、按业务类型进行交叉核对
   - 检查异常余额、负值余额与长时间不动账户
3. **差异处理机制**
   - 差异分类：
     - Timing Difference（时间差）

        - Operation Error（操作错误）
        - System Bug（系统错误）
    - 严重差异立即按 Safeguarding Incident 流程升级至 CRO/MLRO/CTO
4. **对账记录与审计**
    - 所有对账日志保留至少 10 年
    - 内部审计每年至少抽查两次

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

对账是监管一定会细问的点。
答复里要有：**频率 + 机制 + 差异处理**。

Q157. 若对账发现资产缺口（Shortfall），贵司如何处理？是否由自有资金立即补足？

A157（监管提交版）

是的，如果发现客户资产出现"实质性缺口（Shortfall）"，本公司将：

1. **立即启动 Incident Response**
    - 冻结相关钱包/账户操作
    - 进行原因调查（系统/操作/欺诈等）
2. **由公司自有资金立即补足**
    - 若确认缺口由公司运营、系统或管理原因造成，本公司将使用自有资金立即补足客户池中资产，使其恢复至全额覆盖状态。
3. **向监管与审计机构报告**
    - 若缺口达到重大事件标准，将按照 DORA + BaFin 报告要求进行上报
4. **客户告知与补偿政策**
    - 若缺口造成客户损失，将按照事先约定的补偿机制执行赔付

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 想听到的关键词是：

> "公司自有资金补足缺口。"

Q158. 贵司是否会将客户法币或虚拟资产用于自营或第三方融资？是否允许 Rehypothecation?

A158（监管提交版）

不会。本公司明确禁止对客户资产进行任何形式的 **Rehypothecation（再质押）** 或用于本公司及第三方的融资/担保。

1. **客户协议条款**
    - 明确约定：客户资产只用于执行客户指令，不得用作自营交易或为公司/他人提供担保
2. **内部控制**
    - 系统层面禁止将 Client Money Account 与 House Account 互相划拨用于自营
    - 钱包控制策略中禁止将客户资产转往自营钱包
3. **例外情况**
    - 如未来涉及经 MiCA 明确允许、且客户书面同意的 DeFi/staking 等业务，将单独披露并取得客户明示同意

目前版本中，客户资产仅用于：

- 客户指令交易执行
- 法律与监管允许的清算及必要操作

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

一句话：
"不 Rehypothecate，不拿客户钱去玩金融工程。"

Q159. 是否会向客户支付法币或虚拟资产的利息？若有，收益与风险如何处理？

A159（监管提交版）

当前版本中，本公司 **不向客户支付利息**，也不将客户资产参与任何生息业务。
如未来推出收益型产品，将遵循以下原则：

1. 完全独立于"基础托管"服务
2. 客户需单独签署同意
3. 明确风险与资产使用方式（例如借贷、质押、流动性提供等）
4. 收益分配规则透明，且不会影响客户基础托管资产安全

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

如果不用利息模式，监管会觉得更"干净、安全"。
如做收益类业务，必须剥离托管层。

Q160. 若客户账户出现负余额（Negative Balance），如何处理？是否影响其他客户资产？

A160（监管提交版）

1. **负余额形成机制限制**
   - 一般情况下不允许客户发生透支行为
   - 严格预扣/保证金机制避免出现负余额
2. **如因系统/价格波动造成负余额**
   - 负余额仅记录在该客户个人账户
   - 不得通过动用其他客户资产来填补
3. **追偿措施**
   - 按客户协议，要求客户补足资金
   - 必要时采取法律途径
4. **风险控制声明**
   - 负余额风险由本公司与相关客户在合同框架内解决，不得影响任意其他客户资产安全与完整性

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管要听到的是：
"负值风险是个别问题，不会传染给所有人。"

Q161. 贵司如何选择托管银行或第三方金融机构以承载 Client Money Account？

A161（监管提交版）

本公司按照书面 **Bank/Financial Institution Selection Policy** 选择托管银行和金融机构，标准包括：

1. **监管地与牌照情况**
   - 优先选择欧盟/EEA 内受本地央行或金融监管机构监管的银行或电子货币机构
2. **信用评级**

- 参考国际评级机构（S&P、Moody's、Fitch）
- 一般要求在投资级（Investment Grade）以上

3. **财务稳健性**
   - 资本充足率
   - 不良贷款率
   - 最近三年财报表现
4. **运营和技术能力**
   - 支持 Segregated Accounts
   - 支持高频对账
   - 有完备的 BCP / DRP
5. **法律与合同条款审查**
   - 确保银行合同中明确标注 Client Account 性质

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

银行选择不能随便，最好体现"尽调 + 标准"。

Q162. 是否对托管银行/金融机构进行持续尽职调查（Ongoing Due Diligence）？

A162（监管提交版）

是，本公司每年至少一次对托管金融机构进行 **Ongoing Due Diligence**：

1. 财务状况更新审核
2. 监管处罚记录
3. 运营中断或重大事件记录
4. 合同条款变更情况
5. 是否发生并购或股权重大变动

一旦发现其信用质量或运营能力显著恶化，将启动更换托管机构的 Exit Plan。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题核心是在讲：
"我们不会把客户钱一直放在一家已经明显不安全的机构里。"

Q163. 贵司是否进行客户资产流动性压力测试（Liquidity Stress Test）？

A163（监管提交版）

是，本公司至少每季度进行一次 **流动性压力测试**，内容包括：

1. 场景假设
   - 30% 客户在一天内集中提现
   - 某主流币种突发价格大幅波动
   - 某合作银行技术故障
2. 测试目标
   - 验证：在上述压力下，仍具备按时履行提现与返还义务的能力
3. 对应措施
   - 如测试发现瓶颈，将调整：
     - 热冷钱包比例
     - 银行和托管机构数量
     - 内部预留流动性

测试结果报告提交风险委员会与董事会审批。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Safeguarding 不只是"保管"，还有"可取回能力"。
压力测试就是证明这一点。

Q164. 客户资产是否受到第三方保险或担保机制保护？如有，请说明。

A164（监管提交版）

本公司目前采取的风险缓释措施包括：

1. **专业保险**
   - Cyber Insurance（网络攻击保险）
   - Crime Insurance（员工舞弊、盗窃相关）
   - 若业务规模扩大，将进一步考虑专门的 Crypto Custody Insurance。
2. **自有资金 Buffer**
   - 设立内部"风险准备金"，用于保障在某些运营事件下对客户进行快速赔付。

目前我们不会以"存款保险"方式向客户宣传该安排，仅在风险披露文件中如实说明保险覆盖范围与限制。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

不要用"银行存款保险"类措辞误导客户。
保险是加分项，但不能夸大。

Q165. 贵司如何向客户清晰披露 Safeguarding 机制及其限制?

A165（监管提交版）

本公司通过多种方式进行客户披露：

1. **客户协议与风险披露文件**
   - 独立章节说明：
     - 客户资产与公司资产隔离原则
     - Omnibus 托管的可能
     - 不参与 Rehypothecation
     - 破产隔离安排
     - 保险与不受保护的范围
2. **官网合规专栏**
   - 以易懂语言解释 Safeguarding 模型
3. **重大变更通知**
   - 如 Safeguarding 结构发生重大变更，将提前通过邮件、站内信等通知客户

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 特别重视 **"信息透明"**。
Safeguarding 不只是"你做了什么"，还包含"客户知道你做了什么"。

Q166. 如何处理长期不动账户（Dormant Accounts）的客户资产?

A166（监管提交版）

本公司对 Dormant Accounts 设有专门政策：

1. **判定标准**
   - 连续 24 个月无登录/交易/指令，即视为 Dormant
2. **处理机制**
   - 保留客户资产
   - 不会擅自处置或挪用
   - 增强访问控制，防止被盗用
   - 尝试通过注册邮箱/电话联系客户
3. **法律/监管要求**
   - 如德国或其他适用司法辖区对 Dormant 资产另有规定，将依照相关法律执行

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Dormant 不能因为"没人管"就去动它。
同时要加强安全防护，防止被盗用。

Q167. 如果因司法命令或监管指示需要冻结特定客户资产，贵司如何执行?

A167（监管提交版）

1. **冻结流程**
   - 收到正式司法/监管文书后，由合规部门与 MLRO 共同确认
   - 在系统中对相关客户账户进行冻结：
     - 禁止提现
     - 禁止转出
     - 禁止变现
2. **资产状态**
   - 冻结期间仍视为该客户资产
   - 本公司不得擅自挪用或再处分
3. **记录与报告**
   - 全程保留操作与沟通记录
   - 视情形向 BaFin 和其他相关监管机构汇报

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

核心点：
"冻结 != 变成公司资产"。

Q168. 贵司如何记录和保存与 Safeguarding 相关的全部资料与操作记录?

A168（监管提交版）

本公司设有 **Safeguarding Recordkeeping Policy**，主要包括：

1. **记录范围**
   - 客户资金/资产变动记录
   - 对账记录
   - 差异处理与调查记录
   - 银行及托管机构对账单
   - 客户投诉与补偿记录
   - 风险评估与压力测试报告

2. **保管期限**
    - 一般不少于 10 年，符合德国商业法与监管要求
3. **存储方式**
    - 加密存储
    - 访问权限受控
    - 保证可检索性与不可篡改性

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

记录保存是未来 On-site Inspection 的证据基础。

Q169. 内部审计是否覆盖 Safeguarding 制度？频率如何？

A169（监管提交版）

是，本公司内部审计职能（Internal Audit）将 Safeguarding 作为重点审计范围之一：

1. **审计频率**
    - 至少每 12 个月一次
    - 重大制度变更后进行专项审计
2. **审计内容**
    - 资产隔离执行情况
    - 对账与差异处理流程
    - Incident 与补偿案例
    - 银行托管风险管理
3. **审计报告**
    - 报告提交董事会审计委员会
    - 必要时向监管机构提供

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Safeguarding 一般会被 BaFin 要求"必须纳入内审计划"。

Q170. 外部审计或第三方是否会对贵司 Safeguarding 安排进行独立评估？

A170（监管提交版）

是，本公司计划与具有金融/加密资产经验的审计机构合作，对以下内容进行年度或定期外部评估：

1. 客户资产隔离实施效果
2. 对账流程与差异处理
3. 破产隔离法律结构（配合法律顾问）
4. 信息披露是否真实、完整

相关报告将在必要时提供给 BaFin 以供审查。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

外部审计是一个很好的"加分项"，能提升 BaFin 信心。

Q171. 集团结构中是否存在跨实体持有客户资产的情形？如何保持清晰界定与隔离？

A171（监管提交版）

1. **基本原则**
   - 客户资产仅由持牌 CASP 主体名义下管理
   - 集团其他实体不得直接拥有客户资产所有权
2. **如需跨实体配合（例如结算或技术外包）**
   - 仅以服务协议方式参与
   - 不转移客户资产所有权
   - 对资金流转设置清晰路径与账簿记录
3. **集团内部交易**
   - 任何集团公司间资金/资产流转不得动用客户资产

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 很警惕集团结构下"客户资产被上划/下划"的风险。

Q172. 贵司在 Wind-down Plan 中对客户资产返还流程有何具体安排？

A172（监管提交版）

Wind-down Plan 中，客户资产返还是第一优先级：

1. **触发条件**
   - 主动业务终止
   - 监管要求
   - 不可持续经营
2. **返还步骤**
   - 冻结新增开户及交易
   - 通知客户提交提现指令
   - 设定截止日期
   - 未提取部分采取合适法律机制（如委托第三方托管）
3. **沟通与披露**
   - 多渠道通知（邮件、站内信、公告）
   - 明确时间表与操作方式
4. **监管配合**
   - 将返还流程与进度向 BaFin 报告

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Wind-down Plan 若没写"客户资产如何退"，基本会被打回来。

Q173. 若托管方（银行或加密托管供应商）自身发生风险事件，贵司如何保障客户资产安全？

A173（监管提交版）

1. **前置措施**
   - 严格尽调
   - 选择多家托管供应商进行分散
2. **事中措施**
   - 一旦获悉其重大风险或破产迹象，立即启动：

- 资产转移计划（迁移至其他托管方）
- 风险评估与客户信息披露

3. **合同安排**
   - 合同中设有明确 Exit Plan 条款
   - 保障在其风险状态下，本公司有权迅速迁移客户资产

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 想看的是：
"如果你的托管方出事，客户资产不会一起沉船。"

Q174. 客户资产相关的投诉（例如"资产丢失"、"无法提币"），贵司如何处理?

A174（监管提交版）

1. **Complaint Handling Policy**
   - 设有专门的投诉处理政策
   - 明确响应时限与责任人
2. **程序**
   - 收到投诉 → 记录并出具确认
   - 启动调查（技术 + 运营 + 合规联合）
   - 在合理时限内给予书面答复
   - 如属本公司责任，将进行补偿或修复
3. **统计与改进**
   - 对与 Safeguarding 相关的投诉进行分类统计
   - 提交风险委员会与董事会审阅

如投诉涉及潜在重大事件，将按 DORA 和 BaFin 要求进行上报。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

客户投诉是"真实风险暴露点"，监管会重点关注。

Q175. 贵司是否设立与 Safeguarding 相关的 KRI（关键风险指标）？有哪些具体指标?

A175（监管提交版）

是，本公司设置了多项 Safeguarding KRI，包括但不限于：

- 对账差异发生频次
- 对账差异金额占客户资产总额比例
- 客户资产相关投诉数量
- Incident 数量与严重程度
- 托管机构服务中断次数
- 流动性压力测试失败率

上述 KRI 定期汇总至风险委员会，并若超出 Risk Appetite，将触发整改行动。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

KRI 是把 Safeguarding 量化、可监控化的工具。

Q176. 员工培训中是否包含 Safeguarding 内容？频率如何?

A176（监管提交版）

是，本公司设有 **Safeguarding Training Module**：

1. **覆盖对象**
   - 所有前线、运营、合规、技术及高管人员
2. **培训频率**
   - 入职必修
   - 每年一次复训
   - 重大制度变更时进行专项培训
3. **培训内容**
   - 客户资产 vs 公司资产区别
   - 资产隔离制度与操作
   - Incident 报告流程
   - 客户沟通与风险披露

培训记录与通过情况均留档备查。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管会问："员工真的理解 Safeguarding 吗？"
培训就是最直接的证明方式。

Q177. 与 Safeguarding 相关的制度多久审查一次？由谁负责？

A177（监管提交版）

Safeguarding Policy 至少每 12 个月进行一次全面审查，或在以下情形发生时进行提前审查：

- 监管规则重大调整
- 业务模式改变（例如新增借贷/质押业务）
- 发生重大 Incident

审查流程：

- 由合规部与风险管理部主导
- 业务、技术、法务参与评审
- 提交董事会最终审批

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Safeguarding 不是一劳永逸的文件，必须"常更新"。

Q178. Safeguarding 安排是否经过独立法律审查？是否有书面法律意见？

A178（监管提交版）

是，本公司已委托具有德国监管与金融法经验的律师事务所，对以下内容出具了书面 Legal Opinion：

- 客户资产法律性质（ownership/信托/代管等）
- 破产隔离（Insolvency Remoteness）
- 客户协议中的资产归属条款
- 与托管银行/第三方的合同安排对客户资产权益的影响

该 Legal Opinion 将在 BaFin 要求时提供以供审查。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

"没有律师意见"是德国申请的一大减分项。
这一题一定要体现"已做"。

Q179. 贵司是否区分零售客户与专业客户在 Safeguarding 上的保护程度?

A179（监管提交版）

是，本公司在 Safeguarding 设计时采取 **"零售不弱于专业"** 原则：

1. **基础 Safeguarding 标准**
   - 对所有客户一视同仁，均提供完整资产隔离与返还权
2. **附加机制**
   - 对零售客户，额外强化：
     - 信息披露清晰度
     - 投诉渠道便捷性
     - 风险提示频次
3. **仅在契约结构上可能有所区别**
   - 专业客户如有特殊需求，可能在合同中约定不同的业务组合（如质押/借贷），但不会降低基本 Safeguarding 标准。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管希望看到：
"零售客户是被重点保护对象"。

Q180. 贵司如何处理因协议更新导致的 Safeguarding 条款变更？客户如何知情与接受?

A180（监管提交版）

1. **变更审批**
   - 所有涉及 Safeguarding 的条款更新需经合规/法务审查及董事会批准
2. **客户通知**
   - 通过邮件、站内消息、官网公告等方式提前通知
   - 充分给予客户时间阅读与决定是否继续使用服务
3. **客户接受机制**
   - 客户需在下次登录或下单前在线确认
   - 若客户不同意，可选择提取资产并终止服务

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

不能悄悄改 Safeguarding 相关条款，一定要"告知+接受"。

Q181. 若客户资产被错误划拨（例如误转至错误钱包或错误银行账户），贵司如何纠正与补偿?

