德国（MiCA）加密资产服务提供商（CASP）牌照注册指南

Germany MiCA Crypto-Asset Service Provider (CASP) Licensing Guide

牌照名称：德国加密资产服务提供商牌照 – Germany Crypto-Asset Service Provider (CASP) License
监管框架：Regulation (EU) 2023/1114 on Markets in Crypto-Assets（MiCA）+ 德国本地实施法规
主要监管机构：德国联邦金融监管局 BaFin（Bundesanstalt für Finanzdienstleistungsaufsicht）
服务商：仁港永胜（香港）有限公司

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

适用于计划在**德国设立 MiCA-CASP 主体**，并通过**护照机制在欧盟/EEA 30 国展业**的项目团队、金融机构、家族办公室及 Web3/RWA 项目方，用于：

- 内部立项评估与项目决策；
- 与股东 / 投资人沟通德国 CASP 方案；
- 对接 **德国 BaFin** 申请材料、沟通监管逻辑；
- 设计"德国 CASP + 其他欧盟牌照 + 境外结构"的全球合规布局。

以下内容以仁港永胜实战项目及德国 BaFin 最新监管口径为基础，结合欧盟《加密资产市场条例（MiCA，Regulation (EU) 2023/1114）》与《数字运营韧性条例（DORA，Regulation (EU) 2022/2554）》等法规进行系统梳理与重排。文中所有"我方""我们""本团队"，均指仁港永胜合规顾问团队。本文供内部立项、股东决策及与律师 / 审计 / 技术团队协同使用，不构成任何形式的法律意见，具体条款以欧盟法规及德国 BaFin 官方文件为准。

第 1 章｜总论：德国 MiCA-CASP 监管框架与项目定位

《德国 Germany（MiCA）加密资产服务提供商（CASP）牌照申请注册指南》
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。

一、为什么要用"德国视角"重写 MiCA-CASP 指南？

欧盟《加密资产市场规例》（Regulation (EU) 2023/1114，"MiCA"）自 2024 年起分阶段生效，其中与 **加密资产服务提供商（CASP）** 相关的条款，自 2024 年底起全面适用，成员国可以设置最长 18 个月的过渡期。

从法律条文角度，所有欧盟成员国适用的是同一部 MiCA；
但从**实务操作**角度，不同监管机构的风格、要求深度、补件强度完全不同。

- **MiCA：写的是底线；**
- **BaFin：会把底线"向上拧一圈"。**

德国之所以值得单独写一份"深度实操版"指南，原因主要有：

1. **德国是欧盟最强势的金融监管之一**
   - 银行业和证券业监管传统极其严谨，BaFin 对 ICT、托管、风险管理、治理结构都有长期监管经验。
   - 在 MiCA 之前，德国已经通过《德国银行法（KWG）》将 **加密托管业务（Kryptoverwahrgeschäft）** 纳入金融服务活动，由 BaFin 发牌监管，是欧洲最早将加密托管"纳入银行法"的国家之一。
2. **技术与合规的预期"远高于平均水平"**
   - BaFin 长期要求受监管机构遵守包括 **BAIT（Bankaufsichtliche Anforderungen an die IT）**、**MaRisk**、以及现在的 **DORA（Regulation (EU) 2022/2554）** 等 ICT 和风险管理规范。

- MiCA 上线后，BaFin 很自然会把这些传统金融领域的要求"平移"到 CASP 身上，对 ICT、DORA 合规、托管安全、外包管理等提出**接近银行级别**的要求。

3. **德国本身就是"高门槛 + 高认可度"的组合**
   - 在 MiCA 框架下拿到德国 CASP 牌照，再通过 **护照机制（passporting）** 向其他 26 个欧盟成员国及 3 个 EEA 国通报展业，在市场形象与监管信任度上，远优于一些监管较宽松的辖区。

因此，本指南不是简单翻译 MiCA 条文，而是站在：

> **"德国本地视角 + MiCA 条文 + BaFin 监管实践 + DORA/BAIT 等交叉要求"**

来帮你搭好一整套可以真正落地的 **德国 MiCA-CASP 项目蓝图**。

二、德国 MiCA-CASP 的法律基础与监管坐标

1. 欧盟层面：MiCA 的基本结构

MiCA 的正式全名为：
Regulation (EU) 2023/1114 on Markets in Crypto-Assets，属于 **欧盟法规（Regulation）**，对全部成员国直接适用，无需再行本地化立法生效。
与 CASP 密切相关的部分主要包括：

- **Title II – Crypto-asset service providers（CASPs）**
  - 对 **授权条件、组织架构、资本要求、经营行为规则、客户资产保护、外包、ICT、冲突管理、市场滥用** 等提出统一要求。
- **条文对"加密资产服务"的定义**，诸如：
  - 接收与传送订单
  - 代表客户执行订单
  - 运营加密资产交易平台
  - 托管与管理加密资产
  - 交换加密资产与法币或其他加密资产
  - 代客资产管理
  - 就加密资产提供投资建议等

在 MiCA 框架下，所有在欧盟提供上述服务的机构，都必须取得 **CASP 授权**，不再允许"未授权经营"。

2. 德国层面：MiCA 之上的"加码"

虽然 MiCA 直接适用，但德国通过：

- 修改《德国银行法（KWG）》及相关从属法规；
- 将原先对 **加密托管（Kryptoverwahrgeschäft）**、加密交易平台、加密自营等既有监管经验，嵌入 MiCA 体系之中；
- 在 ICT 风险管理上，通过 BAIT、MaRisk 与 DORA 联动，形成一套比单纯 MiCA 更"锋利"的监管工具箱。

实际效果是：

> **在其他国家可能"合格"的 CASP，在德国未必合格；**
> **在德国合格的 CASP，放到其他欧盟国家通常是"超额合规"。**

3. 监管主体：BaFin 与德央行的分工

- **BaFin（Bundesanstalt für Finanzdienstleistungsaufsicht）**：
  负责金融机构授权、持续监管、现场检查、执法处罚，是 MiCA-CASP 审批的直接主管机关。
- **德国联邦银行（Bundesbank）**：
  主要在宏观审慎和支付系统方面配合监管。

对于 MiCA-CASP 项目而言，你几乎所有的交互对象都可以简单理解为：

> **"一个可以非常细致问到代码与运维细节的监管机构——BaFin"。**

三、谁必须在德国申请 MiCA-CASP 牌照?

1. 触发牌照要求的典型业务场景

如果你的项目符合以下任一场景，并且目标客户包括德国或以德国为主的欧盟客户，基本都落入 CASP 范围：

1. **加密资产交易平台（Centralised Exchange / CEX）**
   - 为客户撮合加密资产与加密资产、加密资产与法币的买卖；
   - 持有客户资产（无论是热钱包还是冷钱包）。
2. **托管型钱包 / 托管服务（Custody / Wallet-as-a-Service）**
   - 代表客户保管私钥；
   - 提供托管式钱包管理、批量签名服务。
3. **加密券商 & 经纪（Broker / OTC Desk）**
   - 接收客户订单，再向交易所或流动性提供方下单；
   - 为客户撮合或执行场外大宗交易（OTC）。
4. **资产管理 / RWA / 结构化产品**
   - 以加密资产或代币化资产为标的，提供主动管理服务；
   - 为客户构建加密资产组合并收取管理费/业绩报酬。
5. **做市、流动性提供（Market Maker / Liquidity Provider）**
   - 在自营账户为平台提供深度；
   - 与客户对手方交易。

只要你的商业模式中包含"**代客保管、撮合、执行、管理、建议**"等关键词，基本都逃不开 CASP 的监管视野。

2. "不用牌照"的边界在哪？

在德国，目前被视为 **相对低风险、可能不需要 MiCA-CASP 牌照** 的情况非常有限，例如：

- **纯技术提供商（Tech Vendor）**
  仅提供钱包 SDK、节点服务，不直接面对终端客户、不接触客户资产；
- **链上数据分析、风控工具**
  只对其他受监管机构提供 SaaS 服务，不触及客户资产和交易执行。

但一旦出现：

- 你直接开账户给终端客户；
- 你可以触发或批准转账/提现；
- 你参与订单执行或撮合；

那么在德国语境下，监管非常容易认为你已经构成 **金融服务活动**，必须持牌。

四、德国 MiCA-CASP 的实际定位：高门槛 vs 高价值

1. 与其他欧洲热门辖区的对比

简单感受一下德国与其他常见 MiCA 目的地的定位（仅为实务印象）：

- **德国（BaFin）**：
  - **难度：★★★★★**
  - **技术要求：★★★★★**（BAIT + DORA + DevSecOps 视角）
  - **监管补件（RFI）猛烈度：★★★★★**
  - **牌照含金量：★★★★★**
- **立陶宛（BoL）**：
  - 难度：★★★☆（已有 VASP/EMI 基础）
  - 审查速度相对快，文件方向明确。
- **马耳他（MFSA）**：
  - 在 VFA 到 MiCA 的过渡中经验丰富；
  - 对治理和 IT 也较重视，但整体风格比德国"友好"。
- **奥地利、波兰、荷兰等**：

- 各自有传统金融监管积累；
- MiCA 框架下的实施路线略有差别。

如果你的团队目标是：

> “在欧盟范围内，拿一张技术含量与监管认可度 **最顶级** 的 MiCA-CASP 牌照。”

那么，德国是少数真正值得投入的选择之一。

2. 适合谁来德国申请？

更现实一点的结论是：
适合在德国申请 MiCA-CASP 的主体，一般至少具备以下条件：

1. 已有一定规模的加密 / 金融业务（或大型集团支持）；
2. 能够提供 **欧洲本地的高质量董事与高级管理层**（尤其是 MLRO、CRO、CTO）；
3. 有自己的 **核心技术团队**，而不是完全外包白标系统；
4. 准备好 **100–150 万欧以上的综合投入预算（2 年周期）**；
5. 有中长期在欧盟（尤其是 DACH 区）深耕的战略，而不是“拿牌就跑”。

如果你还处在 **“想先试试看，预算有限，团队也不成熟”** 的阶段，那么仁港永胜会更坦白地建议：

> 先从立陶宛、波兰、马耳他、奥地利等更友好的辖区入手。

五、MiCA、DORA 与德国本地规范的叠加效应

1. MiCA 的“纵向要求”：谁能做 + 怎么做

MiCA 对 CASP 的要求可以概括为：

1. **机构层面**
   - 适当人选（Fit & Proper）
   - 充足资本金与财务稳健
   - 明确的治理结构与三道防线（业务、风险/合规、内部审计）
2. **业务层面**
   - 服务授权范围清晰（哪些 CASP 服务）
   - 客户资产隔离（Safeguarding）
   - 利益冲突管理
   - 透明度与信息披露
   - 投诉处理与消费者保护
3. **风险与合规层面**
   - AML/CFT 制度（协调欧盟 AML 架构）
   - 风险管理框架（RMF）
   - 外包监管与第三方风险管理
   - 运营连续性与压力测试

2. DORA 的“横向要求”：金融行业统一 ICT 标准

DORA（Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector） 是对全金融行业的 ICT 风险管理统一规则，包括 CASP 在内的 MiCA 实体同样适用。
它要求：

- 建立 **ICT 风险管理框架**；
- 重大 ICT 事件 **识别、分类与报告**；
- 进行 **威胁驱动的穿透测试**（如 TIBER-EU）；
- 管理 **第三方 ICT 供应商风险**。

在德国，这层要求会与 **BAIT（IT 监管要求）、MaRisk（风险管理最低标准）** 叠加，使得你的系统架构、钱包设计、灾备方案必须从一开始按"银行级"考虑。

3. 德国本地规范：BAIT / MaRisk / KWG 补强

- **BAIT**：针对银行和金融服务机构的 IT 管理最低要求，涉及 IT 策略、信息安全、运维、授权管理、IT 供应商管理等。
- **MaRisk**：风险管理最低标准，要求设立全面风险管理框架与内部控制体系。
- **KWG**：银行法，将加密托管、某些加密交易服务纳入金融服务。

MiCA 只是一个"地基"，德国会在这个地基上加上：

> "IT 安全屋顶 + 风险治理骨架 + 传统金融监管的墙体"。

六、项目时序与监管互动（总览版）

详细的流程会在后续章节展开，这里先给一个**总览时间轴**概念，方便管理层决策：

0–3 个月：前期评估与结构设计

- 决定是否以德国为 MiCA 基地；
- 明确股东结构、董事会构成、核心管理层（CEO/CTO/MLRO/CRO）；
- 确定商业模式与所需 CASP 服务类别；
- 构建高层次架构图（技术 + 业务 + 风险）。

3–9 个月：文件编制与系统成型

- 完成公司（或 SPV）设立与本地经济实质安排；
- 搭建并验证核心系统（钱包、交易、风控、合规引擎、日志审计）；
- 编制全套 MiCA 申请文件 + DORA/BAIT 对口文件；
- 完成内部治理与政策文件（AML、风险管理、外包、投诉处理等）。

9–18 个月：BaFin 审查、RFI、面谈（Hearing）

- 正式提交申请；
- 若干轮 RFI（监管补件）；
- 一至多轮 BaFin 面谈（董事会、MLRO、CTO、CRO 分别受访）；
- 按监管意见迭代系统与文件。

18–24 个月：获批后运营准备与护照申请

- 拿到德国 CASP 授权；
- 将 MiCA-CASP 牌照护照至其他 EU/EEA；
- 进入常态监管阶段（年度报告、现场检查、持续合规）。

这个时间轴是假定项目**准备充分**的理想情况。若前期条件不成熟或 RFI 回合多，整体周期会进一步拉长。

七、本指南 17 章结构预览（深度实操版）

为了避免"看完一大堆法规还是不知道怎么做"的尴尬，本指南按**从宏观决策到微观落地**的顺序设计 17 个章节，结构大致如下（略）：

1. **总论与监管框架（本章）**
2. 德国 MiCA-CASP 牌照类型、适用业务与战略选型
3. 申请主体结构设计与股东/董事/高管适当人选（Fit & Proper）
4. 资本金、财务规划与成本预算（含 2–3 年经营模型）
5. 业务模式与德国监管偏好的 Business Plan 写法
6. 技术架构、钱包托管与 DORA/BAIT 对接（ICT 框架）
7. 客户资产隔离（Safeguarding）与银行账户/清算安排
8. AML/KYC/KYT 体系与链上风险管理专章
9. 外包与第三方风险：云服务、KYC 供应商、节点服务等

10. 治理与三道防线：董事会、风险委员会、内部审计设计
11. 申请流程实操：时间轴、材料清单与 BaFin 交互节奏
12. 德国 BaFin 监管补件（RFI）常见问题与回答框架（FAQ 结构：Q1、Q2…）
13. 德国 BaFin 面谈（Hearing）准备与 200+ 问答逻辑拆解
14. 持牌后的持续合规：报告、审计、现场检查与变更管理
15. 德国 versus 其他 MiCA 目的地的策略对比与多牌照布局
16. 常见项目类型（交易所、钱包、RWA、做市等）结构化案例分析
17. 仁港永胜对申请人的"实话建议"与配套模板总览

八、本章小结：先把"德国这盘棋"看清楚

站在仁港永胜唐生的角度，给本章一个"管理层可以带走的"简短结论：

1. **MiCA 是统一法规，但德国有自己的"监管性格"**：
   - 监管偏好严谨、量化、可审计、可验证；
   - 会把 DORA、BAIT、MaRisk 一起拉进来考你。
2. **德国 MiCA-CASP 不是为"试水型项目"准备的**：
   - 适合已经有一定体量、愿意在欧盟长期深耕的机构；
   - 预算与时间都必须拉满。
3. **但一旦站上德国这座"监管高地"，你的全球合规故事会完全不同**：
   - 对后续进入其他欧盟国家、英国、中东等地，都有极强背书效应；
   - 对银行合作、清算网络、机构客户信任度，是"硬通货"。

说明：
本章为《德国 Germany（MiCA）加密资产服务提供商（CASP）牌照申请注册指南（深度实操版）》**第 1 章完整内容**，
本文内容由仁港永胜唐生提供讲解，由 仁港永胜（香港）有限公司 拟定。

第 2 章｜德国 MiCA-CASP 牌照类型、适用业务与战略选型

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。

本章将系统性拆解 "在德国申请哪一种 CASP 牌照？"
"我的业务模式需要哪些 CASP 许可？"
"是否应该把牌照拆成多实体、或集中在一个主体？"
"德国 BaFin 对不同 CASP 模式有什么偏好？"

本章旨在帮助项目方在 **最初 0–2 个月战略决策阶段** 就选对方向，避免走错结构导致申请时间延误 6–12 个月。

一、MiCA 明确规定的 CASP 10 大服务类别（欧盟统一标准）

根据 MiCA 第三编（Title II – Crypto-asset service providers），CASP 服务被划分为 **10 大类别**。无论在哪个国家申请 CASP（德国、马耳他、奥地利、立陶宛等），分类完全一致。

仁港永胜唐生根据 MiCA 条文 + 德国 BaFin 实操，将其整理如下：

（1）接收与传送客户订单（Reception and Transmission of Orders）

典型业务：

- 做经纪（Broker）
- 接收客户买卖加密资产的意向
- 再向其他交易所/LP 下单

属于**轻量级但高度监管**的 CASP 类型。

（2）代表客户执行订单（Execution of Orders on Behalf of Clients）

典型业务：

- 代客下单、交易执行
- 大宗 OTC

注意：
在德国，订单执行属于"核心监管行为"，BaFin 会审查你的交易质量、执行政策、冲突管理、透明度等。

（3）运营加密资产交易平台（Operation of a Trading Platform for Crypto-assets）

适用业务：

- 中心化交易所（CEX）
- DeFi 前端聚合（若有撮合/托管功能）

在 MiCA 下这是**监管最重的 CASP 类型之一**。
在德国，BaFin 把"交易平台运营"视为接近传统 MTF/OTF（证券领域）的高风险活动，要求：

- 完整订单簿
- 交易监控（Market Surveillance）
- 市场滥用监测（Market Abuse）
- 极强的 ICT/DORA 体系

此类项目在德国申请周期通常比其他 CASP 更长。

（4）托管与管理加密资产（Custody and Administration of Crypto-assets）

典型业务：

- 托管型钱包
- 私钥管理
- 冷/热钱包管理
- MPC 钱包服务
- 托管审计机制

这是许多项目必须持有的 CASP 类别。
在德国，"托管"最敏感，因为其与 KWG（德国银行法）既有"加密托管业务"(Kryptoverwahrgeschäft）高度重叠。
因此，要求几乎是：

> **银行级 IT 架构 + BAIT 级 IT 规则 + DORA 全覆盖。**

（5）交换加密资产与法币（Exchange of Crypto-assets for Funds）

典型业务：

- CEX 的 Fiat<>Crypto
- OTC 场外兑换
- 集成支付渠道的加密支付系统

德国高度关注：

- 反洗钱分层
- 交易限额
- 风险级别
- "脏钱包"过滤机制（KYT）

（6）交换加密资产与加密资产（Crypto-to-Crypto Exchange）

典型业务：

- CEX
- Swap 服务
- DEX 前端若提供托管或撮合（也可能触发此条）

要求相对前几类较轻，但在德国，BaFin 会要求完整的：

- 交易引擎描述
- 撮合逻辑
- 风险系统
- 钱包结构
- 流动性管理

（7）参与与加密资产发行相关的投行服务（Placing of Crypto-assets）

适用业务：

- Launchpad
- 帮项目发行代币
- 代币首次销售安排（Primary Sales）

此类在德国相对少见，但风险偏高，监管偏紧。

（8）代客管理投资组合（Portfolio Management）

典型业务：

- 加密资产组合管理
- RWA 组合管理
- 投资组合/策略管理

在德国属于"高度监管的传统金融业务在加密中的镜像"，要求：

- 投顾资格
- 风险管理框架
- 客户适当性
- 投资限制

（9）加密资产投资建议（Advice on Crypto-assets）

典型业务：

- 研究报告
- 投资建议
- 机器人投顾
- 投资策略推送

德国要求详细的"投资建议与风险披露模板"。

（10）执行与运营转账服务（Transfer Services）

典型业务：

- 钱包之间转账（代为执行）
- 委托提款服务
- 自动派息/自动分配服务

如果系统能够"主动作出转账"，则必须申请此类别。

二、德国 BaFin 对不同 CASP 类型的监管力度（实操评级）

仁港永胜唐生根据过往案例与监管交互经验，将 BaFin 实操难度做出评级：

CASP 类别	在德国的难度	原因
交易平台运营	☆☆☆☆☆	交易监控、市场滥用、ICT+DORA 最复杂
托管服务	☆☆☆☆☆	最接近银行业务，要求最高
订单执行/接收	☆☆☆☆	涉及对客户负责、执行质量、冲突管理
法币兑换	☆☆☆☆	AML/KYC/KYT 要求非常严格
加密交换（Crypto-Crypto）	☆☆☆	监管中等，但技术需强
投顾建议	☆☆☆	文档工作量大
Launchpad / 发行服务	☆☆☆☆	涉及市场滥用、透明度、结构化文件要求高
Portfolio 管理	☆☆☆☆☆	类似 MiFID 投顾业务的合规要求

一个项目若包含多个高难度 CASP，例如：

- 交易所（Platform）
- 托管（Custody）
- 法币兑换（Exchange）

那么在德国申请的难度会呈现**叠加效应**，RFI 数量可能达到 200–300 个。

三、如何为自己的业务选对 CASP 类型?

仁港永胜唐生提供一套 **5 步法** 来判定需要哪些 CASP：

步骤 1：客户是否需要"开账户"?

如果用户在你这里拥有：

- 钱包
- 账户
- 余额
- 你负责保管资产

则 99% 会触发 **托管 CASP**。

步骤 2：你是否触碰订单簿?

包括：

- 撮合
- 排队
- 订单执行
- 大宗 OTC

则必定触发：
交易平台 / 订单执行 / 订单接收。

步骤 3：有没有出现"代客户操作"动作?

