



# 仁港永胜

协助申请金融牌照及银行开户一站式服务



正直诚信  
恪守信用

地址：深圳市福田区福华三路卓越世纪中心1号楼1106  
网址：www.CNJRP.com 手机：15920002080

## 希腊 Greece (MiCA) 加密资产服务提供商 (CASP) 牌照常见问题 (FAQ 大全)

### Crypto-Asset Service Provider (CASP) under MiCA – Greece Version

本文由 仁港永胜 (香港) 有限公司 拟定, 并由 唐生 提供专业讲解。

适用于：计划在 希腊设立或落地 **MiCA-CASP** 实体, 并通过 MiCA 护照机制在欧盟 / EEA 30 国展业的项目方、家族办公室、交易平台、托管机构及 Web3/RWA 团队, 用于:

- 内部立项与股东决策
- 与投资人沟通希腊 CASP 方案
- 对接当地律师、会计师、托管与技术供应商
- 准备希腊监管申请材料 (申请 + 补件 + 面谈)

牌照名称: 希腊加密资产服务提供商牌照 Crypto-Asset Service Provider (CASP)

服务商: 仁港永胜 (香港) 有限公司

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

✅ 点击这里可以下载 PDF 文件: [关于仁港永胜](#)

## 第 1 章 | 基础概念与监管框架 (Q1–Q10)

### Q1: 什么是希腊 (Greece) MiCA 加密资产服务提供商 (CASP) ?

A:

在 MiCA (Regulation (EU) 2023/1114) 框架下,

**Crypto-Asset Service Provider (CASP, 加密资产服务提供商)** 是指在欧盟提供受监管加密资产服务的机构, 包括但不限于:

- 为第三方托管加密资产 (Custody & Safekeeping)
- 运营加密资产交易平台 (Trading Platform / Exchange)
- 代表客户执行加密资产订单
- 以自营方式进行交易 (Dealing on own account)
- 就加密资产提供投资建议
- 接收并传送加密资产交易指令
- 安排加密资产发行或销售等

在 希腊版 MiCA 实施 下, 取得 CASP 牌照的机构, 可在满足护照机制条件后, 在其他欧盟成员国提供同类服务。

### Q2: 在希腊, MiCA-CASP 的主要监管机构是哪一个?

A:

希腊 CASP 监管涉及两大主体 (视业务类型):

1. 希腊资本市场委员会 **Hellenic Capital Market Commission (HCMC)**
  - 负责证券、投资服务及 MiCA 下与资本市场性质类似的加密服务;
  - 很可能是 **主要 CASP 授权机构** (尤其是交易平台、投资类服务)。
2. 希腊央行 **Bank of Greece (BoG)**
  - 对支付服务、电子货币、部分托管和支付接口相关业务有监管职能;
  - 对“支付型 / 电子货币型”业务 + 加密资产场景可能共同参与审查。

实际项目中，一般由 HCMC 作为主导监管方，必要时与 BoG 协调。

- 你可以简单理解为：
- **HCMC**：类似 **SFC/BaFin** 的资本市场监管者
  - **BoG**：类似央行 + 支付监管者

---

### Q3：MiCA 在希腊大概何时开始全面适用？过渡期如何？

**A：**  
按欧盟 MiCA 时间表：

- 稳定币部分（ART / EMT）自 **2024 年中** 起逐步实施；
- CASP 授权部分自 **2025 年底前后** 全面生效（各国会有过渡细节）；

对于已经在希腊以本地法规注册的加密服务提供者（例如之前在本地“加密注册册”登记的 VASP / CASP），可能享有：

- **最长 18 个月左右过渡期**（具体由希腊本地实施法落地确认）；
- 在过渡期内，必须根据 MiCA 要求 **升级为 CASP 正式牌照** 或退出相关业务。

对“新申请人”而言：  
– 建议不再按旧制度去设计商业模式，而直接按 **MiCA + 希腊本地落地法** 规划。

---

### Q4：选择希腊作为 MiCA-CASP 主体，与德国 / 法国 / 立陶宛 / 马耳他相比，有什么特点？

**A：**  
简明对比可以这样理解（只给你“大轮廓”用于前期判断）：

- **德国 BaFin**：审查极深、文件要求最高、成本高、但“含金量”最高；
- **法国 AMF**：对托管 / Wallet / Safeguarding / 外包特别严格；
- **立陶宛 / 马耳他 / 爱沙尼亚**：灵活、FinTech 生态友好、适合轻资产团队；
- **希腊 HCMC**：
  - 近年积极推动资本市场与 FinTech 发展；
  - 在欧盟框架下趋向与 ESMA / EBA 协调一致；
  - 相比“传统大国”，在商业环境和成本上更有一定空间；
  - 对治理、AML、风险管治仍有较高要求。

如果你的业务是：

- 偏 **投资型 / 资产管理 / 交易平台**，同时希望成本与监管强度在“中间位置”——  
**希腊是一个值得认真评估的 MiCA 主体选项。**

---

### Q5：在希腊设立 CASP 实体，一般采用什么公司形式？

**A：**  
常见法律形式包括：

- **Société Anonyme (S.A., 希腊股份有限公司)**
- 或其他适合监管机构要求的资本性公司形式

通常建议采用 **S.A. 型股份公司**：

- 便于引入股东 / 投资者；
- 便于满足最低资本金要求；
- 易于与其他欧盟监管框架对接（如 AIFM、MiFID firm 结构）。

仁港永胜在设计结构时，会结合：

- 股东结构（集团 vs SPV）
- 实质运营安排

- 税务与资金安排

帮你选最合适的公司形式。

---

## Q6: MiCA-CASP 在希腊需要最低注册资本金吗？具体是多少？

A:

MiCA 对不同 CASP 服务类型设定了 **最低初始资本 (Initial Capital)** 区间，例如：

- 接收与传送 / 投资建议类：约 €50,000 起
- 执行订单 / 经营平台等：约 €125,000 左右
- 自营交易 / 托管：约 €150,000–€750,000 区间（视服务复杂度而定）

在希腊本地落地时，HCMC/BoG 可能结合：

- MiCA 规定的最低门槛
- 本地公司法对 S.A. 的资本要求
- 风险状况与业务规模

最终确定你这家 CASP 的：

**监管认可资本水平 (Regulatory Capital Level)**

实务操作中，我们会在 **商业计划书 + 风险分析 + 财务预测** 中，把“资本金合理性”写清楚，让监管更易接受。

---

## Q7: 在希腊持有 MiCA-CASP 牌照，可以在整个欧盟展业吗？

A: 可以。

一旦在希腊获得正式 **MiCA CASP** 授权，就可以通过 **MiCA 护照机制 (Passporting)**：

- 通知希腊监管机构 (HCMC/BoG)；
- 再由其通知其他欧盟/EEA 国家监管机构；
- 在其他国家 **无需重新取牌**，只需完成通报程序即可提供相同类别服务。

这也是 MiCA 最大的吸引力之一：

**“在一个国获牌，在 30 国展业”。**

---

## Q8: MiCA-CASP 与传统 MiFID 投资公司 / EMI / PI 有什么区别？

A:

简单对照：

- **MiFID firm (投资公司)**：监管对象是“金融工具 / 证券 / 衍生品”，
- **EMI (电子货币机构) / PI (支付机构)**：监管对象是“支付服务 / 电子货币”；
- **MiCA CASP**：监管对象是“**不属于 MiFID 金融工具的加密资产**”以及围绕这些加密资产提供的服务。

在希腊与其他欧盟国家一样，

会出现一类机构：**同时持有 MiFID + MiCA + 支付牌照**，形成多牌照结构。

---

## Q9: 在希腊申请 CASP，项目方需要具备怎样的基本条件？（高维度版）

A:

可以用“五大模块”来理解：

1. **实体条件 (Entity Level)**
  - 在希腊注册合适形式的公司
  - 实质运营：本地办公室 / 员工 / 管理层
2. **股东与董事 (Shareholders & Board)**
  - 适当人选 (Fit & Proper)，无严重不良记录
  - 有真实管理能力，而非挂名
3. **业务与风险结构 (Business & Risk)**