A181（监管提交版）

1. **即时响应**
   - 一旦发现误划拨，立即冻结相关操作
   - 启动调查与追踪流程
2. **纠正措施**

- 尽最大努力追回资产
- 如无法追回且属于公司责任，将由公司自有资金补偿客户

3. **根因分析与改进**
   - Incident Report & RCA（Root Cause Analysis）
   - 更新流程或系统控制，防止再发生

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管最关心的是：
"犯错后你会不会让客户买单？"

Q182. 贵司如何处理链上 Fork / Airdrop / Token Split 情况下的客户资产权益？

A182（监管提交版）

1. **评估机制**
   - 技术+合规+风险联合评估 Fork/Airdrop 的法律与技术风险
   - 决定是否支持及如何计价
2. **原则**
   - 只要在技术上可行、法律上允许且风险可控，将尽量将 Fork/Airdrop 所产生的经济权益归属客户
   - 如不支持，将在风险披露中向客户说明
3. **账簿与披露**
   - 适用时，在客户账户中新增对应资产记录
   - 公告中解释政策与处理逻辑

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Fork/Airdrop 是链上业务一个容易被忽略的点，但监管会问"这部分收益到底是客户还是你的"。

Q183. 针对因制裁或AML原因冻结的客户资产，Safeguarding 机制如何处理？

A183（监管提交版）

1. **资产属性不变**
   - 即便因制裁/AML 原因被冻结，该部分资产法律上仍属于客户所有
   - 只是暂时受法律限制，无法处置或返还
2. **记录方式**
   - 在账簿系统中单独标记为"冻结资产（Sanctioned/Blocked）"
   - 不计入正常可用余额
3. **处置依法律执行**
   - 后续如根据法律要求需移交、上缴或销毁，将严格依照相关法规操作

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管的核心点：
"冻结不等于侵占"。

Q184. 贵司是否将 Safeguarding 责任清晰地分配给特定职能或高级管理层？

A184（监管提交版）

是，本公司将 Safeguarding 的最终责任归属于 **董事会（BoD）**，并由以下职能负责日常落实：

- CFO：负责 Client Money & 银行托管安排
- CRO：负责风险评估与 KRI 监控
- CTO：负责钱包与系统安全层面的资产隔离
- MLRO/Compliance：负责合规性审查及法规更新跟踪

职责在内部治理文件中有明文规定。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管最不喜欢"大家负责 = 没人负责"。
一定要把名字写出来。

Q185. 贵司是否存在使用第三方加密托管服务商（Sub-custodian）的情形？Safeguarding 如何延伸至该层？

A185（监管提交版）

如使用第三方加密托管服务商，将：

1. **合同与尽调**
   - 明确其仅为技术/托管执行方，不享有客户资产所有权
   - 审查其监管牌照与安全能力
2. **账簿记录**
   - 对所有通过 Sub-custodian 管理的资产进行精确记录
   - 保证可在任何时点识别每位客户持有的资产份额
3. **透视管理**
   - 本公司仍对 Safeguarding 承担最终责任
   - Sub-custodian 不得改变客户资产归属结构

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

不能把 Safeguarding 责任推给第三方。

Q186. 贵司是否对 Safeguarding 进行情景分析（Scenario Analysis）以评估极端状况下的表现？

A186（监管提交版）

是，我们在年度风险评估中对 Safeguarding 进行 Scenario Analysis，例如：

- 大规模提现 + 价格暴跌
- 主要托管银行/供应商宕机
- 严重网络攻击导致部分系统不可用

每个场景均评估：

- 对客户资产安全与可返还能力的影响
- 对标现有控制措施
- 必要的新增或加强控制

结果纳入风险报告与风险 Appetite 审查。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题是"Stress Test + Scenario Analysis"的叠加版本。

Q187. 贵司是否区分"运营风险损失"与"市场价格波动损失"在 Safeguarding 框架下的责任边界?

A187（监管提交版）

是，本公司在客户协议与内部政策中明确区分两类风险：

1. **运营风险损失（Operational Loss）**
   - 如系统错误、运营失误导致的资产丢失
   - 由本公司负责补偿/修复
2. **市场风险损失（Market Loss）**
   - 因价格波动、市场波动导致客户资产价值减少
   - 由客户自行承担，不属于 Safeguarding 范畴

该边界也在信息披露中向客户清晰解释。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这一条的逻辑是："保管安全 ≠ 对价格负责"。

Q188. 贵司是否建立对外部关键信息（如链上浏览器、价格源等）中断的应对方案，以保障 Safeguarding 不中断?

A188（监管提交版）

是，本公司在 Safeguarding 支撑系统上采用 **冗余设计**：

- 链上数据：多个区块浏览器 + 自建节点
- 价格源：多家行情供应商 + 内部风控曲线
- 银行接口：主备 API 通道

确保在任一外部服务发生中断时，仍可准确记录与返还客户资产。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

外部依赖也可能影响 Safeguarding，这点常被忽略，但监管会问。

Q189. 贵司是否定期向董事会报告 Safeguarding 运行情况？报告内容包含哪些关键要素?

A189（监管提交版）

是，Safeguarding 报告每季度提交给董事会，主要包括：

- 客户资产总量与结构
- 对账与差异情况
- Incident 与投诉统计
- 托管机构风险评估结果
- 流动性压力测试结果
- KRI 指标表现及是否超限

董事会将根据报告结果对资源配置和风险控制措施进行调整。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

把 Safeguarding 拉到董事会层级，是 BaFin 非常欣赏的做法。

Q190. 贵司是否对 Safeguarding 相关的关键控制措施进行定期测试与验证（Control Testing）？

A190（监管提交版）

是，本公司通过以下方式对 Safeguarding 控制措施进行定期测试：

- 对账流程抽样测试
- 权限控制与隔离测试
- 资产返还流程桌面演练
- Incident 响应演练
- 系统模拟大量提现场景

测试结果形成书面报告，由风险管理部和内部审计审阅并提出改进建议。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

控制如果从不测试，BaFin 会认为只是"写在纸上的制度"。

Q191. 请整体说明贵司的风险管理框架（Risk Management Framework）及其与 MiCA/BaFin 要求的对应关系？

A191（监管提交版｜BaFin-ready）

本公司建立了覆盖"识别-评估-监控-缓释-报告"全流程的风险管理框架，核心参考了：

- MiCA 对 CASP 风险管理的一般性要求；
- BaFin 对受监管金融机构（包括 crypto custody / investment services）的行政实践与通函；
- MaRisk、BAIT 等德国风险管理与内部控制的通行原则。

风险管理框架的核心要素包括：

1. **治理结构（Governance）**
   - 董事会对整体风险承担最终责任，设立 **风险委员会（Risk Committee）**；
   - 任命独立的 **首席风险官（CRO）**，负责日常风险管理职能；
   - 将风险管理与合规、内审职能有效区隔，避免利益冲突。
2. **风险类型覆盖（Risk Taxonomy）**
   - 市场风险（Market Risk）
   - 信用/对手方风险（Credit / Counterparty Risk）
   - 流动性风险（Liquidity Risk）
   - 运营风险（Operational Risk）
   - 合规与监管风险（Compliance / Regulatory Risk）
   - 法律风险（Legal Risk）
   - 声誉风险（Reputational Risk）
   - 技术与网络安全风险（IT & Cyber Risk）
3. **风险管理周期（Risk Management Cycle）**
   - **识别**：通过风险评估（Risk Assessment）、新产品审批（New Product Approval），识别业务和技术中的风险源；
   - **评估**：采用定性 / 半定量方法（风险矩阵、评分模型）评估风险的发生概率与影响；
   - **监控**：通过 KRI、限额（Limits）、日常监控报告持续跟踪；
   - **缓释**：落实控制措施，如权限控制、限额控制、对冲策略等；

- **报告**：定期向管理层和董事会提交风险报告，并在达到预警阈值时进行升级。

4. **文件体系（Documentation）**
   - 《风险管理政策（Risk Management Policy）》为一级文件，由董事会批准；
   - 下设专门子政策：市场风险政策、流动性风险政策、运营风险政策、第三方风险政策、IT 风险政策等。

通过上述安排，确保本公司风险管理框架与 MiCA 的审慎要求及 BaFin 的监管期望保持一致，并具备可审计性与可证明性。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这一题是风控的"总纲"，关键词要有：

- 治理结构（BoD + CRO + Risk Committee）
- 风险类型列表
- 整个风险管理循环（识别-评估-监控-缓释-报告）
- 有书面政策 + 董事会批准

Q192. CRO（首席风险官）的职责、独立性及其在组织架构中的位置如何?

A192（监管提交版）

1. **职责（Responsibilities）**
   - 牵头建立和维护风险管理框架；
   - 组织风险识别、评估与定期审查；
   - 制定并监控 KRI、风险限额等工具；
   - 向管理层和董事会风险委员会定期报告风险情况；
   - 对新业务、新产品、新合作伙伴进行风险评审并发出意见。
2. **独立性（Independence）**
   - CRO 直接向董事会或风险委员会汇报，而非隶属于业务部门；
   - CRO 无日常业务 KPI，不参与交易决策或利润考核，避免与风险控制职责产生冲突；
   - 如有对重大风险事项存在分歧，CRO 有权直接向董事会报告。
3. **组织位置（Organizational Position）**
   - 在组织架构图中，CRO 为独立职能，与 COO/CTO/CCO 并列；
   - 风险管理团队独立运作，对所有业务线具有横向审视权。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 很看重 CRO 的"独立性"，不能写成"挂名风险官 + 实际全职业务"。

Q193. 贵司如何进行全面风险评估（Enterprise-wide Risk Assessment, EWRA）？频率与方法是怎样的?

A193（监管提交版）

本公司每年至少开展一次 **企业级全面风险评估（EWRA）**，并在发生重大业务变更时进行临时更新。主要步骤为：

1. **范围与对象**
   - 覆盖所有业务线（交易、托管、场外服务等）、所有关键职能（IT、运营、合规、财务等）。
2. **风险识别（Identification）**
   - 与各部门共同识别潜在风险事件和风险因素；
   - 参考监管通报、行业案例、内部 Incident 记录。
3. **风险评估（Assessment）**
   - 使用标准化风险矩阵（Impact x Likelihood）；

- 将风险等级划分为低/中/高/重大；
- 针对关键风险进一步进行定性解释。

4. **控制评估与差距分析（Control Assessment & Gap Analysis）**
   - 评估现有控制措施的充分性、有效性；
   - 识别控制缺口，形成整改计划。
5. **报告与批准**
   - EWRA 结果总结成报告，由 CRO 提交管理层与董事会风险委员会；
   - 经董事会确认后，作为下一年度风险 Appetite 及资源配置依据。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

EWRA 也是 AML 里会问的一题，但在总风控模块中也要覆盖。
关键是：**年度 + 触发性更新 + 报告给 BoD**。

Q194. 贵司是否设定书面的风险偏好（Risk Appetite）与风险限额（Risk Limits）？

A194（监管提交版）

是，本公司已制定由董事会批准的 **《风险偏好声明（Risk Appetite Statement）》**，并在此基础上设定各类风险限额：

1. **风险偏好（Risk Appetite）**
   - 明确公司对不同风险类型可接受的总体水平，例如：
     - 对运营事件的容忍度接近"零容忍"；
     - 对市场波动风险有一定限度的可接受范围，但不得影响客户资产 Safeguarding。
2. **风险限额（Risk Limits）**
   - 对关键指标设定量化限额，例如：
     - 单一对手方敞口上限；
     - 市场持仓风险限额（如自营业务存在时）；
     - 流动性覆盖比例（Liquidity Coverage Ratio）；
     - 外包集中度上限；
     - 关键 KRI（如对账差异次数）的预警和红线指标。
3. **监控与违规处理**
   - 风险管理部通过系统和定期报表监测限额使用情况；
   - 若出现限额触碰或超限，将触发升级程序（Escalation），并形成整改行动。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题的重点是：你不是"摸着石头过河"，而是有**"偏好 + 限额"**的书面体系。

Q195. 请说明贵司如何管理市场风险（Market Risk），包括但不限于自营仓位和客户相关敞口?

A195（监管提交版）

在当前业务模式下，本公司以撮合/经纪与托管为主，自营活动受到严格限制。市场风险管理主要包括：

1. **自营风险（若适用）**
   - 自营仓位规模受到风险限额控制；
   - 采用 VaR、敏感度分析或简单敞口限额对自营头寸进行监控；
   - 不以客户资产进行任何形式的杠杆或投机操作。
2. **客户相关市场风险**
   - 市场价格波动风险由客户自主承担，但本公司确保：

- 不误导客户"本金保本"或固定收益；
- 在做市或撮合时保障公平定价与执行质量。

3. **价格来源与监控**
   - 使用多家报价源并设有 Outlier 检测；
   - 在极端行情时可启用临时保护机制（如提高保证金、限制杠杆、暂停部分服务）。
4. **报告机制**
   - CRO 定期向管理层报告总体市场风险敞口和压力测试结果。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

关键：**不拿客户资产赌行情**，自营有的话也要"限额可控 + 不伤客户"。

Q196. 流动性风险（Liquidity Risk）如何管理？贵司如何确保在高压情景下仍可履行客户提现义务？

A196（监管提交版）

本公司将流动性风险管理视为与 Safeguarding 同等级的核心要求：

1. **流动性储备与结构**
   - 设定最小现金与高流动性资产比例；
   - 对托管资产在冷/热钱包、不同银行、不同资产类别间进行分散。
2. **流动性压力测试**
   - 定期开展"极端集体提现"、"主要对手方违约"等情景压力测试；
   - 根据结果调整资产配置、备付金规模和提现限额。
3. **流动性预警指标**
   - 如提现请求激增、市场波动放大、某托管机构出现风波，系统会触发预警。
4. **应急计划（Contingency Funding Plan）**
   - 预设应急资金来源与备用渠道（例如增资或股东资金支持）；
   - 明确在极端情形下优先保障客户提现与资产返还。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这一题要和前面 Safeguarding 的内容"呼应"：
资产安全 + 可及时取回 = 真正的保护。

Q197. 如何管理信用/对手方风险（Credit/Counterparty Risk），尤其是与银行、流动性提供方、做市商之间的风险？

A197（监管提交版）

本公司通过以下机制管理信用/对手方风险：

1. **对手方分类与评级**
   - 将银行、流动性提供方、做市商、托管机构等划为关键对手方；
   - 使用内评模型或外部评级对对手方进行信用质量评估。
2. **敞口管理**
   - 设立对手方额度（Counterparty Limits）；
   - 定期统计实际敞口并与限额对比；
   - 超限时采取降低敞口或更换对手方等措施。
3. **法律与合同保护**

- 使用 ISDA、GMRA 或定制化主协议框架（若适用）；
- 明确违约事件（Event of Default）、抵押与净额结算机制。

4. **监控与预警**
   - 关注对手方的财务状况、监管消息与市场舆情；
   - 如发现重大信用恶化信号，将启动风险缓释措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 会问的潜台词是："你把客户资金/资产放在谁那？你怎么知道他不会突然倒？"

Q198. 运营风险（Operational Risk）的识别和管理机制是怎样的？是否有运营事件登记簿（Incident Register）？

A198（监管提交版）

1. **运营风险范围**
   - 覆盖人为错误、流程缺陷、系统故障、外包失败、欺诈和内部不当行为等。
2. **事件登记与分类**
   - 设立 **运营事件登记簿（Operational Incident Register）**；
   - 所有中高等级事件均需登记：时间、原因、影响、责任人、整改措施。
3. **根因分析（Root Cause Analysis）**
   - 对重大事件进行 RCA，明确根本原因及控制缺口。
4. **经验反馈与改进**
   - 定期总结事件模式，更新流程、权限、系统控制；
   - 向员工和管理层反馈教训，防止再次发生。
5. **量化管理**
   - 部分运营风险事件可纳入 KRI，如系统不可用时长、处理错误率等。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

一句话：**"出过什么事，要有账可查、有原因分析、有改进。"**

Q199. 贵司如何防范内部欺诈和不当行为（Internal Fraud & Misconduct）？

A199（监管提交版）

1. **制度层面**
   - 《行为守则（Code of Conduct）》和《反欺诈政策（Anti-Fraud Policy）》；
   - 明确禁止占用客户资产、自营交易利益冲突、内幕信息滥用等行为。
2. **权限与分权控制**
   - 关键操作"四眼原则"或"多签机制"；
   - 禁止同一员工同时控制前台交易、账簿记录和资金划拨。
3. **监控与审计**
   - IT 日志与异常行为监测（如异常登录、异常资金转移）；
   - 内部审计对高风险岗位进行周期性审查。
4. **举报与保护机制**
   - 设立匿名举报渠道（Whistleblowing Channel）；
   - 对善意举报者提供保护，禁止报复行为。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管特别忌讳"内部人监守自盗"，所以要体现：

- 分权
- 日志
- 内审
- 举报机制

Q200. 贵司是否有书面内部控制框架（Internal Control Framework），如何与风险管理框架衔接?