如：

- 自动扣费
- 自动结算
- 自动分配收益
- 自动转账

则触发：
Transfer Services。

步骤 4：是否提供投资建议？

如：

- 投资策略推送
- 组合模型
- 风险分级
- 定投建议

则触发：
Advice on Crypto-assets。

步骤 5：是否涉及 RWA 或结构化产品？

如：

- 代币化资产组合
- RWA 资产池
- 收益凭证结构

则触发：
Portfolio Management（组合管理）。

四、战略选型：是否要拆成多个实体？（德国监管实务重点）

在德国非常关键的一点：

> **BaFin 不喜欢一个实体同时做太多不同的高风险 CASP。**

仁港永胜唐生一般会给出三种结构：

模式 A：单实体集成（适合小规模初创）

适用于：

- 托管
- Crypto-Crypto
- OTC
- Transfer Services

不适用于：

- 交易所（Platform）
- 投顾 + 托管 双业务
- Launchpad + 托管

模式 B：多实体结构（适合大型集团）

实体 1（德国）：托管 + Transfer
实体 2（德国或欧盟：交易平台）
实体 3（欧盟其他国家：投资服务/ Launchpad）

优势：

- 针对不同风险进行隔离
- 容易通过 BaFin 审查

- 更符合 DORA 与业务外包规范

模式 C：德国 + 友好监管国（护照）组合

德国（BaFin）负责托管与核心合规；
马耳他/立陶宛/波兰负责交易平台或 Launchpad；
通过 MiCA 护照互相授权，形成：

> **“德国做最难的部分，其他国家做扩展业务”的战略组合。**

适合预算较高的大型机构。

五、德国监管特别偏好的业务结构（实操版）

仁港永胜唐生总结 BaFin 在审查中最喜欢的结构特点：

1. **托管与交易分拆到不同实体**
2. **清算银行与客户资产隔离，建立“客户资产信托账户（Trust Account）”**
3. **CTO / MLRO / 风险官必须在德国本地**
4. **核心钱包技术必须自研或可审计，不接受完全白标**
5. **业务量与风险成比例的系统监测与审计机制**
6. **必须有可执行的 DORA 级灾备中心（至少地理隔离 200km）**

六、不同业务场景对应的 CASP 类型（仁港永胜唐生项目映射表）

业务模式	必要 CASP 授权	是否适合在德国申请
CEX（交易所）	交易平台 + 托管 + 订单执行	☆☆☆☆☆（非常难，但认可度最高）
OTC	订单执行 + 兑换	☆☆☆☆
钱包托管	托管	☆☆☆☆☆
RWA 平台	组合管理 + 托管 + 建议	☆☆☆☆
做市（LP）	订单执行 + 自营规则	☆☆☆☆
Launchpad	Placing	☆☆☆
DeFi 前端	若有托管/撮合则需多项 CASP	☆☆☆

七、本章小结：德国的 CASP 战略选型三原则

仁港永胜唐生总结为：

原则 1：能拆就不要合并（降低风险）

避免在一个实体内集成太多高风险 CASP。

原则 2：复杂业务 → 德国；

边缘业务 → 其他欧盟国家
德国负责“硬监管”（托管、合规主体系），
马耳他/立陶宛负责其他扩展业务。

原则 3：不要假设 BaFin 会放宽要求

德国的审慎风格不会因 MiCA 而改变。
你越准备充分，RFI 越少，审批越快。

第 3 章｜申请主体结构设计与适当人选（Fit & Proper）与德国 BaFin 审查要求

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。

（德国 MiCA-CASP 审查的关键章节｜中文版）

本章介绍 MiCA + 德国 BaFin 审查框架中最敏感、也是影响申请是否成功的关键领域：

- 申请主体结构（法人架构、集团架构、控制权关系）
- 股东适当人选（Fit & Proper）
- 董事/管理层适当性
- 是否有"影子管理人（Shadow Director）"风险
- 德国境内管理要求（Mind & Management）
- 实控人（UBO）穿透
- 高级管理层的能力证明
- BaFin 对 "利益冲突" 与 "独立性" 的要求

仁港永胜唐生将在本章以真实监管逻辑、案例经验、德国监管文化等维度，一次性深度拆解。

一、MiCA 与德国 BaFin 对 CASP 的"主体要求"总原则

MiCA 要求所有 CASP 必须满足：

1. **具有欧盟境内法人资格**
2. **管理层需具备金融与加密资产的专业能力**
3. **具备健全治理结构（Governance）**
4. **具备充分资本金（Own Funds）**
5. **符合 ICT/DORA 网络安全要求**
6. **股东须满足适当人选（Fit & Proper）标准**

德国 BaFin 在此基础上，额外增加：

（1）管理层必须有"实际经营能力"

- 不接受挂名董事
- 不接受"外包 CEO"
- 不接受"兼职但无实体主导权"的管理层

（2）必须在德国本地拥有真实的"Mind & Management"

包括：

- 主要管理决策在德国进行
- 关键职能（MLRO、CTO、风险官）必须在德国
- 不能把核心职能外包到非欧盟

（3）股东不能有"名义股东""影子管理人"结构

BaFin 能够深入穿透所有结构，直至确认真实控制者。

二、申请主体法律结构（Legal Structure）设计要求

德国 CASP 最常见的法律实体形式是：

（1）GmbH（有限责任公司）

- 最常见的 MiCA-CASP 实体
- 注册资本：25,000 欧元
- 监管最低资本金：50,000–150,000 欧元（按 CASP 类型）
- 税务合规便捷

- 适合大多数加密项目

（2）AG（股份公司）

- 适用于大型集团或上市路线
- 管治结构复杂
- 对外融资更灵活
- 监管成本更高

仁港永胜唐生实操经验：
90% 以上项目选择 GmbH，因为其灵活、成本低、容易管理。

三、集团结构（Group Structure）与控股要求

BaFin 对集团化结构进行严格审查，特别是在：

- 控股主体在非欧盟
- 存在多层离岸公司
- 股权不透明
- 有基金/信托结构
- 同一集团涉及其他金融业务（如 FX、CFD、MT5 经纪、区块链平台）

BaFin 最关心两点：

① 控股人与管理层关系是否正常？

不能出现：

- 实控人操控管理层
- 管理层只是"代持人"
- 有隐藏控制的安排（Side Letter / Private Agreement）

② 是否存在"监管套利"结构？

如：

- 德国主体负责风险，而利润转移到海外
- 德国主体只是壳公司
- 核心系统都在海外

BaFin 在 RFI 中经常会提出：

> "请解释为何贵集团选择在德国申请 CASP，而将大部分 IT/运营放在第三国？"

仁港永胜唐生的建议：
申请前先优化集团结构，避免多层离岸、避免不必要的股权复杂化。

四、适当人选（Fit & Proper）要求（核心章节）

德国 BaFin 的适当性审查要素包括：

（1）诚信（Integrity）

- 无犯罪记录
- 无金融监管处罚
- 无破产记录
- 无严重税务问题
- 无跨国洗钱调查

- 未涉及诈骗、虚假陈述

材料评估包括：

- 无犯罪证明
- 税务合规证明
- 过往监管信件
- 诉讼纪录（如需）

（2）财务稳健性（Financial Soundness）

要求股东与董事证明自身：

- 无个人破产
- 无重大负债
- 有合理的资产证明
- 有足够的资金支持实体运营
- 投资来源必须"干净、可审计、可解释"

典型需要：

- 资金证明（Bank Statement）
- 资产清单
- 投资来源说明（Source of Funds）

（3）专业能力（Professional Competence）

管理层须具备：

- 金融行业管理经验
- 投资/交易经验
- AML/KYC 合规经验
- 加密资产与技术理解
- 能力覆盖 ICT/DORA

关键岗位包括：

① 管理董事（Geschäftsführer / Managing Director）

必须具备：

- 金融行业 3–5 年经验
- 加密相关经验
- 监管理解能力

② MLRO（反洗钱负责人）

必须具备：

- AML 体系经验
- KYT/WTR 经验
- 德国金融法理解

③ CTO（技术负责人）

必须具备：

- 钱包系统经验
- 网络安全经验

- DORA 实施经验

④ CRO（风险官）

必须具备：

- 风险管理实际经验
- 金融风险/操作风险理解

五、管理层必须在德国境内履行实质职责（Mind & Management in Germany）

BaFin 要求：

- 至少 **2 名董事常驻德国**
- 董事必须具备决策权限
- MLRO 必须常驻德国
- CTO 可以在欧盟境内，但必须能随时被审查
- 电话会议、董事会记录必须可证明"德国是决策中心"

如果管理层都在海外，RFI 会直接问：

> "请解释贵公司如何确保在德国境内运营核心管理功能？"

因此，仁港永胜唐生一般建议：
管理层至少 3 个岗位设在德国：MD、MLRO、CRO。

六、股东/UBO 审查穿透要求（德国最严格）

BaFin 会穿透所有层级股东，直到最终自然人：

- 所有持股 >10% 的自然人必须提供完整资料
- 所有公司股东必须提供：
  - 公司注册文件
  - 董事名单
  - 股东名册
  - 财务报表
  - 实控说明

德国不接受任何"隐形股东"、"代持安排"、"不可解释的 SPV"。

七、监管最关注的风险点（重点提醒）

仁港永胜唐生整理 BaFin 最常提问的风险点：

（1）管理层是否真的懂加密？

不能是"有名无实"的董事。
不能只是"挂名"。

（2）集团是否过度依赖离岸资源？

例如：

- IT 全在亚洲
- 运营全在亚洲
- 核心人员不在欧盟

此时就会触发：**是否存在监管套利？**

（3）资金来源是否干净？

BaFin 对"资金来源说明"极为敏感。

（4）利益冲突是否清晰处理？

如：

- 股东同时是 LP
- 管理层与投资人关系复杂

BaFin 通常会要求"利益冲突政策"。

八、仁港永胜唐生的专业建议（实操可行）

建议 1：管理层不宜全部来自同一国家或集团内部

这样会被视为"影子管理"或"受控董事"。

建议 2：不要使用层级过深的离岸公司控股

两层以内最理想。

建议 3：MLRO 必须具备真实经验，不要用"包装简历"

BaFin 能轻易识别虚假经验。

建议 4：提前准备监管问答材料（Fit & Proper Q&A Pack）

仁港永胜可定制专属问答模板，应对 RFI。

建议 5：申请前必须完成"合规与治理结构审计"

包括：

- 管治框架
- 职权矩阵
- 风险矩阵
- 利益冲突规则

第 4 章｜德国 MiCA-CASP 监管框架、适用法律基础与 BaFin 审查原则

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。

本章是全书最重要的基础章节之一。本章将系统解释：

- CASP 在德国的法律基础
- 欧盟 MiCA（Regulation 2023/1114）与德国本地法规如何衔接
- BaFin 审查原则
- 德国特殊法律（包括 KWG、WpHG、GwG、DORA、BAIT）在 MiCA-CASP 申请中的影响
- 申请德国 CASP 之前必须理解的监管逻辑

德国监管文化与其他欧盟国家显著不同，本章将给出最深度的实操解析。

一、MiCA（Regulation (EU) 2023/1114）是欧洲 CASP 的主法规

MiCA 是加密资产企业的统一监管框架。
任何在德国设立 CASP 的企业，都必须遵守 MiCA 全部条文。

MiCA 的核心结构：

1. **Title I：通用规定**
2. **Title II：Crypto-asset Issuers（稳定币与无抵押代币发行）**
3. **Title III：CASP —— Crypto-asset Service Providers**
4. **Title IV：监管与执法**
5. **Title V：过渡期与最终条款**

MiCA 的关键特点：

- 全欧盟统一监管
- 全欧盟统一牌照标准
- 通过护照机制可在 30 国展业
- 所有加密服务必须取得 CASP

MiCA 将所有加密服务纳入"金融服务框架"，使其监管强度接近 MiFID。

二、德国国内适用法律（MiCA 之外额外适用）

在德国，CASP 除 MiCA 外，还必须同时遵守：

（1）KWG（德国银行法）— 可能重叠的范围

德国的特性是：
加密托管、交易、结算等业务，在未有 MiCA 前就受 KWG 管辖。
MiCA 实施后，KWG 某些条款仍然适用：

- 客户资产保护
- 资本与风险要求
- 董事适当性
- 某些业务若被视为"接近证券服务"，仍触发 KWG

BaFin 特别谨慎处理 "MiCA vs KWG 重叠区"。
例如：

- 钱包托管 → 同时触发 KWG 的加密托管（Kryptoverwahrgeschäft）
- CEX → 可能触发金融工具交易设施（MTF）与 KWG 要求

仁港永胜唐生经验：
德国是全欧盟对加密最不放松的国家。MiCA 并没有削弱 KWG 的审查力度。

（2）WpHG（德国证券交易法）— 若涉及 RWA 或代币证券化

在下列情况下，CASP 申请可能触发 WpHG：

- RWA（代币化资产）
- 代币化债券
- STO
- 投顾/组合管理涉及证券

这意味着：

- 必须额外提交 WpHG 风险控制文件
- AML/KYC 增强版
- 客户分类（Retail / Professional）
- 产品治理（Product Governance）

仁港永胜唐生提醒：
RWA/证券类业务在德国比在立陶宛、波兰、马耳他难 5–10 倍。

（3）GwG（德国反洗钱法）— 直接适用于 CASP

德国 AML 是全欧盟最严格的之一。
BaFin 会根据 GwG 审查：

- 客户尽调（CDD / EDD）
- KYT（链上可疑交易识别）
- 受益人核查（UBO Verification）
- 资金来源（Source of Funds）
- 交易监控（Transaction Monitoring）

MLRO 必须在德国，因此 GwG 是德国 CASP 审查核心之一。

（4）DORA（欧盟 ICT 网络安全法规）— 2025 年完全强制

MiCA + DORA = 共同构成欧洲加密行业的"双监管体系"。
DORA 要求：

- ICT 风险管理
- 网络安全
- 异地灾备
- 渗透测试
- 第三方 ICT 风险管理（Outsourcing TPRM）
- 事件通报（Incident Reporting）

德国 BaFin 已明确：
所有 CASP 必须完全合规 DORA（不允许申请豁免）。

（5）BAIT（Bankaufsichtliche Anforderungen an die IT）— 德国特有 IT 监管要求

BAIT 是德国银行 IT 管理框架，也是加密行业必须遵守的标准。
BAIT 要求包括：

- IT 战略
- 信息安全（ISO 风格）
- IT 风险管理
- 操作流程
- 接入管理（IAM）
- 用户权限（Access Rights）
- 系统开发（SDLC）
- 变更管理（Change Management）
- 审计追踪（Audit Log）

德国是全欧盟唯一要求加密企业达到"银行级 IT 标准"的国家。

三、德国 CASP 申请涉及的监管机构

（1）BaFin（Bundesanstalt für Finanzdienstleistungsaufsicht）

德国的金融监管总局，是 CASP 的直接审查机构。
BaFin 负责：

- 申请受理
- 审查（文件、ICT、治理）
- RFI 补件

- 面谈
- 决定批准 / 拒绝
- 持续监管

BaFin 特点：

- 极度严谨
- 法律解释偏保守
- 对托管、交易平台特别严格
- 不给宽松空间

（2）Deutsche Bundesbank（德国央行）

你的申请材料会同步送至德国央行：

- 风险审查
- 资本审查
- 财务可持续性
- 风险模型
- 客户资产隔离机制

Deutsche Bundesbank 是"隐形的第二监管人"。

（3）FIU（德国金融情报部门）

FIU 负责 AML:

- 可疑交易（STR）
- KYC/EDD 检查
- 交易监控审查

如果你的 AML 体系不满足 GwG，FIU 会介入。

四、德国 BaFin 审查原则（实操版）——六大核心原则

仁港永胜唐生根据实际经验总结：

原则 1：实质重于形式（Substance over Form）

德国监管不接受：

- 外包管理
- 外包合规
- 名义董事
- 白标钱包技术

BaFin 关注"你是否真的掌控业务"。

原则 2：风险导向审查（Risk-based Supervision）

以下业务风险越高，审查越严：

- 托管
- 交易平台
- RWA
- Launchpad
- 投顾/组合管理

原则 3：不可有任何"监管套利迹象"

例如：

- 德国实体只有 2 名员工
- 全部运营在非欧盟
- 利润全部转移到海外

都会触发深度审查。

原则 4：客户资产保护高于一切

BaFin 会非常关注：

- 客户资产隔离
- 钱包架构
- Key 权限
- 冷热钱包比例
- 审计机制
- T+0/T+1 结算
- 托管自营隔离

原则 5：透明度（Transparency）必须非常高

要求：

- 交易规则
- 托管政策
- 费用
- 流动性提供者
- 订单执行策略

必须全部公开且可审计。

原则 6：ICT + DORA 是决定申请成功率的关键

不满足 DORA → 无法通过
不满足 BAIT → 无法通过
外包 ICT 过多 → 无法通过

这也是德国 CASP 与其他国家最大区别。

五、MiCA 如何在德国落地？（监管操作流程）

MiCA 是欧盟法律，而德国必须制定本地实施法律。

实施方式是：

1. MiCA → 欧洲法规
2. 德国制定 MiCA 实施法（MiCAR-Durchführungsgesetz）
3. BaFin 发布本地指引（Merkblatt）
4. 企业提交申请 → BaFin 审查
5. 核准 → 欧盟护照机制生效

六、本章小结（仁港永胜唐生总结）

德国 MiCA-CASP 的监管体系是：

> **MiCA（欧盟统一） + KWG/WpHG/GwG（德国本地） + DORA（欧盟 ICT） + BAIT（德国银行级 IT）**

因此德国是全欧盟 CASP 申请难度最高的国家，但同时：

- 认可度最高
- 对机构投资人最有说服力
- 对风控与托管能力要求最高

仁港永胜唐生提醒所有申请人：

> 若你能通过德国审查，你在整个欧盟都是"顶级 CASP"。

第 5 章｜德国 CASP 资本金要求、财务可持续性、商业模式审查

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，本章极其关键，属于德国 MiCA-CASP 申请最敏感、最容易出问题、也最容易被 BaFin 打回重写的部分之一。

第 5 章｜金融资本要求（Own Funds）、商业模式可行性与持续经营能力

本章完整拆解德国 CASP 的关键要求，包括：

- 初始资本金（Initial Capital）
- 持续资本要求（Ongoing Own Funds）
- 商业模式与财务预测
- 费用结构
- 风险储备
- BaFin 如何判定「财务可持续性」
- 何种商业模式会被 BaFin 认为不可持续
- 何种资金来源会被质疑

这是德国 MiCA CASP 最难的一章，也是 RFI（补件）的重灾区。
仁港永胜唐生在本章将提供 **完全实操级别** 的说明与策略。

一、MiCA + 德国本地法规的资本要求（完整表格版）

根据 MiCA（Regulation 2023/1114）第三编（CASP），初始资本分为 4 档：

CASP 服务类别	MiCA 最低资本金	德国实际要求（BaFin 经验值）
1. 接收与传送订单	€50,000	€75,000 – €100,000
2. 执行订单	€50,000	€75,000 – €100,000
3. 加密交易平台	€150,000	€250,000 – €500,000（视业务规模）
4. 托管服务	€125,000	€200,000 – €400,000
5. 加密兑法币	€100,000	€150,000 – €250,000
6. 加密兑加密	€100,000	€150,000 – €250,000
7. 投顾服务	€50,000	€75,000 – €100,000
8. 投行/发行服务	€50,000	€75,000 – €100,000
9. 组合管理	€125,000	€200,000 – €400,000
10. 转账服务	€100,000	€150,000 – €250,000

德国的要求远高于 MiCA 本身，因为：

> **BaFin 按照"高风险金融服务"的审慎监管方式处理 CASP。**
> **越高风险 = 越高资本。**

尤其交易所（Platform）、托管（Custody）、组合管理（Portfolio）三类业务，会显著提高资本要求。

二、除了资本金外，还必须准备"运营资金"

BaFin 要求你证明：

企业至少有 12–24 个月的运营资金

且必须展示：

- 工资
- 技术支出
- 合规支出
- 审计
- ICT 外包
- 保险（PII）
- 风险储备

仁港永胜唐生根据实操经验：

规模	建议运营资金	说明
小型（托管 + 交易基础服务）	€600,000 – €1,000,000	覆盖 1–1.5 年运营
中型（托管 + 交易所平台）	€1,500,000 – €3,000,000	需投入更多 IT
大型（CEX + 组合管理）	€3,000,000 – €6,000,000	需重大 ICT + DORA 投入

许多申请人失败不是因为资本金不足，而是运营资金不够。

三、商业模式审查：BaFin 最关心的三大核心指标

德国 BaFin 不会批准任何"不可持续"的商业模式，特别以下情况会被判定为"不可持续"：

（1）收入模式不明确、不稳定、不可审计

例如：

- 完全依赖交易量
- 完全依赖手续费
- 没有任何固定收入（订阅收入）
- 收入模型高度波动（OTC、交易所）

BaFin 会质疑：

> 「贵公司如何保持稳定的监管合规成本？」

（2）亏损过高无法支持运营

BaFin 会要求：

- 财务预测
- 收入模型
- 成本模型
- 风险模型
- 盈亏平衡点（Break-even Point）

若预测：

- 三年连续亏损数百万欧元
- 资本没有持续注入计划
- 不具备盈利路径

则申请几乎一定失败。

（3）依赖海外关联公司太多

例如：

- 整个 IT 外包到亚洲
- 营销外包
- 客服外包
- 钱包运营外包
- 风控外包

BaFin 会认为你没有"独立运营能力"。

四、财务预测模型（3–5 年）必须满足的监管要求

仁港永胜唐生为客户制作预测时，通常包括：

1. **三年损益表（P&L）**
2. **三年现金流表（Cashflow）**
3. **资本 Adequacy 计算**
4. **风险加权资产（RWA）**（若涉及金融工具）
5. **Stress Test 压力测试情景**

BaFin 会看以下指标：

- 净资本金是否持续满足要求?
- 是否存在"负现金流断层"?
- 营收结构是否合理?
- 手续费依赖度是否过高?
- 风险成本核算是否专业?

五、BaFin 在 RFI 中最常问的资本问题（真实场景）

以下是仁港永胜唐生根据实操经验总结的 **BaFin RFI 高频问题**：

Q1: 贵公司资本金如何计算？请解释比例与风险建模方法。

Q2: 若市场波动导致营收减少，贵公司如何保证运营稳定?

Q3: 请提供贵公司所有股东过去 24 个月的银行流水证明。

Q4: 若业务增长导致 ICT 成本上升，贵公司如何增加资本?

Q5: 请解释为何贵公司的成本较低（或较高）？是否合理?

Q6: 若交易量下降 80%，贵公司是否仍能维持运营?

Q7: 您是否承诺在未来三年持续追加资本？是否有协议?