- 清晰的商业模式
- 有可行的盈利逻辑
- 完整风险与控制框架

#### 4. 技术与钱包 (Tech & Wallet)

- 钱包架构与私钥管理符合 MiCA + 希腊监管逻辑
- 有灾备、风控、审计能力

#### 5. 合规与 AML (Compliance & AML)

- AML/KYC 政策及实施
- MLRO、合规负责人配置
- 系统与人相结合的监控方案

这些模块你在德国/法国/芬兰/奥地利项目里已经非常熟悉——

希腊版本逻辑一致，只是 **本地监管口径、文件细节、语言表达** 有差异。

---

### Q10：对考虑希腊 MiCA-CASP 的项目方，仁港永胜的总体建议是什么？（战略层面）

A：

我们会先帮你做一个 **高维度三步评估**：

#### 1. 是否真的适合选择希腊作为 MiCA 主体？

- 股东背景 / 项目资源 / 团队语言 / 目标市场
- 与德国 / 法国 / 立陶宛 / 马耳他 / 奥地利相比的综合优劣

#### 2. 若选择希腊，适合哪种“服务组合”？

- 只做托管？
- 托管 + 交易？
- 加密支付？
- 投资建议 + 经纪？

#### 3. 集团整体结构如何配合？

- 总部在哪里？
- 技术团队在哪里？
- 如何设计“税务 + 资金 + 风险 + 合规”的最优平衡？

我们并不会“只帮你填材料”，而是从 **项目架构 + 商业逻辑 + 监管预期** 三个维度一起优化。

---

## 第 2 章 | 希腊版 MiCA 适用范围与业务模式 (Q11–Q20)

---

### Q11：在希腊，哪些类型的加密业务必须申请 MiCA-CASP 牌照？

A：

典型必须持牌的业务包括（举例）：

1. 托管 / 保管客户加密资产
2. 运营加密资产交易平台 (CEX 类)
3. 撮合交易、代表客户执行加密资产订单
4. 经纪 / 中介服务 (接收与传送指令)
5. 自营交易 (如做市商)
6. 就加密资产提供投资建议
7. 承销 / 分销某些类型加密资产 (非 MiFID 金融工具)

如果你的业务中存在：“帮客户管理私钥 / 代持资产 / 代为交易 / 运营撮合平台”

基本可以直接判定需要 CASP 牌照。

---

### Q12：在希腊，如果只是发行项目 Token，是不是一定要 MiCA-CASP 牌照？

A：

要分清两个角色：

#### 1. 发行人 (Issuer)

- 发行 Utility Token / ART / EMT 等
- 是否纳入 MiCA 下的 Crypto-Asset / ART / EMT 类别
- 需要遵守白皮书披露、责任等规则

#### 2. 服务提供商 (CASP)

- 为他人提供托管 / 交易 / 经纪 / 平台等服务

如果你仅是 **单纯发行自家 Token，且不为第三方提供服务**，  
不一定需要 CASP 牌照；  
但如果你：

- 为其他项目方提供发行服务；
- 为投资人托管 Token；
- 为他人撮合、交易 Token；

那就已经进入 CASP 范畴。

---

### Q13：在希腊做纯技术开发（写智能合约 / 提供钱包 SDK），需要 CASP 吗？

A：

若你只是：

- 提供开源钱包 SDK；
- 提供智能合约开发服务；
- 不碰客户资产、不托管、不撮合、不经纪；

通常 **不属于 CASP**。

但必须小心以下“灰区”：

- **托管型钱包服务 (Custodial Wallet)**：就算挂名是“技术服务”，只要实际你控制了私钥 → 属于托管类 CASP；
  - **运营前端 + 聚合 DeFi 流动性 + 帮用户路由交易**：实际可能被认定为经纪 / 平台类 CASP。
- 

### Q14：在希腊，如果只做 OTC 场外撮合（介绍双方交易），算不算 CASP？

A：

要看你扮演的角色：

- 只是“介绍买卖双方认识”，不收取按交易量计费的佣金，不参与价格撮合 → 可能不被视为 CASP；
- 一旦你：
  - 为客户提供报价；
  - 收取点差；
  - 代为撮合；
  - 代为执行订单；那就 **非常接近 CASP 经纪 / 自营 / 平台服务**。

实务中，绝大多数专业 OTC 业务都会被纳入 MiCA-CASP 体系。

---

### Q15：在希腊，如果只做“技术托管”（例如 HSM、MPC 技术服务商），需要 CASP 吗？

A：

关键看：

- 你是否有“独立控制客户资产”的可能性？

如果：

- 你仅提供加密模块 / 硬件设备 / 软件，不拥有密钥片的控制权；
- 最终签名权、迁移权都属于受监管 CASP 客户；

那么你是 **技术服务商**，而不是 CASP。

但如果技术结构设计为：

- 你持有关键一片 MPC 密钥，无你就无法转账；
- 或你可以单方操作链上资产；

那监管会倾向认为你已经承担了“托管 + 控制”角色，极有可能被视为 **实际 CASP**。

---

#### **Q16：在希腊，如果只是提供加密行情 / 研究报告 / 媒体内容，是否需要 CASP 牌照？**

**A：**

一般不会。

纯资讯、媒体、研报、数据服务（不为个别客户提供“一对一建议”）通常不纳入 CASP 范畴。

但若：

- 你针对单一客户提出“买哪种 Token、什么时候买卖”的个别化建议；
- 并收取基于资产规模或业绩的报酬；

那么可能被认定为 **就加密资产提供投资建议服务** → 需要 CASP。

---

#### **Q17：在希腊，做 DeFi 前端聚合器 / 路由器，会不会被 MiCA 认定为 CASP？**

**A：**

这是 MiCA 下的热点问题之一。

法国、德国及 ESMA 目前的倾向是：“看你 **是否在链上行为中扮演中介与控制角色**”。

如果你在希腊运营的 DeFi 前端具备：

- 为用户构造交易；
- 持有用户私钥或有权限代签名；
- 为用户提供一站式路由、撮合及执行；

监管可能认为你属于：

- 接收与传送指令
- 或执行订单
- 或运营平台

进而被视为 CASP。

如果你只是提供：

- 开源 UI；
- 不托管、不控制、不执行，只是引导用户去链上与智能合约交互；

被纳入 CASP 的风险就显著降低。

---

#### **Q18：在希腊，若只面对“专业投资者 / 合格投资者”，是否可以豁免 MiCA？**

**A：**

MiCA 不以“客户类型”作为主要豁免标准。

无论你面对的是：

- 零售客户；
- 专业投资者；
- 家族办公室；

只要你提供的是受监管的加密资产服务 → 就需遵守 MiCA 及希腊本地落地法律。

“只面对专业投资者”最多只能在：

- 合规要求细节
- 产品适合性评估程度
- 信息披露方式

上稍有灵活，并不构成“无须取牌”的理由。

---

### Q19：在希腊，如果我的业务同时涉及 MiFID 金融工具（如证券型代币）和非 MiFID 加密资产，如何监管划分？

**A：**

典型场景：

– 同一平台上既有“证券型代币（Security Token）”又有纯加密 Token。

监管框架通常是：

- **证券型代币（MiFID Instrument）** → 适用 MiFID II + 希腊资本市场法，由 HCMC 以“投资公司 / MTF / OTF”等框架监管；
- **普通加密资产（Non-MiFID Crypto-Assets）** → 属于 MiCA 范畴，由 HCMC 以 CASP 身份监管。

实务中可能出现：

- 同一个集团下：
  - A 公司：MiFID 投资公司；
  - B 公司：MiCA-CASP；
- 或同一实体同时获得多重许可（监管会更严格）。

结构设计要非常小心，避免“混用客户资产”、“业务边界模糊”。

---

### Q20：仁港永胜如何帮助项目判断：我的希腊业务是否落入 CASP 范畴？

**A：**

我们通常会做一个 **“MiCA 适用性 Mapping Workshop”**，用一套标准问题清单帮你梳理：

- 是否托管 / 控制他人私钥或资产？
- 是否为客户撮合交易、执行订单或做自营？
- 是否为客户提供个别化加密资产投资建议？
- 是否向公众开放，或仅内部使用？
- 是否针对欧盟居民 / 希腊本地市场？
- 是否已触及 MiFID / EMD2 / PSD2 / AIFMD 等其他框架？

最后我们会输出一份：

- 《希腊 **MiCA-CASP** 适用性评估备忘录》
- 指明：哪些部分 **必须取牌**、哪些部分 **可优化架构**、哪些部分 **可外包或削减风险**。