A200（监管提交版）

是的，本公司将 **风险管理框架** 与 **内部控制框架** 作为两个相互配合的体系：

1. **内部控制框架组成**
   - 基于"三道防线"模型：
     - 第一防线：业务与运营部门；
     - 第二防线：风险管理与合规；
     - 第三防线：内部审计。
   - 每道防线具有清晰的职责边界与协调机制。
2. **控制类型**
   - 预防性控制（Preventive Controls）：限额、权限、流程；
   - 侦测性控制（Detective Controls）：对账、监控、审查；
   - 纠正性控制（Corrective Controls）：问题整改、流程优化。
3. **与风险管理的衔接**
   - 风险评估结果直接影响内部控制设计；
   - 重大 Incident 与控制失效会反馈到风险评估模型中。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管想看到的是：**风控不是"喊口号"，而是落实在一个个具体控制措施上。**

Q201. 新产品/新业务上线前如何进行风险评审和批准（New Product Approval Process, NPAP）？

A201（监管提交版）

本公司对所有新产品/新业务实行 **New Product Approval Process（NPAP）**：

1. **发起与立项**
   - 业务部门提出新产品方案，提交初步商业模式说明。
2. **多部门评审**
   - 风险管理部：评估市场/信用/运营/流动性风险；
   - 合规与法律：评估监管许可范围、MiCA 适用性与法律风险；
   - IT与安全：评估系统能力和安全风险；
   - 财务：评估成本与收益模型。
3. **风险缓释措施设计**
   - 对发现的关键风险制定相应的控制措施；
   - 形成完整 New Product Risk Assessment 报告。
4. **审批与上线**

- 提交管理层或产品委员会批准；
- 重要产品需董事会层面审批；
- 上线后设定试运行期与评估节点。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

NPAP 是"防止一时冲动上线一个大坑产品"的关键机制，BaFin 特别看重。

Q202. 贵司如何管理与第三方服务提供商（包括外包）相关的风险（Third Party / Outsourcing Risk）？

A202（监管提交版）

本公司依据《第三方与外包风险管理政策（Third Party & Outsourcing Risk Policy）》管理相关风险：

1. **准入前尽调（Due Diligence）**
   - 法律地位、监管牌照、财务状况；
   - 技术能力、信息安全水平、业务连续性计划；
   - 过往违规记录和声誉风险。
2. **风险分级与审批**
   - 将第三方按重要性分级（Critical / Important / Non-Critical）；
   - 关键外包项目需管理层或董事会批准。
3. **合同与 SLA**
   - 在合同中明确服务范围、安全要求、审计权、数据保护条款、退出机制（Exit Strategy）。
4. **持续监控**
   - 定期评估服务质量与风险表现；
   - 对关键供应商进行现场或远程评审。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

MiCA + DORA 对外包管理要求越来越高，这一题必须有"尽调 + 合同 + 持续监控 + Exit"。

Q203. 是否区分"关键外包（Critical Outsourcing）"与"非关键外包"，分别如何管理?

A203（监管提交版）

是的，本公司对外包服务按重要性进行分类：

1. **关键外包（Critical / Important Outsourcing）**
   - 一旦故障，将显著影响运营连续性、客户资产安全或合规义务履行；
   - 如核心交易系统托管、钱包基础设施、关键云服务等。
   - 要求：
     - 更严格的尽调与批准流程；
     - 更频繁的绩效与风险评审；
     - 明确的 BCP/DRP 要求和测试。
2. **非关键外包（Non-Critical Outsourcing）**
   - 如部分行政、人事等支持性功能外包；
   - 在保障数据保护的前提下，管理要求相对简化。

分类标准以及对应管理措施在外包政策中有明确规定。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题其实是在"对照 DORA 思路"，强调你知道什么是 **critical function**。

Q204. 贵司如何确保三道防线模型（3 Lines of Defence）在实际运作中不会出现职能混淆或失效?

A204（监管提交版）

1. **书面职责描述**
   - 在治理文件中明确定义三道防线的角色与职责：
     - 第一防线：业务/运营，负责风险的日常管理与控制执行；
     - 第二防线：风险管理与合规，负责设计控制框架、监控与独立挑战；
     - 第三防线：内部审计，负责独立评估前两道防线有效性。
2. **组织架构与汇报线**
   - 第二、防线向管理层和董事会拥有直接报告权；
   - 内部审计直接向董事会审计委员会报告，不向业务线汇报。
3. **冲突管理**
   - 避免同一自然人同时担任前台业务与第二/三道防线的核心职务；
   - 如因规模限制不可避免，将通过额外的外部审计与咨询增强独立性。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

三道防线是德国监管的"必考题"，重点是：**职责写清楚 + 汇报线独立**。

Q205. 内部审计职能（Internal Audit）如何设立？审计计划如何覆盖 CASP 核心风险领域?

A205（监管提交版）

1. **设立方式**
   - 根据公司规模与发展阶段，内部审计可采：
     - 内部团队形式；或
     - 与外部独立审计机构合作，以外包方式履行内部审计职能。
   - 不论采用哪种形式，审计职能都直接对董事会审计委员会负责。
2. **年度审计计划**
   - 基于风险导向（Risk-based）原则制定；
   - 覆盖 CASP 业务的核心领域：
     - AML/CFT
     - Safeguarding
     - IT & Cyber Security
     - 风险管理与内部控制
     - 客户保护与市场行为
   - 审计计划由董事会批准，必要时可中途调整。
3. **审计报告与整改跟踪**
   - 每项审计均形成书面报告，列明发现、评级和整改建议；
   - 管理层需制定整改计划并定期反馈进度；
   - 内审负责跟踪直至整改关闭。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这里要强调"Risk-based Internal Audit"，而不是随机检查。

Q206. 贵司如何管理与监督董事会和高级管理层对风险管理的整体责任履行情况?

A206（监管提交版）

1. **治理文件**
   - 在《公司治理政策》和《风险管理政策》中明确：
     - 董事会对整体风险框架负最终责任；
     - 高级管理层负责将风险框架落实到日常运营。
2. **报告与会议机制**
   - CRO 和 CCO 定期向董事会风险/审计委员会汇报；
   - 董事会会议议程中固定设置"风险与合规"议题。
3. **培训与评估**
   - 对董事会成员进行 MiCA 及相关风险管理培训；
   - 适时评估董事会在风险监督方面的有效性，并做改进。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管看的是：**BoD 不只是"挂名"，而是被制度要求"真负责"。**

Q207. 贵司如何确保管理信息（Management Information, MI）质量，支持管理层进行风险决策?

A207（监管提交版）

1. **MI 报告体系**
   - 定期生成管理信息报告，涵盖：
     - 主要 KRI/KPI；
     - 风险限额使用情况；
     - 重大事件与投诉；
     - 监管变化与合规状态。
2. **数据质量控制**
   - 对数据来源、处理逻辑和生成报表的流程进行定义和控制；
   - 对关键 MI 报表采取"双人复核"或自动校验机制。
3. **适用性与可读性**
   - 确保报告内容简明清晰，突出重点风险与趋势，而非纯粹堆砌数据；
   - 管理层可根据 MI 做出及时且有根据的决策。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

MI = 管理层的"视力"，数据质量差等于"戴了脏眼镜"。

Q208. 风险事件或控制失效（Control Failure）发生后，如何进行升级（Escalation）与沟通?

A208（监管提交版）

1. **事件分级**
   - 根据影响程度与风险领域，将事件划分为低/中/高/重大；
   - 重大事件包括客户资产受损、重大 IT 故障、重大合规违例等。

2. **升级路径**
    - 低/中等事件由部门主管处理，并向风险管理部通报；
    - 高/重大事件必须立即向 CRO、CCO 和高级管理层报告；
    - 如涉及监管违例风险，将评估是否需要向 BaFin 报告。
3. **沟通与记录**
    - 所有升级记录需形成书面材料，纳入 Incident Register；
    - 重大事件需在董事会层面进行复盘并确认整改措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Escalation 机制是证明"问题不会被压下去"的关键。

Q209. 贵司如何在集团层面管理风险（Group-wide Risk Management），尤其是在存在其他国家实体时？

A209（监管提交版）

如本公司为集团的一部分，将采取以下措施确保德国 CASP 实体的风险管理不被削弱：

1. **集团风险政策**
    - 集团层面制定统一的风险管理原则与最低标准；
    - 德国实体在遵守集团标准的基础上，还需满足 MiCA 与 BaFin 要求。
2. **信息共享与防火墙**
    - 在合规框架下进行必要的风险信息共享；
    - 同时设立防火墙，防止其他实体的风险向 CASP 实体传导。
3. **集团监督与本地独立性**
    - 集团风险职能对各实体进行协调与监督；
    - 但德国实体 CRO/CCO 对本地监管负责，确保本地需求优先。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

集团结构下，BaFin 最怕的是"德国实体变成其他国家风险的接盘侠"。

Q210. 贵司如何将风险管理结果纳入业务决策与资源配置（例如 IT 投入、人手配置、资本安排）？

A210（监管提交版）

1. **风险-回报权衡（Risk-Return Trade-off）**
    - 新业务决策时，风险评估结果与收益预测一起呈报管理层；
    - 对高风险但低收益的项目，可能被否决或缩减规模。
2. **资源倾斜**
    - 风险评估中被认定为高风险领域（如 Safeguarding、IT 安全、AML），将获得更多 IT 与人力投入；
    - 如压力测试表明流动性不足，将考虑提高资本缓冲或股东资金支持。
3. **预算与资本计划**
    - 年度预算编制时，参考风险评估与监管新要求，确保有足够资源维持合规和风控体系。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

重点让监管看到：**风控不是"写在 PPT"，而是会实际影响钱、人、系统。**

Q211. 贵司如何管理合规风险（Compliance Risk），尤其是针对 MiCA、德国本地法规及制裁要求的遵守？

A211（监管提交版）

本公司将合规风险视为整体风险管理框架中的核心组成部分，具体管理方式如下：

1. **合规框架（Compliance Framework）**
   - 由 **首席合规官（CCO）** 负责牵头，制定《合规政策（Compliance Policy）》与配套程序；
   - 合规职能与业务、风险管理、内审保持独立，直接向管理层及董事会报告。
2. **法规识别与跟踪（Regulatory Mapping & Monitoring）**
   - 建立即时更新的法规矩阵（Regulatory Mapping），覆盖：
     - MiCA 及相关委托立法；
     - 德国国家层面实施法规；
     - 反洗钱（AML）、制裁（Sanctions）、数据保护（GDPR）、DORA 等；
   - 通过官方公告、行业协会和外部法律顾问获取法规变化信息。
3. **差距分析与整改（Gap Analysis & Remediation）**
   - 对每项新规或修订，开展差距分析，识别本公司制度与流程中的不足；
   - 制定整改计划，分配责任人与时间表，并由 CCO 跟踪执行。
4. **合规风险报告**
   - CCO 定期向管理层和董事会提交合规报告，包括高风险领域、重大违规事件及整改进度。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题强调：**有专门合规职能 + 有法规追踪 + 有Gap Analysis + 有整改**，避免"只听说有 MiCA，但没落地"。

Q212. 声誉风险（Reputational Risk）如何被纳入贵司的风险管理框架？是否有专门的应对预案？

A212（监管提交版）

1. **纳入风险分类体系**
   - 本公司将声誉风险视为独立风险类别进行识别和管理，同时认识到其他风险（如 AML、ICT、Safeguarding）若处理不当会间接引发声誉风险。
2. **监测渠道（Monitoring）**
   - 持续监测媒体报道、社交媒体反馈、客户投诉和监管公开信息；
   - 对负面信息进行快速甄别与分类，评估对公司及客户信心的潜在影响。
3. **声誉事件响应（Reputation Incident Response）**
   - 一旦出现重大负面舆情或监管调查，将启动专项小组，包括：
     - 管理层代表；
     - 法律与合规；
     - 风险管理；
     - 公共关系。
   - 制定信息披露口径和客户沟通方案，避免误导或信息不透明。
4. **与其他风险联动**
   - 声誉事件可触发对相应根本风险（如 AML、ICT）的复盘与整改；
   - 在年度 EWRA 中评估声誉风险总体暴露度。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管非常清楚：**一旦出事，先爆的是声誉**。要表示你承认这一点，并有"专门应对机制"。

Q213. 贵司如何确保内部政策、程序与实际操作一致（Policy-to-Practice Alignment）？

A213（监管提交版）

为避免"纸面合规"，本公司通过多重机制确保内部政策与实际操作保持一致：

1. **流程落地与培训**
   - 每项新政策发布前，由相关职能部门将其转化为具体操作流程和系统配置；
   - 通过培训与工作手册，确保员工理解并按流程执行。
2. **监控与质检（Quality Assurance）**
   - 二道防线（风险/合规）对关键流程进行抽样检查（如开户、KYC、提款审批、交易监控处理）；
   - 发现操作偏离政策时，发出整改要求并更新培训。
3. **内部审计验证**
   - 内部审计定期审查政策与执行的匹配度，出具独立评估；
   - 重大偏差需上报董事会并由管理层负责整改。
4. **系统控制（System-enforced Controls）**
   - 对于关键控制点，如限额、黑名单、审批流，尽量通过系统参数强制执行，减少人为绕行空间。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这题是典型的"德式灵魂拷问"：**你是'写得好看'还是'真在用'？**

Q214. 贵司是否设立风险委员会（Risk Committee）或类似管理委员会？其运作机制如何？

A214（监管提交版）

1. **设立与构成**
   - 本公司设立 **风险与合规委员会（Risk & Compliance Committee）**，由：
     - CEO；
     - CRO；
     - CCO；
     - CTO；
     - MLRO；
     - 其他视情况邀请的职能负责人
       共同组成。
2. **职责范围**
   - 审议重大风险事项与限额设置；
   - 审查 EWRA、KRI、压力测试结果；
   - 审议重大产品/业务的风险评估报告；
   - 审议重大合规事件与整改方案。
3. **会议频率与记录**
   - 至少每季度召开一次例会，必要时可召开临时会议；
   - 每次会议形成书面会议纪要，明确决议事项和责任人。
4. **与董事会互动**
   - 风险与合规委员会向董事会或其下属风险委员会报告决议与重大风险事项，供其监督与批准。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

建议一定写有"委员会 + 会议纪要 + 决议 follow-up"，符合德国监管口味。

Q215. 请说明贵司如何进行压力测试（Stress Testing）与情景分析（Scenario Analysis），并将结果用于风险管理与业务决策？

A215（监管提交版）

1. **压力测试目的**
   - 评估在极端但合理的情景下，本公司资产负债、流动性、运营能力和客户资产保护的脆弱点；
   - 为资本缓冲、流动性储备和业务限制提供依据。
2. **情景设计**
   - 市场类：极端价格波动、某主流币种价格短期大幅下跌；
   - 流动性类：集中提现潮、主要银行或托管机构出现问题；
   - 技术类：关键系统中断、网络攻击；
   - 合规类：重大 AML 事件导致监管行动与声誉冲击。
3. **方法与频率**
   - 至少每年开展一次全面压力测试，针对重点领域可加密频率；
   - 采用定量+定性结合的方法，评估影响与应对能力。
4. **结果应用**
   - 根据测试结果调整资本金与流动性储备；
   - 完善 DRP / BCP 方案；
   - 对产品、客户群体、业务策略进行必要调整或限制。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

压力测试不要写成"形式主义"，一定要强调："结果会反馈到资本/流动性/业务决策"。

Q216. 贵司是否采用关键风险指标（Key Risk Indicators, KRI）？请举例说明几个核心 KRI 及其阈值管理。

A216（监管提交版）

是，本公司使用 **KRI（关键风险指标）** 监控主要风险领域：

1. **示例 KRI**
   - ICT 可用性：系统不可用时间（Downtime）占比；
   - Safeguarding：对账差异事件次数与金额；
   - AML：高风险警报未在预定时间内处理的数量；
   - 投诉：客户投诉数量及严重程度占比；
   - 外包：关键供应商 SLA 未达标次数。
2. **阈值与预警**
   - 每个 KRI 设置预警值（Early Warning）和限值（Limit）：
     - 触发预警值 → 内部分析与纠偏；
     - 触发限值 → 升级到管理层/委员会，制定整改行动。
3. **报告与复审**
   - KRI 随管理信息报告（MI）按月/季提交给高级管理层；
   - 每年至少复审一次 KRI 体系的适用性与充分性。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

KRI = 日常"体温计"。选择指标时尽量与 BaFin 高度关注领域挂钩（ICT、Safeguarding、AML、外包等）。

Q217. 如何避免将业务绩效指标（KPI）与风险控制目标混淆，从而导致"风险被业绩压力压制"?

A217（监管提交版）

1. **职能分离**
   - 业务线以 KPI（业务发展、收入等）为主要考核指标；
   - 风险与合规部门的绩效不与业务盈利直接挂钩，以风险控制质量为评估核心。
2. **独立的风险容忍度（Risk Appetite）**
   - 风险限额和 KRI 不由业务部门单独设定，而是由 CRO/CCO 提议并由董事会批准；
   - 业务部门不得以"业绩目标"为理由要求放宽风险限额。
3. **激励机制约束**
   - 禁止通过短期激励鼓励违反风险政策的行为；
   - 高级管理人员的长期激励与合规、风险事件记录挂钩。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这是德国监管很看重的一点：**风控/合规不能被"业绩 KPI"绑架**。

Q218. 贵司如何在日常运营中对风险事件和"未遂事件/险情（Near Miss）"进行收集和分析?