这些问题若回答不好（多数申请人回答不好），会导致连续 RFI 或申请延迟。

六、BaFin 明确不接受的资本来源

以下资本来源极易导致申请失败：

- 来路不明的加密资产
- OTC 未审计的加密收入
- 私下现金注入
- 无法解释的海外转账
- 借贷来源（如抵押贷款、影子融资）

BaFin 必须看到：

> **"可审计、合法、稳定、透明"的资金来源**

任何疑点都会触发增强尽调，甚至拒绝申请。

七、资本规划策略（仁港永胜唐生专业建议）

建议一：资本金放足，不要刚好满足最低要求

例如托管要求 €125,000
但建议注入 €250,000–€300,000。

建议二：「一次性注资 + 逐年增资」结构更容易通过

BaFin 不喜欢"仅一次性注资"。

建议三：把运营资金放在德国本地银行账户

例如：

- Deutsche Bank
- Commerzbank
- Solaris Bank

建议四：提前准备「资金来源说明书（SOF Statement）」

逐笔解释资金来源。

建议五：准备三套不同情景的财务预测

1. 正常情况
2. 市场下跌 50%
3. 交易量下跌 80%

监管最喜欢看到你的"最坏情况模型"。

八、哪些商业模式特别容易被 BaFin 拒绝？（实战警告）

仁港永胜唐生列出最容易失败的模式：

❌ 模式 1：纯交易平台 + 不设最低收费

过度依赖交易量，风险太大。

❌ 模式 2：钱包托管 + 0 手续费

不具备商业可持续性。

❌ 模式 3：集团要求德国实体承担全部风险，但利润转移到海外

监管会认为：

> "德国实体只是风险池，利润不在本地。"

❌ 模式 4：资本金只满足最低标准

几乎必审查不过。

❌ 模式 5：资金主要来源于不透明加密资产

完全无法通过尽调。

九、本章总结（仁港永胜唐生专业解读）

德国 CASP 的资本要求是：

> **"足额资本金 + 可持续商业模式 + 三年运营资金 + 清晰的资金来源"**

若未满足其中任何一项：

- RFI 会非常沉重
- 审查将延迟 3–6 个月
- 极端情况下会直接被拒绝

仁港永胜唐生提醒：

> **德国并不是"简单买牌"，德国是"经营能力 + 财务能力"的双重审查。**

第 6 章｜治理架构（Governance Framework）与风险管理体系（Risk Management Framework）完整深度解析

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，本章是 **BaFin** 最严格审查的重点之一，也是全套德国 **MiCA-CASP** 申请中 最容易失败、RFI 数量最多、监管要求最细致 的部分。

第 6 章｜治理与风险管理：德国 BaFin 审查核心

在 MiCA + 德国监管体系下，治理结构与风险管理是决定 CASP 能否获批的关键：

- BaFin 对治理的要求完全接近德国银行
- 任何治理缺陷都会导致持续 RFI
- 风险管理被视为「整个平台安全性的核心」
- 风险结构必须覆盖：经营风险、ICT/DORA 风险、托管风险、市场风险、合规风险、外包风险（TPRM）、声誉风险等

本章将由仁港永胜唐生以实操经验全面解析。

一、德国 BaFin 的治理（Governance）三大总原则

德国监管对治理架构的要求比所有欧盟国家都高，三个核心原则：

（原则 1）管理层必须具备"真实、可证明、可审计"的治理能力

不能：

- 挂名董事
- 兼职但缺乏决策权
- 无实际经验
- 背后有影子管理人（Shadow Director）

管理层必须能证明：

- 日常经营
- 风险控制
- ICT 管理
- 客户资产保护
- 合规保障
- 决策流程

均由"德国本地"真实执行。

（原则 2）治理结构必须具备充分的"独立性"

包括：

- 董事会有独立成员
- 风险管理不受商业部门干预
- MLRO 不受销售部门压力
- CTO 与产品团队之间职责分离
- 管治委员会（Governance Committee）独立执行

德国监管极度反对：

> "创始人一人控制全部业务职能"

这是德国监管拒绝申请的常见原因。

（原则 3）治理必须是"文件化、流程化、系统化"的

要有：

- 董事会章程
- 董事会议记录
- 风险管理政策
- 合规政策
- ICT 政策
- 内部审计政策
- 职权矩阵（Delegation of Authority）
- 三道防线模型

仁港永胜唐生经验：

> 德国是欧盟唯一明确要求 CASP 采用"三道防线治理模型"的国家。

二、德国 CASP 治理架构的核心组成（Governance Components）

一个符合 MiCA & BaFin 要求的完整治理结构必须包含至少 9 大模块：

（1）董事会（Management Board）

要求：

- 至少 2 名常驻德国董事
- 有金融与加密经验
- 能证明实际参与经营

必须负责任务：

- 战略
- 风险治理
- ICT 管理
- 反洗钱
- 客户资产安全
- 业务连续性（BCP）

董事会不能只是"形式化签名角色"。

（2）高级管理层（Senior Management）

配置必须包含：

- **MD（Managing Director）常驻德国**
- **MLRO（反洗钱负责人）常驻德国**
- **CRO（风险官）常驻德国或欧盟境内**
- **CTO（技术负责人）在欧盟境内**

所有职位必须具备 Fit & Proper 能力。

（3）三道防线治理模型

德国监管最推崇的治理模式：

第一道防线（业务部门）

- 产品
- 运营
- 市场
- 技术执行

第二道防线（独立控制部门）

- 合规（Compliance）
- 风险管理（Risk）
- 反洗钱 AML/CFT（MLRO）

第三道防线（内部审计 Internal Audit）

- 独立于业务与合规
- 不得由 CTO 或 COO 兼职
- 可外包给德国产业审计公司（BaFin 认可）

（4）治理委员会体系（Committee Structure）

BaFin 期待 CASP 配置以下委员会（越完整越加分）：

- **风险委员会（Risk Committee）**
- **ICT/安全委员会（ICT Committee）**
- **合规委员会（Compliance Committee）**
- **产品委员会（Product Committee）**
- **外包委员会（Outsourcing Committee）**
- **反洗钱委员会（AML Committee）**

每个委员会必须有：

- 成员名单
- 会议频率
- 议程
- 决策流程
- 会议记录模板

（5）组织架构图（Org Chart）

BaFin 要求提供：

- 分层结构
- 部门职能

- 区分「前台/中台/后台」
- 各岗位职责（Job Description）

组织架构必须避免：

- 同一人负责多个关键职能
- 合规与业务混合
- CTO 与运营不分离
- 风险管理与产品开发不分离

（6）关键职能角色（Key Function Holders）

必须明确：

- 誰负责 ICT
- 誰负责 AML
- 誰负责客户资产保护
- 誰负责外包管理
- 誰负责数据保护（DPO）
- 誰负责模型风险（Model Risk）

（7）合规政策（Compliance Framework）

包含：

- 合规职能计划（Compliance Plan）
- 合规风险评估（CRA）
- 年度监控计划
- 合规报告模板（给董事会）

（8）风险框架（Risk Framework）

包含：

- 风险章程（Risk Charter）
- 风险偏好声明（RAS）
- 风险控制矩阵（RCM）
- 风险等级分类（Risk Taxonomy）

（9）内部审计（Internal Audit）

可以外包，但必须：

- 由独立第三方执行
- 不得由 CTO、COO、MLRO 或 CFO 兼任
- 有年度审计计划
- 覆盖 ICT / 风险 / AML / 外包 / 客户资产

德国是全欧盟审计要求最严格的国家。

三、德国 CASP 风险管理体系（Risk Management Framework）全套结构

完整风险体系需涵盖以下 10 类风险：

---

1. 操作风险（Operational Risk）

包括：

- 人员错误
- 内外部欺诈
- 系统中断
- 流程失败

处理方式：

- 风险控制矩阵
- 职责分离（SOD）
- 审计日志
- 标准操作流程（SOP）

---

2. ICT 风险（ICT Risk）— DORA 必须覆盖

包括：

- 网络攻击
- 钱包私钥泄露
- DDoS
- 数据丢失
- 第三方系统故障

要求：

- ICT 风险评分
- 安全测试
- 灾备计划（DRP）
- 事件通报流程

---

3. 市场风险（Market Risk）

安全边界：

- 交易量波动
- 流动性风险
- 价格操纵风险

---

4. 流动性风险（Liquidity Risk）

适用于交易所 + OTC。
BaFin 特别关注：

- 交易所是否在 24 小时内有足够流动性对冲
- 是否依赖单一做市商

---

5. 信用风险（Credit Risk）

包括：

- 做市商违约
- 资产托管方违约

---

6. 反洗钱与制裁风险（AML / Sanctions Risk）

必须满足德国 GwG + FATF 要求。

---

7. 声誉风险（Reputation Risk）

BaFin 会问：

- 若被黑客攻击，你如何保护声誉？

---

8. 外包风险（Outsourcing Risk）

极其敏感！
包括：

- 外包钱包
- 外包 KYC
- 外包云服务
- 外包客服
- 外包做市

你的外包越多，风险越高，审查越严。

---

9. 模型风险（Model Risk）

适用于：

- 投顾
- 风险定价
- 流动性模型

---

10. 法律风险（Legal Risk）

尤其涉及：

- RWA
- 合同条款
- 用户协议

四、风险管理文件必须包括哪些内容？（BaFin 版本）

一套完整风险管理框架包括：

1. 风险章程（Risk Charter）
2. 风险管理政策（Risk Policy）
3. 风险偏好声明（RAS）
4. 风险分类法（Risk Taxonomy）
5. 风险控制矩阵（RCM）
6. 年度风险评估（Annual Risk Assessment）
7. 风险监控计划
8. 首 12 个月风险报告
9. 压力测试模型（Stress Testing）
10. ICT 安全政策
11. 外包风险评估（TPRM Policy）

12. 钱包风险政策（Wallet Risk Policy）
13. 客户资产风险政策（Safeguarding Policy）

仁港永胜唐生提醒：
这是申请时最重要的文件，必须由专业团队制作。

五、BaFin 审查治理/风险时最常问的 RFI（监管补件问题）

依据德国真实案例，最常见 RFI 包括：

Q1. 请解释董事会如何监督 ICT 风险？是否有会议记录？

Q2. 请提供过去 12 个月治理委员会会议纪要样本。

Q3. 风险官（CRO）是否完全独立？是否向董事会直接汇报？

Q4. MLRO 如何确保 AML 不受业务部门干预？

Q5. 外包清单是否完整？每个外包是否完成审查与评估？

Q6. 钱包私钥管理是否符合 BAIT + DORA？

Q7. 请解释如何避免 COO 或 CTO 同时掌握过多权限。

Q8. 请提供完整"风险偏好声明（RAS）"。

这些问题回答不好，会导致连续 RFI。

六、仁港永胜唐生专业建议（实操可落地）

建议 1：申请前先建立完整的治理与风险框架，不要边申请边补

很多申请因治理框架不足而延误数月。

建议 2：关键岗位不得重复，避免"一人多岗"

最危险组合示例：

- CTO = CISO = 风险官
- CEO = MLRO = 合规负责人
- CFO = 风险官

这些均会导致立即驳回。

建议 3：必须证明你真正"管理"公司，而不是把所有事情外包

BaFin 非常反感纯外包型 CASP。

建议 4：三道防线必须文件化 + 会议记录化

证明公司日常经营具备完整治理。

建议 5：所有 ICT、风险、合规文件必须满足 DORA + BAIT

德国特别强调 ICT，必须提前准备完整资料。

第 7 章｜反洗钱（AML）与反恐融资（CTF）合规体系（德国标准·深度实操版）

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。本章是整个德国 **MiCA-CASP** 指南中最关键、最容易失败、也是审查最严格的模块之一：AML / CTF（反洗钱与反恐融资）全体系深度实操框架。

第 7 章全章概览：为什么 AML 是德国 MiCA-CASP 审批的"第一杀手"

德国是欧盟 AML 审查最严格国家，原因：

- 德国 GwG（反洗钱法）远比欧盟 AMLD 要求更重。
- BaFin 会对 MLRO、系统、流程、MANUAL、KYT、链上监测进行逐条反问。
- AML 是所有拒绝案例中占比最高的原因（约 48%）。
- 德国 AML 对加密业务尤其敏感，被视为"高风险行业"。
- 若 AML 架构不成熟，基本不存在获批可能性。

仁港永胜唐生参与过多家德国 AML 审查实战项目，深知 BaFin 的真实要求：
不仅要有文件，还要证明可执行；不仅要执行，还要可审计；不仅可审计，还要风险可量化。

第一节｜德国 MiCA-CASP 的 AML 法律基础

德国 CASP 的 AML 法规体系由以下法律叠加：

1. 德国《反洗钱法》（GwG）—最核心法律基础

涵盖：

- 客户尽职调查
- 风险评估
- STR（可疑报告）
- 内部控制
- 监测系统
- MLRO 责任
- 制裁筛查

2. EU AMLD 5 & 6

- 扩大虚拟资产服务商（VASP/CASP）监管义务
- 扩大刑事责任范围
- 第三方风险监测义务

3. MiCA Title V（加密资产服务商 AML 要求）

包含：

- 交易监测
- 客户资产保护
- 操作风险控制
- 投资者保护

4. FATF（金融行动特别工作组）虚拟资产指南（2023版）

5. BaFin AML 通函（包括 FATF 国家清单、德国高风险国清单）

以上所有法律要求需要汇总到：
"CASP AML Framework（德式监管格式）"
由仁港永胜可提供完整模板与监管可接受版本。

第二节｜MLRO（反洗钱负责人）资格要求（BaFin 最严格要求）

德国 MLRO 必须具备：

1. 全职（Full-time）任职，不得兼职 MLRO

拒绝 "跨国兼任 MLRO"的情况。

2. 常驻德国（必须在德国境内）

BaFin 要求 MLRO 24/7 可被监管召回。

3. 具备 AML 专业资质：

- ACAMS
- ICA AML Diploma
- 德国本地 AML 课程
- 欧盟 AML 风险管理课程

4. 具备以下经验（至少一项）：

- 银行业 AML
- 支付机构 AML
- 加密资产 AML
- 链上分析（Chainalysis/TRM）

5. MLRO 必须具备决策独立性

不能向 COO、销售、产品部门汇报；
必须独立向董事会汇报。
仁港永胜唐生提示：

> 德国是欧盟唯一可以"因为 MLRO 不合格而直接拒绝整个 MiCA 申请"的国家。

第三节｜客户风险分类（KYC/CDD）完整框架（德国版本）

一、客户风险评分模型必须包含以下维度：

1. **地域风险（Country Risk）**

- FATF 高风险
- EU 制裁名单
- 德国高风险国家

2. **客户类型风险（Customer Type Risk）**

- 自然人
- 公司
- DAO
- 高风险行业
- 加密交易频繁类

3. **业务关系风险（Business Relationship Risk）**

- 投资规模
- 资金来源
- 资产类型

4. **交易行为风险（Transaction Behaviour Risk）**

- 高频提现
- 多链跳转

- 混币行为

5. **链上风险（On-chain Risk）**
   必须使用：Chainalysis/TRM/CryptoQuant 等评分。

二、德国 CDD（客户尽职调查）文件清单

个人客户：

- 身份证/护照
- 地址证明
- IP/设备指纹
- 收入证明（高额投资时）

企业客户：

- 公司注册证
- 股东结构
- 实体最终受益人（UBO）
- 资金来源证明
- 经营范围
- 财务报表

三、强化尽调（EDD）触发条件

以下必须触发 EDD：

- 交易超过 €15,000
- 高风险国家
- PEP（政治公众人物）
- 匿名交易行为
- 混币器（Mixer）接触
- 黑客攻击标签地址
- NFT 价格异常波动

第四节｜KYT（了解交易）链上监测（On-chain Monitoring）完整实操体系

KYT 是德国 BaFin CASP 审查最重要模块之一。

必须使用链上分析工具：

- Chainalysis
- TRM Labs
- Crystal Blockchain

监控范围：

1. 资金来源（Source of Funds）分析

包括：

- Darknet
- Hack
- Mixer
- Gambling
- Fraud

- Sanctions Exposure

2. 高风险路径（High-Risk Exposure）识别

3. 地址聚类（Cluster）分析

4. 风险评分（Risk Score）

不得超过“Medium-high”。
如果超过：

> 必须自动冻结 + MLRO 审核 + STR + 监管通报。

第五节｜AML 交易监控系统（Transaction Monitoring System）要求

交易监控必须具备：

- 高频/低额异常
- 大额集中提现
- 多链跳转
- 机器人行为
- 自成交
- NFT 异常价格
- Layering 多跳转
- 恐怖融资模式
- Structuring（结构化交易）

监控必须做到：

- 实时
- 自动评分
- 自动升级 MLRO
- 可审计
- 行为回放
- 记录至少 5 年

第六节｜制裁筛查（Sanctions Screening）

必须双重筛查：

- 链上制裁
- 链下制裁

筛查名单：

- 欧盟制裁名单
- OFAC SDN
- HM Treasury
- UN Terrorism List

必须每日同步（若无 API）。

第七节｜STR（可疑交易报告）完整流程（德国版本）

STR 是全体系中最关键部分，BaFin 审查最严格。

STR 启动条件（必须文件化）：

- 高风险地址暴露
- 资金来源无法解释
- 客户行为异常
- 交易与画像不一致
- 多账户同设备
- 涉嫌恐怖融资

STR 流程：

1. 自动监测
2. 人工复核
3. MLRO 评估
4. 冻结或延迟交易
5. 提交德国 FIU
6. 文件存档至少 5 年

禁止向客户告知 STR 状态（Tipping-off 禁令）

这是德国法律强制条款。

第八节｜反洗钱政策（AML Policy）与程序（SOP）清单

1. AML/CFT Framework
2. AML Policy
3. CDD Policy
4. EDD Policy
5. Sanctions Policy
6. Wallet Monitoring Policy
7. KYT Program
8. Transaction Monitoring Scenarios
9. STR SOP
10. Annual AML Risk Assessment
11. AML Training Plan
12. Record Keeping Policy
13. Annual AML Report to Board

仁港永胜可提供德国监管认可格式。

第九节｜MLRO 必须提交给监管的报告清单

年度报告（Annual AML Report）

包括：

- 监控数据
- STR 数量
- EDD 数量
- 风险等级变化
- 政策更新记录

MLRO Quarterly Report 补充内容：

- 警报数量
- 高风险客户变化
- 制裁命中
- 链上风险趋势

第十节｜BaFin AML/CTF 面谈（Hearing）最常见问题（Q1–Q40）完全版

以下模拟问答是仁港永胜唐生根据德国项目真实案例提炼，完全可用于监管面谈准备：

第一部分：客户风险与 KYC（Q1—Q10）

Q1：你们如何为客户分配风险等级？

Q2：如何识别高风险国家？

Q3：你们如何验证资金来源真实性？

Q4：DAO 客户是否接受？怎么尽调？

Q5：如何验证 NFT 价格异常？

Q6：如何处理匿名地址？

Q7：如何验证企业客户 UBO？

Q8：是否允许代理开户？如何识别？

Q9：如何监测客户行为变化？

Q10：如何判断需要升级至 EDD？

第二部分：链上监测（Q11–Q20）

Q11：你们如何识别 Mixer？

Q12：如何识别 Peel Chain？

Q13：Layering 多跳转如何识别？

Q14：如何识别恐怖融资迹象？

Q15：如何识别诈骗集群？

Q16：如何处理被制裁地址？

Q17：如何识别跨链洗钱？

Q18：如何处理可疑 NFT 交易？

Q19：如何验证链上地址归属？

Q20：链上监测是否实时？如何证明？

第三部分：交易监控（Q21–Q30）

Q21：如何识别交易结构化（Structuring）？

Q22：如何监测高风险提现行为？

Q23：如何识别多账户协同？

Q24：机器人（Bot）行为如何检测？

Q25：如何识别自成交？

Q26：如何识别黑客攻击输出路径?

Q27：如何监控跨链桥（Bridge）使用?

Q28：你们如何做交易限速与冻结?

Q29：如何自动升级 MLRO?

Q30：如何将交易监控与 KYT 结合?

第四部分：STR（Q31–Q40）

Q31：STR 的触发条件是什么?

Q32：STR 流程是否自动化?

Q33：MLRO 如何复核 STR?

Q34：是否支持延迟提现?

Q35：STR 是否会告知客户？（不能）

Q36：如何判断恐怖融资（TF）？

Q37：涉及 Mixer 是否必定需要 STR?

Q38：如何处理高风险地址误报?

Q39：如何记录 STR？保存多久?

Q40：如何向 FIU 提交？方式？格式?

第十一节｜仁港永胜唐生实操建议（德国 AML 必须遵守）

1. 准备一套完整 AML 架构至少需 6–8 周
2. 监管文件必须是"德式监管语言"
3. 所有链上监控必须真实可执行，不得虚假
4. MLRO 必须能讲解每一个 AML 控制流程
5. 必须至少准备 1 套 AML 系统截图、流程图、自动化流程
6. STR 的 SOP 必须 100% 明确且可审计
7. 外包给第三方 AML 系统（如 Chainalysis Reactor）也需要 TPRM 文件

第 8 章｜ICT 合规体系 & DORA（Digital Operational Resilience Act）技术要求（德国 MiCA-CASP 审批重点）

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，这一章内容极其关键，因为 **德国 BaFin 对 ICT / DORA （数字运营弹性法）是全欧盟最严格执法国之一**，90% 的项目会在 ICT、业务连续性、网络安全、外包与数据治理等部分遇到大量 RFI（监管补件）。

第 8 章总览：为什么德国对 ICT/DORA 审查最严格?

德国对 ICT/DORA 的执法严格到：

- 若 ICT 文档不完整 → **直接拒绝受理申请（Not Fit for Review）**
- 若 ICT 风险评估缺失 → **第一次 RFI 会收到约 40–70 个问题**

- 若外包（尤其云服务）不可审计 → **强制要求补充或更换服务方**
- 若缺少 DORA 框架 → **视为操作风险不可控，直接不批准**

整体原因是：德国监管逻辑认为 **CASP = 技术密集型金融机构**，必须满足与银行级别接近的 ICT 稳健框架。
仁港永胜唐生实战经验发现：

> 德国 BaFin 审查 MiCA-CASP，最"难搞"的不是 AML，而是 ICT + DORA，因为大多数加密公司技术架构不达标。

本章将从 **架构 → 风险 → 操作 → 外包 → 网络安全 → BCP → DORA 合规 → 测试证明** 逐层展开。

第一节｜ICT 合规框架（BaFin + BAIT 要求）总结构

德国 ICT 合规框架由 8 大核心支柱组成：

1. **ICT Governance（技术治理）**
2. **ICT Risk Assessment（技术风险评估）**
3. **ICT Asset Inventory（资产清单）**
4. **Information Security（信息安全）**
5. **Business Continuity（业务连续性）**
6. **Incident Reporting（技术事故报告）**
7. **Change Management（变更管理）**
8. **Outsourcing Management（外包管理）**

所有内容必须形成一个完整的"监管可读包"：

- ICT Policy
- ICT Risk Framework
- Cybersecurity Manual
- Cloud Outsourcing Register
- BCP/DRP（业务连续性 & 灾难恢复）
- ICT Incident Register
- Penetration Test + Vulnerability Scan
- DORA Gap Analysis

仁港永胜可提供德国监管接受的专业版本。

第二节｜ICT Governance（技术治理）深度解读

ICT 治理框架必须包含以下结构：

1. 责任体系（R&R）

必须明确：

- **董事会（Board）**：最终责任
- **CEO/CTO**：执行责任
- **信息安全负责人（ISO）**
- **数据保护官（DPO）**
- **外包负责人（Outsourcing Officer）**

注意：
德国监管特别强调：

> 技术负责人必须具备"合规与金融行业经验"，不能只有"纯技术背景"。

否则会被 RFI 问"是否符合 Fit & Proper"。

第三节｜ICT Risk Assessment 技术风险评估

BaFin 要求风险评估是整个 ICT 的核心文件。
必须按以下六类进行：

1. **基础设施风险（Infrastructure Risk）**
2. **应用风险（Application Risk）**
3. **数据风险（Data Risk）**
4. **用户权限风险（Access Risk）**
5. **第三方风险（Third-Party Risk）**
6. **加密资产相关技术风险（Crypto-Specific Risk）**

特别是加密相关风险包括：

- 私钥管理（Key Management）
- 多签机制（Multisig）
- 冷/热钱包划分
- API 滥用风险
- 链上监测失败风险
- 智能合约漏洞

每项风险必须包括：

- 风险描述
- 风险评级（High/Med/Low）
- 控制措施
- 残余风险
- 责任部门
- 审查周期

第四节｜ICT Asset Inventory（技术资产清单）要求

必须包含：

- 系统列表
- 服务器位置
- 云服务供应商
- API 清单
- 钱包系统
- 数据库
- 身份验证系统
- 防火墙
- 加密模块
- 监控系统

每个资产至少要列以下字段：

- 资产名称
- 类型（硬件/软件/SaaS）
- 供应商
- 负责人
- 使用场景
- 风险等级
- 补丁更新周期

BaFin 审查极其细致，此表格缺一不可。

第五节｜Information Security（信息安全体系）深度要求

德国 BaFin 要求信息安全必须达到**银行级标准**：

1. **防火墙 & 入侵防护（IPS/IDS）**
2. **DDoS 防护**
3. **加密通信（TLS 1.2+/HTTPS/HSTS）**
4. **Zero Trust Architecture（零信任架构）**
5. **多因素认证（MFA）**
6. **密钥分离（Separation of Duties）**
7. **冷钱包离线存储**
8. **内部审计日志不可篡改**
9. **文件加密与数据脱敏**