---

## 第 3 章 | 希腊 CASP 申请流程、时间表与监管交互（Q21–Q40）

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

### Q21：在希腊申请 MiCA-CASP 牌照的流程是什么？（高层级 6 步法）

**A：** 希腊 HCMC + MiCA 标准流程可总结为 6 步：

#### 第 1 步 | Pre-Filing（非正式沟通阶段）

- 与 HCMC（希腊资本市场委员会）进行前期沟通
- 确认服务类型、监管路径、资本金预期
- 讨论是否需要同时与希腊央行（BoG）沟通（如涉及支付/托管）

#### 第 2 步 | 设立希腊实体 + 本地实质（Substance）规划

- 设立 S.A. 法人
- 任命董事、MLRO、合规总监、CISO、CTO
- 租赁办公室、聘用本地员工
- 建立内部控制框架

第 3 步 | 准备申请材料（核心阶段）

仁港永胜会协助准备：

- 商业计划书（监管版）
- AML/CFT 政策
- Wallet & Custody Policy
- Outsourcing Policy
- Risk Management Framework
- Safeguarding 方案
- 治理结构（Board Charter）
- IT & Cybersecurity Framework

最终组成 200–600 页完整申请包。

第 4 步 | 正式提交（Submission）

- 向 HCMC 正式提交 CASP 授权申请
- 支付官方申请费用
- HCMC 安排受理并进入审查流程

第 5 步 | 补件（RFI）与面谈（Hearing）

HCMC 会发出：

- RFI（Request for Information）补件
- 现场/视频面谈（Hearing）

此阶段对申请成败影响最大。

第 6 步 | 批准（Authorization）+ 护照（Passporting）

- 获得 CASP 授权
- 向 HCMC 提交护照通报（Passporting Notification）
- 在 EU/EEA 30 国展业

Q22：在希腊提交 MiCA-CASP 申请，一般需要准备多久？

A：一般为 2–4 个月。

细分为：

阶段	时间
架构设计 + 实质安排	2–4 周
文件编写（仁港永胜）	4–8 周
内部审查 + 翻译（如需）	1–2 周

如果团队已有完善 AML / Wallet / 技术文档，时长可缩短。

Q23：提交后，希腊监管审批需要多久？

A：根据 MiCA 统一框架，通常为 3–6 个月。

但真实时长会因以下因素波动：

- 补件数量多 → 时间延长
- 技术架构复杂（托管/交易平台） → 面谈增加
- 董事适当人选（Fit & Proper）审查拖延 → 时间延长



- 外包结构复杂 → 需额外沟通

仁港永胜通常帮助客户把申请材料做到“接近零补件”，可显著缩短审查周期。

---

## Q24：希腊监管机关会不会像法国 AMF 或德国 BaFin 那样发非常多补件？

**A：会，但强度略低于法国 / 德国。**

压力程度大致排序：

德国 BaFin > 法国 AMF ≥ 荷兰 AFM > 希腊 HCMC ≥ 奥地利 FMA > 立陶宛

但希腊也绝非“宽松”，尤其在以下方面会深入问：

- 托管与密钥管理（MPC / HSM / 冷热钱包架构）
  - Outsourcing（尤其外包到非欧盟的服务）
  - 实质运营（Substance）
  - 董事履历与适当人选
  - AML/CFT 程序
  - Safeguarding（客户资产隔离）
- 

## Q25：在希腊 CASP 申请中，哪些文件最容易被 HCMC 要求补件？

补件热点主要集中在：

1. **Wallet & Key Management**（私钥管理）
2. **IT & Cybersecurity**（网络安全）
3. **Outsourcing Arrangements**（外包）
4. **Safeguarding** 客户资产方案
5. 董事与高管适当人选（Fit & Proper）
6. 交易平台架构 & 流动性管理方案

仁港永胜会提前为每个高风险文件准备 **RFI 回答模板**，确保补件阶段从容应对。

---

## Q26：希腊监管会对 CASP 申请人进行面谈（Hearing）吗？

**A：会，而且越来越常态化。**

面谈通常涉及：

- CEO —— 治理、战略、合规文化
- CTO —— 技术、钱包、安全
- MLRO —— AML/KYC/制裁
- CISO —— 网络安全与数据管理
- Chief Risk Officer —— 风险评估与应对框架

面谈问题往往技术与合规深度兼具，仁港永胜会提前：

- 提供完整 **面谈脚本（100–300 问）**
- 组织模拟实战面谈

确保团队“回答即专业”“陈述即通过”。

---

## Q27：在希腊申请 CASP，必须有本地实体与人员吗？（Substance 要求）

**A：是的。**

与德国、法国一样，希腊明确要求：

**必须具备：**

- 本地董事至少 1–2 人

- 本地 MLRO 或 Deputy MLRO
- 本地合规 / 风险职能人员
- 实质办公室（非虚拟地址）
- 可展示的最低运营能力

**不接受：**

- 完全虚拟运营
- 所有关键岗位位于境外
- 由母公司实际控制所有业务

这是希腊实施 MiCA 的关键点之一。

---

## **Q28：若集团总部在中国/香港/新加坡，是否会影响希腊 CASP 申请？**

**A：不会直接影响，但会增加监管关注度。**

关注点主要包括：

- 是否存在“影子控制人”
- 集团是否对关键运营施压
- 数据是否保留在欧盟
- 决策链条是否真正发生在希腊实体内
- 境外母公司是否会干预 Safeguarding 或客户资产管理

仁港永胜会为此设计：

- 双实体治理结构
- 决策矩阵（Decision Matrix）
- 运营隔离方案

确保监管“看得懂、接受、可监督”。

---

## **Q29：在希腊申请 CASP，是否可以把 IT / 安全 / 风控等外包给非欧盟公司？**

**A：可以，但限制严格。**

关键条件：

- 外包不能导致 CASP “失去关键职能控制权”
- 管理层必须能随时审查外包方
- 必须有退出机制（Exit Plan）
- 数据转移必须符合 GDPR
- 若外包到第三国（如香港/新加坡），需额外文件证明“无需等效 Adequacy”

我们会为客户编写：

- Outsourcing Register
- Outsourcing Risk Assessment
- Data Transfer Impact Assessment (DTIA)
- SLA / KPI / Escalation 流程图

确保监管认可。

---

## **Q30：希腊 CASP 申请中，哪类服务会受到监管最严格审查？**

排名如下：

### **托管（Custody & Safekeeping）**

- 私钥管理

- 多签/MPC
- 冷热钱包区隔
- 访问控制
- 资产隔离 (Safeguarding)

## 交易平台 (Operating a Trading Platform)

- 撮合引擎
- 流动性冲突
- 交易监控 (Market Abuse Detection)
- API 控制
- 内部账户操控风险

## 执行订单 (Execution) 和自营 (Dealing on own account)

- 最佳执行 (Best Execution)
- 流动性来源
- 利益冲突管理

---

## Q31: 在希腊申请 CASP 时, 是否需要提交审计报告或财务预测?

需要。

包括:

- 3 年财务预测
- 资本充足性评估
- 审计师声明或愿意合作信
- 盈利模型与费用结构说明

财务模型必须“能支持监管要求”, 不可过于理想化。

---

## Q32: 申请希腊 CASP 的官方语言是什么? 材料需用希腊语吗?

A: 英语通常可接受, 但可能要求部分文件提供希腊语版本。

一般实践:

- 主要申请文件英语版即可
- 公司章程、执照、董事文件等需希腊语
- 与监管沟通可能需双语支持

仁港永胜会提供:

- 英文监管材料
- 希腊语翻译协调
- 与希腊律师联合作业

---

## Q33: 监管在审查时最看重哪三项? (希腊版“三大必看点”)

### 1) 治理结构 (Governance)

董事会 = 真正能控制公司, 而非“挂名”。

### 2) 资产保护 (Safeguarding)

客户资产必须做到:

- 完全隔离

- 可审计
- 可证明你的员工无法单方挪用资产

### 3) 外包与运营风险 (Outsourcing & Operational Risks)

尤其涉及：

- 钱包安全
- 审计跟踪
- 数据流转
- 第三国外包

---

### Q34：希腊监管是否关心集团结构？跨国集团会不会有风险？

**A：会，非常关注。**

重点包括：

- 股东穿透 (Ultimate Beneficial Owner)
- 是否存在复杂结构
- 是否避税或监管套利
- 母公司监管情况
- 母公司财务稳定性
- 母公司的合规文化

我们会为集团准备：

- 股权穿透图
- 控股结构说明书
- 集团合规声明 (Compliance Attestation)

---

### Q35：在希腊 CASP 申请中，公司章程是否需要修改？

**A：多数情况下需要。**

章程需体现：

- 业务范围符合 MiCA 要求
- 治理机制满足 HCMC 监管逻辑
- 董事权责清晰
- 允许设立监督职能 (Audit / Risk / Compliance)

我们会提供监管兼容章程模板。

---

### Q36：在希腊申请 CASP 时，公司必须聘请哪些“关键职能人员”？

最低配置：

- **CEO / Managing Director**
- **Chief Compliance Officer (CCO)**
- **MLRO** (反洗钱负责人)
- **CTO** (技术负责人)
- **CISO** (安全负责人)
- **Risk Manager** (若业务复杂)