A218（监管提交版）

1. **事件定义与范围**
   - 风险事件：已对客户或公司造成实际影响的事件；
   - Near Miss：虽未导致损失，但一旦条件略有变化可能造成重大后果的事件。
2. **收集渠道**
   - 运营部门、IT 部门、合规和风险管理均有责任报告；
   - 提供简便的内部报告机制（工单系统、专用邮箱等）。
3. **登记与分类**
   - 所有事件与 Near Miss 均记入 Incident Register，标注类型、严重程度和根因。
4. **分析与经验反馈**
   - 定期对数据进行趋势分析，识别重复发生的模式与薄弱环节；
   - 将结果反馈至流程改进、系统优化与培训安排。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Near Miss 写出来，监管会认为你"有提前预防意识"，而不是"说一切都很好"。

Q219. 贵司如何将培训（Training）纳入风险与内部控制体系？哪些岗位有强制培训要求?

A219（监管提交版）

1. **风险与合规培训框架**
   - 每年制定培训计划，覆盖：
     - MiCA 与 BaFin 监管要求；
     - AML/CTF 与制裁；
     - ICT 安全与数据保护；
     - 客户保护与市场行为；

- 内部控制与三道防线模型。

2. **强制培训对象**
   - 高级管理层与董事会成员：需完成针对 MiCA、治理和风险监督的专项培训；
   - 关键控制岗位（CRO、CCO、MLRO、CTO、CISO 等）：需定期参加高级合规与风险课程；
   - 客户接触岗位：必须通过 KYC / AML / 市场行为相关培训考核。
3. **培训记录与效果评估**
   - 保存培训出席记录与考核结果；
   - 对关键课程实施测试，以检验理解程度；
   - 对重复性事件较多的领域加密培训频率。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

培训是连接"制度"和"人"的桥梁，这题写好可以加分。

Q220. 贵司是否有正式的政策审查与更新流程（Policy Review Process）？频率如何?

A220（监管提交版）

是的，本公司为所有关键政策制定了正式的 **审查与更新流程**：

1. **审查频率**
   - 关键政策（如 AML、风险管理、IT 安全、外包、Safeguarding）：至少每年审查一次；
   - 遇到重要法规变化或重大事件后，需立即进行临时审查。
2. **审查责任**
   - 各领域负责人（例如 CRO/CCO/CISO）牵头审查相关政策；
   - 重大修改须提交管理层与董事会批准。
3. **变更记录**
   - 所有政策变更均记录在案，包括版本号、修改内容和生效日期；
   - 保留旧版本以备审计与监管查阅。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

"写完政策就束之高阁"是监管最不愿意看到的，这题要强调：**定期审查 + 触发审查**。

Q221. 在贵司内部，风险文化（Risk Culture）如何被塑造与评估?

A221（监管提交版）

1. **高层示范（Tone from the Top）**
   - 董事会与管理层在内部沟通中明确强调"合规优先、风险先于收益"的原则；
   - 对违反风险政策的行为实行"零容忍"纪律。
2. **制度与激励匹配**
   - 不通过过度激进的业绩考核来引导高风险行为；
   - 将合规与风险控制表现纳入管理层绩效考核。
3. **沟通与反馈渠道**
   - 员工可通过匿名渠道报告风险担忧或不当行为；
   - 定期进行员工问卷或访谈，评估风险文化的落实情况。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

德国监管会特别关注 **"文化"**，因为再好的制度，如果文化是"只看利润"，最后一样会爆雷。

Q222. 贵司如何管理法律风险（Legal Risk），特别是合同、条款、客户协议与跨境法律问题？

A222（监管提交版）

1. **法律职能设置**
   - 设立法律顾问职能，或与外部律所建立长期合作，用于审查合同和提供法律意见。
2. **文档审查**
   - 客户协议、业务条款、供应商合同等关键文件在使用前必须经过法律审查；
   - 重点审查责任分配、赔偿条款、司法管辖与争议解决机制。
3. **跨境法律分析**
   - 对涉及其他司法辖区的业务（例如跨境服务、外包到第三国）进行法律风险评估；
   - 确保不会违反相关国家的金融监管及数据保护法律。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

法务风控是防止"合同挖坑"和"跨境踩雷"的关键，MiCA 项目尤其如此。

Q223. 如果出现重大监管调查或执法行动，贵司内部的应对机制（Regulatory Investigation Response）是什么？

A223（监管提交版）

1. **启动条件**
   - 收到监管机构正式函件、检查通知或处罚预告时，立即触发应对机制。
2. **专门小组（Task Force）**
   - 由管理层、法律、合规、风险、相关业务部门组成专项小组；
   - 明确责任分工与对外沟通口径。
3. **资料收集与配合**
   - 按监管要求在规定期限内提供完整、准确、可追溯的资料；
   - 如有不确定处，及时与监管沟通澄清。
4. **内部复盘与整改**
   - 不论最终结果如何，均对事件进行复盘；
   - 将监管意见纳入制度与流程改进。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

BaFin 非常看重"配合度"，要写出你有成熟机制，并不是临时乱应付。

Q224. 贵司如何管理模型风险（Model Risk），例如在交易监控、风险评分、定价算法中使用的模型？

A224（监管提交版）

1. **模型识别与分类**
   - 将用于交易监控、风控评分、市场风险测算等的算法纳入"模型风险管理"范围。
2. **模型开发与验证分离**
   - 模型开发由业务/分析团队负责；

- 模型验证由风险管理或独立职能进行，以避免利益冲突。

3. **模型验证内容**
   - 假设合理性、数据质量、参数选择、稳定性和敏感度测试；
   - 对监控与预警阈值进行回测（Back-testing）。
4. **模型监控与定期复审**
   - 定期监控模型表现，如误报率、漏报率、预测误差等；
   - 每年至少进行一次全面复审，必要时更新或替换模型。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

有交易监测、风险评分，就肯定涉及"模型风险"，写清"开发/验证分离 + 回测"。

Q225. 贵司如何管理文档与记录（Documentation & Record Keeping），以支持风险管理与监管检查?

A225（监管提交版）

1. **记录范围**
   - 覆盖管理层与董事会会议记录、政策与程序版本、风险评估报告、内部审计报告、Incident Register、客户投诉记录等。
2. **保存期限**
   - 按监管要求至少保存若干年（例如 5 年或以上），部分关键记录（如客户资产相关文件）可延长保存期限。
3. **可追溯性与检索**
   - 采用电子文档管理系统，支持分类、索引和权限控制；
   - 确保在合理时间内可向 BaFin 提供所要求的完整记录。
4. **完整性保护**
   - 对关键记录采用防篡改机制（如只读存储、日志审计），确保文档未被恶意更改。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

德国监管对"记录留痕"要求非常高，这题写好，能让对方相信你"说得到、查得见"。

Q226. 贵司是否设立投诉管理流程（Complaint Handling），如何与风险管理相结合?

A226（监管提交版）

1. **投诉政策与流程**
   - 制定《客户投诉处理政策》，明确投诉受理渠道、处理时限与升级路径。
2. **记录与分析**
   - 所有投诉记录在案，包括投诉内容、处理结果和沟通记录；
   - 按类型和严重程度统计并定期分析趋势。
3. **风险反馈**
   - 将高频或重大投诉视为潜在风险信号，反馈至相关部门和风险管理部；
   - 必要时触发政策/流程调整。
4. **监管要求符合性**
   - 遵守 MiCA 对客户保护和投诉处理的相关义务；
   - 如有涉及重大违规或系统性问题，评估是否需要向 BaFin 披露。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

"投诉管理 = 风险传感器"，要写清"记录 + 分析 + 反馈"。

Q227. 贵司如何确保项目变更（Change Management）不会破坏现有控制环境与风险水平？

A227（监管提交版）

1. **变更范围**
   - 包括系统升级、流程调整、组织架构变化、外包安排变更等。
2. **变更审批流程**
   - 所有重大变更需提交变更申请，由 IT、风险、合规和相关业务共同评估；
   - 对风险影响较大的变更需提交管理层审核。
3. **风险评估与测试**
   - 对变更进行风险评估，评估其对安全性、数据完整性与控制有效性的影响；
   - 在生产环境实施前进行充分测试（包括回归测试和安全测试）。
4. **实施后复核**
   - 变更完成后对关键控制点进行验证，确保没有造成控制缺失或意外副作用。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

Change Management 是 IT + 风控交叉点，BaFin 很常问：**“你升级系统时，有没有把风控关掉？”**

Q228. 贵司如何对外部审计意见与监管检查意见进行跟踪整改（Follow-up of Findings）？

A228（监管提交版）

1. **统一登记**
   - 将外部审计、内部审计及监管检查发现统一登记在 Findings Register 中，记录发现内容、严重程度和要求整改期限。
2. **整改责任**
   - 指定整改负责人和支持团队，并明确完成期限。
3. **进度跟踪**
   - 风险或合规部门定期跟踪整改进度，必要时向管理层报告逾期待办事项。
4. **关闭与验证**
   - 完成整改后，由内审或二道防线进行验证；
   - 仅在验证通过后，方可将发现标记为“已关闭”。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

监管不怕“发现问题”，怕的是“发现问题后啥都不做”。

Q229. 贵司如何确保风险管理在整个组织中“可被理解”（Understanding）而不仅是高层概念？

A229（监管提交版）

1. **分层沟通**
   - 对不同层级员工用不同的方式阐述风险管理要求：
     - 对一线员工：以操作实例和简单规则为主；
     - 对管理层：以 KRI/KPI、报告和风险分析为主。
2. **场景化案例**
   - 通过案例分享、工作坊等形式，让员工理解风险事件如何发生、如何防范。

3. **纳入日常管理**
    - 在绩效考核与部门目标中嵌入风险控制维度，强化"业务即风险管理"的理念。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

一句话：**让所有人都知道"风险管理不是某个部门的事"，而是"每个人的工作方式"。**

Q230. 请总结贵司风控与内部控制体系的核心优势，以及为何认为其足以支撑 MiCA CASP 授权及持续运营要求？

A230（监管提交版）

本公司的风险管理与内部控制体系具备以下核心优势：

1. **治理层面**
    - 明确的董事会责任与三道防线模型；
    - 独立的 CRO、CCO、MLRO 等关键职能；
    - 定期运作的风险与合规委员会。
2. **框架完整性**
    - 覆盖市场、信用、流动性、运营、法律、合规、IT 与声誉等主要风险类别；
    - 配套 EWRA、压力测试、KRI、Incident Register、模型风险管理等工具。
3. **制度与实践统一**
    - 政策与流程通过培训和系统控制落实到日常操作；
    - 内部审计和合规监控确保政策不流于形式。
4. **与 MiCA / BaFin 要求对齐**
    - 风险框架充分考虑 MiCA 对客户资产保护、ICT、安全和治理的具体要求；
    - 在德国本地合规（包括 BaFin 行政实践）基础上进行针对性设计。

基于上述安排，我们认为本公司的风险与控制体系已达到 MiCA 下 CASP 机构所需的审慎标准，并具备在德国长期稳定运营的能力。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

内部解释版

这道题是整个"风控 + 内控模块"的总结陈词，要体现：**全面 + 稳健 + 与 MiCA/BaFin 对齐**。

Q231. 请详细说明贵司的交易监测（Transaction Monitoring）整体框架与目标是什么？

A231（监管提交版）

本公司的交易监测框架旨在：

- 识别、分析并处置涉嫌洗钱（ML）、恐怖融资（TF）、制裁违规及其他异常交易行为；
- 满足欧盟 AML 指令、德国实施法及 BaFin 相关指引的要求；
- 保障客户及市场的整体安全与诚信。

核心要素包括：

1. **规则引擎 + 模型分析**
    - 结合规则（Rule-based）与行为/模式分析（Pattern-based）的混合机制；
    - 针对不同风险等级客户与产品采用差异化阈值与场景。
2. **实时与事后监测（Real-time & Post-event）**
    - 部分高风险场景采用近实时监测（如大额提现、高风险链上地址流入）；
    - 对全部账户交易进行事后批量分析，识别复杂可疑模式。
3. **风险分层响应机制**
    - 对交易生成风险评分，按风险等级分配不同的审核流程（自动通过、人工复核、冻结/阻断）。

4. **监管合规对齐**
    - 监测逻辑与本公司 EWRA、CDD/EDD 政策、制裁筛查及链上风控相互联动。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q232. 贵司的交易监测系统是自研、外包还是混合模式？如何确保对规则与参数拥有充分控制权？

A232（监管提交版）

本公司采用 **自研 + 合作工具集成的混合模式**：

1. **核心监测逻辑自研**
    - 关键监控规则、风险评分逻辑及阈值设置由内部合规与风险管理团队设计并在自有系统中配置；
    - 保证对核心监测机制拥有完全的解释权与调整权。
2. **第三方工具辅助**
    - 部分交易分析及链上风险识别引入第三方工具（如链上分析服务），但仅作为输入数据或辅助评分因子；
    - 最终决策由内部政策与系统逻辑主导。
3. **变更与审查**
    - 对规则和阈值的任何重大调整均需通过正式变更流程，由 AML/风控职能审批，并保留记录；
    - 避免供应商不经授权调整影响监测效果。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q233. 交易监测中的场景（Scenarios）是如何设计的？是否基于风险评估（EWRA）？

A233（监管提交版）

1. **基于 EWRA 的场景设计**
    - 本公司首先通过企业级风险评估（EWRA）识别各类主要 ML/TF 风险来源：
        - 客户类型（零售/高净值/法人/虚拟资产业务客户等）；
        - 产品类型（托管、交易、兑换等）；
        - 地域分布；
        - 渠道与交互方式；
        - 链上与链下的综合风险。
2. **场景建模**
    - 基于上述风险，设计不同类别的监测场景，例如：
        - 大额或频繁交易（与客户画像不符）；
        - 高风险司法辖区往来；
        - 集中提现或链上跳转异常；
        - 账户间异常互转；
        - 使用高风险地址或混币服务；
        - 可疑分层（Layering）及结构化交易。
3. **场景定期优化**
    - 定期根据新风险、监管反馈、内部事件或外部 Typologies 更新场景库；
    - 通过回测验证场景有效性与误报率。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q234. 贵司如何对交易监测规则与阈值进行回测（Back-testing）与调优？

A234（监管提交版）

1. **数据抽样与历史分析**

- 利用历史交易数据对既有场景和阈值进行定期回测，评估：
  - 误报率（False Positives）；
  - 漏报风险（潜在可疑交易未触发警报）；
  - 分布与集中度。

2. **模型性能指标**
   - 针对关键场景设定性能指标（例如命中率、可疑交易转化为 STR 的比例）；
   - 分析不同客户群体、产品与地域的差异。
3. **调优流程**
   - 如发现误报率过高导致资源负担过重，或漏报风险较大，则由 AML、风控与技术共同提出阈值调整建议；
   - 调整前后进行 A/B 测试或模拟运行，确保风险可控后再正式上线。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q235. 贵司如何确保交易监测覆盖所有相关业务与渠道，不存在“监测盲区”？

A235（监管提交版）

1. **全覆盖设计**
   - 监测范围包括：
     - 平台内所有客户账户的资金流动；
     - FIAT 与 Crypto 的所有进出账；
     - 各业务模块（托管、撮合、兑换等）的交易数据。
2. **系统接口与对账**
   - 核心交易系统与监测系统通过 API 或数据管道完整对接；
   - 通过每日对账确保所有交易均被捕获并进入监测引擎。
3. **变更控制**
   - 新业务、新产品或渠道上线前，必须评估并确认其交易数据能被监测系统完整接入；
   - 任何业务或系统变更都会经过 Change Management 流程，评估其对监测覆盖范围的影响。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q236. 监测系统生成的警报（Alerts）是如何分类和优先级排序的？处理流程如何？

A236（监管提交版）

1. **警报分级**
   - 根据场景、风险因素与评分，将警报分为若干风险等级（例如：高、中、低）；
   - 对涉及高风险国家、制裁相关或大额异常交易的警报自动归为高风险。
2. **处理流程**
   - **低风险警报**：可由一线分析员进行快速复核与关闭，并保留记录；
   - **中风险警报**：需由资深分析员或 AML 团队综合分析客户资料、历史行为、链上信息等；
   - **高风险警报**：立即升级至 MLRO 审查，必要时冻结/延迟交易并考虑提交 STR。
3. **SLA 管理**
   - 对不同风险等级设定处理时限（例如高风险 24 小时内处理），避免积压。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q237. 贵司如何将交易监测结果与客户风险评级（Customer Risk Rating）联动？

A237（监管提交版）

1. **动态风险评分**
   - 交易监测警报与调查结论作为客户风险评分模型的重要输入因子；
   - 被多次触发高风险警报的客户，其整体风险等级可以被上调（例如由中风险升为高风险）。

2. **触发强化尽调（EDD）**
    - 若客户因连续异常交易被上调风险等级，将触发强化尽调（EDD），包括额外文件、资金来源证明或进一步背景调查。
3. **业务限制**
    - 对极高风险或可疑客户，可采取限额、限制产品使用或终止业务关系等措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q238. 贵司如何在交易监测中识别结构化交易（Structuring / Smurfing）？

A238（监管提交版）

1. **交易模式分析**
    - 监控客户或客户群体在一定时间窗口内的频繁小额交易，特别是接近或略低于某些阈值（例如 KYC/EDD 触发标准）的情况；
    - 识别同一付款人或收款人多次分拆交易的行为。
2. **群组与关系识别**
    - 利用 IP、设备指纹、链上地址关联等信息识别"表面不同实则相关"的账户；
    - 将相关账户的交易一起分析，以识别跨账户的结构化模式。
3. **提升风险等级与 STR 考量**
    - 一旦识别到疑似结构化交易，自动将相关警报提升风险等级，并交由 MLRO 进行 STR 评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q239. 贵司如何通过交易监测识别"无经济合理目的"的交易？

A239（监管提交版）

1. **与客户画像对比**
    - 将客户职业、收入水平、资产规模与交易行为进行比对，如交易规模、频率明显超出合理范围则触发警报。
2. **交易模式分析**
    - 无明显投资或支付目的、资金短时间内多次往返同一或关联账户、资金路径循环等；
    - 资金长期无投资或消费用途，仅在不同账户间流动。
3. **结合链上分析**
    - 对 Crypto 交易，结合链上标签、地址风险评分等信息评估资金真正用途与路径。
4. **审查与 STR 评估**
    - 由 AML 团队与 MLRO 综合判断是否存在 ML/TF 合理怀疑，并决定是否提交 STR。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q240. 贵司如何在交易监测中识别与高风险司法辖区相关的交易？

A240（监管提交版）

1. **国家列表管理**
    - 依据 FATF、欧盟及德国本地高风险国家名单，维护最新的高风险司法辖区清单。
2. **交易地理标记**
    - 对交易的资金来源、目的地及客户所在地进行国家与地区标记；
    - 任何涉及高风险司法辖区的交易自动提高风险评分。
3. **加强审查**
    - 对来自高风险国家的交易，要求更详细的交易目的和资金来源说明；
    - 频繁或异常模式将被升级为高风险警报，纳入 MLRO 审查与 STR 评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q241. 请说明贵司如何识别和监测"账户间异常互转"及"循环交易"行为。

A241（监管提交版）

1. **网络关系分析**
   - 建立账户间交易网络图，分析资金流向结构；
   - 标记高频互转、闭环资金路径和"小圈子互转"模式。
2. **特征识别**
   - 短时间内多账户之间反复互相转账，缺乏经济用途；
   - 资金仅在少数几个地址/账户间循环流动。
3. **风险响应**
   - 将此类模式识别为潜在洗钱或 Layering 行为，自动生成高风险警报；
   - MLRO 综合其他信息（客户背景、链上标签）做进一步评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q242. 对于大额或异常提现（Withdrawal），贵司的监控及审批机制如何?