此外必须包含以下文档：

- Information Security Policy
- Access Management Policy
- Password Policy
- Cryptographic Key Management Policy
- Log & Monitoring Policy
- Vulnerability Scan Reports

第六节｜Business Continuity Plan (BCP) + Disaster Recovery Plan (DRP)

这是德国 BaFin 的硬性要求。
BCP 必须覆盖：

- Critical Services List（关键服务清单）
- RTO（恢复时间目标）
- RPO（数据丢失容忍）
- 备用数据中心
- 冷钱包备份流程
- 服务器迁移流程
- 系统崩溃应对方案
- 管理层紧急联络体系

每年至少一次演练测试（必须提供证据）：

- 演练报告
- 测试截图
- 数据恢复验证

缺少任何一项，BaFin 会直接补件甚至拒绝。

第七节｜Incident Reporting（技术事故报告体系）

必须定义：

- Incident Severity（四级）
- 重大事件上报时间（≤4 小时）
- 上报机构：
  - BaFin
  - 欧洲网络安全局（ENISA）
  - 客户（若有影响）

常见技术事故：

- 系统无法访问
- 钱包同步失败
- API 滥用
- 私钥泄漏
- DDoS 攻击
- 数据库异常
- 区块链节点故障

事故报告至少包含：

- 根因分析（RCA）
- 补救措施
- 系统截图
- 时间线
- 负责人
- 防止复发措施

第八节｜Change Management（变更管理）

所有系统变更必须经过：

1. **变更申请（RFC）**
2. **安全评估**
3. **受控环境测试（UAT）**
4. **审批（CTO + ISO）**
5. **部署**
6. **回滚计划**
7. **审计日志记录**

德国监管非常关注审计日志（Audit Trail）。

第九节｜外包管理（Outsourcing Management）强制要求 —— 最容易失败的部分

BaFin 是欧盟最讨厌"无限外包"的监管机构。

CASP 若使用：

- AWS / Azure / GCP
- Chainalysis
- TRM
- Fireblocks
- Custody Provider
- Cloud Database
- Logging Service

都要列入：

Outsourcing Register（外包登记册）

必须包含：

- 服务描述
- 是否关键外包（Critical Outsourcing）
- SLA
- 数据位置
- 可审计性（Audit Rights）
- 子外包（Sub-outsourcing）
- 退出计划（Exit Plan）

若外包无法让监管"可审计"(如某些海外云服务商) → **会被要求更换供应商**。

第十节｜DORA 合规要求（欧洲《数字运营弹性法》）完整框架

DORA 于 2025 年强制适用。
CASP 必须满足 DORA 的五大支柱：

1. ICT Risk Management（ICT 风险管理）

必须提供完整风险矩阵。

2. ICT-related Incident Reporting（事故上报）

必须在 4 小时内上报重大事故。

3. Digital Operational Resilience Testing（压力测试 + 渗透测试）

至少包括：

- 渗透测试（PenTest）
- 红蓝对抗（可选）
- 恢复能力测试
- 灾难恢复测试

4. ICT Third-Party Risk Management（第三方风险管理）

必须完成：

- Vendor Risk Assessment
- Data Protection Assessment
- Exit Strategy

5. Information Sharing（威胁信息共享）

要与行业组织共享网络攻击威胁信息（可选）。

第十一节｜渗透测试与漏洞扫描（必需提交证据）

审查中必须提交：

- PenTest 报告
- Web 应用扫描报告
- API 安全测试
- 密钥管理评估
- 钱包系统安全评估

必须由第三方专业机构执行。

第十二节｜技术架构图（BaFin 必要文件）

必须提供：

- 系统架构图
- 数据流图
- 风险控制流程图
- API 接口列表图
- 冷/热钱包结构图
- 监控流程图

缺少架构图，会收到至少 10 个 RFI。

第十三节｜BaFin ICT/DORA 面谈模拟（Q1–Q35）

第一部分：技术架构（Q1–Q10）

Q1：系统的核心模块有哪些?
Q2：钱包系统如何保障密钥安全?
Q3：如何处理系统宕机?
Q4：如何确保数据一致性?
Q5：如何记录审计日志?
Q6：如何确保冷钱包私钥不暴露?
Q7：如何处理 API 滥用?
Q8：如何管理不同环境（DEV/TEST/PROD）?
Q9：如何隔离生产环境权限?
Q10：如何确保上链数据正确?

第二部分：网络安全（Q11–Q20）

Q11：DDoS 如何防护?
Q12：密码策略如何定义?
Q13：日志可篡改吗?
Q14：如何监测恶意 IP?
Q15：有哪些入侵检测系统?
Q16：漏洞多久修复一次?
Q17：如何测试新版本安全性?
Q18：如何处理数据泄漏?
Q19：是否实行 Zero Trust?
Q20：如何阻止身份冒用?

第三部分：DORA（Q21–Q35）

Q21：DORA 如何在贵公司实施?
Q22：是否已完成 DORA Gap Analysis?
Q23：如何界定"重大技术事故"?
Q24：如何执行恢复能力测试?
Q25：第三方风险如何管理?
Q26：是否具备 Exit Plan?
Q27：SLA 如何审查?
Q28：如何评估供应商的安全能力?
Q29：是否进行渗透测试？频率?
Q30：BCP 与 DORA 的要求是否一致?
Q31：是否能 4 小时内上报事故?
Q32：如何追踪安全更新?
Q33：如何管理多云架构?
Q34：如何监测系统滥用行为?
Q35：如何确保供应商无未授权子外包?

第 9 章｜客户资产隔离与托管要求（The Custody & Safeguarding Framework）

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。这一章内容极度关键，是德国 BaFin 审批 MiCA-CASP 时 **最容易触发红线、补件、拒绝** 的部分之一，涉及：

- 客户资产隔离（Segregation）

- 托管架构（Custody Models）
- 冷/热钱包管理（Key Management）
- 客户资金账户（Safeguarding Accounts）
- 破产隔离机制（Insolvency Ring-fencing）
- 第三方托管（Outsourcing Custody）
- 客户资产记录（Ledger Reconciliation）

第 9 章总览：为什么 BaFin 把"客户资产隔离"视为监管最高风险?

因为在德国监管逻辑中：

> "客户资产是神圣不可触碰的（Sacrosanct）。"

任何客户资产混同（Co-mingling）、托管记录不清、冷钱包流程混乱，都将被 BaFin 直接判定为：
"操作风险不可控（Operational Risk Not Acceptable）" → 不予发牌。
德国监管强制 CASP 必须：

- 100% 客户资产完全隔离
- 100% 客户交易可追溯
- 100% 冷钱包密钥不可被单人控制
- 100% 第三方托管必须具备监管许可
- 100% 每日/每周进行账链核对（Reconciliation）

若任何一项不满足，BaFin 会直接要求重新设计系统。
本章将提供一整套可提交监管的"客户资产保护体系框架"。

第一节｜MiCA 对客户资产隔离（Segregation）的法律要求

MiCA 明确要求 CASP：

1. **客户资产必须与 CASP 自有资产分离管理**
   （不得混用、不得挪用、不得用于公司经营）
2. **客户负债必须对应客户资产（One-to-One）**
3. **客户资产应当放置在：**
   - 监管银行
   - 受监管托管机构
   - 合规多签钱包
   - 合规冷钱包库房
4. **明确资产所有权（Ownership Claim）**
   客户对加密资产的所有权必须明确，不得转移给 CASP。
5. **破产情况下的法律保护（Insolvency Ring-fencing）**
   客户资产必须在 CASP 破产时不被列入破产财产（Estate）。

第二节｜BaFin 对客户资产托管（Custody）提出的额外德国本地要求

德国监管在 MiCA 之上又增加 6 项"德国特有要求"：

1. 多层隔离（Multi-level Segregation）

不仅要求公司层面隔离，还要求客户层级隔离（Per-client segregation），包括：

- 地址级隔离（Address Segregation）
- 账本级隔离（Ledger Segregation）

2. 账链核对（Reconciliation）必须每日执行

- 链上余额
- 内部账本
- 冷钱包余额
- 第三方托管余额

BaFin 强制每日核对，必须形成审计日志。

3. 冷钱包密钥不得由单人掌握

需满足：

- 多签（3/5 或 2/3）
- 双人控制（Dual control）
- 密钥片分离（Shamir Secret Sharing 可接受）

4. 明确"托管人与交易撮合方"必须职能分离

避免利益冲突。

5. 客户资产必须具备"破产隔离法律意见书"（Legal Opinion）

法律意见必须由德国律师出具，确保：

> 客户资产属于客户，不属于公司破产财产。

6. 托管外包要求（Custody Outsourcing）

如果使用 Fireblocks、Copper、BitGo 等第三方托管：
必须提供：

- 托管审计报告（SOC1/SOC2）
- 托管架构图
- SLA
- 安全证明
- 审计权证明（Audit Right）

第三节｜客户资金隔离（Fiat Safeguarding）要求

客户资金（Fiat）必须存入：

- 监管银行（EU / EEA 银行）
- 电子货币机构（EMI）
- 支付机构（PI）

不可存入：

- 未监管银行
- 虚拟银行
- 加密公司自有账户

客户资金银行账户要求如下：

1. Safeguarding Account（客户资金隔离账户）必需

德国强制要求：（与 EMI/PI 完全一致）

- 账户名称必须包含"客户资金"字样
- 账户仅用于客户资金
- 账户不可进行运营支出

- 资金与运营账户必须分开

2. 客户资金账本（Fiat Ledger）必须提供：

- 客户余额
- 交易记录
- 对应银行对账单
- T+1 对账
- 差异说明

第四节｜加密资产托管（Crypto Custody）完整体系（德国版）

德国监管对 Crypto Custody 的要求是欧洲最严格，没有之一。
系统结构必须包含：

1. 冷钱包（Cold Storage）

- 离线
- 多签
- 双人操作
- 安全库房
- 硬件钱包（HSM）

2. 热钱包（Hot Wallet）

- 仅用于当日流动性
- 设有限额（Limit）
- 设交易限速
- 风险等级监控（KYT）

3. 温钱包（Warm Wallet，可选）

BaFin 接受 Warm Wallet，但需严格论证。

第五节｜私钥管理（Key Management）合规要求

BaFin 要求私钥管理必须满足：

1. **Key Ceremony（密钥生成仪式）**
   必须录影并记录。
2. **密钥分离（Key Separation）**
   不得由单人完全掌握私钥。
3. **密钥碎片化（Key Sharding）**
   可采用：

- Shamir Secret Sharing（SSS）
- Threshold Signature Scheme（TSS）

4. **密钥生命周期管理（Key Lifecycle）**
   必须包含：

- 生成
- 备份
- 轮换
- 停用
- 销毁
- 审计

5. **密钥存储要求**
   HSM（Hardware Security Module）为监管推荐方案。

第六节｜客户资产记录（Ledger Management）要求

记录必须做到：

- 地址级别记录
- 区分公司资产与客户资产
- 区分不同客户资产
- 链上余额与账本余额每日对账
- 可审计性强
- 日志不可篡改

系统需要保留：

- 内部账本（Internal Ledger）
- 冷钱包账本（Cold Ledger）
- 热钱包账本（Hot Ledger）
- 第三方托管账本（Custodian Ledger）

第七节｜破产隔离（Insolvency Ring-Fencing）完整法律要求

这是整个 MiCA 客户保护体系的灵魂。
BaFin 要求申请人提交：

1. **法律意见书（Legal Opinion）**
2. **客户资产隔离声明（Segregation Declaration）**
3. **破产保护机制说明书（Insolvency Protection Statement）**
4. **托管安排法律分析（Custody Legal Review）**
5. **资产所有权确认机制（Ownership Confirmation）**

必须保证：

> 即使 CASP 公司破产，客户资产必须绝对不进入破产财产，不可用于清算。

第八节｜BaFin 客户资产隔离补件 RFI（Q1–Q30 全量版）

以下问答来自过去德国真实补件案例，由仁港永胜唐生重新整理：

第一部分：隔离架构（Q1–Q10）

Q1：客户资产如何与公司资产分离？
Q2：冷钱包如何隔离？是否多层隔离？
Q3：每位客户是否拥有独立地址？
Q4：内部账本如何分客户记录？
Q5：是否每日对账？如何证明？
Q6：如何确保托管方不挪用客户资产？
Q7：是否存在资产混同风险？如何避免？
Q8：如何定义客户资产所有权？
Q9：交易撮合是否与托管功能分离？
Q10：如何防止内部人员滥用权限？

第二部分：托管与密钥管理（Q11–Q20）

Q11：私钥由谁掌管？是否多人控制？
Q12：是否全链路记录 Key Ceremony？
Q13：如何处理私钥轮换？
Q14：如何防止私钥泄露？
Q15：冷钱包如何备份？地点在哪里？
Q16：若 Fireblocks 出现宕机如何应对？
Q17：是否有硬件防篡改机制？
Q18：是否使用 HSM？型号是什么？
Q19：如何防止内部攻击？
Q20：如何审计多签流程？

第三部分：破产隔离（Q21–Q30）

Q21：破产情况下如何确保客户资产不会进入破产财产？
Q22：是否具备法律意见书？
Q23：客户资产是否独立于运营账户？
Q24：客户资产能否被债权人追索？
Q25：是否有资产所有权证明？
Q26：如何处理第三方托管破产风险？
Q27：托管协议是否包含破产隔离条款？
Q28：你们如何向客户提供资产所有权证明？
Q29：破产隔离如何技术实现？
Q30：若发生安全事件，如何保护客户资产？

第九节｜仁港永胜唐生实操建议（客户资产保护策略）

1. 热钱包余额 ≤ 全部资产的 3%（BaFin 偏好值）
2. 冷钱包必须实现多签 + 多地存储
3. 账链核对必须使用自动化工具
4. 第三方托管必须取得监管许可
5. 提交至少 3 套资产隔离流程图
6. 准备钱包系统截图 + 日志
7. 破产隔离法律意见必须由德国律师出具
8. 托管供应商必须提供 SOC2 或同等证明

第 10 章｜市场滥用防范（Market Abuse Prevention）

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，本章为德国 MiCA-CASP 审批中的"核心高风险部分"之一，与 AML/CTF、ICT 一样会产生大量 BaFin 补件。

第 10 章总览：Market Abuse 是 MiCA 下最容易"踩雷"的高风险领域

德国 BaFin 在全欧盟范围内属于最严格执行"市场诚信"(Market Integrity）与"防市场滥用"监管的机构。
MiCA 对市场滥用有非常清晰的三大要求：

1. **禁止内幕交易（Insider Dealing）**
2. **禁止市场操纵（Market Manipulation）**
3. **禁止散布虚假或误导信息（Dissemination of False or Misleading Information）**

德国是欧盟最早将加密资产市场纳入 **类证券级 Market Abuse 监管框架** 的国家，因此监管逻辑严格程度比其他国家高数倍。
仁港永胜唐生在德国项目中的实际体会：

> "BaFin 对 Market Abuse 的理解比 MiCA 更严格，接近对证券交易平台的监管深度。"

因此本章是申请德国 CASP 必须提交的最核心合规模块之一。

第一节｜MiCA 下 Market Abuse 的法律框架（全量）

MiCA Title VI 明确要求 CASP 采取实质措施防止市场滥用行为，包括：

1. **禁止内部人利用非公开信息进行交易**
2. **禁止价格操纵**
3. **禁止制造虚假交易量**
4. **禁止传播误导性信息**
5. **必须具备市场监控系统（Market Surveillance System）**
6. **必须具备内部举报机制（Whistleblowing Mechanism）**
7. **必须保存市场监测证据**
8. **必须制定政策、流程、培训体系（Policies, SOPs, Recordkeeping）**

德国额外增加了：

- 风险评估（Market Abuse Risk Assessment）
- 内幕信息登记册（Insider List）
- 高风险地址监控（关联方监控）
- 市场操纵模式清单
- 自动化监控系统（AI/规则引擎）
- 价格异常警报体系（Flash Crash Protection）

第二节｜市场滥用三大风险类别（MiCA + MAR + BaFin 标准）

A. 内幕交易（Insider Trading / Insider Dealing）

包括：

- 管理层提前知悉重大消息
- 项目方内部人员提前知悉技术更新
- 合作伙伴提前知悉上币消息
- 内幕信息泄漏后产生交易行为

MiCA 要求必须：

- 定义“内部人”(Insider）范围
- 管理“内幕信息”(Inside Information)
- 保存“内幕信息接触记录”
- 维护“内幕人员清单”(Insider List)
- MLRO 必须监控相关交易行为

B. 市场操纵（Market Manipulation）

包括：

- Wash Trading（自成交）
- Pump & Dump
- Spoofing（虚假挂单）
- Layering（多层虚假挂单）
- Quote Stuffing（大量订单冲击系统）
- Price Cornering（控制价格）
- 虚假交易量制造 Fake Volume

MiCA 要求 CASP 必须能检测并阻止以上行为。

C. 误导性信息传播（Market Misconduct – Misleading Information）

包括：

- 故意散布虚假信息
- 社交媒体误导市场（Twitter/X、Telegram、Discord）
- 假冒官方公告
- 项目方夸大宣传

监管要求 CASP 必须能够识别此类信息并作风险警告。

第三节｜德国监管额外要求（BaFin 特有 6 大条款）

MiCA 是基线，德国加了更多：

1. 内幕人员（Insiders）必须实名登记

包括：

- 董事
- 股东
- 项目方核心人员
- 技术方关键人员
- 合规人员

2. 市场监控系统必须具备行为识别能力

例如：

- 异常交易量
- 异常订单簿
- 高频交易行为
- 交易与价格关联分析
- 多账户协同行为（Sybil Behavior）
- 社群活动关联度

3. 所有市场滥用信号必须提供可审计日志

包括：

- 系统警报
- 人工复核过程
- 最终处理结论
- MLRO 决策文件

4. 必须具备 Market Abuse Incident 报告机制

严重事件必须在 24 小时内报告 BaFin。

5. 必须具备"公共公告机制"

用于重大事件或风险公告。

6. 必须设立"举报保护机制"（Whistleblower Protection）

内部员工举报内幕违法行为时必须受到保护。

第四节｜市场滥用风险评估（Market Abuse Risk Assessment, MARA）

这是 BaFin 的硬性要求，是必须提交的文件之一。
必须对以下进行风险评估：

1. **用户结构**
2. **资产类型**
3. **链上交易模式**
4. **订单簿行为**
5. **价格波动模式**
6. **代币经济模型（Tokenomics）**
7. **合作方行为风险**
8. **内幕信息处理风险**

每项风险必须描述：

- 风险来源
- 风险评级（High/Med/Low）
- 控制措施
- 残余风险
- 风险负责人

仁港永胜可有偿提供完整模板。

第五节｜市场监控系统（Market Surveillance System）要求（核心）

德国 BaFin 明确要求 CASP 必须部署"市场监控系统"，类似证券交易所的 Market Surveillance。
必须具备：

1. 实时监控（Real-time）

包括：

- 订单簿
- 成交行为
- 深度变化
- 巨量挂单
- 瞬间撤单
- 链上交易与订单关联分析

2. 行为识别（Pattern Recognition）

必须能识别：

- Wash Trading
- Spoofing
- Pump & Dump
- Self-trading
- Insider pattern
- Arbitrage Exploits
- Miner Extractable Value (MEV)

3. 风险分级（Tiered Alerts）

每种行为都要设：

- 低级警报
- 中级警报
- 高级警报（需立即升级 MLRO）

同时必须保存：

- 监控日志
- 决策过程
- 复核记录

第六节｜内幕信息管理体系（Insider Information Management）

监管要求包括：

1. 内幕信息仓（Insider Information Vault）

用于储存：

- 商业计划
- 合作协议草稿
- 上币计划
- 技术升级计划
- 战略合作文件

必须记录访问日志。

---

2. 内幕人员清单（Insider List）

包括：

- 内幕人姓名
- 职位
- 联系方式
- 内部信息接触时间
- 受限期间（Closed Period）

---

3. 内幕交易限制（Restricted Trading）

内部员工不得在特定期间进行自家代币交易。

第七节｜社交媒体与外部传播监控体系（Social Media Market Conduct Control）

MiCA 强调"避免误导性信息传播"。
CASP 必须监控：

- Twitter
- Telegram
- Discord
- Reddit
- Medium
- YouTube

监控重点：

- 项目虚假宣传
- 利好消息提前泄漏
- 价格操纵型 KOL
- 定向误导用户行为

并必须记录"市场滥用风险事件"。

第八节｜Market Abuse 调查流程（Investigation Procedure）

以下流程必须形成政策（Policy + SOP）：

1. 系统产生警报
2. 市场团队初步复核
3. MLRO 升级调查
4. 要求客户解释
5. 暂停交易/冻结账户（如必要）
6. 记录完整调查过程
7. 向监管报告（如触发）
8. 事件根因分析（RCA）

第九节｜市场操纵模式（BaFin 强制识别清单）

包括：

- Fake Volume
- Flash Pump
- Momentum Ignition
- Marking the Close
- Stop-loss Hunting
- Insider Front-running
- Wash Trade
- Layering
- Spoofing
- Whale Order Manipulation
- Arbitrage Exploits

每项模式必须有：

- 监测逻辑
- 触发条件
- 预警机制

第十节｜Market Abuse 补件问答（RFI Q1–Q40 全套）

以下问答来自真实 BaFin 补件，由仁港永胜唐生整理：

第一部分：市场监控（Q1–Q10）

Q1：你们如何识别 Wash Trading?
Q2：是否能识别自成交?
Q3：如何监测 Pump & Dump 行为?
Q4：是否实时监控订单簿?
Q5：系统如何识别 Spoofing?
Q6：如何监测巨大订单变化?
Q7：如何监测社交媒体造势?
Q8：如何处理异常波动?
Q9：如何进行大额订单审核?
Q10：如何保留市场监控证据?

第二部分：内幕交易（Q11–Q20）

Q11：谁是你们的内幕人员?
Q12：如何维护 Insider List?
Q13：如何识别 Insider Pattern?
Q14：内幕信息如何保存?
Q15：如何防止泄露?

Q16：内幕人员如何受限?
Q17：是否定义 Closed Period?
Q18：内幕交易如何调查?
Q19：如何处理内部人员可疑交易?
Q20：如何配合当局调查?

第三部分：市场操纵（Q21–Q30）

Q21：如何识别价格操纵行为?
Q22：是否支持跨交易所监控?
Q23：如何识别虚假流动性?
Q24：如何处理机器人操纵行为?
Q25：如何识别异常订单簿波动?
Q26：如何监测鲸鱼账户?
Q27：如何识别套利攻击?
Q28：如何监测 MEV?
Q29：如何识别大宗单操纵?
Q30：如何监控清算风险引发的操纵?

第四部分：误导性信息（Q31–Q40）

Q31：如何识别社交媒体误导内容?
Q32：如何记录市场误导事件?
Q33：项目方发布误导性声明如何应对?
Q34：如何防止员工泄漏未公开信息?
Q35：如何监测非官方渠道消息?
Q36：是否检查合作方媒体稿件?
Q37：如何监控 KOL 推文?
Q38：是否监测第三方研究报告?
Q39：如何发现假冒"官方公告"?
Q40：如何验证价格波动是否与外部新闻有关?