这些人员必须有：

- 真实履历
- 可证明经验

- 可参与监管面谈

不可挂名。

---

## Q37：关键岗位是否必须在希腊当地居住？

**A：**绝大多数情况下需要至少部分关键岗位在希腊。

- MLRO 必须在希腊
- 合规负责人一般必须在希腊
- CEO 通常需常驻欧洲（最好在希腊）
- CTO/CISO 可部分远程，但需明确监管可监督性

若团队全部海外，申请通过率会大幅下降。

---

## Q38：设立和运营希腊 CASP 的预计成本是多少？

成本由 3 部分构成：

### 1) 监管成本 (Regulatory Cost)

- 官方申请费用
- 年费
- 审计费

### 2) 实质成本 (Substance Cost)

- 本地人员薪酬
- 办公室 rent
- 运营支出

### 3) 咨询与架构成本 (由仁港永胜协助)

- 文件制作
- RFI 支持
- 面谈准备
- IT/Wallet 架构合规咨询

整体预算水平约：

**€150,000 – €450,000/年**（视服务类型与规模而定）

---

## Q39：是否可以在未完全准备好文件的情况下先行提交申请？

不建议。

希腊监管不接受“占位式申请”，若材料不完整：

- 不会受理
- 会直接退件
- 会影响后续评价
- 可能导致项目时间延误 3–6 个月

仁港永胜统一采用“一次性提交接近成品”模式，减少补件与退件概率。

---

## Q40：仁港永胜在希腊 CASP 申请流程中提供哪些具体服务？

包括但不限于：

- 业务合规设计 (Business Mapping)

- 钱包架构审查 (Wallet Architecture Review)
- 治理结构设计 (Governance Design)
- 监管材料制作 (MiCA Full Pack)
- 外包 + GDPR 合规方案
- AML/KYC 完整体系搭建
- 与希腊监管沟通对接
- 面谈脚本与模拟面谈 (Mock Hearing)
- 护照通报与跨境展业规划

实操性与落地能力是仁港永胜最大的优势。

---

## 第 4 章 | 治理结构、股东与董事适当人选 (Fit & Proper) (Q41–Q80 | 希腊版)

本文由 仁港永胜 (香港) 有限公司 拟定, 并由 唐生 提供专业讲解。  
(适用于: 计划在希腊设立 MiCA-CASP 实体, 并面向欧盟 30 国展业的项目方。)

---

### Q41: 希腊 CASP 的治理总体要求是什么? 监管最关注什么?

A: 可以用一句话概括:

“谁在真正管理这家公司? 他们是否可靠、专业、可被监管?”

具体来说, 希腊 HCMC 重点关注三点:

1. 清晰稳定的治理架构 (Governance Framework)
  2. 适当人选 (Fit & Proper) —— 股东、董事、高管的诚信 & 能力
  3. 本地实质管理 (Local Mind & Management) —— 不是“空壳公司 + 海外遥控”。
- 

### Q42: 希腊 CASP 至少需要多少名董事? 有没有最低人数要求?

A: 一般建议:

- 至少 2 名董事 (Directors);
- 对大中型平台, 最好 3 名以上, 以便分工治理 (风险、合规、技术等);
- 董事必须是 自然人, 不能全是法人董事。

实践上:

“1 人董事会 + 顾问团队”在希腊 MiCA 审查下风险非常高, 不建议采用。

---

### Q43: 董事是否必须居住在希腊? 可以是其他欧盟国家吗?

A: 实务口径通常是:

- 至少 1 名核心董事 / 高管 在希腊常驻;
- 其他董事可以居住在欧盟其他成员国;
- 若全部核心管理层都在欧盟以外 (香港/新加坡/中国大陆), 通过率显著下降。

监管希望看到的, 是 希腊本地确实有人在“亲手管事”。

---

### Q44: 什么是“适当人选 (Fit & Proper)”审核? 主要看哪三点?

A: Fit & Proper 一般分为三大块:

1. 品行诚信 (Honesty & Integrity)
  - 无严重刑事犯罪

- 无金融诈骗、洗钱、恐怖融资记录
- 无重大监管处罚

## 2. 专业能力 (Competence)

- 有足够行业经验
- 能理解 CASP 业务模式与风险
- 面谈能回答问题

## 3. 财务稳健 (Financial Soundness)

- 无严重破产案件 (或已妥善解释)
- 无大额违约、税务黑历史

希腊 HCMC 会通过问卷、证明、面谈等方式综合判断。

---

## Q45: 在希腊 CASP 中, “关键岗位 (Key Function Holders)”有哪些?

通常包括:

- **CEO / General Manager** ——全面负责经营管理;
- **Board of Directors** ——决策与监督;
- **Compliance Officer** (合规负责人);
- **MLRO** (反洗钱报告官);
- **Risk Manager** (风险负责人);
- **CTO / CISO** (技术 / 安全负责人);
- **Head of Custody / Safeguarding** (如有托管服务)。

这些人都属于 **Fit & Proper** 审查范围。

---

## Q46: 股东 (Shareholders) 也要做 Fit & Proper 吗? 持股多少会被审查?

**A:** 会的, 尤其是:

- 直接或间接持有 **≥10% 股权或投票权** 的股东;
- 有“重大影响 (Significant Influence)”的股东 (即使持股 <10%)。

需要审查的内容包括:

- 股东背景与司法记录;
  - 资金来源 (Source of Funds & Source of Wealth);
  - 是否来自高风险司法辖区;
  - 过去是否涉及严重合规或监管事件。
- 

## Q47: 适当人选 (董事/高管/股东) 需要提交哪些材料?

典型材料包括:

- 详细简历 (CV);
- 护照 / 身份证复印件;
- 近期无犯罪记录证明;
- 破产/清盘记录声明 (如有);
- 过往任职公司列表与职位证明;
- 学历、专业资格 (如金融/法律/IT/FRM/CFA 等);
- 监管问卷 (Fit & Proper Questionnaire);
- 股东资金来源证明 (银行证明/报税单/股权交易协议等)。

不同角色, 材料清单略有差异, 但整体逻辑相同:

“这个人是谁? 从哪里来? 靠谱么?”

---

## Q48：如果董事曾经担任一家破产公司的董事，会被直接拒绝吗？

**A：** 不一定。

关键看：

- 破产是否与欺诈、不当管理、洗钱有关；
- 是否如实披露，而不是刻意隐瞒；
- 是否能提供合理商业背景说明（如宏观经济原因、行业剧变等）；
- 是否在破产过程中被法院或监管点名为“失职”。

**“有问题 + 坦诚说明 + 有合理解释”**

往往比“故意不提 + 被监管查出来”安全得多。

---

## Q49：希腊 CASP 的 CEO / 总经理需要具备什么背景更容易获批？

建议配置：

- 在银行 / 证券 / 支付 / 金融机构任职管理层经历；
- 熟悉欧盟金融监管框架（MiFID / MiCA / AMLD / PSD2 等）；
- 对加密资产、钱包、交易结构有基本理解；
- 能在面谈中清楚解释商业模式与风险控制。

**“纯技术背景 + 零金融/合规经验”的 CEO 组合并不理想。**

如果团队是技术主导，可考虑：

- 技术合伙人做 CTO；
  - 招聘一位有金融监管经验的 CEO 或 COO 做对外窗口。
- 

## Q50：合规负责人（Compliance Officer）与 MLRO 可以是同一个人吗？

**A：** 小型 CASP：可以由同一人兼任，但要证明其有：

- 足够时间和资源；
- 不被业务线干扰；
- 对 AML 和一般合规都具备能力。

中大型平台 / 托管机构：

**最好设立独立 Compliance Officer + 独立 MLRO，监管会更放心。**

---

## Q51：MLRO（反洗钱报告官）在希腊 CASP 中扮演什么角色？

MLRO 是 AML/CFT 的核心人物，职责包括：

- 负责日常 AML/KYC 政策落实；
- 监控链上与链下可疑交易；
- 决定何时提交可疑交易报告（STR/SAR）；
- 向董事会汇报 AML 风险状况；
- 与希腊金融情报部门（FIU）沟通。