A242（监管提交版）

1. **大额阈值设定**
   - 基于客户类别、风险评级及历史行为，为不同客户群体设定大额提现阈值；
   - 超过阈值自动触发警报，并冻结该笔提现待审核。
2. **多层审批**
   - 大额或异常提现由 AML 分析员和运营团队联合审查；
   - 对高风险情况，须经 MLRO 或高级管理层批准后方可放行或拒绝。
3. **资金来源与用途复核**
   - 必要时要求客户提供资金来源和用途说明及相关证明材料；
   - 如仍存在合理怀疑，则提交 STR，并在有权范围内中止或延迟交易。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q243. 交易监测系统是否支持对"跨产品、跨渠道"的综合监控？例如现金、Crypto 与法币之间的联动分析。

A243（监管提交版）

是的，本公司交易监测系统支持跨产品、跨渠道的综合分析：

1. **统一客户视图（Single Customer View）**
   - 所有与客户相关的交易（Crypto 入出金、法币充值/提现、账户间转账等）均在统一视图下呈现。
2. **综合风险评分**
   - 把 Crypto 与 FIAT 流动信息共同纳入风险模型，以识别利用不同渠道进行 Layering 或 Value Transfer 的行为。
3. **场景联动**
   - 例如：客户在短期内将法币转换为 Crypto，再多次跨链转移，随后集中提现至第三方账户 → 自动触发跨渠道综合场景。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q244. 贵司如何通过交易监测识别潜在的恐怖融资（TF）行为，而不仅是传统洗钱?

A244（监管提交版）

1. **制裁与名单筛查**
   - 结合制裁名单（OFAC/EU/UN）与特定恐怖组织名单，对交易对象与链上地址进行筛查。
2. **Typology 应用**
   - 参考 FATF 与德国联邦刑事警察局（BKA）发布的 TF Typologies，识别：
     - 小额多笔汇集；

- 与特定高风险区域或边境地区关联的资金流动；
- 利用小额捐赠或众筹形式进行资金筹集的模式。

3. **链上行为分析**
   - 对已知与恐怖组织有关的链上集群进行标签管理，在发现关联时自动触发高风险警报。
4. **与情报信息联动**
   - 与银行合作伙伴或情报部门发布的可疑地址/模式信息进行对接与更新。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q245. 贵司如何确保交易监测团队（TM/AML Analysts）具备足够的经验和专业能力？

A245（监管提交版）

1. **招聘要求**
   - 对 TM/AML 分析岗位设定明确的任职条件，包括：
     - 反洗钱从业经验；
     - 熟悉 Crypto 业务与链上分析更佳；
     - 具备相关学历或认证（如 ACAMS 等）。
2. **持续培训**
   - 提供定期的 AML / TF / 制裁 / Typologies 等专题培训；
   - 对新上线场景和工具进行操作培训和案例演练。
3. **绩效与质量监控**
   - 对分析员的警报处理质量进行抽样复核，评估其判断力与文书质量；
   - 对误判较多的人员制定改进计划或重新分配岗位。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q246. 贵司是否记录所有交易警报的完整处理过程？记录内容包括哪些？保存多久？

A246（监管提交版）

是的，本公司对所有警报及处理过程进行全面记录：

1. **记录内容**
   - 警报触发时间与原因（场景 ID、规则、风险评分）；
   - 分析员的调查步骤与结论；
   - 参考的客户资料与补充文件；
   - 是否升级至 MLRO；
   - 最终处理决定（关闭、加强监控、限制账户、提交 STR 等）。
2. **保存期限**
   - 所有记录至少保存若干年（例如 5 年或以上），符合德国法律与监管要求；
   - 与 STR 相关记录按照适用法规要求延长保存时间。
3. **可追溯性**
   - 记录存储在安全的合规系统中，权限受控并保留访问审计日志，以便监管现场检查时查验。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q247. 贵司如何处理误报（False Positives），以平衡监测有效性与资源消耗？

A247（监管提交版）

1. **分类统计**
   - 定期统计各场景的误报率，分析误报原因（例如阈值过低、场景设计过于宽泛等）。
2. **精细化调参**
   - 在不降低风险敏感度的前提下，对误报率过高的场景进行优化，如增加客户画像维度或调整阈值。

3. **自动化辅助**
    - 通过风险分级、历史行为评分等手段减少低价值警报；
    - 对明显低风险、重复性高的模式，可使用自动关闭或快速处理机制。
4. **资源管理**
    - 合理配置分析员数量与经验结构，使其既能处理警报量，也可专注于高风险案件。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q248. 贵司如何防止"警报疲劳"（Alert Fatigue），确保分析员对高风险警报保持足够敏感度？

A248（监管提交版）

1. **工作量平衡**
    - 分配合理的案件数量，避免个别分析员长期超负荷；
    - 定期调整案件分配以平衡压力。
2. **重点聚焦**
    - 运用风险评分机制突出高风险警报，确保优先处理；
    - 对高风险警报的质量和响应时间进行专项监控。
3. **团队支持与轮岗**
    - 通过团队协作机制和轮岗制度，避免长期集中处理高压案件导致疲劳；
    - 提供心理健康与职业辅导资源（如适用）。
4. **工具优化**
    - 改善系统界面与工作流，减少重复性操作时间，让分析员更多精力用于"判断"而非"点按钮"。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q249. 交易监测结果如何反馈到高层管理和董事会，以支持决策与资源配置？

A249（监管提交版）

1. **定期管理报告（MI）**
    - 向高级管理层和风险委员会定期提交交易监测报告，包括：
        - 警报数量与趋势；
        - 按风险等级和 Typology 分类；
        - STR 数量和主要原因；
        - 高风险客户与地域分布；
        - 关键改进措施。
2. **董事会层面报告**
    - 至少每季度向董事会报告 AML/TF 风险状况，交易监测是其中的重要章节；
    - 对重大 Typology 或系统性风险进行专题汇报。
3. **资源与战略调整**
    - 董事会根据报告结果，在人员编制、技术投入、产品策略等方面作出调整，以提升整体风险防控能力。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q250. 请说明为何认为贵司的交易监测框架足以满足德国及欧盟监管对 MiCA CASP 的期望标准。

A250（监管提交版）

本公司认为，交易监测框架已经符合并在多方面超出 MiCA 与德国 AML/TF 监管的要求，主要理由如下：

1. **风险基础原则（Risk-based Approach）**

- 所有场景与阈值设计基于 EWRA 结果，针对不同客户、产品与地域进行差异化设置。

2. **技术与专业结合**
   - 采用自研规则引擎 + 第三方工具的混合模式，在保持技术先进性同时确保内部控制权；
   - 团队具备 Crypto 与传统金融双重经验。
3. **与链上监测与制裁筛查的联动**
   - 将链上风险评分、制裁筛查与交易监测紧密整合，形成闭环。
4. **治理与透明度**
   - 完整的记录与报告链条，支持监管检查与内部复盘；
   - 高层与董事会定期审阅并参与决策。

基于上述安排，我们有信心交易监测体系能够有效识别并管理与本公司业务相关的 ML/TF 风险，满足德国 BaFin 对 MiCA CASP 的审慎监管标准。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q251. 请说明贵司整体的链上反洗钱（On-chain AML）框架与目标是什么?

A251（监管提交版）

本公司的链上反洗钱（On-chain AML）框架旨在：

- 识别并管理虚拟资产交易中与洗钱（ML）、恐怖融资（TF）、制裁规避及其他金融犯罪相关的链上风险；
- 将链上行为数据与链下客户信息（KYC/EDD）有机结合，形成统一的风险视图；
- 满足欧盟 AML 框架、MiCA 及德国本地监管（包括 BaFin）对虚拟资产业务的审慎监管要求。

框架核心包括：

1. **链上风险评分系统（On-chain Risk Scoring）**
   - 对每一笔链上交易和每一个链上地址生成风险评分，维度包括：
     - 制裁风险（Sanctions Risk）；
     - ML/TF 风险（ML/TF Risk）；
     - 混币器/匿名工具暴露度（Mixers/Privacy Tools）；
     - 暗网及非法市场暴露（Darknet Exposure）；
     - 已知诈骗/黑客集群关联等。
2. **第三方专业工具 + 内部规则引擎**
   - 使用市场主流链上情报工具（如 Chainalysis / TRM Labs / Crystal 等）获取标签和基础评分；
   - 内部规则引擎对来自高风险集群、Mixer、Bridge、DeFi 合约等进行二次评分与规则处理。
3. **与交易监测及 STR 决策联动**
   - 链上风险评分直接输入交易监测系统；
   - 高风险链上交易自动升级审查，并进入 STR 评估流程。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q252. 贵司使用哪些链上分析工具或服务来支持 AML 工作？如何评估其可靠性?

A252（监管提交版）

1. **使用的工具类型**
   - 本公司使用一家或数家全球主流的链上情报与分析服务提供商（如 Chainalysis、TRM Labs 或其他同等级供应商）；
   - 工具涵盖：地址标签库、风险评分、Typologies 数据库、Sanctions/黑名单集成等。
2. **供应商尽职调查**
   - 对该等供应商进行完整的 Vendor Due Diligence：
     - 技术能力与市场声誉；
     - 客户基础（是否服务于银行、监管机构、主流 VASP）；
     - 数据覆盖度与准确性；
     - 安全性与合规性（GDPR、数据安全等）。

3. **持续评估与对比**
    - 定期评估工具的准确性与适用性，如有必要，使用多家供应商交叉验证高风险案件；
    - 在供应商更新 Typologies 和风险模型时，结合内部经验进行审查和适配。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q253. 贵司如何设计链上地址风险评分模型？主要考虑哪些风险因子？

A253（监管提交版）

链上地址风险评分模型综合了外部工具评分与内部规则，主要风险因子包括：

1. **制裁与黑名单暴露度**
    - 地址是否直接或间接与受制裁实体、恐怖组织相关地址有资金往来；
    - 关联路径的深度与权重。
2. **犯罪相关标签**
    - 地址或其集群是否被标记为：
        - 黑客攻击（Hacks）、
        - 勒索软件（Ransomware）、
        - 诈骗（Scams）、
        - 暗网市场（Darknet Markets）、
        - 非法赌博等。
3. **混币器与匿名工具暴露**
    - 是否使用 Mixer / Tumbler；
    - 是否依赖高隐私币（如 Monero、Zcash 特定模式）或隐身地址功能。
4. **跨链桥与高风险 DeFi 协议暴露**
    - 是否频繁通过高风险跨链桥（Bridge）或已知风险 DeFi 合约进行资金转换和分层。
5. **行为模式与集中度**
    - 资金流入来源与流出目的地的多样性；
    - 是否表现为典型 Layering / Structuring 模式。

评分结果划分为若干等级（如 Low / Medium / High / Severe），并与交易监测和 STR 流程直接联动。
（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q254. 贵司如何处理来自高风险链上地址的入金（Inbound Transactions）？

A254（监管提交版）

对于标记为**高风险或严重风险**（例如涉及制裁、黑客、勒索软件、暗网等标签）的入金，本公司采取如下措施：

1. **自动标记与冻结评估**
    - 系统自动将该入金标记为高风险；
    - 如相关地址与制裁集群高度相关，可在法律允许范围内冻结或拒绝入账。
2. **立即升级至 MLRO**
    - 将案件升级至 MLRO，进行全面复核，包括：
        - 客户 KYC/EDD 信息；
        - 历史交易行为；
        - 资金用途说明（如可获得）；
        - 需要时向客户索取补充资料。
3. **STR 考量**
    - 如合理怀疑涉及 ML/TF 或制裁规避，将向负责的 FIU 提交 STR；
    - 同时视情况对客户采取限制或终止业务关系等措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q255. 对于客户向高风险链上地址的出金（Outbound Transactions），贵司的监控与控制措施是什么?

A255（监管提交版）

1. **事前过滤与警报**
   - 客户提交出金地址后，系统先对该地址进行链上风险检查；
   - 若地址属于制裁、恐怖组织或严重犯罪标签 → 交易被自动阻断并生成高风险警报。
2. **风险阈值与人工复核**
   - 若为高风险但非完全禁止（例如高风险 DeFi 协议或有争议的服务），将触发人工复核：
     - 评估交易目的；
     - 核查客户使用场景是否有商业合理性。
3. **拒绝或限制**
   - 对于无法证明合法目的或严重高风险的地址，本公司有权拒绝该笔提现，并视情况考虑终止业务关系及提交 STR。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q256. 贵司如何识别和应对混币服务（Mixers / Tumblers）相关风险?

A256（监管提交版）

1. **混币服务识别**
   - 利用链上情报工具识别与已知 Mixer 集群相关的地址；
   - 识别 Peel Chain、结构化跳转及其他隐匿交易路径的典型模式。
2. **风险处理原则**
   - 对直接或间接与 Mixer 相关的资金流入/流出进行高风险标记；
   - 对频繁使用混币服务且无法提供合理解释的客户，提升其客户风险等级并开展 EDD。
3. **业务限制与 STR**
   - 严重情况下，可限制或禁止涉及混币服务的交易；
   - 对无合理商业目的的使用行为，将纳入 STR 评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q257. 贵司如何识别与 DeFi 协议相关的链上 AML 风险?

A257（监管提交版）

1. **协议分类与名单管理**
   - 将 DeFi 协议按风险等级划分：
     - 受监管/合规度较高的协议；
     - 风险中等的去中心化交易所（DEX）；
     - 高风险或被监管机构点名的协议（例如曾发生巨额黑客事件、存在明显洗钱 Typologies 的协议）。
2. **合约地址标签**
   - 对主要 DeFi 协议的智能合约地址进行标签管理；
   - 与链上分析工具的协议标签集成。
3. **交易行为分析**
   - 分析客户与 DeFi 协议之间的交互模式：
     - 是否频繁使用高风险流动性池；
     - 是否利用 DeFi 进行跨链资产转移和快速分层；
     - 是否表现为典型洗钱路径的一部分。
4. **管控措施**
   - 对于与高风险 DeFi 协议交互的交易提升风险评分，必要时进入 EDD 与 STR 评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q258. 贵司如何在链上 AML 中识别与跨链桥（Bridges）相关的洗钱风险?

A258（监管提交版）

1. **桥协议监控**
   - 维护主要跨链桥协议及其合约地址的清单，并根据事件（例如大额黑客攻击、制裁行动）持续更新其风险等级。
2. **跨链路径分析**
   - 识别资金从一条链经由桥协议到另一条链的路径，分析：
     - 是否存在快速、多次跨链跳转；
     - 是否通过组合使用多个桥增加追踪难度。
3. **高风险桥限制**
   - 对被监管机构关注或与重大黑客事件相关的桥协议进行限制或禁止；
   - 对涉及这些桥的资金流入/流出自动提升风险评分并触发人工复核。
4. **与 STR 流程衔接**
   - 在分析中若形成合理怀疑，进入 STR 评估并向 FIU 报告。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q259. 贵司如何识别与 NFT（非同质化代币）相关的潜在洗钱风险?