第十一节｜仁港永胜唐生 Market Abuse 实操建议

1. **务必购买专业 Market Surveillance 系统**
   （如 Solidus、Chainalysis Market Intel、Surveillance-as-a-Service）
2. **建立 24/7 交易监测团队**
3. **准备 30+ 个高频监控场景**
   （BaFin 会要求演示）
4. **准备三套关键文档：**

- Market Abuse Policy
- Market Surveillance SOP
- Insider List Template

5. **必须能在面谈中解释"每一种市场操纵模式"**
   BaFin 会逐条问。
6. **向 BaFin 提交月度 Market Integrity 报告（推荐）**

第 11 章｜运营风险管理（Operational Risk Management Framework）

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，这一章节是 **德国 BaFin 审批 MiCA-CASP 的三大核心模块之一（ICT / AML / OPR）**，德国对运营风险的要求远高于其他欧盟国家。

第 11 章总览：为什么 BaFin 把运营风险视为"监管生命线"?

运营风险（Operational Risk）是德国 BaFin 审批 MiCA-CASP 时重点关注的项目，因为加密资产服务商本质上是：

> “技术驱动的金融机构 + 高波动性资产 + 高监管敏感度行业”

因此，运营风险对于 CASP 的稳定性与投资者保护至关重要。
德国监管逻辑认为：

> “没有完善的运营风险框架，就不可能成为一家合格的 CASP。”

本章将全面讲解 CASP 在德国必须具备的运营风险框架。

第一节｜运营风险管理（OpRisk Framework）总体架构

根据 BaFin、MiCA、EBA 监管要求，CASP 需具备以下 **运营风险框架（OpRisk Framework）**：

1. **风险治理（OpRisk Governance）**
2. **重大运营风险识别（Risk Identification）**
3. **关键风险指标（KRIs）体系**
4. **风险评估矩阵（Risk & Control Self-Assessment, RCSA）**
5. **内部控制体系（Internal Controls）**
6. **事件报告机制（Incident Reporting – Non-ICT）**
7. **外包风险管理（Third-Party Risk）**
8. **人员风险管理（People Risk）**
9. **流程风险管理（Process Risk）**
10. **业务持续性（Business Continuity Planning, BCP）**
11. **独立审计（Internal Audit）**
12. **年度 OpRisk 报告**

这整套体系必须形成“监管可读”合规包。

第二节｜运营风险治理结构（OpRisk Governance）

监管要求明确：

1. 董事会（Board）

- 对运营风险承担最终责任
- 每季度审查 OpRisk 报告

2. 高级管理层（Senior Management）

- 实施运营风险策略
- 确保资源充足

3. 运营风险负责人（Operational Risk Officer）

必须具备：

- 金融或加密行业经验
- 风险管理经验
- 熟悉德国 BaFin 要求

4. 三道防线模型（Three Lines of Defense）

第一线（部门业务线）

负责识别与报告运营风险

第二线（风险管理 & 合规）

负责制定政策、独立监督

第三线（内部审计 Audit）

负责审查运营风险框架有效性

第三节｜运营风险识别（Risk Identification）

必须至少识别 10 大类运营风险：

1. **技术风险（ICT Risk）**
2. **人员风险（HR Risk）**
3. **内部欺诈（Internal Fraud）**
4. **外部欺诈（External Fraud）**
5. **流程风险（Process Risk）**
6. **客户欺诈（Customer Fraud）**
7. **法律风险（Legal Risk）**
8. **合规风险（Compliance Risk）**
9. **运营中断风险（Business Disruption Risk）**
10. **外包风险（Outsourcing Risk）**

监管要求必须：

- 列出每项风险来源
- 说明风险发生概率
- 说明风险影响程度
- 列出控制措施

第四节｜关键风险指标（Key Risk Indicators, KRIs）

这是德国 BaFin 最重视的部分之一。
CASP 必须建立完整 KRIs，包括：

1. 技术 KRIs

- 系统可用性（Uptime %）
- 钱包同步失败次数
- DDoS 自我防护事件数
- 节点宕机次数
- API 错误率

2. 运营 KRIs

- 客户投诉数量
- 出入金失败率
- 对账差异率
- 客户服务延迟时间

3. 安全 KRIs

- 入侵尝试次数
- 高危漏洞数量
- 员工权限滥用事件数

KRIs 必须绑定：

- 预警阈值
- 升级机制
- 响应流程

第五节｜RCSA（Risk & Control Self-Assessment）风险与控制自评体系

RCSA 是监管会要求重点查看的文件。
内容必须包括：

- 风险清单
- 控制措施
- 控制有效性评分
- 残余风险
- 改进计划
- 年度审查流程

RCSA 必须每年执行一次。

第六节｜关键业务流程（Core Processes）风险管理

CASP 必须识别各业务流程风险，包括：

1. 客户开户流程

- 身份验证失败
- 资料伪造
- 欺诈
- 系统异常

2. 充值/提现流程

- 充值入账错误
- 提现异常
- 地址填写错误
- 欺诈攻击

3. 交易撮合

- 错误撮合
- 市场操纵风险
- 订单处理失败

4. 冷/热钱包操作

- 私钥管理风险
- 多签流程失败
- 人为操作错误

5. 对账流程

- 账链不一致
- 数据异常
- 对账延迟

必须为每项流程编写：

- 风险描述

- 风险等级
- 控制措施
- 应急措施

第七节｜人员风险管理（People Risk）

包括：

1. 授权与权限管理（Access Management）

需实现：

- 最小权限原则
- 职责分离
- 权限审查（至少季度一次）

2. 员工背景调查（Background Check）

必须对：

- MLRO
- CTO
- 钱包管理员
- 财务人员

做 KYE（Know-Your-Employee）。

3. 培训（Training）

至少包括：

- AML/CTF 培训
- Market Abuse 培训
- ICT 安全培训
- 数据保护（GDPR）培训

第八节｜外包风险管理（Third-Party Risk Management）

MiCA + DORA 强制要求：

- Vendor Risk Assessment
- Data Processing Agreement
- SLA
- Sub-outsourcing 管理机制
- 退出计划（Exit Strategy）

对以下外包特别敏感：

- 云服务（AWS/Azure/GCP）
- Chainalysis / TRM
- 钱包托管（Fireblocks / BitGo）
- KYC 提供商（Sumsub、Onfido）

德国监管会在补件中要求：

> “证明你们能够完全审计供应商（Audit Rights）”。
> 若无法证明 → 补件甚至失败。

第九节｜事件管理（Incident Management）

运营事故与 ICT 事故不同，监管要求分开记录。
运营事故包括：

- 提现延迟
- 数据库错误
- 手工操作错误
- 多签流程卡滞
- 交易异常
- 客户投诉
- 操作失误

必须：

- 分级
- 报告
- 复盘
- 改进
- 保存记录（5 年以上）

第十节｜业务连续性（BCP）与灾难恢复（DRP）

BCP 必须覆盖：

- 关键岗位清单
- 备员计划
- 异地办公预案
- 关键供应商备份
- 业务恢复优先级
- 应急沟通机制

所有流程必须配套：

- BCP 演练报告
- DRP 测试结果
- 截图证据

BaFin 会要求查看证据。

第十一节｜运营风险内部审计（Internal Audit – OpRisk Scope）

内部审计必须包含：

- 风险控制评估
- 流程有效性检查
- 日志审计
- 多签审计
- 外包审计
- KRI 审查

审计报告必须至少每年一次提交董事会。

第十二节｜运营风险补件（RFI）Q1–Q35（全量）

仁港永胜唐生整理德国真实案例：

第一部分：治理与人员（Q1–Q10）

Q1：谁负责运营风险管理?
Q2：是否有 OpRisk 委员会?
Q3：职责分离如何实现?
Q4：权限如何管理?
Q5：员工背景如何调查?
Q6：员工如何接受培训?
Q7：如何处理员工违规?
Q8：内部人滥用权限如何防范?
Q9：是否已建立三道防线?
Q10：风险管理向谁汇报?

第二部分：流程与控制（Q11–Q20）

Q11：如何识别关键流程?
Q12：如何识别操作错误?
Q13：如何记录手工操作?
Q14：如何处理多签流程失败?
Q15：如何防止账链不一致?
Q16：如何控制提现审批?
Q17：如何管理订单撮合错误?
Q18：如何识别超额交易?
Q19：如何处理供应商导致的失败?
Q20：如何识别欺诈风险?

第三部分：外包与供应商（Q21–Q30）

Q21：你们如何评估第三方风险?
Q22：是否完成 Vendor Risk Assessment?
Q23：外包合同是否包含审计权?
Q24：如何审查供应商安全能力?
Q25：若云服务中断如何恢复?
Q26：是否拥有 Exit Strategy?
Q27：如何确保供应商不违规?
Q28：是否管理子外包?
Q29：如何监测供应商绩效?
Q30：是否提供供应商年度审计报告?

第四部分：运营事故与 BCP（Q31–Q35）

Q31：如何定义运营事故?
Q32：事故如何记录?
Q33：是否有应急预案?
Q34：BCP 如何测试?
Q35：如何确保关键岗位恢复?

第十三节｜仁港永胜唐生实操建议（OpRisk）

1. 建立 50+ 风险控制点（KCOs）
2. 准备 20+ KRIs
3. 准备完整 RCSA 套件（含风险地图）
4. 制作 3 套关键流程图（提现、对账、多签）
5. 准备 1 套运营事故案例库（10+）
6. 提供至少 1 次 BCP 演练"截图证据"
7. 提供完整 Outsourcing Register
8. 供应商需提交 SOC2 / ISO27001 证书

第 12 章｜合规框架（Compliance Framework）

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，本章为 MiCA-CASP 在德国获批的必要条件之一，与 **AML（第 7 章）、ICT（第 8 章）、运营风险（第 11 章）** 一起被 BaFin 定义为"核心监管支柱（Pillars of Supervision）"。

第 12 章总览：为什么德国要求 CASP 必须建立"银行级合规体系"？

德国 BaFin 将 MiCA-CASP 视为：

> "受到与银行、证券商接近水平监管的金融机构"。

因此，即便 MiCA 并未强制要求 CASP 完全采用银行式合规体系，
BaFin 仍然要求 CASP 落实一套完整的 Compliance Framework（合规体系），包括：

- 合规职能（Compliance Function）
- 合规政策（Compliance Policies）
- 合规监测（Compliance Monitoring Program）
- 合规报告（Compliance Reporting）
- 年度合规评估（Annual Compliance Review）
- 合规培训（Compliance Training）
- 合规风险识别（Compliance Risk Assessment）
- 法规监测（Regulatory Watch）

这套体系必须达到"可监管审核（Supervisory Review Ready）"标准。

第一节｜合规职能（Compliance Function）结构

MiCA 明确要求 CASP 设立独立合规职能。BaFin 则进一步要求：

1. 合规负责人（Compliance Officer, CO）必须满足：

- Fit & Proper（适当人选）
- 合规从业经验
- 熟悉欧盟 MiCA / AML / MAR
- 具备金融机构背景优先
- 与 MLRO 角色分离（不得兼任 AML 负责人）

注：

> 若团队规模过小，可 MLRO 与 CO 双角色，但 BaFin 强烈不建议，通常会补件要求提供理由。

2. 合规部门必须独立运作

- 不隶属于商业部门
- 不隶属于产品研发
- 不隶属于市场推广
  而应直接向 CEO 或董事会汇报。

3. 合规团队必须具备最低配置

- 合规负责人（CO）
- 合规分析员（Compliance Analyst）
- 法规监测人员（Regulatory Watch）

仁港永胜唐生建议：

> 德国项目普遍采用 2–4 人合规团队，以便通过 BaFin 的"资源充足性审查"。

第二节｜合规政策体系（Compliance Policies）完整清单

BaFin 要求 CASP 必须具备至少 20 套核心政策文件，覆盖：

A. MiCA 要求类政策

1. CASP Governance Manual
2. Conflict of Interest Policy
3. Complaints Handling Policy
4. Market Abuse Prevention Policy
5. Client Asset Safeguarding Policy
6. ICT Governance Policy
7. Outsourcing Policy（含 DORA 要求）
8. Operational Risk Policy

B. 法规类政策

9. Compliance Charter（合规宪章）
10. Compliance Monitoring Plan
11. Compliance Reporting SOP
12. Regulatory Watch Procedure（法规更新监测）

C. 客户保护类政策

13. Investor Protection Policy
14. Transparency & Disclosure Policy
15. Product Governance（产品适当性）

D. 员工规范类政策

16. Personal Account Dealing Policy（员工具有资产时需申报）
17. Code of Conduct（行为准则）
18. Anti-Bribery & Corruption（反贿赂）

E. 数据保护类政策

19. GDPR Data Protection Policy
20. Data Breach Handling Procedure

这些文件必须全部提交给 BaFin。

仁港永胜可提供完整德式监管格式（可用于面谈）。

第三节｜合规风险评估（Compliance Risk Assessment, CRA）

每一家 CASP 在申请时必须提交 CRA，内容包括：

1. 识别主要合规风险

例如：

- MiCA 合规风险
- 资讯披露风险
- 市场操纵风险
- 客户保护风险
- 产品风险
- 洗钱风险（与 AML 分开处理）
- ICT 合规风险
- 外包风险（第三方提供商）

- 员工行为风险

2. 风险评分（RAG：红黄绿）

- Impact（影响程度）
- Likelihood（发生可能性）

3. 风险控制点（KCOs）

每项风险必须至少列 2–3 个控制措施。

4. 残余风险

5. 改进计划

CRA 必须每年更新一次并提交董事会审批。

第四节｜合规监测计划（Compliance Monitoring Program, CMP）

CMP 是 BaFin 要求最严格的文件之一，也是补件（RFI）高发区。
CMP 必须包含：

A. 年度监测周期（Yearly Cycle）

- 每月：KPI/KRI 监测
- 每季：政策复审
- 每半年：合规测试
- 每年：全量合规检查

B. 合规测试范围

包括：

1. KYC 质量测试
2. 交易监控有效性
3. 市场滥用监测
4. 投诉处理
5. 披露义务检查
6. 员工行为监控
7. 外包风险审查
8. 隐私与数据保护检查

C. 抽样逻辑（Sampling Method）

必须清楚写明如何抽样。

D. 合规报告机制

必须说明：

- 异常如何升级
- 向谁报告
- 报告格式
- 审计证据如何保存

第五节｜法规监测（Regulatory Watch）机制

MiCA 是动态法规，ESMA 与 EBA 不断推出新要求。
BaFin 也会发布 Germany-specific updates。

因此 CASP 必须具备：

1. 法规监测清单（Regulatory Watch List）

监测范围包括：

- MiCA
- ESMA MAR（市场滥用）
- EBA AML 指引
- BaFin Rundschreiben（监管通函）
- 德国 KwG（银行法）
- GDPR
- DORA
- 国家层级 AML 法（GwG）

2. 法规更新评估（Impact Assessment）

例如：

- 新规是否影响客户资产隔离？
- 新规是否影响 AML？
- 新规是否影响 ICT？

3. 实施时间表（Implementation Plan）

BaFin 会重点查此项。

第六节｜合规培训体系（Compliance Training Program）

合规培训必须做到：

A. 年度培训计划（Annual Plan）

必须包含：

- MiCA 合规
- AML/CTF
- Market Abuse
- ICT 安全
- 数据保护（GDPR）
- 外包风险
- 客户保护（Investor Protection）

B. 培训对象

- 管理层
- 员工
- 关键岗位（高频监控、钱包管理员）
- 合规/风险部门

C. 培训证据

必须保留：

- PPT
- 员工出勤记录
- 考试成绩
- 考核题库

监管将会要求提供这些证明。

第七节｜合规事件管理（Compliance Incidents）

合规事件包括：

- 政策违规
- 披露义务未履行
- 员工未遵守行为准则
- 第三方供应商违规
- 客户适当性错误
- 产品风险未披露

必须建立：

- 事件分级
- 通知流程
- 调查机制
- 根因分析（RCA）
- 改进计划
- 记录文件（至少保存 5 年）

第八节｜投诉处理（Complaints Handling）

MiCA 明确要求 CASP 建立投诉机制。
德国 BaFin 的要求更严格（参考《消费者保护法》）。
必须包含：

- 投诉受理渠道
- 处理时限（10–15 个工作日）
- 处理流程图
- 投诉分类
- 投诉报告（每月）
- 投诉分析报告（每季度）
- 投诉统计（每年）

并且必须保证：

> 客户投诉独立于商业部门处理。

第九节｜利益冲突管理（Conflict of Interest, CoI）

必须识别并管理：

1. 股东带来的利益冲突
2. 管理层持有代币产生的利益冲突
3. 产品团队对价格敏感信息的接触
4. 关联公司间的交易
5. 员工个人账户交易（PA Trading）

所有冲突必须记录：

- 冲突来源
- 冲突等级
- 缓解措施
- 监控机制

第十节｜合规年度报告（Annual Compliance Report, ACR）

BaFin 明确要求每年提供：

- 合规状况总结
- 违规事件
- 控制措施有效性评估
- 政策更新情况
- 风险状况变化
- 下一年度计划
- 董事会审阅记录

这是 CASP 持续监管的核心。

第十一节｜合规补件（RFI Q1–Q40 全量模拟问答）

以下内容来自德国真实案例，由仁港永胜唐生整理：

第一部分：合规架构（Q1–Q10）

Q1：合规负责人具备什么资质?
Q2：合规团队规模如何确定?
Q3：如何确保合规独立性?
Q4：合规部门向谁汇报?
Q5：如何定义合规职责?
Q6：如何管理利益冲突?
Q7：如何管理 PA Trading?
Q8：如何管理员工行为准则?
Q9：如何监督关键流程?
Q10：如何与风险管理部门协作?

第二部分：合规监测（Q11–Q20）

Q11：CMP 如何执行?
Q12：抽样逻辑是什么?
Q13：谁负责合规测试?
Q14：测试证据如何保存?
Q15：如何监测 Market Abuse?
Q16：如何监测产品风险?
Q17：如何处理政策例外?
Q18：如何发现未披露风险?
Q19：如何纠正政策违规?
Q20：如何记录监测日志?

第三部分：法规监测（Q21–Q30）

Q21：法规变动如何监测?
Q22：如何评估影响?
Q23：如何落实新法规?
Q24：如何记录法规评估?
Q25：如何评估 MiCA 更新风险?
Q26：如何跟踪 ESMA 咨询文件?
Q27：如何管理 BaFin 通函?
Q28：对 DORA 的更新如何处理?
Q29：如何向董事会汇报法规风险?
Q30：如何确保持续合规?

第四部分：投诉、利益冲突（Q31–Q40）

Q31：投诉流程如何定义？
Q32：投诉结案标准是什么？
Q33：如何记录投诉？
Q34：如何统计投诉？
Q35：如何评估投诉趋势？
Q36：如何识别利益冲突？
Q37：如何处理冲突事件？
Q38：如何禁止员工内幕交易？
Q39：如何管理团队内部信息壁垒？
Q40：如何评估合规有效性？

第十二节｜仁港永胜唐生实操建议

1. 建立 30+ 合规控制点（KCOs）
2. 建立完整 CMP（包含 1 年周期 + 样本）
3. 准备 25 套合规政策（德式结构）
4. 构建完整 Regulatory Watch 流程与日志模板
5. 提供 2–3 次年度培训记录
6. 准备投诉案例（至少 5 个）
7. 提供利益冲突登记册（CoI Register）
8. 必须能在面谈中解释 CMP 执行方法

第 13 章｜金融犯罪风险管理（Financial Crime Framework）

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，本章是德国 BaFin 在 MiCA-CASP 审查中最严格的部分之一，与 **AML（第 7 章）** 并列为监管"高风险审查点"。

第 13 章概述｜为什么德国 BaFin 把"金融犯罪管理"视为 MiCA-CASP 的准入底线？

德国监管机构 BaFin 的态度是明确的：

> "所有 CASP 必须达到与银行相近的 AML/CTF（反洗钱/反恐融资）与金融犯罪风控标准，否则不会获批。"

原因包括：

- 德国是欧盟最严格 AML 法律国家之一（GwG + AMLD6 强制实施）
- 加密资产被视为高风险行业
- 存在恐怖融资风险（特别是 P2P 交易、链上转账）
- 客户资产托管产生资金流向透明度问题
- 链上活动高度匿名
- 外包（特别是钱包、交易系统）风险巨大

因此，BaFin 要求 CASP 建立 **完整金融犯罪风险管理体系**，涵盖：

- AML
- CTF
- Fraud（欺诈）
- Market Abuse（市场滥用）
- Sanctions（制裁）
- Transaction Monitoring（交易监测）
- Chain-analysis（链上分析）
- Wallet Risk Rating（钱包风险等级）
- Screening（制裁 + PEP + Adverse Media）

本章比分章节更加严格与专业，务必在申请时准备完整材料。

第一节｜金融犯罪管理框架（FCF）整体架构

FCF 必须覆盖 7 个核心模块：

1. **AML/CTF（反洗钱/反恐融资）**
2. **制裁（Sanctions Screening）**
3. **欺诈管理（Fraud Prevention）**
4. **市场滥用（Market Abuse）**
5. **交易监测（Transaction Monitoring）**
6. **链上分析（Chain-Analysis）**
7. **钱包地址风险评估（Wallet Risk Rating）**

并必须满足三项 BaFin 的底层要求：

（1）风险为本（Risk-Based Approach, RBA）

每项工作必须基于风险等级来执行。

（2）可被审计（Audit-Ready）

包括日志、证据、流程、抽样。

（3）可监管审核（Regulator-Ready）

文件必须满足监管可阅读格式（Germany-standard）。
仁港永胜提供的模板全部已按"德国格式"优化。

第二节｜AML / CTF（反洗钱与反恐融资）体系

此部分与第 7 章有关，但本章是更深层次的"实操级 FC 框架"。

1. KYC / CDD / EDD（客户尽职调查）

BaFin 要求 3 层结构：

A. 基础 KYC（Basic CDD）

适用于低风险客户。
包括：

- 身份文件验证
- 地址证明
- 活体识别
- Sanctions Screening
- PEP Screening

B. 加强尽调（EDD）

适用于：

- 高净值客户
- 使用隐私币
- 来自高风险国家
- 大额交易
- 企业客户（特别是链上业务）

EDD 包含：

- 资金来源证明（SOF）
- 财富来源（SOW）
- 链上历史追踪
- 企业结构图（UBO 穿透）
- 董事背景调查（Fit & Proper）

C. 企业客户（KYB）

需提供：

- 注册证明
- 公司章程
- 董事名单
- 股东穿透至自然人
- UBO 验证
- 商业模型解释
- 资金来源解释

2. 客户风险等级（CRR）

BaFin 要求至少三种等级：

- 低风险
- 中风险
- 高风险

风险等级必须基于：

- 国籍
- 交易模式
- 产品使用
- 链上历史
- 资金来源
- 行为模式
- 历史异常

系统必须自动生成风险评级并定期复审（每年一次）。

第三节｜制裁 Screening（Sanctions）

制裁系统必须涵盖：

- UN Sanctions（联合国）
- EU Sanctions（欧盟）
- OFAC SDN
- UK HMT Sanctions
- 德国本地制裁清单

Screening 必须涵盖：

1. 客户姓名
2. 公司名称
3. UBO
4. 钱包地址（Address Screening）
5. 交易对象（Counterparty）

任何命中（Hit）必须执行：

- L1 初筛
- L2 人工复核
- L3 合规负责人确认
- 记录保存五年

第四节｜欺诈管理（Fraud Management）

CASP 容易面对的欺诈包括：

- 被盗账户
- SIM 卡劫持
- 社交工程诈骗
- 网络钓鱼
- 钱包私钥被盗
- 交易所转移诈骗
- 假冒技术支持团队
- Robot/Bot 式攻击
- 流动性欺诈（Swap 滑点攻击）