监管通常会对 MLRO 进行 **单独问答/面谈**，测试其专业程度。

---

## Q52：CTO / CISO 是否也会被视为“适当人选”审查对象？

**A：** 是的，尤其在以下情况：

- 提供托管服务（Custody）；
- 经营加密资产交易平台（Exchange）；
- 大量使用外包 IT 服务 / 云服务。



监管会问 CTO / CISO：

- 钱包架构、私钥保护方案；
- 冷/热钱包比例；
- DDoS、防火墙、日志系统设计；
- 渗透测试 / 漏洞管理流程；
- 外包技术管理与应急预案。

技术负责人回答水平会直接影响获牌成功率。

---

## Q53：是否可以聘请“名义董事（Nominee Director）”来满足本地要求？

**A：** 理论上可以设董事，但“挂名董事 + 无实质管理”是监管最不喜欢的情況。

HCMC 通常会看：

- 董事是否参与决策（有无会议纪要、签署记录）；
- 是否参与监管沟通；
- 面谈中是否能回答关键问题。

若被识别为“纯挂名”，风险包括：

- 强制要求更换董事；
  - 拒绝当前申请；
  - 将来对该申请人/股东留下负面印象。
- 

## Q54：家族成员共同担任董事 / 股东会有问题吗？

**A：** 家族成员参与不是问题，问题在于：

- 是否因此削弱治理独立性；
- 是否影响内部制衡；
- AML / 风险 / 合规岗位是否也完全由家族掌控。

建议：

- 最核心监管职能（合规 / AML / 风控）中至少引入一位非家族成员的专业人士；
  - 利益冲突政策（Conflict of Interest Policy）中要专门提及家族结构的冲突管理。
- 

## Q55：董事会需要设立哪些委员会（Committee）比较合规？

建议配置：

- 风险委员会（Risk Committee）
- 合规与 AML 委员会（Compliance & AML Committee）
- IT/安全委员会（IT & Security Committee）
- 如规模较大：审计委员会（Audit Committee）

这些委员会可以由董事 + 高管组成，定期召开会议，并留存：

- 议程（Agenda）
- 会议纪要（Minutes）
- 决议记录（Resolutions）

为将来应对监管检查提供证据。

---

## Q56：希腊 CASP 董事会会议频率有什么期待标准？

建议：

- 董事会至少 **季度会议 (Quarterly)**；
- 年度审查：风险报告、AML 报告、外包报告、IT 安全报告；
- 重大事件发生（黑客攻击、大规模系统故障、监管函件）时，立即召开临时会议。

申请文件中可附：

- **预期年度会议时间表**
- **典型会议议程样本**

---

## Q57：如何向 HCMC 证明“董事会是真正在管事”？

可通过以下“证据组合”：

1. 董事会会议纪要体现：
  - 讨论风险、合规、IT、安全、客户资产等主题；
  - 审阅并批准关键政策/报告。
2. 提供董事与高管间的沟通记录样本（如 Board Pack 示例）。
3. 将董事的职责写入：
  - Board Charter（董事会章程）
  - 职责说明书（Role Description）。

越能呈现“实质治理”，越利于获批。

---

## Q58：股东结构复杂（多层 SPV / 境外信托）会影响 CASP 审查吗？

**A：** 会增加审查难度，但不是绝对否决。

关键是：

- 是否可以穿透到最终实益拥有人（UBO）；
- 是否能提供完整的股权链文件；
- 是否涉及高风险司法辖区或制裁对象；
- 是否存在“影子控制人”。

我们会协助客户制作：

- **股权穿透图 (Shareholding Transparency Chart)**
- **控制结构说明书 (Control Structure Memo)**

向监管说明清楚“谁在后面”。

---

## Q59：如何设计股东 + 董事组合，更有利于希腊 CASP 审查？

实务建议：

- 股东层：
  - 1-2 个控股股东（集团或家族），结构透明；
  - 不要过多小股东造成决策混乱；
- 董事层：
  - 至少 1 名具有欧盟金融监管经验的人；
  - 至少 1 名懂加密技术 / 钱包的人；
  - 至少 1 名懂风险 / 合规的人；

**避免：** 董事会成员全部来自同一背景（全技术、全投行、全家族）。

---

## Q60：集团总部如何参与治理，而又不被视为“完全遥控希腊实体”？

可以采用“**集团指导 + 本地自主**”模式：

- 集团制定：Global Policies & Standards；
- 希腊实体制定：Local Addendum，本地化实施细则；
- 集团派代表进入董事会，但不能掌控全部决策；
- 关键运营决策必须由希腊实体董事会审批。

申请材料中要清楚解释：

- 集团层级与希腊实体之间的权责分工；
- 如何确保希腊实体对本地客户和监管“独立负责”。

---

## Q61：高管是否可以兼职其他公司？监管如何看“多重职位（Multiple Roles）”？

A：可以，但需满足：

- 有足够时间履职（Time Commitment）；
- 不在直接竞争对手担任关键职务；
- 无利益冲突；
- 对关键岗位（如 MLRO/Compliance）最好 减少外部兼职。

申请资料中通常需要申报：

- 候选人目前所有职务；
- 每周为每个职位投入的大约工时。

---

## Q62：能否由顾问（Consultant）担任关键岗位，例如合规、MLRO？

A：监管允许使用外部顾问，但 不能代替内部关键岗位。

即：

- 可以聘请外部合规顾问协助起草文件、搭建制度；
- 但最终签名的 MLRO / Compliance Officer 必须是 公司内部指定的人，对监管负责。

“完全外包合规职能” 是非常大的扣分项。

---

## Q63：利益冲突（Conflict of Interest）在治理中如何体现？

你需要：

1. 有书面 **Conflict of Interest Policy**；
2. 列出可能的冲突场景：
  - 董事同时在供应商任职；
  - 家族成员控制关键岗位；
  - 股东既是平台大客户；
3. 确立机制：
  - 披露（Disclosure）
  - 回避（Recusal）
  - 决议记录中标注某人因利益冲突未参与表决。

监管会抽查实际案例。

---

## Q64：如果未来更换董事 / 高管，需要重新报批吗？

A：通常对于关键岗位（如 CEO、MLRO、Compliance Officer、Risk Manager）：

- 需要 事先或即时通知 HCMC（视具体实施法条款）；
- 提交新人的 Fit & Proper 材料；
- 监管有权拒绝某个人选。

频繁更换关键职务，会引起监管额外关注。

---

## Q65：希腊 CASP 是否需要设立内部审计（Internal Audit）职能？

**A：** 取决于规模，但监管倾向于：

- 中大型 CASP：必须有独立内部审计功能；
- 小型 CASP：可外包部分审计工作，但需要“负责内部审核协调的人”。

内部审计覆盖：

- AML 流程
  - 钱包与 IT 控制
  - Outsourcing 管理
  - 风险管理框架
  - 董事会治理运作情况
- 

## Q66：董事 / 高管是否需要参加持续合规培训？

**A：** 强烈建议，也有助于审查：

- 上任初期：一套系统性的“MiCA + 希腊本地法规入职培训”；
- 每年至少一次：AML / 合规 / 风险 / IT 安全培训。

培训记录（时间、参与人、内容）可以作为“良好治理文化”的证据。

---

## Q67：监管如何看待“影子控制人（Shadow Controller）”？

**A：** 影子控制人一般指：

- 实际掌控公司经营，但在法律结构中“隐身”的人；
- 例如：某“顾问”实际下达指令，董事只是执行；
- 或某资金提供者虽不直接持股，却通过协议控制公司。

MiCA 和希腊实施法都会对“未披露控制人”高度反感，风险包括：

- 直接拒牌；
  - 要求重组股权与治理；
  - 将来对集团所有项目审查更严。
- 

## Q68：项目若主要面向非欧盟客户，是否可以放松治理要求？

**A：** 不可以。

只要：

- 你在希腊设立实体；
- 申请的是欧盟范围内有效的 MiCA-CASP 牌照；

就必须达到 **欧盟 + 希腊本地标准的 Full Governance**，  
不能因为“主要做亚洲客户”而要求减配。

---

## Q69：能否用“顾问委员会（Advisory Board）”增强专业性？监管怎么看？

**A：** 可以，是加分项，但要记住：

- 决策权在正式董事会；
- 顾问委员会只提供意见，无表决权；
- 不得让“顾问”实质控制业务却不承担法律责任。

我们通常建议：

- 在资产管理 / 结构复杂平台项目中设立 Advisory Board；
- 顾问成员包括：前监管官、学者、金融合规专家等。

---

## Q70：希腊 CASP 申请中，是否需要提交完整的治理架构图（Governance Chart）？

**A：** 必须。

至少展示：

- 股东层（集团 / SPV / 自然人）结构图；
- 董事会结构与委员会；
- 高管层（Management）与职能部门；
- 合规 / 风险 / AML / IT / 审计等报告线；
- 与集团层治理的衔接路径。