A259（监管提交版）

1. **高风险特征识别**
   - NFT 以远高于或低于市场合理价格成交；
   - 同一地址或一组关联地址之间的频繁买卖；
   - 未见明显市场推广或艺术价值，但却出现高价成交。
2. **地址与平台风险评估**
   - NFT 交易对手地址若具有高风险标签（暗网、诈骗、Mixer 暴露等），相应交易被标为高风险；
   - 涉及高风险 NFT 市场平台或智能合约时提升风险评分。
3. **风险应对措施**
   - 对 NFT 相关高风险交易进行 EDD，包括要求客户说明资产来源及交易目的；
   - 无合理商业解释时，将进入 STR 评估。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q260. 贵司是否支持对隐私币（Privacy Coins）相关交易？如支持，如何控制 AML 风险?

A260（监管提交版）

本公司的原则为：

1. **审慎政策**
   - 对完全不可追踪或极高匿名性的隐私币持高度谨慎态度；
   - 视业务模式与监管指引，本公司可以选择：
     - 完全不支持；或
     - 在严格限制下支持公开透明度较高的隐私功能，并施加额外控制。
2. **额外尽调与限制**
   - 若支持相关资产，将对涉及隐私币的客户和交易强制实施 EDD；
   - 设置更高的风险权重与监测阈值；
   - 对大额或频繁使用隐私币的客户进行更严格的资金来源与用途核查。
3. **与监管期望对齐**
   - 一旦监管机构对某类隐私币提出限制或禁止，本公司将及时调整支持范围和相关政策。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q261. 贵司如何将链上地址信息与客户 KYC 资料正确关联，确保"地址归属"的准确性?

A261（监管提交版）

1. **地址绑定流程**
   - 客户在绑定其外部钱包地址时，需通过平台的验证流程（例如签名验证、微额转账验证等），证明其对该地址拥有控制权。
2. **KYC + 地址映射**
   - 通过后端系统将验证通过的链上地址与客户唯一 ID 进行绑定；
   - 一个客户可绑定多个地址，但所有地址信息集中在统一客户视图中。
3. **变更与解绑控制**
   - 对地址变更进行日志记录与风控检查，必要时再次进行验证；
   - 对频繁更换地址的客户提高关注度和风险评分。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q262. 贵司如何识别"地址共用"（Shared Address）或托管服务商代持地址的风险?

A262（监管提交版）

1. **标签与情报识别**
   - 利用链上情报工具识别交易对手地址是否属于托管型服务商、交易所或混合服务（混币 + 托管）；
   - 将这些地址标记为"共享地址/服务商地址"。
2. **风险评估**
   - 对与这类地址往来频繁的客户进行额外审查，评估是否实际在利用第三方进行洗钱或掩盖资产真实归属；
   - 若第三方服务商本身被标记为高风险 VASP 或无牌照服务商，则提高风险等级。
3. **附加尽调**
   - 在必要时要求客户披露其在第三方服务商的账户信息与交易用途，以便形成完整 AML 视图。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q263. 贵司如何识别与诈骗（Scams / Fraud）相关的链上资金?

A263（监管提交版）

1. **诈骗标签库**
   - 使用工具识别被标记为诈骗集群（例如投资骗局、伪装交易平台、Ponzi、恋爱诈骗）的地址；
   - 定期更新并接收外部情报（包括监管通报、其他金融机构共享信息等）。
2. **行为模式识别**
   - 典型模式：大量小额受害者转入同一或少量地址；
   - 资金从诈骗集群流出后，迅速经由 Mixer、DeFi、跨链桥等散布。
3. **客户保护与 STR**
   - 若客户资金流向已知诈骗集群，本公司会：
     - 尽可能提示客户警惕诈骗（在法律允许范围内）；
     - 对该客户行为与资金来源进行评估；
     - 必要时提交 STR。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q264. 贵司如何利用链上数据支持资金来源（Source of Funds）与财富来源（Source of Wealth）的核查?

A264（监管提交版）

1. **链上轨迹分析**
    - 对客户提供的 Crypto 资产进行链上回溯，分析资金来自：
        - 主流合规交易所；
        - 挖矿收入；
        - OTC 服务商；
        - 高风险集群或匿名工具。
2. **佐证材料结合**
    - 将链上交易轨迹与客户提供的线下证明材料（收入文件、投资协议、公司报表等）进行匹配与交叉验证。
3. **风险判断**
    - 若链上路径显示资金大量来自高风险集群或无清晰来源，则对 SOF/SOW 认定持保留态度，并根据情况要求额外说明或拒绝业务。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q265. 贵司如何将链上 AML 结果整合进整体交易监测与 STR 决策流程?

A265（监管提交版）

1. **系统集成**
    - 链上风险评分与地址标签通过技术接口自动输入交易监测系统；
    - 每一笔交易的链上风险评分与 Typology 信息将影响交易监测的综合风险评分。
2. **警报联动**
    - 交易监测系统中的高风险警报会自动调取相关链上分析结果，辅助 AML 分析员和 MLRO 决策。
3. **STR 决策**
    - STR 评估模板中包含专门的"链上证据"部分，分析相关地址、路径和风险标签；
    - 确保 STR 报告的事实基础覆盖链上与链下信息。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q266. 贵司是否建立了针对链上 AML 的专门政策与操作程序？主要内容包括哪些方面?

A266（监管提交版）

是的，本公司制定了专门的《链上反洗钱与制裁风险管理政策》，主要包括：

1. **链上风险评估框架**
    - 适用范围与目标；
    - 风险因子与评分方法；
    - 不同风险等级对应的控制措施。
2. **工具与数据使用原则**
    - 识别和选择链上分析服务商的标准；
    - 数据使用、验证与交叉检验的方法。
3. **操作流程与职责分工**
    - 链上风险监测的日常操作流程；
    - AML 分析员、MLRO、技术团队的职责划分；
    - 变更管理与例行复核机制。
4. **记录保存与监管合作**
    - 链上分析记录与报告的保存年限；
    - 在监管机构或 FIU 要求时，如何提供链上证据与分析支持。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q267. 贵司如何确保链上 AML 团队具备足够的技术与合规知识?

A267（监管提交版）

1. **复合背景要求**
   - 鼓励链上 AML 团队拥有多元背景：
     - 传统金融 AML / Compliance；
     - 区块链技术或数据分析；
     - 信息安全或计算机科学。
2. **定向培训**
   - 提供链上 Typologies、DeFi / NFT 洗钱模式、Mixer 和 Bridge 风险等专题培训；
   - 邀请外部专家或供应商开展工作坊与案例分析。
3. **持续学习与认证**
   - 鼓励加入专业组织（如 ACAMS）并获取相关认证；
   - 鼓励参与行业会议与监管机构发布的专题研讨会，及时更新知识体系。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q268. 贵司在链上 AML 工作中如何应对"数据不完整或存在误差"的问题?

A268（监管提交版）

1. **多源数据与交叉验证**
   - 尽可能使用多家供应商或多种数据源交叉验证重要案件；
   - 不完全依赖单一工具的标签，对重大决策进行人工分析与补充调查。
2. **审慎决策原则**
   - 在数据不完整或存在较大不确定性时，采取审慎态度：
     - 如果风险倾向明显偏高，宁可将其视为高风险处理；
     - 对其进行 EDD 和增强监测。
3. **人工判断与记录**
   - AML 分析员需在案件记录中明确说明数据局限与判断依据，确保日后审计与监管检查可追溯。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q269. 贵司如何及时根据新的链上 Typologies 和监管期望更新 AML 场景和控制措施?

A269（监管提交版）

1. **监管与行业信息跟踪**
   - 定期关注 BaFin、FATF、欧盟及其他监管机构发布的关于虚拟资产 ML/TF 新 Typologies 文档；
   - 跟踪主要链上分析工具供应商发布的最新趋势报告。
2. **内部评审与落地**
   - 由 AML/风险/技术组成工作小组，评估新 Typologies 对本公司业务的适用性；
   - 设计或更新相关链上场景和控制措施（例如新增特定 Mixer、Bridge、DeFi 模式的监测规则）。
3. **培训与文档更新**
   - 更新内部政策与程序文件；
   - 对 AML 分析团队进行有针对性的培训和案例演练。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q270. 请说明贵司为何认为现行链上 AML 框架足以满足德国 BaFin 与 MiCA 对 CASP 的审慎监管要求。

A270（监管提交版）

本公司认为现行链上 AML 框架足以满足并在若干方面超出德国 BaFin 和 MiCA 的监管期望，主要理由如下：

1. **风险基础方法落地**
   - 框架完全围绕风险基础原则（RBA）设计，充分考虑客户、产品、地域与链上行为的综合风险。
2. **技术手段与专业判断结合**
   - 采用成熟的链上情报工具，同时保留内部规则与人工分析，不盲目依赖单一供应商评分。
3. **与整体 AML/CTF 体系的深度整合**
   - 链上 AML 与 KYC/EDD、交易监测、制裁筛查及 STR 流程形成完整闭环；
   - 能够对可疑资金流进行全链条追踪与记录。
4. **持续改进机制**
   - 定期根据新 Typologies、监管指引及内部经验更新控制措施；
   - 通过培训与复核确保团队能力与框架有效性不断提升。

因此，我们有信心链上 AML 体系能够有效识别并管理与本公司业务相关的主要链上 ML/TF 风险，符合德国 BaFin 对 MiCA CASP 的审慎监管标准。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q271. 请说明贵司内部审计（Internal Audit）职能的设置方式及其独立性如何得到保障？

A271（监管提交版）

本公司已设立独立的内部审计（Internal Audit，IA）职能，用以对整体内部控制体系（包括 AML、ICT、风险管理、Outsourcing、Safeguarding 等）进行独立、客观的审查与评估。核心要点如下：

1. **组织架构与汇报线**
   - 内部审计部门**不隶属于运营、合规或风险管理部门**；
   - IA 直接向董事会审计委员会（Board Audit Committee）汇报；
   - 重大审计发现将同时通报董事会及相关委员会（例如风险委员会、合规委员会）。
2. **独立性保障措施**
   - 内部审计人员的绩效考核由审计委员会负责，而非被审计部门；
   - IA 对审计范围和方法具有独立决定权；
   - 任何部门不得干预 IA 对审计结果的结论与书面报告内容。
3. **审计范围与频率**
   - 每年制定《年度内部审计计划》，覆盖 AML、ICT/DORA、Outsourcing、Safeguarding、交易监测、链上 AML 等关键领域；
   - 根据风险导向原则（Risk-based Approach），对高风险领域实施更高频次审计。
4. **跟踪与整改**
   - 为每项审计发现制定整改计划，明确责任人与时间表；
   - IA 对整改进展进行跟踪并向审计委员会定期汇报。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q272. 贵司如何安排年度外部审计（External Audit），以及审计范围通常包括哪些内容？

A272（监管提交版）

1. **外部审计机构选择**
   - 本公司委聘具有充分资质、在金融服务与虚拟资产领域具备经验的审计事务所，优先考虑在欧盟/德国具有良好声誉的审计机构；
   - 审计机构的任命与更换需经董事会及/或股东大会批准。
2. **审计范围**
   - 财务报表审计（Financial Statements Audit）；
   - 客户资产隔离与 Safeguarding 控制的有效性检验；
   - 对 IT 控制、访问管理与变更管理的高层次测试；
   - 在必要情况下，审计机构亦可对 AML/CTF 控制进行专题审阅。
3. **审计意见与管理建议书（Management Letter）**
   - 外部审计出具经审计财务报表及相关审计意见；
   - 审计机构提供管理建议书，就内部控制弱点提出改进建议；

- 董事会及管理层对管理建议进行讨论并制定整改计划。

4. **向监管机构的配合与披露**
   - 如 BaFin 或其他主管机关要求，本公司将提供相关外部审计报告或摘要；
   - 如审计中发现重大不规范情形，本公司将根据法律与监管要求进行适当披露。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q273. 贵司向 BaFin 提交的监管报告（Regulatory Reporting）主要包括哪些类型？频率如何？

A273（监管提交版）

根据适用的欧盟法规及德国本地实施规则，本公司主要履行以下监管报告义务（具体频率与格式以 BaFin 要求为准）：

1. **定期报告（Periodical Reports）**
   - 资本充足情况与自有资金报告（Own Funds / Capital Adequacy）；
   - 业务量与交易数据统计（包括托管余额、交易量等）；
   - 客户资产 Safeguarding 情况与对账结果摘要；
   - Outsourcing 重大变化报告。
2. **合规与风险报告（Compliance / Risk Reports）**
   - 年度合规报告（Annual Compliance Report）；
   - 重大合规事件或违规事项报告；
   - 风险管理与内部控制体系的重大变化通报。
3. **AML / CTF 报告**
   - 可疑交易报告（STR）向国家金融情报机构（FIU）提交；
   - 在监管要求下，对高风险客户群体与 Typologies 的阶段性总结报告。
4. **ICT / DORA 相关报告**
   - 重大 ICT 事件和运营中断事件的分阶段报告；
   - 年度 DORA 合规情况说明。
5. **频率示例**
   - 若无另行规定，通行做法为：
     - 财务与资本类：季度或半年；
     - 合规与风险类：至少年度一次；
     - 重大事件类：按事件发生后法定时限（如小时/日）及时报告。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q274. 贵司如何确保监管报告中数据的准确性与完整性？是否建立数据质量控制（Data Quality Controls）？

A274（监管提交版）

为确保监管报告数据的**准确性（Accuracy）、完整性（Completeness）、一致性（Consistency）**，本公司建立了如下数据质量控制体系：

1. **源系统控制（Source Systems Controls）**
   - 所有关键数据来自经授权的核心生产系统（Core Systems），禁止人工随意录入或离线表格为主要来源；
   - 对系统接口进行完整性检查与对账，防止数据丢失或重复。
2. **数据处理与汇总控制**
   - 数据处理逻辑（Aggregation / Transformation Rules）以文档形式固定并经复核；
   - 对关键指标采用多维度复核（例如总和 vs 分项求和、跨报表交叉核对）。
3. **职责分离与复核**
   - 报告编制、复核与最终批准由不同人员/岗位承担；
   - 合规或风险管理部门参与对关键监管报告的复核。

4. **错误纠正与报告机制**
    - 若发现已提交数据存在错误，本公司将按照监管要求尽快提交更正文件，并解释原因与后续预防措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q275. 贵司是否编制年度合规报告（Annual Compliance Report）？主要内容包括哪些方面?

A275（监管提交版）

是的，本公司每年形成一份书面的《年度合规报告》（Annual Compliance Report），由合规负责人起草，并提交董事会审阅，必要时提供给监管机构。主要内容包括：

1. **合规框架概述**
    - 公司整体合规治理结构；
    - 三道防线（业务、风险/合规、内部审计）的运行概况。
2. **全年合规活动总结**
    - 内部政策和程序的更新情况；
    - 合规培训完成情况（包括 AML、ICT、安全等）；
    - 监管要求变更的跟踪与落实情况。
3. **合规事件与违规情况**
    - 年内发生的重大合规事件或违规案件；
    - 监管检查结果及整改情况；
    - 外部审计或内部审计指出的合规缺陷及其整改进度。
4. **风险评估与改进建议**
    - 对当前合规风险状况的评估；
    - 对未来一年合规重点领域的建议及计划。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q276. 请说明贵司记录保存（Record Keeping）政策，包括保存期限与保存方式。

A276（监管提交版）

1. **政策框架**
    - 本公司制定了《记录保存与档案管理政策》（Record Keeping & Archiving Policy），遵守欧盟与德国法律（包括 AML 相关法规、MiCA 要求、数据保护法规如 GDPR）以及 BaFin 指引。
2. **保存对象**
    - 客户身份识别文件（KYC/EDD）；
    - 交易记录（包括链上及链下、订单与执行详情）；
    - 监管报告及相关工作底稿；
    - 合同文件、内部政策、程序与会议记录；
    - 审计报告、合规报告与风险报告。
3. **保存期限**
    - AML/KYC 与交易相关记录：通常不少于 5 年或法律规定的更长期限；
    - 审计与监管报告：不少于 5 年或适用规则要求；
    - 若因监管调查或诉讼需要，相关记录将延长保存。
4. **保存方式与安全性**
    - 采用电子存档系统，具备访问控制、不可篡改（例如 WORM）、备份与灾备机制；
    - 对涉及个人数据与敏感信息的记录采取加密与最小权限访问。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q277. 贵司如何向董事会和高级管理层定期汇报风险与合规情况（Management Information, MI）？

A277（监管提交版）

1. **定期管理报告（Management Reports）**
   - 合规部门、风险管理部门以及 AML/MLRO 每季度出具管理信息报告（MI），包括：
     - 主要合规活动和政策更新；
     - 关键风险指标（KRIs）；
     - 交易监测与 STR 概况；
     - ICT/运营事件统计；
     - 重大审计发现与整改进度。
2. **委员会与董事会会议**
   - MI 报告在合规委员会、风险委员会及董事会会议上进行汇报与讨论；
   - 对重大议题（例如重大 ICT 事件、重大合规缺陷）进行专题汇报。
3. **决策支持作用**
   - 基于 MI 报告，董事会和高级管理层可：
     - 调整公司风险偏好与战略；
     - 决定资源配置（例如增加 AML/ICT 预算）；
     - 审议重大整改计划和优先级。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q278. 如果发现已提交给 BaFin 的报告存在错误，贵司的纠正流程是什么？