BaFin 要求建立：

- 检测机制（Monitoring）
- 自动警报
- 手动复核流程
- 欺诈黑名单（Fraud Blacklist）
- 与执法机构合作（Police Reporting）

第五节｜市场滥用（Market Abuse）防控

依据 **MAR（Market Abuse Regulation）**，MiCA 要求 CASP：

- 禁止内幕交易（Insider Trading）
- 禁止市场操纵（Price Manipulation）
- 禁止虚假交易（Wash Trading）
- 禁止诱骗性行为（Spoofing）
- 禁止 Pump & Dump

BaFin 常见提问包括：

Q：如何识别 Wash Trading?
Q：如何监控团队内部是否访问重要消息?
Q：如何隔离市场敏感信息？（Insider List）

仁港永胜建议：

- 建立"市场监控系统"
- 建立"内部信息壁垒（Chinese Wall）"
- 每日生成交易异常报告

第六节｜交易监测（Transaction Monitoring）

BaFin 将此视为"硬性审批条件"。

系统必须覆盖：

1. 规则（Rules-based）

例如：

- 大额交易
- 高频交易
- 夜间频繁交易
- 多次失败尝试
- 与高风险地址往来
- Layering（分层洗钱）
- Structuring（拆分交易）

2. 行为监控（Behaviour-based）

例如：

- 行为突然改变
- 异常链上模式
- 买卖频率不符经济合理性
- 产品使用异常
- IP 地理位置跳变

3. 链上监测（On-chain Monitoring）

必须包括：

- 钱包地址风险评分
- 历史交易分析
- 可疑资金流关联图
- Tornado Cash 等混币器识别
- 隐私币识别

4. 自动警报（Alerts）

必须具备：

- Alerts Dashboard
- L1 复审
- L2 复审
- 升级机制（Escalation）
- SAR/STR 自动记录

第七节｜链上分析（Chain-Analysis）

德国 BaFin 强制要求：

> 只要涉及加密资产转账，就必须进行链上分析。

必须采用以下工具中的至少一个：

- Chainalysis
- TRM Labs
- Elliptic
- AML Bot
- Scorechain

链上分析必须包含：

1. 钱包风险等级
2. 资金来源路径
3. 资金去向路径
4. 与犯罪活动的关联程度
5. 是否与黑市钱包相关

6. 是否与暗网混币器相关
7. 是否与恐怖组织地址相关

报告必须保存至少 5 年。

第八节｜钱包地址风险评分（Wallet Risk Rating）

钱包必须分为：

- 低风险
- 中风险
- 高风险
- 禁用（Prohibited）

高风险包括：

- 混币器
- 即将制裁地址
- OFAC 命中
- Hack 地址
- 新创建且无历史
- 高风险国家
- Jumping patterns

监管通常会问：

Q：钱包如何被分类？
Q：评分的依据是？
Q：如何监控新的高风险钱包？
仁港永胜提供完整模板。

第九节｜STR / SAR（可疑交易报告）

德国在 AML 方面极其严格，STR 提交必须依据《GwG》和 FIU 要求。
流程包括：

1. L1 初级复审
2. L2 高级复审
3. MLRO 确认
4. 评估依据（Chain-analysis + 行为监控）
5. 提交给 FIU（德国金融情报部门）
6. 与执法机关互动
7. 记录保存 5 年

监管常问：

- STR 提交比例？
- 评估标准？
- 是否会冻结资产？

第十节｜金融犯罪补件（RFI Q1–Q50 全量示例）

以下内容经仁港永胜唐生基于真实案例总结：

第一部分（Q1–Q10）：KYC/EDD

Q1：EDD 的触发条件是什么？
Q2：如何评估资金来源？
Q3：如何识别高风险国籍？
Q4：如何评估企业结构？
Q5：如何确认 UBO？
Q6：如何识别链上匿名风险？
Q7：如何判断是否需要文件补充？
Q8：如何处理客户拒绝提供资料？
Q9：如何复核第三方文件？
Q10：如何记录 KYC 证据？

第二部分（Q11–Q20）：交易监控

Q11：交易监测逻辑是什么？
Q12：每日监控频率？
Q13：如何执行链上警报？
Q14：如何判断 Layering？
Q15：如何识别结构化交易？
Q16：如何识别恐怖融资？
Q17：如何处理高风险链上流向？
Q18：如何判断风险是否解除？
Q19：如何记录警报？
Q20：如何关闭警报？

第三部分（Q21–Q30）：制裁 Screening

Q21：Screening 工具是什么？
Q22：如何识别假阳性（False Positive）？
Q23：命中 OFAC 如何处理？
Q24：如何判断钱包是否命制裁？
Q25：如何处理姓名相似？
Q26：如何记录复审？
Q27：如何保持名单更新？
Q28：如何评估制裁风险？
Q29：如何与法律团队协作？
Q30：如何向 BaFin 报告？

第四部分（Q31–Q40）：欺诈与市场滥用

Q31：如何识别被诈骗受害客户？
Q32：如何判断是否需冻结账户？
Q33：如何识别 Pump & Dump？
Q34：如何识别 Wash Trading？
Q35：如何监控内幕交易？
Q36：如何执行 Chinese Wall？
Q37：如何与执法机关对接？
Q38：如何处理员工违规？
Q39：如何评估市场滥用风险？
Q40：如何保留证据？

第五部分（Q41–Q50）：整体控制框架

Q41：如何定义整体金融犯罪框架？
Q42：如何向董事会报告？
Q43：控制点是否足够？
Q44：如何评估系统有效性？
Q45：如何处理系统事故？
Q46：如何跨部门协作？

Q47：如何评估风险变化?
Q48：如何更新政策?
Q49：如何培训员工?
Q50：如何确保可监管审核?

第十一节｜仁港永胜唐生实操建议（独家补充）

1. **务必引入 TRM Labs / Chainalysis**（德国监管极度重视链上分析）
2. **设置至少 20 条链上监控规则**
3. **准备 1 套完整 STR 提交样例**
4. **创建 Wallet Risk Register（钱包风险登记册）**
5. **在面谈前准备 30 个警报案例**
6. **建立 End-to-End 金融犯罪流程图**
7. **实现 AML/KYC 全系统化（不可纯手工）**
8. **创建常见欺诈场景测试集（Fraud Scenarios）**
9. **配备一名 AML 高级专员与 MLRO 并行**
10. **至少准备 40 个 RFI 预案答案**

仁港永胜可提供全套模板 + 面谈辅导 + 系统搭建咨询。

第 14 章｜信息通讯技术与网络安全（ICT & Cybersecurity, DORA Fully-Compliant）

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，本章是德国 BaFin 审查 MiCA-CASP 时最严格的 TOP3 模块之一（另两项为：AML 与 客户资产隔离）。

此章节将依据：

- 欧盟《DORA – Digital Operational Resilience Act》
- MiCA 第 63–68 条 ICT 要求
- BaFin《BAIT（银行 IT 要求）》
- BaFin《KAMaRisk》IT 控制
- EBA ICT 风险管理框架

第 14 章概述｜为什么 ICT 是德国 CASP 审批最苛刻的环节?

德国 BaFin 是欧盟监管中对"技术合规"要求最严格的国家，原因包括：

- 德国是欧盟境内 IT 审查制度最成熟的国家
- BaFin 已经对银行、证券机构执行多年 **BAIT（Bankaufsichtliche Anforderungen an die IT）**
- CASP 属于"高风险行业"，必须达到 **类银行级别** IT 控制标准
- 欧盟 DORA（2025 年生效）强制要求所有金融机构（包括 CASP）建立完整 ICT 风控体系

BaFin 在 CASP 审查中会重点审查：

- 技术架构
- 网络安全
- 数据治理
- 持续运营（Business Continuity）
- 灾难恢复（DRP）
- 外包 IT 风险（Outsourcing – ICT）
- 供应链风险
- 安全开发（SDLC）
- 加密资产技术安全

- 钱包安全（私钥管理）

本章将完整呈现德国 CASP 获批所需的 **ICT & Cybersecurity（深度实操版）**。

第一节｜ICT & Cybersecurity 架构要求（BaFin + MiCA + DORA 全覆盖）

BaFin 要求的 ICT 架构必须包含 7 个核心模块：

1. ICT Framework（ICT 管理框架）
2. IT Risk Management（IT 风险管理）
3. Information Security（信息安全）
4. Cybersecurity（网络安全）
5. IT Operations（IT 运维）
6. Incident Management（事故管理）
7. Business Continuity & Disaster Recovery（业务连续性 + 灾难恢复）

所有模块必须遵循：

- **"系统可审计"**（audit-ready）
- **"控制点可验证"**
- **"文档可监管读取"**（regulator-readable）

仁港永胜的模板全部按德国 BaFin 格式整理。

第二节｜ICT 管理框架（ICT Governance Framework）

一个完全合规的 ICT Framework 必须包含：

（1）ICT 政策体系（ICT Policy Suite）

包括：

- ICT Framework Policy
- Information Security Policy
- Cybersecurity Policy
- Cryptographic Key Management Policy
- IT Operations Manual
- System Access Policy
- Password & MFA Policy
- Change Management Policy
- Incident Reporting Policy
- Logging & Monitoring Policy
- Outsourcing ICT Policy
- Data Governance Policy

BaFin 会要求查看：

- 文档版本
- 发布记录
- 董事会批准记录

（2）ICT 组织架构（ICT Org Structure）

必须包含：

- CIO / CTO（技术负责人）
- Security Officer（安全负责人）
- DPO（数据保护官）
- DevOps
- IT Operations

- Cybersecurity Analyst
- Vendor Manager（外包管理）

BaFin 必问：

Q：CTO 是否全职？是否有加密行业经验？
Q：Security Officer 是否独立？

仁港永胜会协助准备简历 + Fit & Proper 文件。

（3）角色与职责矩阵（RACI）

包括：

- 谁负责
- 谁执行
- 谁监督
- 谁批准

RACI 是德国监管的"必检项"。

第三节｜IT 风险管理（IT Risk Management, DORA-Compliant）

德国 BaFin 会要求 CASP 建立"类银行级" IT 风险管理框架，包括：

（1）IT 风险识别（Risk Identification）

例如：

- 网络攻击
- 密钥泄露
- 系统中断
- API 故障
- 钱包被黑
- DDoS
- 外包服务中断
- 服务器崩溃
- 数据丢失
- 员工权限滥用

（2）IT 风险评估（Risk Assessment）

基于：

- Likelihood（发生概率）
- Impact（影响程度）

生成风险矩阵（Risk Matrix）。

（3）IT 风险控制（Risk Mitigation）

包括：

- MFA
- 访问控制
- 加密
- 防火墙
- IDS/IPS
- WAF
- 日志管理
- 职权分离（SoD）

- 隐私保护

（4）IT 风险报告

必须定期提交给：

- 董事会
- 合规官
- 风险管理委员会

第四节｜信息安全（Information Security）

德国 IT 审查遵循 **ISO 27001** 与 **BAIT** 要求。
核心包括：

（1）访问控制（Access Control）

- RBAC（基于角色的访问）
- MFA
- Least Privilege（最小权限）
- 职责分离（SoD）

（2）加密（Encryption）

- AES256 / RSA2048
- 私钥冷存储（hardware security module）
- 数据传输加密（TLS 1.2+）

（3）数据保护（Data Protection）

符合 GDPR：

- 数据分类（Data Classification）
- 数据最小化（Minimality）
- 数据保留（Retention）
- 数据销毁（Secure Disposal）

（4）日志与监控（Logging & Monitoring）

必须：

- 记录所有系统操作
- 审计管理员操作
- 保存至少 5 年

第五节｜网络安全（Cybersecurity – BaFin 最关注部分）

必须建立完整网络安全体系，包括：

（1）防火墙（Firewall）

（2）入侵检测（IDS）

（3）入侵防御（IPS）

（4）Web 防火墙（WAF）

（5）DDoS 防御

（6）端点安全（Endpoint Protection）

（7）反恶意软件系统

（8）漏洞扫描（Vulnerability Scanning）

（9）渗透测试（Penetration Testing）

监管常问：

Q：渗透测试的频率是什么？
Q：谁执行？是否第三方？
Q：验证报告是否可以提交？

仁港永胜提供全套渗透测试报告模板。

第六节｜IT 运维（IT Operations）

BaFin 要求包括：

1. 变更管理（Change Management）

- 变更申请（RFC）
- 变更审批
- 风险评估
- 回滚计划
- 测试环境（UAT）

2. 发布管理（Release Management）

- CI/CD pipeline
- 版本控制（Git）

3. 监控（System Monitoring）

- 系统性能
- API 可用性
- 错误率
- 交易失败率

4. 备份（Backup）

包括：

- 全备
- 增量备
- 异地备份
- 保留策略

监管要求：
备份必须异地保存 > 50 km。

第七节｜信息安全事故管理（Incident Management）

必须包含：

- 事故分类（Severity 1–4）
- 响应时间（SLAs）
- 升级流程（Escalation）
- 警报机制

- 根因分析（RCA）
- 行动计划（Action Plan）
- 通知监管机构时机
- 向客户通知条件

DORA 要求 CASP 在事故发生后 **24 小时内** 进行通报。

第八节｜业务连续性与灾难恢复（BCP / DRP）

BaFin 要求 CASP 拥有：

- BCP（Business Continuity Plan）
- DRP（Disaster Recovery Plan）

包括：

- 关键业务识别
- 恢复时间目标（RTO）
- 恢复点目标（RPO）
- 灾备演练
- 异地数据中心

MiCA 要求 CASP **半年一次灾备演练**。

第九节｜私钥管理（Cryptographic Key Management — BaFin 最重视）

此部分是加密行业最重要的技术合规点。
监管强制要求：

（1）私钥必须冷存储（HSM / MPC）

（2）私钥不得由单人控制（No single control）

（3）私钥必须使用 MPC 或 HSM 管理

（4）必须记录每一次密钥操作

（5）密钥必须在防火设施下保存

高风险行为包括：

- 私钥存于软件钱包
- 私钥由单个员工控制
- 私钥未使用硬件隔离
- 无密钥轮换流程

BaFin 面谈必问：

Q：私钥是否支持多重签名？
Q：Key material 是否完全离线？
Q：是否有密钥轮换？频率？如何执行？

仁港永胜提供 MPC Key Management 模板。

第十节｜外包 ICT（ICT Outsourcing – 最常见 RFI 点）

MiCA + DORA + BaFin 要求：

- 外包供应商必须评估（Due Diligence）
- 必须建立外包登记册（Outsourcing Register）

- 供应商必须符合 DORA 要求
- 合同必须包含：
  - SLA
  - 数据处理条款
  - 退出策略
  - 审计权（Audit Right）
  - 监管访问权（Regulator Access）

BaFin 常问：

Q：供应商是否可以提供 SOC2?
Q：供应商是否通过渗透测试?
Q：是否可以提供灾难恢复能力证据?

第十一节｜监管补件（RFI）示例（Q1–Q40）

此为仁港永胜唐生整理的真实 BaFin 审查问题。

ICT Governance（Q1–Q10）

Q1：ICT Framework 如何设计?
Q2：ICT Policy 包含哪些内容?
Q3：谁批准 ICT 政策?
Q4：ICT RACI 如何定义?
Q5：CTO 的资历是否满足监管要求?
Q6：如何确保安全开发？（SDLC）
Q7：如何记录 DevOps 操作?
Q8：如何控制管理员权限?
Q9：如何防止内部滥用权限?
Q10：如何管理访问控制日志?

Cybersecurity（Q11–Q20）

Q11：年度渗透测试是否强制?
Q12：执行方是否独立?
Q13：DDoS 防护是否足够?
Q14：如何监控异常登录?
Q15：如何控制 API 访问?
Q16：如何隔离内部开发人员权限?
Q17：如何保证代码安全?
Q18：如何控制第三方库风险?
Q19：如何处理重大零日漏洞?
Q20：如何记录攻击痕迹?

IT Operations（Q21–Q30）

Q21：如何管理变更?
Q22：如何记录变更日志?
Q23：如何测试变更?
Q24：如何监控系统健康?
Q25：如何管理备份?
Q26：备份保存在哪里?
Q27：如何验证备份可恢复?
Q28：如何确保运维人员不滥用权限?
Q29：如何记录系统警报?
Q30：如何管理证书（SSL/TLS）?

Business Continuity（Q31–Q40）

Q31：RTO 如何定义？
Q32：RPO 如何定义？
Q33：灾备演练是否完成？
Q34：如何验证演练结果？
Q35：如何通知监管机构？
Q36：备援数据中心是否跨地区？
Q37：灾难发生时客户如何受影响？
Q38：恢复计划是否可执行？
Q39：内部责任分工是否清晰？
Q40：如何管理应急通讯？

第十二节｜仁港永胜唐生专属建议（真实经验）

1. **ICT 文档必须达到"银行级"质量**
2. **必须使用 HSM / MPC 方案，不得只用软件钱包**
3. **必须准备一次渗透测试报告（含执行证明）**
4. **必须建立完整外包登记册（Outsourcing Register）**
5. **必须准备至少 3 份灾备演练记录**
6. **必须建立密码政策（含 MFA 强制化）**
7. **必须准备 SDLC（安全开发）流程图**
8. **必须建立访问控制矩阵（Access Matrix）**
9. **必须准备系统架构图（Regulator Version）**
10. **必须准备 Incident Response Plan（含模拟测试）**

仁港永胜可代为构建：

- ICT Framework
- Cybersecurity Policies
- Key Management
- 渗透测试
- Disaster Recovery
- Outsourcing Register
- ICT RFI 回答材料

第 15 章｜外包管理（Outsourcing Framework）

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。

第 15 章概述｜为什么外包（Outsourcing）是德国 CASP 最常遇到的拒批原因?

因为 MiCA + DORA + BaFin 共同对 CASP 外包提出极高要求：

- 任何与 ICT、钱包托管、交易撮合、数据处理相关的外包
  → **均被视为"关键外包"（Critical Outsourcing）**
- 若外包管理不足，BaFin 会直接拒绝牌照
- 外包供应链复杂性被视为加密行业的系统性风险
- DORA 要求 CASP 对外包第三方执行 **强监管级别控制**

德国监管最担心三件事：

1. 核心系统被外包 → CASP 无法控制风险
2. 外包商不受监管 → 无法监管穿透
3. 外包中断 → 造成客户资产损失或交易系统中断

因此，本章将提供一套 **可提交给 BaFin 的外包管理体系（深度实操版）**。

第一节｜外包定义（Outsourcing Definition – MiCA + DORA 标准）

符合以下任意一项，即被视为外包：

- 系统由第三方托管或运营（cloud、服务器、钱包、KMS）
- 交易撮合引擎外包
- 钱包托管外包（如 Fireblocks、Copper）
- 链上监测工具（Chainalysis、TRM Labs）
- 客户 KYC 服务外包
- 反洗钱监测外包
- 客服外包
- 技术开发团队外包
- 服务器托管（AWS / Google / Azure）

MiCA 特殊规定：

> "凡涉及客户资产托管、交易执行、风控、IT 系统者，均视为关键外包（Critical Outsourcing）。"

这意味着德国 CASP 基本不可能没有外包。
但 BaFin 要求：**必须对外包执行"完全监管化管理"。**

第二节｜外包分类（Outsourcing Classification）

德国 BaFin 区分三类外包：

A. Critical Outsourcing（关键外包）— 最严格

必须满足：

- 合规可控性
- 战略影响
- 业务连续性
- 客户资金安全
- ICT 风险
- 供应链可监管化
- 数据安全
- 渗透测试可执行

例子：

- 云服务器（AWS / Google / Azure）
- 钱包托管（Fireblocks / Copper）
- MPC Key Management
- 交易撮合 / 清算系统
- 核心数据库
- AML/KYC 系统

B. Important Outsourcing（重要外包）

例如：

- KYC 人工复核
- 风险监测工具
- 市场监控系统

C. Non-critical Outsourcing（非关键外包）

例如：
市场营销、翻译、行政支持。

第三节｜外包治理（Outsourcing Governance）

必须建立 **Outsourcing Governance Framework**，包括：

1. Outsourcing Policy（外包管理政策）
2. Outsourcing Register（外包登记册 – 最重要）
3. Vendor Risk Assessment（供应商风险评估）
4. Contractual Requirements（合同要求）
5. Performance Monitoring（绩效监控）
6. Exit Strategy（退出策略）
7. Concentration Risk Control（集中度风险控制）
8. 监管访问权（Regulator Access Rights）

这些内容都是 BaFin 最爱问的。

第四节｜外包登记册（Outsourcing Register – 核心监管要求）

这是 BaFin 审查的第一文件，必须包含：

字段	内容
Supplier Name	第三方供应商名称
Service Type	服务类型（Cloud、Wallet、KYC 等）
Criticality	关键、重要、非关键
Regulatory Impact	是否影响 MiCA 要求
Data Access	是否接触客户数据
Location	数据存储地（EU/Non-EU）
Sub-outsourcing	是否有再外包
Risk Level	高/中/低
Monitoring Frequency	监控频率
Contract Signed Date	合同签署日期
Exit Strategy	退出计划
DRP	灾备能力

外包登记册必须每季度更新一次。
仁港永胜可代提供完整登记册模板。

第五节｜供应商尽职调查（Vendor Due Diligence – VDD）

MiCA + DORA 强制要求 CASP 对供应商进行 **全生命周期尽调**。
必须评估三个维度：

（1）法律与监管风险（Legal & Regulatory Risk）

包括：

- 数据是否可能泄露?
- 供应商是否符合 GDPR?
- 是否位于高风险司法辖区?
- 供应商是否受监管?
- 是否具备合规证书（ISO、SOC2）？

（2）信息安全风险（Cyber/IT Risk）

必须确认：

- 是否进行渗透测试?

- 是否符合 ISO 27001?
- 是否进行漏洞扫描?
- 加密措施?
- 身份管理措施?

（3）运营风险（Operational Risk）

包括：

- 是否存在单点故障?
- 是否可提供可用性证明（Uptime > 99%）?
- 是否有灾备?
- 是否有服务中断记录?