图越清晰，补件越少。

---

## Q71：如果董事会全是技术背景、没有金融合规经验，会怎样？

**A：** 这是一个高风险组合。

建议：

- 引入至少一名具有监管、金融、合规相关经验的董事；
- 或将技术合伙人降为 CTO，另聘 CEO/董事负责对外合规与监管沟通。

监管希望看到的是“**技术 + 金融 + 合规的互补组合**”，  
而不是“技术一把抓”。

---

## Q72：董事 / 高管是否会被要求亲自参与监管面谈？

**A：** 会。

常见做法：

- CEO 与董事会主席：回答治理、战略、风险文化问题；
- MLRO / Compliance：回答 AML/KYC 与监管合规问题；
- CTO / CISO：回答技术与安全问题。

面谈表现往往直接影响监管对“适当人选”的评价。

---

## Q73：如何准备适当人选（Fit & Proper）面谈？

实务技巧包括：

1. 提前熟悉自己提交的所有文件内容（BP、Policy、架构图）；
2. 熟悉 MiCA 核心条款与希腊本地落实要点；
3. 对公司业务、流程、技术路径做到“能画、能讲、能解释风险”；
4. 对“为什么选希腊 / 为什么选这个结构”有清晰说法；
5. 通过模拟问答训练（Mock Interview）。

仁港永胜可以提供 **定制化的面谈题库 + 实战训练**。

---

## Q74：治理结构文件一般包括哪些？（可直接做 Checklist）

建议至少包括：

- Board Charter（董事会章程）

- Committee Charter（各委员会章程）
- Fit & Proper Policy
- Conflict of Interest Policy
- Delegation of Authority Matrix（权限授权矩阵）
- Governance & Organization Manual
- Reporting Framework（向董事会/股东/监管报告的框架）

这些文件在德国/法国项目中你已经很熟，可以整体复制结构，再本地化为希腊版。

---

## Q75：项目规模较小，是否可以适当简化治理结构？

**A：** 监管允许“比例原则（Proportionality）”，但并不意味着可以缺失要件。

可以简化的是：

- 委员会数量：小型机构可合并为一个“风控与合规委员会”；
- 部分职能兼职：如 Risk Manager 与 Compliance Officer 可兼任（但不建议 MLRO 再兼太多）。

不能简化的是：

- 实质治理
  - 适当人选
  - 董事会对风险和合规的责任
- 

## Q76：董事 / 高管的薪酬政策（Remuneration Policy）是否需要向监管披露？

**A：** 对中大型 CASP 或涉及复杂风险者，通常需要。

监管会看：

- 是否存在“鼓励短期高风险收益”的薪酬结构；
- 是否将合规与风险指标纳入绩效考核；
- 是否对关键职能（合规/AML/风险）有独立薪酬保护。

Remuneration Policy 是 MiFID / CRD 的标准配置，也会逐步扩展至 MiCA 实务。

---

## Q77：是否需要设立“风险偏好声明（Risk Appetite Statement）”？

**A：** 强烈建议，尤其是：

- 托管规模较大；
- 运营交易平台；
- 参与复杂 DeFi/Re-Staking / Derivatives。

Risk Appetite Statement 通常由：

- 董事会制定
- 风险委员会审阅
- 管理层执行

内容包括：对运营、市场、流动性、合规等各风险类别的容忍度。

---

## Q78：监管对“合规文化（Compliance Culture）”有何期望？

他们希望看到：

- 高层公开支持合规（Tone from the Top）；
- 部门之间乐于配合 MLRO / Compliance 要求；
- 合规部门有独立话语权与否决权；
- 员工愿意报告问题而不担心被打击报复（Whistleblowing 机制）。

## Q79：如果申请过程中监管认为适当人选不合格，会怎样？

可能发生以下几种情况：

1. 要求更换某一董事/高管；
2. 要求引入更多有经验的人补位；
3. 要求增加培训和过渡安排；
4. 在极端情况下，直接拒绝整个牌照申请。

所以 一开始就选对人，很关键。

后期修改成本高、时间长，还会影响监管印象。

---

## Q80：仁港永胜在适当人选与治理结构方面，具体能帮到什么？

我们通常会提供一整套服务：

1. 候选人结构设计建议
    - 帮你判断现有股东/董事/高管组合是否“监管友好”；
    - 给出“缺口清单”（少了谁 / 哪块能力不足）。
  2. Fit & Proper 文件打包
    - 简历优化（强调合规与监管相关经验）；
    - 问卷填报指导；
    - 书面声明文本模板。
  3. 治理结构文档
    - Board Charter / Committee Charter 模板；
    - 决策与报告矩阵；
    - 冲突管理机制。
  4. 模拟面谈 & 监管沟通
    - 预测监管会在哪些点挑战董事 / 高管；
    - 提前演练回答；
    - 协助准备英文/希腊文表达要点。
- 

## 第 5 章 | AML/KYC、制裁与链上交易监控（Q81–Q140 | 希腊版）

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

### Q81：在希腊，MiCA-CASP 必须遵守哪些 AML/KYC 法规？主管机关是谁？

A：希腊 CASP 必须遵守：

#### 1) 欧盟层面：

- AMLD5 / AMLD6（即将并入欧盟新 AMLA 机制）
- MiCA 对 AML 的补充要求（尤其在 Custody / Exchange 场景）

#### 2) 希腊本地 AML 法律：

- Law 4557/2018（希腊 AML 主体法）
- 后续修订法案
- HCMC 与 Bank of Greece 的 AML 指引

#### 3) 主管机关：

- **HCMC**（主监管）
  - **希腊 FIU**（金情局）
  - 若涉及支付流程，**希腊央行（Bank of Greece）** 也可能参与。
- 

## Q82：希腊 CASP 必须设立 MLRO 吗？MLRO 的资格要求是什么？

**A：**必须设立 **MLRO**（Money Laundering Reporting Officer）。

**资格要求包括：**

- 熟悉 AMLD、MiCA、Travel Rule、FATF 标准
- 理解链上分析
- 有金融行业 AML 工作经验
- 最好在希腊常驻（强烈建议）
- 能与 FIU / 监管直接沟通
- 能独立做出 STR 决策而不受业务部门干预

**MLRO 是希腊 CASP 审批中的“必考位”。**

---

## Q83：MLRO 是否必须全职？是否可兼职？

**A：**取决于业务规模。

- 小型 CASP：可以兼职，但需证明“有足够资源与时间”；
- 中大型 CASP（交易平台 / 托管机构）：**MLRO 必须全职**，否则会被补件。

监管最讨厌“挂名 MLRO”。

---

## Q84：希腊 CASP 是否需要设立 Deputy MLRO（副 MLRO）？

**A：**

- 建议设立，特别是中大型平台；
- 若 MLRO 不在希腊本地，Deputy MLRO 必须常驻希腊。

Deputy MLRO 是降低监管风险的关键角色。

---

## Q85：希腊 CASP 的 AML 政策（AML Policy）必须包含哪些模块？

典型模块包括：

1. 风险评估（Risk Assessment）
2. 客户分类（Retail / Professional / High-risk）
3. KYC/CDD 流程
4. EDD（高风险客户强化尽调）
5. FATF & EU 制裁规则
6. 链上分析（On-chain Analytics）
7. 交易监控（Transaction Monitoring）
8. 可疑交易报告（STR）流程
9. 政治公众人物（PEP）管理
10. 记录保存（Record Keeping）
11. 培训机制
12. 内部审计机制
13. Outsourcing & Third-party Risk

仁港永胜会根据希腊监管口径提供“定制化版本”。

---



## Q86：希腊是否要求 CASP 制定独立的“AML 企业风险评估 BRA（Business Risk Assessment）”？

**A：**是的，而且是必备文件。

BRA 必须覆盖：

- 客户风险
- 地区风险
- 产品风险
- 交易风险
- 渠道风险
- 技术风险
- 去中心化工具（DEX/Bridge/Mixer）风险
- 监管风险

BRA 通常由 MLRO + Risk Manager 共同完成。

---

## Q87：客户 KYC 必须在开户前完成吗？是否允许“先存款后 KYC”？

**A：**不允许。

希腊 AML 法明文要求：

- **KYC 必须在商业关系开始前完成。**
- 不能“先存款，后验证”。

允许的例外非常有限（例如低风险、限额极小的情况），但不适用于 CASP。

---

## Q88：希腊 CASP 的 KYC 识别要求有哪些？（最低门槛）

自然人至少需提交：

- 身份证/护照
- 地址证明
- 活体检测 / 视频验证
- 面部识别（强烈建议）
- 制裁名单筛查（Sanctions Screening）
- PEP + Adverse Media Screening