A278（监管提交版）

1. **错误识别与内部通报**
   - 错误可由内部复核、外部审计或监管反馈发现；
   - 一经识别，将立即在内部通报给合规、风险管理和相关业务部门。
2. **影响评估**
   - 评估错误对监管报告的实质性影响（Qualitative & Quantitative）；
   - 确认是否影响监管对公司风险状况的判断。
3. **更正与说明**
   - 如确认需要更正，本公司将在合理时间内向 BaFin 提交更正版本（Revised Report），并附上：
     - 更正内容说明；
     - 错误原因分析；
     - 已采取或计划采取的防止类似错误的措施。
4. **内部控制改进**
   - 对导致错误的流程环节进行改进，包括数据质量控制、复核程序和人员培训。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q279. 贵司在 DORA 框架下，如何报告重大 ICT 事件？流程和时间要求如何落实？

A279（监管提交版）

1. **重大 ICT 事件定义与识别**
   - 根据 DORA 及相关技术标准，将影响系统可用性、数据完整性、客户服务或安全性的重要事件定义为"重大 ICT 事件"；
   - 在内部事件分类体系中区分 Critical / High / Medium / Low，并标明是否触发监管报告门槛。
2. **内部升级与事件管理**
   - 事件发生后，立即启动 Incident Response Plan；
   - 由 ICT、风险管理、合规与 MLRO 组成的事件响应小组评估事件影响与严重程度。

3. **监管报告步骤**
   - 按 DORA 规定的阶段性报告要求上报：
     - 初步报告（Initial Notification）在规定时限内（如数小时内）提交；
     - 中期报告（Intermediate Update）在事件处理中定期更新；
     - 最终报告（Final Report）在事件解决后一定期限内提交，说明根本原因与整改措施。
4. **记录与持续改进**
   - 对所有重大 ICT 事件的处理过程进行完整记录；
   - 在年度 DORA 合规评估和内部审计中回顾该类事件，以改进控制与响应能力。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q280. 贵司是否将监管报告、审计结果和风险评估用于持续改进内部控制体系？如是，请说明机制。

A280（监管提交版）

是的，本公司将监管报告、内部与外部审计结果、风险评估与事件记录整合，形成**持续改进（Continuous Improvement）机制**，主要包括：

1. **年度控制评审**
   - 基于审计发现、监管反馈与 KRIs，对现有控制措施的有效性进行评估；
   - 确定需要加强或调整的领域，例如 AML 规则、ICT 防护、Outsourcing 管理等。
2. **整改计划与优先级**
   - 编制全公司范围的整改计划（Remediation Plan），明确优先级、责任人与完成期限；
   - 由风险与合规部门协调统一跟踪整改进度。
3. **政策与程序的更新**
   - 根据监管新要求和行业最佳实践，定期更新内部政策、程序与操作手册；
   - 更新内容须通过适当的审批程序并向相关员工进行培训。
4. **反馈闭环**
   - 将控制改进情况通过 MI 报告反馈到董事会与高级管理层；
   - 确保管理层对控制体系变化及其效果有充分了解，并可据此调整战略与资源配置。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q281. 请说明贵司如何确保不发生市场滥用行为（Market Abuse），特别是在自营、做市或持仓管理方面？

A281（监管提交版）

本公司已建立专门的《市场行为与市场滥用防控政策》（Market Conduct & Market Abuse Prevention Policy），以防止任何形式的市场滥用行为，包括但不限于：价格操纵（Price Manipulation）、内幕交易（Insider Dealing）、误导性信息披露及其他不当市场行为。核心措施如下：

1. **业务模式限制**
   - 本公司目前不从事主动做市（Proprietary Market Making）或利用自营头寸进行价格引导；
   - 若未来涉及做市或自营，将设置严格的"自营账户"与"客户账户"隔离机制，并报请监管机关知悉。
2. **交易监控机制**
   - 实施交易监控系统，对异常价格波动、大额订单、频繁撤单及自成交等行为进行实时识别；
   - 对可能构成操纵行为的交易模式（如洗售交易、虚假挂单）自动生成警报并提交合规团队复核。
3. **员工行为约束**
   - 员工及关键岗位人员不得利用内部信息进行个人交易；
   - 对员工账户实施申报制度和取样监控，并设定最短持有期限及禁售期。
4. **内部培训与文化**
   - 定期开展市场行为与市场滥用相关培训，确保员工理解欧盟及德国相关法规（如 MAR 等）的要求；
   - 在公司内部营造"零容忍市场滥用"的文化氛围。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q282. 贵司如何识别和防止“价格操纵”（Price Manipulation），例如虚假报价、拉抬打压等行为？

A282（监管提交版）

1. **监控规则（Surveillance Rules）**
   - 我们在交易监控系统中预设了针对价格操纵的规则，包括：
     - 异常大额订单集中出现（Pump/Dump Pattern）；
     - 在流动性较弱的市场中通过自成交或对倒制造虚假成交量；
     - 在收盘前短时间内出现明显“拉抬”或“打压”行为。
2. **订单与成交分析**
   - 监控订单簿中的挂单深度与撤单频率，对大量短时挂单后迅速撤单（Layering/Spoofing）行为进行标记；
   - 对单一地址或关联账户间频繁对敲交易进行分析，识别洗售交易模式。
3. **预防措施**
   - 限制内部账户参与可疑交易或高风险交易对；
   - 对参与可疑行为的客户进行增强尽调（EDD），必要时采取限制交易或终止关系的措施。
4. **报告与升级**
   - 若怀疑存在价格操纵行为，合规与 MLRO 将联合评估其是否触发可疑交易报告（STR）与监管通报义务；
   - 对确认违规的账户采取果断措施，包括冻结账户、终止服务，并向有关机构报告。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q283. 贵司如何防范及识别“洗售交易 / 对倒交易”（Wash Trading）行为？

A283（监管提交版）

1. **定义与风险认知**
   - 洗售交易指客户通过自买自卖或关联账户间交易，制造虚假成交量或价格信号；
   - 此类行为严重影响市场公正性，易被用于洗钱或操纵市场。
2. **技术监控措施**
   - 通过交易监控系统识别：
     - 相同客户或高度疑似关联账户之间的频繁对敲交易；
     - 无明确经济目的的高频买入卖出；
     - 几乎持平价格的短时往返交易（Round-trip Trades）。
3. **行为模式分析**
   - 将订单时间、成交价格、IP 地址、设备指纹等信息结合分析，以识别可能的“自我成交”或者“关联账户群”协同交易；
   - 针对单一资产短时间内异乎寻常的成交量激增进行深度排查。
4. **后续行动**
   - 对被识别为高疑似洗售的交易进行合规审查；
   - 必要时将相关交易列为可疑行为，纳入 STR 提交；
   - 按照内部政策对相关客户采取限制或终止措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q284. 贵司如何防止内部人员滥用未公开信息（Inside Information / MNPI）进行交易或向第三方泄露？

A284（监管提交版）

1. **内部信息定义与识别**

- 本公司将尚未公开、可能对某一加密资产价格产生实质影响的信息定义为"内部信息"(MNPI)，包括重大技术变更、安全事件、重大合作或下线计划等。

2. **信息隔离制度（Chinese Walls）**
   - 对产品开发、风控和合规团队之间的信息流动进行规范，限制与交易相关敏感信息的非必要共享；
   - 对可能接触内部信息的员工设定单独的访问权限与记录审计。
3. **员工交易管理**
   - 要求关键岗位员工申报个人交易账户并建立"员工账户白名单"；
   - 设置交易窗口期与禁售期，对涉及敏感事件的相关资产设定临时禁止交易（blackout period）；
   - 合规部门定期抽样检查员工交易记录。
4. **纪律与问责**
   - 对泄露内部信息或者利用 MNPI 交易的行为实行零容忍政策；
   - 视情况可采取解雇、追责以及向监管机关或司法机关报告等措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q285. 贵司是否允许员工在公司平台上进行个人交易？如允许，如何控制利益冲突与市场行为风险？

A285（监管提交版）

1. **基本原则**
   - 本公司在严格控制前提下，允许部分员工在公司平台进行有限度的个人交易；
   - 对于高风险或敏感岗位人员（如合规、风险管理、交易监控、核心技术等），将实施更加严格的限制或完全禁止。
2. **事先审批与申报**
   - 员工需事先申报个人交易账户并获得合规部门批准；
   - 禁止员工使用未申报账户进行交易。
3. **交易限制**
   - 员工不得在涉及敏感内部信息的资产上进行交易，尤其在公告前的敏感窗口期内；
   - 对短线频繁交易设定最低持有期限，以减少"过度投机"。
4. **监控与审查**
   - 合规团队定期审查员工交易记录和行为；
   - 对疑似利用内部信息或参与异常交易的行为进行调查，必要时采取纪律处分和报告措施。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q286. 贵司如何识别并管理"利益冲突"(Conflict of Interest)，特别是在多业务线并行的情况下？

A286（监管提交版）

1. **利益冲突识别框架**
   - 制定《利益冲突管理政策》(Conflict of Interest Policy)，对可能出现的利益冲突场景进行分类，如：
     - 公司自营与客户利益冲突；
     - 不同客户之间利益冲突；
     - 员工个人利益与客户/公司利益冲突。
2. **事前评估与登记**
   - 要求管理层和关键岗位人员定期填写"利益冲突申报表"，申报外部任职、重大投资以及与客户或供应商的关系；
   - 对识别出的重大利益冲突情景进行记录并制定相应缓解措施。
3. **缓解措施**
   - 信息隔离墙（Chinese Walls）；
   - 适当的职能分离（Segregation of Duties）；
   - 对特定交易或产品设置销售限制；

- 在必要情况下向客户披露相关利益冲突并征得其知情同意。

4. **监督与问责**
   - 合规部门定期对利益冲突情况进行检查与报告；
   - 对故意隐瞒或未按规定申报的人员实施纪律处分。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q287. 请说明贵司的"投诉处理机制"（Complaint Handling），如何确保公平、及时地处理客户投诉？

A287（监管提交版）

1. **政策与程序**
   - 本公司制定了《客户投诉处理政策》（Complaint Handling Policy），符合 MiCA 客户保护要求及德国本地监管期望；
   - 将投诉定义为客户对公司服务质量、执行价格、平台稳定性、费用及信息披露等不满的正式反馈。
2. **投诉渠道**
   - 提供多种投诉渠道，包括在线表单、电子邮件及专门客服邮箱；
   - 在官网和 APP 中明确列出投诉渠道及处理流程说明。
3. **处理流程与时限**
   - 收到投诉后立即生成工单并发送确认通知给客户；
   - 按既定时限（例如 15 个工作日内给出实质性答复）进行调查与回复；
   - 如投诉事项复杂，向客户解释原因并定期更新进展。
4. **记录与分析**
   - 对所有投诉及处理结果进行记录并纳入 MIS 报告；
   - 定期分析投诉数据，用于改进产品设计、系统稳定性和客户沟通。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q288. 贵司如何确保在市场营销和产品宣传中不出现误导性陈述或不当推广？

A288（监管提交版）

1. **营销材料合规审查**
   - 所有营销内容（包括线上广告、社交媒体发布、推广文案等）在对外发布前必须经过合规部门审查；
   - 审查的重点包括：是否存在收益保证、过度承诺、遗漏重大风险信息等。
2. **禁止条款**
   - 禁止使用"保本"、"保证收益"等字眼；
   - 禁止暗示监管机构或政府对投资收益提供保障；
   - 禁止对加密资产风险进行淡化或选择性披露。
3. **风险揭示与平衡信息**
   - 在营销材料中显著位置披露风险警示语，说明加密资产的波动性、技术风险及可能的损失；
   - 确保"风险信息"与"收益或优势描述"在版面上具备足够权重和可见性。
4. **第三方推广管理**
   - 对合作渠道、KOL 或代理推广机构进行尽职调查；
   - 要求其遵守公司标准模板与话术，不得擅自夸大或扭曲产品特性。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q289. 贵司是否对"高风险产品"或"复杂产品"采用更谨慎的销售与适当性评估机制？

A289（监管提交版）

1. **产品分类**
   - 根据风险、复杂程度与目标客户群对产品进行分类，如：

- 基础型产品（适合零售客户）；
- 复杂或高风险产品（例如杠杆衍生品、结构化代币等）。

2. **适当性与合适性评估**
   - 对复杂或高风险产品进行更加严格的适当性评估，包括风险承受能力、投资经验、财务状况等；
   - 如评估结果显示客户并不适合该类产品，将进行风险提示或限制其交易权限。
3. **针对高风险产品的额外措施**
   - 强制显示附加风险披露页面；
   - 要求客户完成风险确认测验或测试问卷；
   - 对部分高风险产品设置默认关闭状态，仅在客户明确申请且通过评估后才开放权限。
4. **持续监控与回访**
   - 定期监测高风险产品持有者的交易行为与损益情况；
   - 通过客户服务或合规渠道了解客户对产品的理解程度和风险承受感受。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q290. 若 BaFin 或其他监管机构对市场行为提出关注或调查，贵司的应对与配合机制是什么？

A290（监管提交版）

1. **监管联络官（Regulatory Liaison Officer）**
   - 本公司指定专职监管联络官负责与 BaFin 及其他相关机构沟通；
   - 所有关于市场行为或市场滥用的监管询问将首先集中至该角色进行协调。
2. **内部响应团队**
   - 一旦收到监管询问或调查通知，将立即启动内部响应机制，由合规、法律、风险管理与相关业务部门组成专项小组；
   - 快速收集和整理交易记录、监控报告、内部沟通和政策文件。
3. **资料提供与透明度**
   - 根据监管要求及时、完整、准确地提供所需资料；
   - 对已发现的问题和缺陷保持坦诚态度，并主动说明已采取或计划采取的整改措施。
4. **后续整改与报告**
   - 如监管调查发现实质性缺陷，本公司将根据要求制定书面的整改计划，并在限定时间内向监管机构进行进度更新；
   - 将此类事件纳入内部学习与改进机制，更新相关政策和培训内容。

（本条答复由仁港永胜唐生拟定并提供专业讲解。）

Q291. 请说明贵司申请的 MiCA CASP 服务类别（Service Types）及其范围界定依据。

A291（监管提交版｜BaFin-ready）

本公司根据《Regulation (EU) 2023/1114（MiCA）》附件 III～V 之服务分类，并结合实际业务模式，申请如下 CASP 服务类别：

（一）确认申请的服务类别

1. **接收与传递订单（MiCA Art. 3(1)(9)(a)）**
   - 即客户指示的接收与传递（非自营），包括委托撮合交易。
2. **执行订单（Art. 3(1)(9)(b)）**
   - 代表客户在交易场所执行买卖指令。
3. **运营交易平台（Art. 3(1)(9)(g)）**
   - 运营多边系统，使买方与卖方能够互动并达成交易。
4. **托管与管理加密资产（Custody, Art. 3(1)(9)(c)）**
   - 代表客户保管私钥并管理其加密资产（如采用冷/热钱包方式）。

5. **提供加密资产的转移服务（Art. 3(1)(9)(e)）**
6. **提供加密资产的建议（Advice, Art. 3(1)(9)(f)）**
    - 在客户授权情况下提供投资型建议。

（如贵司仅申请 1～2 项，我可根据你指定的范围重新收敛。）

（二）法律依据

- 《MiCA》第 3 条、第 59 条、第 62 条
- **德国 BaFin 对 MiCA 本地化解释（MiCA national transposition）**
- 德国 KWG（Banking Act）关于"金融服务"与"加密托管"之边界

（三）确保无越权经营

本公司确保不从事以下由其他许可覆盖的业务：

- 不发行电子货币（EMI 范畴）
- 不提供支付服务（PSD2 范畴）
- 不提供 MiFID II 投资服务
- 不运营受监管的多边交易设施（MTF）
- 不进行自营交易（prop trading）

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q292. 请说明贵司如何界定"虚拟资产托管服务（Custody）"与单纯的技术钱包服务的区别。

A292（监管提交版｜BaFin-ready）

根据 MiCA 与德国 KWG/Kryptoverwahrgeschäft 之法律定义，本公司明确区分：

✓ 托管服务（Custody）必须满足：

1. **代表客户保管或控制私钥**
    - 有能力发起或阻止交易
    - 客户对资产的完整控制需依赖本公司
2. **承担"资产安全责任"**（Safeguarding）
    - 必须执行分账
    - 必须建立 Safeguarding 控制
    - 必须按 MiCA 规定赔偿损失
3. **具备合规义务：**
    - AML / CTF
    - ICT 安全
    - 运营风险
    - 客户披露
    - 分离客户资产（Client Asset Segregation）

✓ 技术钱包服务不属于托管：

- 公司不掌握私钥
- 仅提供软件界面（non-custodial wallet）
- 不参与客户资产管理
- 不触发 Safeguarding 义务

✓ 本公司法律立场

本公司提供的服务属于 MiCA 定义的"托管服务"类别，即掌握客户私钥并执行保管职责。

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q293. 贵司是否涉及"自营交易（Proprietary Trading）"？如无，请说明如何避免被视为自营。

A293（监管提交版｜BaFin-ready）

本公司**不从事任何形式的自营交易**，并严格区分：

（一）本公司不进行以下行为：

- 不为公司自身盈利目的而交易加密资产
- 不承担市场方向性风险
- 不从事"内部账户对外交易"
- 不进行"仓位投机"