BaFin 常问：

- **"你如何对 AWS 执行尽职调查？"**
- **"供应商若在美国境内，你如何管理 GDPR 风险？"**
- **"供应商是否提供 SOC2 报告？"**

仁港永胜将准备完整 Vendor DDQ（供应商尽调问卷）。

第六节｜合同要求（Contractual Requirements）

MiCA + DORA 要求外包合同必须包含 **10 项必备条款**：

1. SLA（服务级别协议）
2. 数据访问、加密、安全要求
3. 供应商向监管开放数据的义务（Regulator Access）
4. 审计权（Audit Right）
5. 再外包限制（Sub-outsourcing Restriction）
6. 退出策略（Exit Plan）
7. 服务中断通知义务
8. 事件通报（Incident Reporting）
9. 数据保留
10. 适用法律（Preferably EU）

尤其第 3 条和第 4 条，BaFin 最看重。

第七节｜外包绩效监控（Performance Monitoring）

CASP 必须对所有供应商建立监控机制，包括：

- 月度报告
- SLA 审查
- 事件通报记录
- 系统宕机记录
- 问题整改情况
- 风险变化监控
- 半年一次供应商风险复审

不能只是"记录"，必须有：

- Control Evidence（证据）
- Logs（日志）
- Reports（报告）

第八节｜外包风险管理（Risk Management）

包括：

（1）集中度风险（Concentration Risk）

例如：

- 90% 关键服务都在 AWS 上 → 高风险

（2）系统性风险

例如：

- 钱包托管采用单一供应商

（3）供应链风险（Supply Chain Risk）

供应商若有再外包 → 必须穿透识别风险。

第九节｜退出策略（Exit Strategy – 必备）

必须包括：

- 平滑退出流程
- 服务迁移计划
- 数据迁移
- 密钥迁移
- 客户资产不受影响
- 替代供应商
- 风险评估
- 时间表
- 回滚方案

MiCA 明确要求"不得因外包导致服务终止"。

第十节｜外包事故管理（Outsourcing Incident Management）

外包事故包含：

- 云服务器宕机
- 钱包供应商不可用
- KYC 工具停机
- 交易撮合引擎故障
- 供应商数据泄露
- 供应商受到网络攻击

必须执行：

1. 事件识别
2. 风险评估
3. 通报监管机构
4. 启动 DRP
5. 证据保留
6. 根因分析
7. 执行整改
8. 更新供应商风险评级

DORA 要求关键外包事件在 **24 小时内通报监管**。

第十一节｜监管补件（RFI Q1–Q30）

以下由仁港永胜唐生基于真实案例总结：

供应商管理（Q1–Q10）

Q1：供应商筛选标准是什么？
Q2：如何执行尽职调查？
Q3：供应商是否符合 GDPR？
Q4：是否审查供应商的财务稳定性？
Q5：是否存在再外包？如何管理？
Q6：是否有供应商风险评估？
Q7：如何监控供应商 SLA？
Q8：如何评估外包风险变化？
Q9：供应商是否提供渗透测试报告？
Q10：与供应商的合同是否包含监管访问权？

关键外包（Q11–Q20）

Q11：为什么将某服务设为关键外包？
Q12：如何验证供应商的数据保护能力？
Q13：供应商的 ICT 架构是否符合 DORA？
Q14：如何确保外包不中断核心服务？
Q15：若供应商破产，如何处理？
Q16：如何管理云服务提供商？
Q17：如何评估供应商安全事件？
Q18：如何监督供应商的合规状况？
Q19：如何验证灾备计划有效性？
Q20：是否存在供应商变更程序？

合同管理（Q21–Q30）

Q21：合同是否包含审计权？
Q22：合同是否允许监管访问？
Q23：如何管理合同生命周期？
Q24：供应商是否需遵守 SLA？
Q25：如何评估合同条款的合规性？
Q26：合同是否禁止未经批准的再外包？
Q27：合同是否定义事件通报时间？
Q28：合同是否要求加密？
Q29：合同是否要求备份验证？
Q30：合同是否包含退出计划？

第十二节｜仁港永胜唐生专属建议

作为德国 MiCA-CASP 实操顾问，我们的建议：

1. **所有关键外包必须进行一次完整 Vendor Due Diligence（DD）**
2. **必须建立 Outsourcing Register（外包登记册）**
3. **必须建立 SLA 绩效跟踪机制**
4. **必须要求供应商提供 SOC2 Type II 报告**
5. **合同必须包含 10 项 MiCA 强制条款**
6. **对钱包托管商（如 Fireblocks）必须执行增强尽调**
7. **避免使用无监管或无资质的外包商**
8. **必须准备 20 份外包场景的 Incident Simulation（事故模拟）**

9. **在面谈前必须准备至少 30 个 RFI 预案答案**
10. **建立"供应商替代策略"，以应对技术中断**

仁港永胜可提供：

- 外包政策（Outsourcing Policy）
- 外包登记册（Outsourcing Register）
- 供应商尽调（DDQ）
- 合规合同条款模板
- 外包风险评估
- Outsourcing RFI 回答包

第 16 章｜客户资产保护（Safeguarding of Client Assets）

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。此章节是整个德国 MiCA-CASP 审批流程中 **最关键的核心点（Top 1）**。只要 Safeguarding 不合格 → BaFin 会直接拒绝，不进入下一轮 RFI。
本章内容将基于：

- **MiCA 第 68 条 Safeguarding 要求**
- **德国 ZAG（支付服务监管法）** 及 KWG 银行业务要求
- **BaFin 客户资金保全准则（Sicherungsanforderungen）**
- **EBA Guidelines on Safeguarding**

第 16 章总览｜为什么 BaFin 对客户资产保护比任何国家都严格?

德国监管认为加密资产具有以下高风险特征：

- 钱包私钥可能被盗
- 加密资产属于高波动资产
- 客户资产易被与公司资产混同（commingling）
- 托管业务（custody）属于 MiCA 下的最高监管级服务
- 错误的密钥管理会直接导致资产永久损失

因此 BaFin 强制要求：

> "客户资产必须与公司自有资产完全隔离（100% segregation），不得混合使用。"

且必须具备：

- 资产隔离结构
- 托管架构说明
- 私钥管理（Key Management）
- 冷存储 + MPC/HSM
- 交易对账 + 链上对账
- 运营风险防护
- 客户资金专户（Client Safeguarding Account）
- 严格 IT 权限管理
- 客户提款监控与欺诈防控

德国是全球对"加密资产托管"要求最高的国家之一。
本章将完整呈现 **德国监管要求 + 实操级执行方案**。

第一节｜本章结构（Safeguarding Framework 总览）

MiCA + BaFin 要求 CASP 构建一个可审计的客户资产保护体系，包括：

1. **资产隔离（Segregation）**
2. **钱包结构（Wallet Architecture）**
3. **私钥管理（Key Management – MPC/HSM）**
4. **链上对账（Onchain Reconciliation）**
5. **现金 Safeguarding（Fiat Safeguarding Account）**
6. **客户资产账簿（Client Asset Ledger）**
7. **提款流程与权限（Withdrawal Controls）**
8. **访问控制（Access Control & SoD）**
9. **资产损失事件处理（Loss & Incident Management）**
10. **保险机制（Insurance / Crime Policy）**

每项均必须提交 **文件证明 + 系统证明 + 组织结构证明**。
仁港永胜已为多国托管类牌照准备过完整 Safeguarding 套件，可直接用于德国材料。

第二节｜资产隔离（Segregation of Client Assets）

MiCA 明确规定：

> 客户资产必须与公司自有资产（Own Funds）在技术上、账务上、法律上 100% 隔离。

德国 BaFin 强制执行"三层隔离"结构：

A. 技术隔离（Technical Segregation）

- 客户资产必须存于独立钱包（Multi-tenant wallet with logical segregation 或 Multi-wallet segregation）
- 公司自有资产不得存放于客户钱包
- 公私钥必须独立，"密钥不共用"

B. 账簿隔离（Accounting Segregation）

必须建立：

- Client Asset Ledger
- Corporate Asset Ledger

每一项资产必须可溯源到：

- 钱包地址
- 客户 ID
- TxID
- 交易时间
- 余额证明

C. 法律隔离（Legal Segregation）

法规要求：

- 托管合约（Custody Agreement）
- 资产法律所有权（Legal Title）
- 明确 CASP 仅为 Custodian，不拥有客户资产

仁港永胜的模板可直接用于 BaFin 审批。

第三节｜钱包架构（Wallet Architecture）

必须向 BaFin 提交完整的钱包架构示意图，包括：

1. 冷钱包（Cold Wallet）

- 100% 离线

- 使用 HSM/MPC
- 不接触互联网
- 仅用于长期储存

2. 热钱包（Hot Wallet）

- 仅用于即时交易
- 必须有限度（≤ 资产总额 3–5%）
- 必须进行限额控制

3. 温钱包（Warm Wallet – 若使用）

- 用于批量提款
- 有网络访问，但风险低于热钱包

4. 钱包风险等级（Wallet Risk Rating）

- High Risk
- Medium Risk
- Low Risk

监管会问：

- 钱包如何分类?
- 钱包限额是多少?
- 是否使用 MPC?
- 是否使用 HSM?

第四节｜私钥管理（Key Management – MPC/HSM 强制要求）

BaFin 明确反对：

- 单人控制私钥
- 软件钱包（Software Wallet）
- 未加密保存密钥
- 未进行密钥轮换
- 热钱包持有过多资产

监管要求：

（1）必须使用 HSM 或 MPC

HSM（Hardware Security Module）
MPC（Multi-Party Computation）
两者都满足：

- 物理隔离
- 密钥分片
- 无人单独控制

（2）密钥操作日志必须可审计

包括：

- 签名操作
- 密钥生成
- 密钥备份
- 密钥恢复
- 密钥轮换

（3）密钥必须执行角色分离（SoD）

至少 3 人：

- 发起人
- 执行人
- 批准人

必须相互不可替代。

（4）密钥恢复流程（Key Recovery Plan）必须提交

包括：

- Key shard 地理位置
- 恢复流程
- 灾备恢复
- 是否使用 Shamir Secret Sharing（SSS）

第五节｜链上对账（Onchain Reconciliation）

这是德国监管最重视的托管能力证明。

必须做到：

操作	频率	要求
链上余额对账	每日（Daily）	必须对所有地址进行链上查询并核对内部账簿
交易对账（Tx Reconciliation）	即时/每日	对每笔 TxID 与数据库记录进行匹配
资产缺口分析	实时	若资产不足必须立刻触发 Incident
报告生成	每日	自动生成报表并提交给 MLRO/CTO

BaFin 会要求：

- 日常链上对账报告样本
- 系统截图
- 对账算法描述
- 异常资金流处理流程

仁港永胜可提供完整 Onchain Reconciliation 方案。

第六节｜客户资金（法币）保护（Fiat Safeguarding Account）

若 CASP 涉及托管法币（Fiat），必须提供：

A. 客户资金专户（Safeguarding Account）

- 在德国或欧盟受监管银行开设
- 名称必须显示"客户资金"(Client Safeguarding)
- CASP 不得使用客户资金

B. 每日银行对账

包括：

- 银行余额
- 客户账簿余额
- 差异分析
- 异常上报

C. 资金隔离法律文件

- 三方协议（Tri-party agreement）

- 银行确认信
- 合规声明

第七节｜提款流程（Withdrawal Controls）

提款是 BaFin 审查的重点风险场景。
CASP 必须建立：

1. Anti-fraud 提款监控

包括：

- 提款限额
- 提款地址白名单
- 多因子认证（MFA）
- 异常行为识别
- 高风险国家限制

2. 多级审批（Multi-step Approval）

金额	审批人
小额	CS → OPS
中额	OPS → MLRO
大额	OPS → MLRO → CTO

3. 风险国家黑名单

包括：

- 制裁国家
- 战争/冲突国家
- 洗钱高风险地区

第八节｜访问控制（Access Control – SoD 强制要求）

所有与客户资产相关的系统必须执行：

- RBAC
- SoD（至少三人分权）
- MFA 强制
- Admin 权限必须受控
- 所有敏感操作必须日志化
- 系统自动记录资产相关权限的变更

第九节｜资产损失事件管理（Loss / Incident Management）

必须包含：

- 事故识别
- 风险评估
- 客户资产保护措施
- 监管通报（MiCA 要求 24 小时）
- 警方通报（如涉及欺诈/盗窃）
- 客户赔付机制（如适用）
- 损失报告（Loss Report）
- 修复计划

BaFin 必问：

Q：若钱包被黑，如何赔偿客户？
Q：是否有保险？
Q：是否有责任归因机制？

第十节｜保险（Insurance / Crime Policy）

MiCA 不强制保险，但 BaFin 强烈建议：

- Crime Insurance（商业犯罪保险）
- Cyber Insurance（网络安全保险）
- Wallet Theft Insurance（钱包被盗保险）

这不仅提高审查通过率，也提升机构抗风险能力。

第十一节｜监管补件（RFI Q1–Q40）

以下内容由仁港永胜唐生基于 BaFin 真实补件总结：

钱包安全（Q1–Q10）

Q1：热钱包限额是多少？为什么？
Q2：冷钱包是否完全离线？
Q3：是否使用 MPC/HSM？
Q4：密钥是否由多人控制？
Q5：密钥备份如何管理？
Q6：冷钱包地址是否公开？
Q7：是否经过渗透测试？
Q8：如何防止内部人员盗取私钥？
Q9：如何记录密钥操作？
Q10：如何执行密钥轮换？

资产隔离（Q11–Q20）

Q11：如何保证客户资产不被挪用？
Q12：如何记录每个客户的钱包余额？
Q13：是否有独立账簿？
Q14：如何进行链上对账？
Q15：如何处理资产缺口？
Q16：如何管理客户地址白名单？
Q17：如何控制提款审批？
Q18：客户资产是否保险覆盖？
Q19：资产损失如何赔付？
Q20：如何处理遗失私钥？

法币资金保护（Q21–Q30）

Q21：Safeguarding Account 是否开设？
Q22：银行是否提供确认信？
Q23：是否进行每日对账？
Q24：差异如何识别？
Q25：银行账户是否被隔离？
Q26：是否授权多人操作？
Q27：是否禁止从客户资金账户支付公司费用？
Q28：是否存在高风险银行？
Q29：如何处理银行服务中断？
Q30：是否有 SEPA 风险控制？

提款安全（Q31–Q40）

Q31：提款审批流程是什么？
Q32：提款限额如何设定？
Q33：是否检查提款地址？
Q34：是否执行 AML 风控？
Q35：提款异常如何识别？
Q36：是否有欺诈报告流程？
Q37：OTP/MFA 是否强制？
Q38：提款失败是否有记录？
Q39：是否有提款延迟机制？
Q40：如何向客户解释风控措施？

第十二节｜仁港永胜唐生实操建议（独家）

1. **使用 MPC（Fireblocks / Copper）大幅提高审查通过率**
2. **可视化钱包架构和密钥管理流程图是加分项**
3. **必须准备链上对账日报（CSV+截图）给 BaFin**
4. **准备 20 个提款警报案例（Use Cases）**
5. **冷钱包必须放置在国外安全机房（建议瑞士/德国）**
6. **必须建立 Withdrawal Risk Engine（提款风险引擎）**
7. **强烈建议购买 Wallet Theft Insurance**
8. **建立 Client Asset Ledger（客户资产账簿）**
9. **生成 Asset Segregation Testing（资产隔离测试报告）**
10. **准备至少 30 条 RFI 预案答案（监管补件）**

仁港永胜可以提供：

- 钱包架构图
- Key Management Framework
- 链上对账工具
- 资产隔离证明文件
- Withdrawal Control Policy
- Safeguarding RFI 回答包

第 17 章｜反洗钱与反恐融资（AML/CTF Framework）

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，本章是德国 BaFin 审查 MiCA-CASP 牌照时 **最重要的核心章节之一（TOP 2，仅次于 Safeguarding）**，并且属于"不可妥协的强审查项"。

本章内容将基于：

- **MiCA（Regulation (EU) 2023/1114）第 63–67 条 AML 要求**
- **欧盟第六号反洗钱指令（AMLD6）**
- **德国《GwG 洗钱法》（Geldwäschegesetz）**
- **BaFin AML Circular（Interpretative Notes）**
- **EBA AML/CTF Guidance**
- **BaFin FCTR（金融犯罪风控技术监管要求）**

第 17 章概述｜为什么 BaFin 的 AML/CTF 是欧洲最强监管？

德国是全欧盟 AML（反洗钱）监管强度最高的国家之一，原因包括：

- 德国是欧盟 AMLD6 的最早实施国
- 德国本地《GwG 洗钱法》要求严于欧盟标准

- 德国金融情报部门（FIU）对加密交易极其敏感
- 加密资产被德国监管定位为「极高洗钱风险行业」
- 德国是全球 STR/SAR（可疑交易报告）提交量最高国家之一
- BaFin 一直对加密机构保持"高风险、高监管、高审查"态度

因此：

> **一个 CASP 的 AML/CTF 框架必须达到与银行同等级别，不得低于传统金融机构标准。**

本章将全面呈现德国 MiCA-CASP 必备的 AML/CTF 完整体系（深度实操版）。

第一节｜AML/CTF 框架总体结构（AML Framework Architecture）

德国 AML 框架必须涵盖：

1. **业务风险评估（Business-Wide Risk Assessment, BWRA）**
2. **客户尽职调查（CDD/KYC/KYB）**
3. **加强尽调（EDD）**
4. **交易监测（Transaction Monitoring）**
5. **制裁筛查（Sanctions Screening）**
6. **PEP/Adverse Media 筛查**
7. **链上分析（Onchain AML）**
8. **SAR/STR 报告（提交给德国 FIU）**
9. **AML 政策与操作手册（Policies & Procedures）**
10. **AML 职责结构（MLRO + AML Officer）**
11. **记录保留（Record Keeping – 5 years）**
12. **员工培训（AML Training）**
13. **AML 内部审计（AML Audit）**

此框架任何部分不合格都可能导致 BaFin 拒批。

第二节｜业务风险评估（Business-Wide Risk Assessment – BWRA）

德国 AML 法规要求每个 CASP 都必须执行：

> **BWRA = 对整个业务进行 AML 风险识别 + 评估 + 建议 mitigation**

风险评估包括：

1. 产品风险（Product Risk）

- 交易服务
- 托管服务
- OTC
- Staking
- 兑换服务
- 法币入金/出金

2. 客户风险（Customer Risk）

- 个人/企业
- 高净值客户
- 高风险国家（FATF 列表）
- 匿名客户
- 复杂公司结构（UBO 穿透至自然人）

3. 地域风险（Geographical Risk）

- 制裁地区
- 欧盟以外高风险地区
- 反洗钱制度薄弱国家

4. 交易风险（Transaction Risk）

- 大额
- 高频
- OTC
- 隐私币（Monero、Zcash）
- 混币器（Tornado Cash）

5. 渠道风险（Delivery Channel Risk）

- 线上开户
- 无面对面识别（Non-face-to-face）
- 自动化流程

BWRA 必须每年更新并向 BaFin 提交。
仁港永胜可协助准备完整 BWRA 模板。

第三节｜客户尽职调查（CDD – KYC/KYB）

德国 AMLD6 + GwG 要求 CASP 建立：

A. 身份验证（Identity Verification）

个人客户必须：

- 身份证/护照 OCR
- 地址证明（3 个月内）
- 活体检查（Liveness Detection）
- IP + 手机验证

企业客户（KYB）必须：

- 注册证明
- 公司章程
- 董事登记册
- 股东登记册
- UBO 穿透至自然人
- 公司业务说明
- 资金来源（SOF/SOW）

B. 风险评级（Risk Rating）

必须使用 3 级体系：

- 低风险
- 中风险
- 高风险

每位客户必须：

- 初次评级
- 定期复审（Annual Review）
- 如果触发 EDD → 强制重新评级

C. 客户风险触发 EDD 的情况：

- 高风险国家
- 高净值客户
- 大额资金
- 匿名钱包
- 复杂企业结构
- 使用隐私币
- OTC 大额买卖

第四节｜加强尽调（EDD – Enhanced Due Diligence）

EDD 是 BaFin 审查 CASP 能力的重点。
必须包含：

1. 资金来源（Source of Funds – SOF）

例如：

- 工资单
- 银行流水
- 投资收益
- 公司收入证明
- 税务证明

2. 财富来源（Source of Wealth – SOW）

例如：

- 公司股权证明
- 房产证明
- 证券资产
- 继承证明

3. 客户背景调查（Background Check）

包括：

- 职业
- 企业合法性
- 行业性质
- 业务目的

4. 链上历史（On-chain profiling）

必须使用：

- Chainalysis
- TRM Labs
- Elliptic

风险包括：

- 暗网
- 混币器
- 黑市交易
- OFAC 地址
- 勒索软件地址

第五节｜制裁筛查（Sanctions Screening）

必须覆盖：

- UN（联合国）
- EU（欧盟）
- OFAC（美国）
- UK HMT（英国）
- 德国国家制裁清单

必须对以下对象进行 screening：

- 客户姓名
- 企业名称
- UBO
- 钱包地址
- 交易对手方

任何 match（命中）必须：

- 立即冻结
- 执行 L1 + L2 复核
- MLRO 终审
- 记录保存 5 年
- 评估是否 SAR（可疑交易报告）

第六节｜PEP & Adverse Media（政治公众人物、负面媒体）筛查

必须进行：

- Politically Exposed Persons（PEP）检查
- 地址风险检查
- 负面新闻检查

高风险情况包括：

- PEP
- 涉嫌诈骗
- 犯罪关联
- 被执法机关调查
- 与战争区域有关

高风险客户必须启动 EDD。

第七节｜交易监测（Transaction Monitoring – 行为 + 规则模型）

这是 BaFin 最关注的 AML 技术模块。

必须具备 2 大模型：

A. Rule-based（规则模型）

例如：

- 高频交易
- 大额交易
- 分拆交易

- 资金流向黑名单
- 使用隐私币
- 夜间频繁操作
- 多地址跳转（Layering）

B. Behavior-based（行为模型）

例如：

- 行为突然变化
- 交易与客户画像不符
- 异常重复性交易
- 高风险地理位置跳变

每条监控必须：

- 生成 alarm
- 由 L1 → L2 审查
- 记录警报闭环（Case Management）
- 若异常严重 → SAR

第八节｜链上交易监测（Onchain Transaction Risk Monitoring）

所有链上交易必须：

- 使用 Chainalysis/TRM 监控
- 评估地址风险（Wallet Risk Scoring）
- 识别可疑交易路径
- 检查是否经混币器
- 识别制裁地址
- 识别关联风险群集（Graph Clustering）

MiCA 强制要求链上监控，这与传统金融高度不同。

第九节｜可疑交易报告（SAR / STR – 向德国 FIU 提交）

SAR（Suspicious Activity Report）提交流程：

1. 生成警报（系统）
2. L1 初审
3. L2 高级审查
4. MLRO 决策
5. 提交给 FIU（24 小时内）
6. 保存证据 5 年

必须准备：

- SAR 模板
- SAR 决策依据
- SAR 使用案例（≥20 个）
- SAR 历史记录（如适用）

BaFin 必问：

- “SAR 比例是否正常？”
- “SAR 触发逻辑是什么？”

第十节｜AML 文档体系（Policies & Procedures）

必须准备：

- AML Policy
- AML Manual
- CDD Procedure
- EDD Procedure
- Transaction Monitoring Procedure
- SAR Procedure
- Sanctions Policy
- Wallet Risk Policy
- Customer Risk Scoring Method
- Training Policy
- Record Keeping Policy

所有文件必须由董事会批准。

仁港永胜可以提供德国格式文件套装。

第十一节｜角色与职责（MLRO + AML Officer）

MiCA + GwG 要求：

MLRO（反洗钱负责人）

必须：

- 全职
- 位于德国或欧盟
- 有反洗钱经验
- Fit & Proper（专业 + 品行）
- 深入了解链上交易

Deputy MLRO（副 MLRO）

用于：

- 代替 MLRO
- 分权控制（SoD）

AML Officer

负责：

- CDD/EDD
- 报告
- 风险评估

第十二节｜记录保留（Record Keeping – 5 years）

必须保存：

- 身份资料
- EDD 资料
- 链上分析报告
- 警报记录
- SAR 报告
- 交易日志
- 联系记录

- 报告提交证据

德国监管要求保留 5–10 年。

第十三节｜员工 AML 培训（AML Training）

所有员工必须：

- 每年 1 次 AML 培训
- 特殊岗位（MLRO/Compliance）每半年一次
- 保存培训证据

培训内容包括：

- AMLD6
- GwG
- 交易监测
- 链上分析
- SAR 提交
- 制裁

仁港永胜提供 AML 培训材料。

第十四节｜AML 内部审计（Independent AML Audit）

MiCA 强制要求：

- AML 每年一次独立审计
- 审计报告必须提交给董事会
- 审计对象包括：
  - CDD
  - EDD
  - TM
  - SAR
  - Sanctions
  - Onchain AML

第十五节｜监管补件（RFI – Q1 ~ Q50）

以下是仁港永胜唐生基于德国 BaFin 真实补件整理：

CDD / EDD（Q1–Q10）

Q1：CDD 流程如何自动化？
Q2：EDD 触发标准是什么？
Q3：如何验证 SOF/SOW？
Q4：KYB 如何穿透股东？
Q5：如何识别高风险行业？
Q6：是否复审客户风险？
Q7：怎么处理资料缺失？
Q8：如何进行 Address Verification？
Q9：如何处理假阳性？
Q10：EDD 如何记录？

Transaction Monitoring（Q11–Q20）

Q11：监控规则有哪些?
Q12：如何识别分拆交易?
Q13：如何识别混币器交易?
Q14：如何处理高风险交易?
Q15：如何执行行为监控?
Q16：如何处理异常警报?
Q17：关闭警报的标准是什么?
Q18：如何保证系统有效性?
Q19：如何评估交易风险变化?
Q20：如何进行年度模型验证?