法人需要提交：

- 公司注册文件
- 董事名单
- 股东穿透（UBO）
- 控股结构图
- 合规政策（视情形）
- 合法来源证明

希腊监管期望严格遵守 **FATF + EU AMLD**。

---

## Q89：对于来自高风险国家（FATF High-Risk / EU List）的客户，需要做什么？

必须进行：

1. **强化尽调（EDD）**
2. 要求更多文件（如资金来源证明）
3. 加强链上监控

- 4. 增强交易审查（例如人工审核）
- 5. 更短的监控周期
- 6. MLRO 最终批准

监管会特别关注你是否识别 & 拒绝高风险客户。

---

## Q90: MiCA 是否要求对加密资产出入金进行链上分析？

**A: 是的，必须。**

HCMC 期望 CASP 具备：

- 链上地址风险评分
- 交易路径分析
- 路由可视化追踪
- 识别 Mixer / Tornado / Bridge / 深度匿名工具
- 识别盗窃资产或已知攻击者地址

常用工具包括：

- Chainalysis
- Elliptic
- TRM Labs
- Scorechain

仁港永胜会帮你写链上监控框架，并配置供应商逻辑。

---

## Q91: 链上监控系统必须与 KYC 系统联动吗？

**A: 是的。**

必须能够：

- 识别用户来源地址
- 对客户资金流向进行风险标记
- 通知 MLRO 并自动创建告警（Alert）
- 作为 STR 的证据链（Evidence Trail）

若系统割裂，监管会认为你 AML 风险过高。

---

## Q92: 是否必须对每笔交易进行链上分析？

**A: 不需要逐笔人工分析，但需要“实时自动监控”。**

要求包括：

- 自动评分（实时）
- 大额交易人工审核
- 高风险模式自动告警
- 反常行为识别（行为监控）

选择性人工审核 + 大额监控是常见组合。

---

## Q93: Travel Rule（旅行规则）在希腊是否适用？CASP 必须遵守吗？

**A: MiCA + 欧盟 AMLA 体系内，Travel Rule 完全适用。**

希腊 CASP 必须：

- 收集转账发起方与收款方信息
- 在链上/链下传递数据
- 与其他 CASP 对接 Travel Rule API

- 为非托管钱包（Unhosted Wallet）创建风险分类机制

这部分是监管补件热点。

---

## Q94: Travel Rule 对 Unhosted Wallet（自托管钱包）如何处理？

必须：

- 识别钱包是否属于客户本人
- 对大额交易要求额外验证（签名验证等）
- 对高风险交易执行链上 EDD
- MLRO 决定是否触发 STR

HCMC 会重点问：“你如何确认这个钱包不是犯罪分子的冷钱包？”

---

## Q95: 什么样的情况需要向希腊 FIU 提交 STR（可疑交易报告）？

包括但不限于：

- 客户拒绝提供 KYC/KYT 信息
- 地址被链上工具标记为高风险
- 资金来自已知攻击者 / 黑客 / 诈骗者
- 高频度进出金但无商业逻辑
- 使用 Mixer、匿名工具、隐匿链
- 客户行为与资料不符（KYC mismatch）

MLRO 必须保留 STR 决策记录。

---

## Q96: STR 是否可以延迟？是否需要先冻结资产？

**A：不能延迟，必须在“合理时间”内提交。**

是否冻结资产要看：

- 涉及制裁名单？ → **必须立即冻结**；
- 涉及洗钱？ → MLRO 可自行决定是否冻结，需评估风险。

冻结必须记录流程，并在文件中解释“法理依据 + 决策链条”。

---

## Q97: 客户风险分类（Risk Rating）如何定义？监管有没有期望？

常见三层模型：

- **低风险：** 欧盟居民、正当职业、活动透明
- **中风险：** 一般客户
- **高风险：**
  - 高风险司法辖区
  - PEP
  - 加密行业从业者
  - 使用匿名币
  - OTC 大额交易者

监管期待你：

- 有模型
  - 有打分逻辑
  - 有文件描述
  - 有跟踪机制（动态调整）
-

## Q98：是否可以“拒绝高风险客户以降低 AML 风险”？

**A：可以，而且监管高度鼓励。**

MiCA 体系下，“风险不可控的客户”必须拒绝：

- 匿名币（Monero 等）交易者
- 使用 Mixer / Tornado 工具者
- 结构模糊的境外基金
- 可疑 OTC 客户

你只需：

- 提供拒绝流程
  - 保留记录
  - 在 AML Policy 中明确风险容忍度
- 

## Q99：希腊是否要求 CASP 使用制裁筛查系统？要筛查哪些名单？

**A：必须使用系统（自动化工具）。**

筛查必须包括：

- EU 制裁名单
- UN 制裁名单
- OFAC SDN（虽然不是欧盟义务，但强烈建议）
- 英国 OFSI 制裁名单
- 希腊本地名单（如有）

每一次登录、每一次新增钱包、每一次大额交易都应重新筛查。

---

## Q100：如果触发制裁名单，必须立即冻结账户吗？

**A：必须。**

流程：

1. 冻结资产
2. 通知 MLRO
3. MLRO 通知 HCMC 或 FIU
4. 评估是否提交 STR
5. 保存所有证据记录（日期/金额/地址）

监管对制裁违规“零容忍”。

---

## Q101：希腊 CASP 是否必须执行持续监控（Ongoing Monitoring）？

**A：必须。**

内容包括：

- 定期重新验证客户资料
- 定期重新评估风险等级
- 定期重新跑制裁名单
- 监控行为模式（行为监控）
- 自动化链上监控

频率：

- 高风险客户：每 6-12 个月
- 低风险客户：每 2-3 年

---

## Q102：是否要求对法人客户执行 UBO 穿透？需要穿透几层？

**A：**必须穿透至最终自然人。

穿透层数没有上限，但要求：

- 穿透至实际控制自然人（>25% 或重大控制）
- 若存在信托结构，必须识别：Settlor / Trustee / Protector / Beneficiary
- UBO 材料必须合法公证或认证

不允许“部分穿透”“穿透到一半不继续”。

---

## Q103：如何审查客户的资金来源（Source of Funds）？

可以要求：

- 银行流水
- 税务证明
- 加密资产购买记录
- 交易所出入金历史
- 持仓截图（需交叉验证）
- 合同或发票（商业客户）

资金来源必须“合理 + 一致 + 可验证”。

---

## Q104：如何审查客户财富来源（Source of Wealth）？

如果是高风险客户或高净值人士，需要解释：

- 职业与收入
- 企业收益
- 投资回报
- 加密资产早期投资
- 家族资产继承等

尽可能收集证明文件并保存证据链。

---

## Q105：是否可以接受加密资产作为客户 KYC 的资金来源证明？

理论上可以，但必须加强验证：

- 追溯交易路径
- 识别第一个法币入口（Fiat Onramp）
- 检查是否涉及 Mixer
- 核对客户提供的地址是否属于客户本人
- 结合链上工具评分（Chainalysis/Elliptic）

若涉及高风险隐私链，建议拒绝。

---

## Q106：OTC 场外交易客户的 AML 风险如何管理？

必须实施：

1. 强化身份验证（EDD）
2. 针对 OTC 交易设定具体限额
3. 要求资金/资产来源证明
4. 使用链上工具进行逐笔分析

- 5. 每笔大额交易人工复核
- 6. 记录 OTC 交易特有风险场景（政策文件中必须写明）

监管对 OTC 风控非常敏感。

---

## Q107：是否必须保存 AML 记录？保存多久？

**A：至少保存 5 年（一般）**

部分资料应保存 7 年以上（取决于希腊本地实施法）。

记录包括：

- KYC 文件
- 交易记录
- STR 决策
- 链上分析截图
- 风险评分
- AML 内部沟通记录

监管可能抽查。

---

## Q108：是否可以将 AML 系统外包？例如给第三方 KYC/AML 提供商？

**A：可以，但必须符合：**

- Outsourcing Policy
- 风险评估（Outsourcing Risk Assessment）
- 供应商尽调（Vendor Due Diligence）
- 退出机制（Exit Plan）
- 数据保护（GDPR）

外包 ≠ 免责。

最终责任仍由希腊 CASP 承担。

---

## Q109：GDPR（欧盟隐私保护）如何影响 AML/KYC？是否有冲突？

监管要求：

- 数据收集必须具备合法基础（Legal Basis）
- 必须限制最小化原则（Data Minimization）
- 必须确保数据加密、保留、删除机制合规
- 必须提供隐私政策给客户