（二）如何避免被视为自营（BaFin 核心关切）

1. **客户与公司资金完全隔离**
   - 分户制钱包
   - 分离账簿记录
   - 银行账户与 crypto wallet 严格区分
2. **撮合模式为"代理模式"**
   - 客户对客户（C2C）撮合
   - 公司不参与价格发现
3. **平台不承担市场风险**
4. **不会使用公司账户参与撮合深度**

（三）如果必须进行平台钱包里最小化的调仓

仅用于钱包流动性安全管理，不构成自营行为，且：

- 不涉及投机
- 无盈亏目的
- 有实时审计轨迹
- MLRO 与风险管理共同监督

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q294. 请说明贵司是否提供"收益产品（Yield / Earn）"或"Staking / Lending"服务，并阐述其法律归类。

A294（监管提交版｜BaFin-ready）

本公司**不提供**以下任何可能触发额外许可的产品：

- 加密资产"收益产品（Earn）"
- 托管式 Staking（Custodial Staking）
- 借贷 / 放贷（Lending）
- 产品结构化收益

❗若提供，将触发法律风险

服务	MiCA 归类	是否触发额外牌照
托管式 Staking	"加密资产管理"或"服务组合"	可能触发金融工具监管 + BaFin 审查
Lending	与信贷类似	**可能触发 KWG §32 银行业许可**
Earn 产品	视为投资合约	**可能触发 MiFID II**

✓ 本公司当前业务模式：

- 不参与 Staking、Yield、Lending
- 不从事 Earn 产品设计
- 不向客户提供收益类承诺或固收产品

确保完全在 MiCA CASP 范围内，避免越权经营。

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q295. 贵司是否提供"法币充值/提现"？是否涉及 PSD2 支付服务？

A295（监管提交版｜BaFin-ready）

✓ 本公司不提供任何 PSD2 定义的支付服务：

- 不提供资金转账（money remittance）
- 不提供账户开立（payment account）
- 不提供支付发起（PIS）
- 不提供账户信息服务（AIS）

✓ 法币部分仅限：

- 客户向本公司合作银行进行充值
- 本公司向客户银行账户返款
- 始终由受监管金融机构执行支付职能

✓ 我们不触发 PSD2 牌照

原因如下：

1. 本公司不"持有"法币（仅托管 crypto）
2. 所有法币流转由合作银行执行
3. 本公司仅在加密资产领域提供代理服务
4. 不提供支付服务的核心要素（如指令执行或支付账户）

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q296. 请说明贵司的"撮合交易"模式是否构成运营多边交易系统（MTF / OTF）。

A296（监管提交版｜BaFin-ready）

✓ 本公司运营 MiCA 定义的加密资产交易平台，但不属于 MiFID II 的 MTF / OTF。

原因如下：

（一）MiCA 与 MiFID II 的监管边界明确

- 本平台仅撮合 **不属于金融工具** 的加密资产
- 不涉及证券、衍生品、债券等 MiFID II 资产

（二）MiCA 特定豁免条款适用

MiCA 为加密资产设立独立的 CASP 交易平台框架，不将其视为传统 MTF。

（三）运营结构符合 MiCA 定义：

1. 平台撮合加密资产，不涉及金融工具
2. 不进行自营
3. 不承担资本市场监管义务（如 MAR/MiFID 披露）

（四）明确向客户说明：

本交易平台是 MiCA CASP 交易平台，而非欧盟受监管的 MTF / OTF。
（本条由仁港永胜唐生拟定并提供专业讲解。）

Q297. 请说明贵司是否发行或销售"加密资产发行（ICO / Token Issuance）"，如有是否触发 Whitepaper 要求。

A297（监管提交版｜BaFin-ready）

✓ 本公司不发行任何加密资产，不进行 ICO，不操作 Token Sale。

如未来计划发行 Token，将触发 MiCA 相关义务：

1. **发行人必须编制 Whitepaper（Art. 56 起草要求）**
2. **需进行通知监管（Notification to Competent Authority）**
3. **需披露风险与技术细节**
4. **必须确保不违反市场滥用规定**

当前状态：

- 本公司仅作为服务提供商，不提供加密资产发行服务
- 平台不参与任何 Token 的初级市场销售
- 平台不进行代币承销或募集

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q298. 贵司是否对某些加密资产进行"分类（Classification）"，例如区分 Payment Token、Utility Token、Asset-referenced Token（ART）等?

A298（监管提交版｜BaFin-ready）

是，本公司建立了加密资产分类框架，基于：

- MiCA Chapter II（Definitions）
- ESMA 指引
- BaFin 对"证券型代币 / 资产参考代币"的本地化解释

分类框架包含：

1. **支付代币（Payment Token）**
   - 比特币、莱特币等
   - 非投资属性、不构成金融工具
2. **功能代币（Utility Token）**
   - 用于访问平台或服务
   - 不构成证券型权利

3. **资产参考代币（ART）**
    - 由多资产/篮子资产支持
    - 由 MiCA Title III（ART Issuers）监管
4. **电子货币代币（EMT）**
    - 与单一法币挂钩
    - 属于 E-money Token Issuer 范畴

本公司政策：

- 仅上市支付代币与 Utility Token
- 不上市 ART 与 EMT（需更高监管要求）
- 不上市具有证券属性的代币（可能触发 MiFID）

（本条由仁港永胜唐生拟定并提供专业讲解。）

Q299. 请说明贵司如何确保不触发其他金融监管（例如 EMI、MiFID II、KWG 银行许可等）。

A299（监管提交版｜BaFin-ready）

本公司已进行 **全面的监管边界评估**。

（一）不触发 EMI（电子货币机构）

- 不发行电子货币
- 不发行 EMT
- 不提供支付账户
- 不提供提现支付服务（由银行负责）

（二）不触发 PSD2 支付服务

- 本公司不执行法币支付指令
- 不提供 Payment Initiation 或 Account Information 服务
- 不持有客户法币

（三）不触发 MiFID II 投资服务

- 不交易证券型代币
- 不提供投资组合管理
- 不承销
- 不提供 MiFID 工具交易

（四）不触发 KWG 银行业务（§32）

- 不进行信贷
- 不吸收公众存款
- 不开展资产管理（MiFID）

本公司所有服务均限于 MiCA CASP 范围内。
（本条由仁港永胜唐生拟定并提供专业讲解。）

Q300. 请总结贵司为何认为自身业务完全属于 MiCA CASP 范畴，不会触发更高等级的监管要求。

A300（监管提交版｜BaFin-ready）

综合业务模式、技术架构、客户关系与运营方式，本公司确认如下：

（一）服务范围完全符合 MiCA CASP 分类

- 提供订单传递、执行、交易平台与托管服务
- 不提供超出 MiCA 框架的服务

（二）不涉及更严格监管的触发点

- 不发行代币
- 不提供支付/电子货币
- 不提供投资服务
- 不提供信贷
- 不进行自营
- 不结构化收益产品

（三）内部控制体系符合 MiCA 要求

- AML（链上 + 链下）
- ICT / DORA / BAIT
- Safeguarding 分账
- 风控体系
- 高级管理层"适当人选"要求
- 外包管理与监管报告

（四）已建立完整合规框架，可直接满足 BaFin 牌照审查

包括：

- 全面风险评估
- 内部政策体系
- 程序文件（SOP）
- 审计与持续性报告
- 客户保护机制
- 市场行为规范
- 运营应急与灾备体系

因此，本公司业务完全符合 MiCA CASP 定位，不触发其他牌照要求。
（本条由仁港永胜唐生拟定并提供专业讲解。）

关于仁港永胜（香港）有限公司

全球 MiCA / CASP / EMI / VASP / VARA / 银行牌照 全栈合规服务提供商
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。
本章作为全指南的最终部分，将为您完整呈现：

- 仁港永胜的公司背景
- 全球持牌/合规服务能力
- 专注领域
- 在 MiCA / CASP / 传统金融 / 银行业务中累积的经验
- 为什么我们在行业中具备显著优势
- 我们的核心团队
- 我们能为企业提供哪些实操性服务
- 如何进一步与唐生取得联系

公司简介：仁港永胜（香港）有限公司

仁港永胜（香港）有限公司是一家深耕**全球金融监管、国际牌照申请及监管合规体系搭建**的专业机构。
我们在：

- **香港、深圳**拥有核心合规团队
- **中国内地六大城市**设有长期合作顾问
- 与 **欧洲、美国、中东、非洲及东盟**多国的监管机构、金融执照顾问、金融律师、审计机构、监管科技供应商保持常年协作

我们专注于：

- 银行业执照（传统银行/离岸银行）
- 金融机构授权（EMI、PI、MSB、MTL、CASP、VASP）
- 证券牌照（香港 SFC 1/4/7/9/10/11 类）
- 支付牌照（英国 FCA、欧盟 EMI/PI、新加坡 MPI/MAS 等）
- 虚拟资产牌照（MiCA、VARA、香港 SFC VASP）
- 家族办公室架构搭建
- 离岸公司 + 金融架构规划
- 风险管理体系搭建
- AML/KYC 合规体系建设
- 监管沟通与稽查应对

在过去十多年间，我们在全球协助超过：

> **1,800+ 企业客户、320+ 金融机构**
> 完成各类监管牌照申请及合规体系搭建。

全球合规服务版图（世界五区布局）

我们的业务覆盖：

1、欧洲（EU & EEA）

- 德国 BaFin
- 马耳他 MFSA
- 立陶宛 BoL
- 波兰 KNF
- 爱沙尼亚 FIU
- 荷兰 DNB
- 爱尔兰 CBI
- 瑞士 FINMA（非欧盟，但高度协同）

主要服务类别：
✓ MiCA CASP
✓ EMI/PI 支付机构
✓ 银行牌照
✓ 投资公司（IFR/IFR-perm）
✓ 加密交易平台 / 托管
✓ 家族办公室
✓ 监管沙盒
✓ 金融科技项目

2、香港 & 中国内地

✓ MSO 金钱服务
✓ SFC 证券及期货条例全类牌照（1/2/3/4/5/6/7/9/10/11/12/13）
✓ HKMA SVF（储值支付工具）
✓ 稳定币发行牌照（2025）
✓ 虚拟资产交易平台（VATP）

✓ 家族办公室架构
✓ 香港税务 & 公司架构

3、东南亚（新加坡 / 马来西亚 / 印尼 / 泰国 / 越南）

✓ MAS 支付牌照（MPI / SPI）
✓ 金融机构合规体系
✓ 印尼金融牌照（深度实操版）
✓ 东盟监管架构
✓ 金融科技落地服务

4、中东（UAE 阿联酋）

✓ DIFC / DFSA 金融牌照
✓ ADGM FSRA 金融机构
✓ VARA 虚拟资产牌照
✓ 交易所、托管、经纪服务
✓ 沙特 / 卡塔尔 金融架构

五、非洲 & 离岸司法管辖区

✓ 科摩罗（安儒昂）银行牌照
✓ 安圭拉金融机构牌照
✓ 塞舌尔（FSA）
✓ 毛里求斯（FSC）
✓ 伯利兹（IFSC）
✓ 圣文森特 / 多米尼克
✓ 巴哈马 / 开曼群岛
✓ BVI

仁港永胜五大专业核心能力（行业领先）

能力一：全球金融牌照申请（全链路交付）

从可行性分析 → 结构设计 → 监管沟通 → 文件制作 → 面谈辅导 → 获批运营
我们提供的是：

"从 0 到落地"的整体解决方案，而不只是写文件。

能力二：合规体系搭建（可直接运营）

我们为监管机构认可的文件包括：

- AML 手册（40+ 模块）
- 交易监测政策（链上 + 链下）
- 风险管理框架
- IT 安全框架
- HR 合规体系
- Outsourcing 外包管理
- Safeguarding 资金隔离机制
- DORA 信息安全体系
- GDPR 隐私保护体系
- 业务持续性（BCP）

我们交付的不是模板，而是：

> **可直接用于运营的合规体系。**

能力三：监管沟通（Regulator Communication）

我们可协助：

- 回应监管补件（RFI）
- 回应审计要求
- 回应监管检查（On-site Inspection）
- 回应监管质询（Inquiry）
- 与监管机构进行正式沟通（书面与面谈）

能力四：在欧洲与中东"高难度牌照"的实际通过经验

我们在：

- **德国 BaFin（极高难度）**
- **阿联酋 VARA（高难度）**
- **立陶宛 BoL（高难度）**
- **马耳他 MFSA（中高难度）**

均成功帮助客户获得授权。

能力五：唐生个人的合规交付与结构设计优势

唐生长期负责：

- 全球金融牌照项目管理
- 合规体系搭建
- 监管沟通策略
- 面谈辅导
- 监管补件逻辑制定
- 金融结构设计（银行、支付、加密）

擅长：

- 复杂跨境结构设计（香港 → 欧盟 → 中东）
- 多牌照集团架构规划
- 金融业务合规文档的系统化构建
- MiCA、DORA、AMLD6、PSD2 等法规解读

仁港永胜提供的服务总览（适用于德国 MiCA-CASP）

以下为我们能够为德国 CASP 申请人提供的全链路服务：

服务 1｜申请前评估 & 结构设计（必做）

- 业务模型评估
- 牌照匹配度分析
- MiCA 服务类别判断
- 德国法律分类（CASP + WpIG + KWG）
- 风险评估报告
- 德国实体架构搭建
- 资金要求测算

服务 2｜完整申请文件（80–120 份）制作

包含：

- AML（40+ 文件）
- 风险管理（20+）
- IT & 网络安全（20–30 文件）
- Outsourcing
- Governance
- Safeguarding
- 交易监测（TM + 链上 AML）
- 内部审计
- 组织结构
- 董事会治理
- 风险控制矩阵
- 数据流图 + 系统架构图

这是监管最关注的部分，我们将为你全部制作。

服务 3｜监管补件（RFI）应对（最关键）

补件通常 90–180 条，我们负责：

- 全部问题分析
- 合规化回答
- 补件策略设计
- 修订文件补件
- 监管逻辑整合
- 风险点排查
- 提交与解释文件

这是德国申请的"重头戏"，仁港永胜经验最为丰富。

服务 4｜监管面谈（Interview）训练与陪同

我们提供：

- 董事面谈训练
- RO 面谈训练
- MLRO 深度训练
- CTO/系统面谈训练
- 场景模拟问答
- 监管提问预估（60–120 题）

服务 5｜德国本地资源协助

- 本地董事
- 本地 RO / MLRO
- 本地审计机构
- 本地办公室安排
- 本地银行开户
- 本地服务商资源对接

服务 6｜获批后的持续合规（必做）

- 年度合规报告

- AML 流程执行
- 风控监测
- 交易监测
- 合规顾问长期支持
- 内部审计
- 员工培训
- 监管持续沟通

德国是长期监管，持续合规比申请更重要。

为什么选择仁港永胜?

1. 熟悉德国 BaFin 审查逻辑

我们掌握：

- 所有补件类型
- 面谈真实问题
- 监管逻辑
- 文件要求标准
- 风险关注点

---

2. 文件不是模板，而是"监管级专案交付"

每一个文件、每一段政策、每一个流程图都"可落地"。

---

3. 真实案例经验，而非理论

我们手上的资料、问答、流程、场景均来自：

✓ 实际补件
✓ 实际面谈
✓ 实际审查
✓ 实际获批

---

4. 监管沟通 → 面谈 → 合规体系，全流程支持

不是提供文件，而是陪你走完全流程。

---

5. 强大的跨境结构设计能力

可协助构建：

- 德国母公司
- 香港资金承接平台
- 阿联酋交易节点
- 欧洲支付清算路径
- 私钥管理（多地 HSM）
- 集团风险隔离结构

总结

仁港永胜作为全球领先的金融合规服务机构，致力于：

- 让企业在**欧洲、亚洲、中东、非洲**安全合规地开展业务
- 让金融机构具备完整监管体系
- 协助企业通过全球高难度牌照申请

- 建立长期合规文化
- 在 MiCA（欧盟）这一全球最重要的新监管时代中，为企业构建完整、可持续的监管体系与业务架构

我们不做模板化服务，而是：

> **真正理解监管、理解金融、理解技术、理解企业的专业伙伴。**

联系方式

- 官网：**www.jrp-hk.com**
- 香港：**852-92984213**（WhatsApp 同号）
- 深圳：**15920002080**（微信同号）

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

业务联系与资料索取：
仁港永胜（香港）有限公司 — 唐上永 业务经理
手机：15920002080（深圳 / 微信同号）
电话：852-92984213（Hong Kong / WhatsApp）

免责声明

本文由 **仁港永胜（香港）有限公司 拟定，并由 唐上永 业务经理提供专业讲解**，仅供一般信息用途，不构成任何形式的法律、会计或投资建议。
具体条款、监管要求及收费标准以欧盟法规及德国联邦金融监管局（BaFin）最新官方文件为准。
仁港永胜保留对本文内容进行更新与修订的权利。

如需就 **德国 MiCA-CASP 申请 / 收购、合规落地与后续维护** 获得一对一协助，欢迎通过上述方式联系仁港永胜，以确保你的业务在德国及欧盟范围内合法、稳健、合规运营。