Sanctions & Screening（Q21–Q30）

Q21：Screening 工具是什么?
Q22：如何处理 OFAC 命中?
Q23：如何执行钱包筛查?
Q24：如何记录复核?
Q25：如何更新名单?
Q26：如何处理假阳性?
Q27：是否有双人复核?
Q28：Screening 频率是什么?
Q29：是否 screening 对手方?
Q30：链上地址如何 screening?

SAR（Q31–Q40）

Q31：SAR 触发标准是什么?
Q32：如何判断是否提交 SAR?
Q33：SAR 是否有内部审批?
Q34：如何保存 STR 记录?
Q35：如何处理法币可疑交易?
Q36：如何处理链上可疑交易?
Q37：如何处理匿名威胁?
Q38：是否具有拒绝交易机制?
Q39：是否通知客户 SAR?（不得通知）
Q40：如何与 FIU 协作?

整体框架（Q41–Q50）

Q41：AML 是否遵循风险为本（RBA）?
Q42：BWRA 如何执行?
Q43：如何保证 AML 资源充足?
Q44：如何向董事会报告?
Q45：如何测试 AML 控制有效性?
Q46：如何进行 AML 培训?
Q47：如何进行内审?
Q48：如何监控 AML 法规更新?
Q49：如何管理供应商（KYC/AML Tools）?
Q50：如何保证系统不被滥用?

第十六节｜仁港永胜唐生实操建议

1. **必须使用 Chainalysis/TRM 作为链上 AML 工具**
2. **必须准备至少 30 条交易监控规则**
3. **必须准备 20 条 EDD 案例（SOF/SOW）**
4. **必须准备 SAR 提交流程图（Regulator-ready）**
5. **必须准备 Screening Sample（命中示例）**

6. **必须建立 Customer Risk Matrix**
7. **KYB 必须穿透到自然人 UBO**
8. **必须准备 AML 培训与证书**
9. **必须准备 BWRA（业务风险评估）完整版**
10. **准备 50 条 AML RFI 回答（提前准备可大幅提高通过率）**

仁港永胜可以提供：

- AML 政策全套
- AML 系统架构图
- AML 数据流程图
- Transaction Monitoring Rules
- SAR 样本
- EDD 样本
- AML RFI 应对模板

第 18 章｜BaFin 审查流程、监管补件（RFI）应对策略与面谈机制

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

本章是德国 CASP 审批中**最重要的章节之一（TOP 3 核心章节）**，它决定申请能否顺利通过。

德国是全欧盟监管要求最深入、补件最多、周期最长的国家之一，本章基于仁港永胜唐生团队多年的监管交付经验，完整呈现真实执行路径。

> **一句话总结：德国 BaFin 的审查重点是"补件"与"面谈"，不是最初提交。**
> **要申 MiCA，必须掌握 BaFin 的审查节奏。**

第 18 章 全结构目录

1. **BaFin 审批整体时间线（12–24 个月）**
2. **审查流程 6 大阶段（入门 → RFI → 面谈 → 决策）**
3. **监管补件（RFI）全解析（平均 90–180 个问题）**
4. **BaFin 最常提问的 8 类高频问题**
5. **仁港永胜整理：300 条 BaFin RFI 问题类型大表（结构化）**
6. **监管面谈（Interview）流程 + 问题 + 模拟应答**
7. **为什么德国 MiCA-CASP 申请难度全欧第一?**
8. **仁港永胜唐生：德国审查成功策略（系统级深度建议）**

第一节｜BaFin 审批整体时间线（12–24 个月）

德国申请 CASP 的典型周期为：

阶段	内容	预计时间
0	前期预审 + 架构搭建	1–2 个月
1	递交申请文件	T = 0
2	形式审查（Formal Check）	1–2 个月
3	第一次 RFI（补件）	2–4 个月
4	第二次 RFI（补件）	2–3 个月
5	监管面谈（Interview）	1 个月
6	最终 RFI / Clarification	1–3 个月
7	批准/拒绝	全流程 12–24 个月

德国没有"快通道"，所有申请都必须经历大量补件与面谈。

第二节｜德国 BaFin 审查流程六大阶段（完整图解）

阶段 1：Formal Check（形式审核）

BaFin 会检查：

- 文件是否齐全
- 董事、RO、MLRO 是否具备资格
- 股权结构是否清晰
- 申请材料是否符合 MiCA 要求格式

重点： 在这个阶段被退件 ≈ 失败。

阶段 2：Substance Review（实质审查）

会检查：

- 商业模式
- 资金安全（Safeguarding）
- IT 安全架构
- AML 体系完整性
- 交易监测与链上AML
- 风险管理框架
- 运营计划完整性

这是第一次真正的审查阶段。

阶段 3：第一次 RFI（Regulator Feedback / 补件）

第一次 RFI 一般包含：

- **60–120 个问题**
- 属于全方位实质审查
- 主要集中在 IT、AML、Safeguarding、RO 经验、交易监控

申请机构需要：

- 正式书面回答
- 提供附加政策文件
- 完整的流程图、架构图、数据流图

阶段 4：第二次 RFI

第二次 RFI：

- **20–60 个问题**
- 重点在验证第 1 次 RFI 的回答是否可执行
- 案例类问题会大幅增加

例如 AML 案例：

- "如果客户转入 3 个钱包形成链路，你如何判断风险？"
- "如何处理疑似分拆交易？"

阶段 5：监管面谈（Interview）

通常包含：

- 董事会面谈

- RO 面谈
- MLRO 面谈
- CTO/IT 面谈

面谈通常：

- 每场 1–2 小时
- 采用线上视频会议（近 3 年）
- 重点考察团队真实能力
- 深入问细节，而非文件

面谈后一般会在 2–4 周收到 "Final RFI"。

阶段 6：Final RFI（最后补件）→ 牌照决定

最后 RFI：

- 数量较少（5–20 条）
- 目的是确认申请方全部准备就绪

如果回答良好 → 授权
如果不佳 → 驳回 / 要求重新提交

第三节｜RFI（补件）结构化拆解｜平均 90–180 条问题

德国申请 MiCA CASP 的平均补件数量：

> **第一次 RFI：60–120 条**
> **第二次 RFI：20–60 条**
> **最终 RFI：5–20 条**
> 合计：≈ **90–180 个问题（实际案例最高 300+）**

问题 1：为什么德国补件数量如此大?

因为：

1. 德国监管认为 **"加密行业天然高风险"**
2. MiCA 在德国执行时更严格
3. BaFin 要求**文件必须达到银行级别**
4. 德国 AML 中心（FIU）对加密交易敏感
5. IT 安全要求等同于金融基础设施

第四节｜BaFin 高频问题（分 8 类）

类别 A｜商业模式（Business Model）

- 为什么选择在德国申请?
- 目标市场是什么?
- 如何盈利?
- 是否涉及 Staking? 是否属于 MiCA 监管范围?
- OTC 如何管理风险?

类别 B｜Safeguarding（资金安全）

这是德国最严格部分之一：

- 客户资金在哪里托管?
- 风险隔离机制?

- 银行账户签署权限?
- 当银行破产时如何保护客户资金?
- 客户资产是否可用于公司运营?（不能）

类别 C｜IT 安全（信息安全 + 系统架构）

- 数据中心在哪里?
- 冷/热钱包如何管理?
- 私钥管理流程?
- 日志保存多久?
- 是否进行渗透测试?
- 是否具备 DDoS 防护?

类别 D｜AML/CTF

（此部分在第 17 章已详细说明）

- CDD/EDD 如何执行?
- 链上风险如何识别?
- 混币器交易如何处理?
- SAR（STR）如何提交?
- 交易监测规则有哪些?

类别 E｜治理结构（Governance）

- 董事是否具备行业经验?
- 股东是否透明?
- UBO 是否有风险?
- RO 是否具备 Fit & Proper?

类别 F｜合规与报告（Compliance & Reporting）

- 如何向 BaFin 报告年度合规?
- 内部审计如何执行?
- 员工合规培训计划?

类别 G｜金融犯罪风险（Financial Crime）

- 如何识别欺诈交易?
- 如何阻止高风险交易?
- 如何识别暗网地址?

类别 H｜业务可持续性（Financial Plan）

- 未来三年财务模型?
- 是否有足够资本维持运营?
- 是否能覆盖初期亏损?

第五节｜仁港永胜独家整理：BaFin 300 条 RFI 结构化大纲

仁港永胜唐生根据历次德国补件，整理出：

300 条常见 RFI 框架（结构化）

（此为本指南第 17 章中已部分展示，这里按类别总结）

- **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。

另外点击这里可以直接下载完整版的：

✅ **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。

第六节｜监管面谈（Interview）｜流程 + 问题 + 模拟回答

德国监管面谈分四类：

1. **董事面谈（Board Interview）**
2. **RO 面谈（监管负责人）**
3. **MLRO 面谈（反洗钱负责人）**
4. **CTO/IT 面谈（系统安全）**

董事面谈重点（示例）

问题：为什么选择德国而非其他欧盟国家?
示例（仁港永胜唐生版回答）：

- 德国有深厚金融基础设施
- 市场更成熟
- 与机构客户合作多
- 长期将以德国为区域合规中心

RO 面谈重点

问题：RO 是否参与日常合规?
示例回答：

- 参与董事会
- 每周合规例会
- 每月风险审查
- 每季合规报告提交

MLRO 面谈重点

问题：如何识别链上可疑交易?
示例答案：

- 使用 Chainalysis 风险评分
- 检查路径是否经过混币器或暗网节点
- 检查是否属于高风险地址 cluster
- 检查交易行为是否符合客户画像

CTO 面谈重点

问题：私钥如何管理?
示例答案：

- 多签（Multi-Sig）
- 冷存储为主
- 硬件 HSM
- 访问控制（RBAC）
- 记录所有操作日志

第七节｜为什么德国难度全欧第一?

理由：

1. **监管最严格，补件数量最多**
2. **在 AML、IT、Safeguarding 方面要求超高**
3. **偏向传统金融体系管理方式**
4. **无"简单路径"，必须提交全套完整文件**
5. **德国金融体系对加密资产具天然警惕性**

一句话总结：

> **德国 MiCA-CASP = 欧盟难度最高，但护照价值最大。**

第八节｜仁港永胜唐生的成功策略

1. 文件必须一次性提交"银行级别质量"

MiCA 在德国执行 = 银行标准
文件必须包括 100+ 份：

- AML
- Safeguarding
- Outsourcing
- 风控
- IT 安全
- 交易监测
- 链上风控
- 审计
- 组织结构
- 员工制度
- IT 架构图
- 数据流向图
- 交易流程图

---

2. RFI 必须提前准备（不要等监管提问才写）

仁港永胜唐生可有偿为你准备：

- 300 条 RFI 模板
- 面谈问答集（含正确回答示范）
- 可直接提交的文件模板

---

3. 在德国必须配备"真正上得台面"的 RO/MLRO

不能临时找人。
BaFin 会深入面谈，问大量技术细节。
必须：

- 真实经验
- 能说明机制
- 能回答 AML、TM、IT 深度问题

---

4. IT 安全要达到德国银行级水平（最容易被补件）

必须准备：

- 系统架构图
- 私钥管理流程
- 访问控制矩阵（RBAC）
- 日志保存
- 备份机制
- 应急预案

---

5. 必须提前准备面谈（Interview）模拟

仁港永胜可以提供：

- 董事面谈
- RO 面谈
- MLRO 面谈
- CTO 面谈

全部模拟问答，模拟监管对话。

第 19 章｜仁港永胜对德国 MiCA-CASP 申请人的"实话建议"

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。

> **本章不是宣传，而是实战经验的总结。**
> **仁港永胜唐生将以"最真实、最高度专业、最直接"的方式告诉你：**
> **在德国申请 CASP，你真正需要准备什么、应该避免什么、怎样才能提高成功率。**

本章内容基于我们过去在欧盟（尤其是德国、奥地利、立陶宛、马耳他、荷兰、爱沙尼亚）处理的申请案例、监管沟通轨迹、补件记录、面谈数据以及实际获批经验，是全指南中最"内部级、行动级、决策级"的一章。

请开始阅读实话实说的深度建议：

第 19 章目录

11. **实话十一：过度宣传、过度包装，会导致直接反效果**
12. **实话十二：德国授权是欧洲最难，也最有价值的**
13. **仁港永胜唐生：我们怎样帮助申请人提高成功率（专业说明）**
14. **本章总结：德国是"硬骨头"，但只要方法正确，完全可行**

实话一：德国不是"提交文件即可获批"的国家

德国 BaFin 是欧洲最严格的监管机构之一。

以下观念请必须明确：

❌ **你不能"一次性"提交文件然后等待审批。**
❌ **你不能依赖模板化政策文件希望蒙混过关。**
❌ **你不能只准备表面层面的治理架构。**

德国是整个欧盟少数几个：

✓ 会问数百个 RFI（补件）
✓ 会做深入面谈
✓ 会把文件逐条对照法规
✓ 会要求现场验证
✓ 会要求关键人员亲自回答技术问题

的国家。

德国不是"递件 → 过审"，德国是：

> **"递件 → 多轮补件 → 深度审查 → 多轮面谈 → 再补件 → 再审查 → 最终批准"。**

德国 CASP 的流程比部分银行牌照还复杂。
这是事实，不是恐吓。

实话二：文件必须做到"接近银行级"质量

许多申请人在立陶宛、马耳他、波兰等国家申请过牌照，因此误以为：

> "MiCA 是统一规则，文件只要达标即可。"

然而德国的执行标准比其他国家更高。

举例：

- AML 政策必须包含 **40+ 模块**
- IT 安全政策必须覆盖 **DORA 法规要求**
- 风险管理必须包含 **风险评估矩阵 + 风险计量工具**
- Safeguarding 要求 **银行级资金隔离机制**
- 日志管理要满足 **德国联邦数据安全标准**

德国要求的政策量 = 其他国家的 1.5–2 倍。

仁港永胜唐生团队编制的德国 CASP 文件包，通常超过：

> **80–120 份文件（可逐项对应 BaFin 检查表）**

才能确保稳健。

实话三：德国监管最关心不是技术，而是治理能力

许多 Web3 团队以为 MiCA 监管主要在看：

- 技术
- 钱包安全
- 链上透明度
- 系统架构

这些确实重要，但 BaFin 最关心的是：

> **"谁在实际管理公司？谁在承担法律责任？谁能为德国本地用户负责？"**

治理能力 > 技术能力
这点非常现实。
BaFin 特别关注：

- 董事是否在欧洲具备真实经验
- RO 是否具备"德式合规文化"
- MLRO 是否能用专业语言解释 AML
- 是否具备"开会、审核、记录、报告"的能力
- 是否具备内部制衡体系

德国监管认为：

> **企业的治理体系决定其是否能长期合规，而不是技术能力。**

实话四：RO / MLRO 人选决定 50% 成败

这是全指南最重要的结论之一。
德国监管对 RO / MLRO 的要求：

- 必须在德国/EU 金融机构有经验
- 必须能回答深度问题（不是读稿）
- 必须参与运营，而不是挂名
- 必须懂 AML + IT + 风险管理
- 必须能解释商业模式的风险点
- 必须能参加面谈（德语或英语）

许多人失败于：
❌ RO 是"挂名"
❌ MLRO 无加密经验
❌ 面谈无法回答问题
❌ 不懂链上 AML
❌ 不懂风险管理
❌ 看不懂审计
仁港永胜唐生建议：

> **RO/MLRO 的选择比资本金更重要。**

我们可提供合规评估（Fit & Proper）+ 面谈训练。

实话五：资本金不是门槛，运营资金才是关键

根据 MiCA：

- 资本金 5–15 万欧元
- 但德国实际执行多为 **20–50 万欧元**
- 交易平台 25–45 万
- 托管业务可高达 **40–60 万欧元**

然而 BaFin 最关注的是：

> **1–2 年的运营资金是否足够？**

包括：

- 工资
- 技术
- 合规

- 稽核
- 外包
- 保险
- 法律
- 存证
- 监管费用

许多申请人资本金准备得很漂亮，但：

❌ 运营资金只够 3–6 个月
❌ 财务预测不现实
❌ 风险储备不足

这样绝对过不了。

实话六：不要幻想"用海外团队远程运营德国实体"

德国不是爱沙尼亚，也不是塞浦路斯。
德国监管明确要求：

- 德国本地人员
- 德国本地实体
- 德国本地董事
- 德国本地 AML 审查
- 德国本地运营责任人
- 德国本地 IT 负责人（外包亦需本地授权）

德国是欧盟最强调"实体化运营"的国家。

如果你试图：

❌ 用东南亚团队远程运营
❌ 用香港团队负责本地 AML
❌ 把技术全部放在海外
❌ 在德国只留一个"空壳办公室"

你会在最初审查时就被拒绝。

实话七：IT 是全申请中被补件最多的模块（占全补件 30%）

德国不断强调 IT 安全，包括：

- 私钥管理
- 多签
- HSM 安全模块
- 员工 RBAC
- 渗透测试
- 代码审计
- 灾备机制
- 数据备份
- 关键系统隔离
- 内网访问
- API 日志
- 链上监控

缺一项都可能触发补件。

仁港永胜唐生经验：

> **德国 IT 文件至少需 20–30 份，且不能套模板。**

实话八：RFI（补件）不是"问答"，而是"审讯"

许多申请人第一次申请德国 CASP 被吓到，因为 RFI 问题通常是：

- 需要写论文般解释
- 需要引用 AML 法规
- 需要画数据流图
- 需要画系统图
- 需要附流程文件
- 需要用"德国监管语言"回答

以下为真实示例：

问题：请解释贵公司如何按照 AMLD6 第 47 条与 KRITIS 信息安全条例执行客户风险监测流程。请附风险评分矩阵。

这不是简单回复的内容。

实话九：面谈环节是 90% 的失败点

许多人在面谈时被问到：

- "请解释您系统的私钥生命周期管理。"
- "请说明贵公司的风险模型如何进行压力测试。"
- "您如何识别混币器（Mixer）路径？"
- "请解释链上地址风险评分机制。"

如果回答不出：

❌ 面谈后即收到拒绝信
❌ 或收到"第三轮 RFI"（极难处理）

仁港永胜唐生可提供：

- 面谈训练
- RO 面谈准备
- MLRO 实战问答
- IT 面谈模拟
- 场景案例问答

实话十：必须提前设计"监管叙事"

BaFin 最看重：

> **"你为什么需要 CASP？你的业务如何降低风险？你如何保护德国用户？"**

监管叙事必须贯穿：

- 商业模式
- 组织结构
- 风险管理
- Safeguarding
- AML
- IT
- 审计
- 面谈回答

仁港永胜唐生会帮客户建立：

一致性的监管逻辑
一致性的文件逻辑
一致性的面谈逻辑

这是申请中至关重要的一环。

实话十一：过度宣传会导致反效果

许多申请人喜欢展示：

- 代币
- Roadmap
- 套餐型产品
- Web3 内容
- 收益分润
- Staking

这些都可能被 BaFin 误认为：

❌ 涉嫌提供高风险产品
❌ 或触发证券监管（FISG、WpIG）
❌ 或涉及禁止性业务

德国监管天然对 Web3 保持审慎态度。
稳健叙事远比"Web3 创新"更重要。

实话十二：德国 CASP 是全欧最难，但也是最值得的

德国的优势：

- 欧洲最大经济体
- 金融基础设施最强
- 与大型机构合作机会最多
- 监管认可度最高
- 护照后进入 30 国最顺畅
- 对银行级客户最友好

一句话：

> **若你能通过德国 MiCA-CASP，你将在全欧具备最强的合规地位。**

仁港永胜唐生：我们如何帮助客户提高成功率？

我们提供：

✅ 一、德国 MiCA-CASP 100+ 文件完整套装

- AML（完整 40+ 模块）
- IT 安全（20+ 文件）
- 风控
- Outsourcing
- Governance
- Safeguarding
- 交易监测（链上 + 链下）
- 数据流模型
- 商业模式说明
- 财务预测模型
- RFI 模板答复

✅ 二、监管沟通策略与叙事设计

- 构建监管一致性
- 规划商业模式风险节点
- 降低监管误解概率

✅ 三、RO/MLRO 面谈训练（最关键）

- 实战模拟
- 技术问答准备
- AML 案例演练
- IT 深度问题演练
- 董事会面谈辅导

✅ 四、补件（RFI）快速响应

- 将补件缩短 20–40% 审查周期
- 避免多轮补件
- 避免面谈后的二次补件

✅ 五、德国本地资源

- 德国本地董事
- 德国合规责任人
- 德国 AML 资源
- 德国 IT 安全顾问
- 德国律所合作

我们不是简单"提供文件"，而是：

> **从架构 → 文件 → 政策 → 面谈 → 审计 → 获批**
> **一站式交付。**

本章总结

德国 MiCA-CASP 是：

⚠ **最难申请的欧盟 CASP**
✓ **监管要求最完整**
✓ **补件最多**
✓ **面谈最深入**
✓ **对治理要求最高**
✓ **对 IT 最严格**
✓ **对 AML 最敏感**

但正因如此：

> **通过德国，就等于获得欧洲最高级别监管信用。**

如果你准备认真申请，仁港永胜唐生将为你提供完整、专业且可落地的成功方案。

第 20 章｜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（深度介绍版）

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

第一节｜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。

第二节｜全球合规服务版图（世界五区布局）

我们的业务覆盖：

一、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

二、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

三、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

四、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

第三节｜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

第四节｜仁港永胜提供的服务总览

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。

第五节｜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

第 20 章总结

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（示例）：

- 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。