GDPR 与 AML 没有冲突，只是 AML 目的必须明确记录。

---

## Q110：能否将所有 AML 工作外包给海外团队（如香港/新加坡）？

**A：风险极高，不建议。**

希腊监管会问：

- 你如何确保本地监管可监督？
- MLRO 如何行使实时控制？
- 数据是否转移到第三国？

本地 AML 职能必须保持“实质在希腊”。

---

## Q111：链上危险地址（High-risk Address）怎样定义？

通过链上工具识别的地址：

- 与诈骗 / 黑客事件相关
- 与暗网市场有关
- 与 Mixer / Bridge 深度混淆交易
- 与 OFAC 或其他制裁方关联
- 与高风险国家的 VASP 有频繁往来
- 异常高风险评分（>65 或 >75）

这些地址一旦出现，通常必须：

- 提示 MLRO
- 调查
- 决定是否 STR
- 冻结相关资产

---

## Q112：是否可以接受来自匿名币（Monero/XMR）的入金？

强烈不建议。

希腊监管对匿名币态度趋向严格：

- 难以追踪来源
- 难以执行链上分析
- AML 风险极高

建议在政策中明确写明：

“本平台不接受 Monero、Zcash、Dash 等高度匿名资产的入金。”

---

## Q113：是否必须识别客户使用的交易所来源（如 Binance/Kraken/OKX）？

A：是的。

链上监控系统必须识别：

- 来自受监管 VASP 的资金
- 来自无牌照交易所的资金
- 来自混币工具的资金
- 来自高风险 VASP 的资金

若客户来自高风险交易所 → 必须执行 EDD。

---

## Q114：是否需要对客户使用的加密资产建立“资产风险评级”？

A：必须。

例如：

加密资产类型	风险等级	原因
BTC/ETH	中等	波动性 + 去中心化
Stablecoin (USDT/USDC)	中等	发行方风险
Privacy Coin (XMR/ZEC)	极高	匿名性
Meme Coin	高	无基本面

必须在 AML Policy 中明确。

---

## Q115：如何确保“客户钱包确实属于客户本人”？

技术方案包括：

- 自签名验证 (cryptographic signature)

- 微额回转验证 (micro-transaction test)
- 区块链地址绑定流程
- 风险评分反查链上历史
- 设备指纹识别 + 地址匹配

监管最关注“你如何确认 Unhosted Wallet 不属于第三方”。

---

## Q116：是否必须对第三国客户执行额外尽调？

**A：必须。**

对于来自欧盟以外的客户必须：

- 执行 EDD
- 要求资金证明
- 检查其所在国是否为高风险
- 进行更频繁的审查

希腊对第三国特别敏感。

---

## Q117：客户通过 VPN 登录（无法确认位置）是否允许？

**A：风险非常高。**

建议实施：

- 禁止高风险 VPN
  - 地理定位识别 (IP + Device ID)
  - 异常行为监控
  - 若无法确认客户真实位置 → 触发人工审核
- 

## Q118：是否需要设立“可疑活动监控规则 (Behaviour Monitoring)”？

必须包括：

- 高频登录
- 异地短时间内多次尝试登录
- 大额进出金短期内反复操作
- 账户行为与 KYC 职业/收入不符
- 使用大量不同地址

这些行为要自动触发告警。

---

## Q119：如何处理来自 DeFi 工具的资金？ (DEX/Bridge/Flashloan)

监管会关注：

- 交易路径是否可追踪
- 是否与高风险合约交互
- 是否存在匿名性增强工具
- 金额是否合理
- 是否频繁使用 Flashloan

需要：

- 加强链上分析
  - 增强 EDD
  - MLRO 进行手动复核
-



**Q120：是否需要设立大额交易报告（Large Transaction Review）？ 限额是多少？**

建议采用：

- **€1,000 – €3,000**（入金/出金 EDD 限额）
- **€10,000 – €15,000**（人工复核 + KYT）
- **>€50,000**（MLRO 强制复核）

具体金额可在 AML Policy 中定制。

---

**Q121：是否需要建立“客户风险评分（CRS）系统”？**

**A：必须。**

评分维度包括：

- 国籍
- 地址
- 资产来源
- 职业
- 使用的加密资产类型
- 链上行为
- 交易量
- 交易频率
- 使用地理区域

客户等级必须“动态更新”。

---

**Q122：是否允许客户使用企业账户作为加密交易账户？**

可以，但需执行：

- 详细法人 KYC
- 董事与 UBO 穿透
- 控制权评估
- 法人业务逻辑是否与加密业务相符
- 企业资金来源验证

对“空壳公司”“无实质业务”的企业必须拒绝。

---

**Q123：是否需要为企业客户编写单独的 EDD 模块？**

**A：需要。**

包括：

- 行业风险（如博彩、石油贸易、高现金行业）
- 国家风险
- 股权结构复杂度
- 真实受益人识别
- 与加密领域历史关联

文件中需呈现逻辑。

---

**Q124：是否需要为员工执行 AML 培训？ 频率多少？**

**A：必须。**

频率：

- 上岗前培训 (Mandatory Onboarding Training)
- 每年至少 1 次
- 对 AML / 风控 / 交易部门：每半年 1 次
- 内容必须保存记录：主题、时间、参与者、培训材料

培训不足会直接被监管点名。

---

## Q125：是否必须设立 Whistleblowing（内部举报）机制？

**A：必须，AMLD 要求。**

要求：

- 可匿名
  - 不能打击报复
  - MLRO 必须记录所有举报内容
  - 向监管呈现年度摘要（如要求）
- 

## Q126：是否需要定期向希腊监管提交 AML 报告？

视业务规模而定：

- 年度 AML 报告 (Annual AML Report)
- MLRO 年度总结
- 外部审计的 AML 部分（如适用）
- 外包 AML 服务的评估报告

仁港永胜可编写“监管友好型报告”。

---

## Q127：如何在申请文件中呈现 AML 系统的“端到端流程”？

需要提交：

- 客户开户流程图
- KYC 验证路径
- 风险评分模型
- 链上监控流程图
- Travel Rule 数据流向图
- STR 提交流程
- 例外处理流程 (Exception Handling)
- 系统联动 (KYC ↔ KYT)

越可视化，越容易通过。

---

## Q128：是否可以只使用人工 AML 审核，不使用自动化系统？

不可以。

自动化系统必须具备：

- 列表筛查
- 黑名单识别
- 链上地址分析
- 行为监控
- 风险评分

人工仅在高风险场景补充。

---

## Q129：监管是否要求 CASP 制定“禁入客户清单”？

必须包括：

- 高风险国家客户
- 匿名币交易者
- 使用 Mixer 的客户
- 虚构身份客户
- 高风险行业（视政策设定）

与 Risk Appetite 配套。

---

## Q130：是否必须遵守反恐融资（CFT）要求？

**A：是的。**

包括：

- CFT 风险评估
- 制裁筛查
- 资金流向监控
- STR 提交 CFT 标签
- 内部报告流程

希腊监管对此非常敏感。

---

## Q131：交易监控系统需要识别哪些模式？

必须识别：

- 洗钱典型路径
- 快速买卖 (layering)
- 资金结构不一致
- 高频微额转账
- 高风险币种使用
- 偏离正常行为模式
- DeFi 工具与匿名技术

系统必须能输出 Report。

---

## Q132：是否必须保留链上监控的原始证据？

**A：必须。**

包括：

- 地址评分
- 风险标记
- 交易路径截图
- 工具报告 PDF
- 内部审查记录

监管可随时抽查。

---

## Q133：能否向客户解释自己被标记为“高风险地址”？

可以，但需谨慎：

- 不能泄露机密数据

- 不能影响 STR 决策
- 可给予一般性解释：  
“根据链上工具，该地址涉及高风险路径。”

---

## Q134：是否可以接受“未完成 KYC 的客户”进行小额交易？

不可以。

希腊 AML 法明确：

“KYC 必须在建立商业关系前完成。”

不能采用“先交易、后验证”模式。

---

## Q135：是否需要检查客户是否是 PEP（政治公众人物）？

**A：必须。**

若客户是 PEP，需：

- 加强 EDD
  - MLRO 批准
  - 设置更严格的交易监控
  - 更频繁审查其资料
- 

## Q136：如何识别客户是否涉及诈骗、黑客等非法历史？

需要结合：

1. Adverse Media（负面新闻）
2. 链上路径分析
3. KYC 文件比对
4. 交易模式监控
5. 社交媒体公开信息（辅助）

若高度可疑 → STR。

---

## Q137：是否需要为 AML/KYC 提供年度独立审计？

中大型平台：**必须。**

小型平台：**建议。**

审计由第三方完成，内容包括：

- KYC 流程有效性
  - AML 系统评估
  - STR 流程检查
  - 培训记录验证
  - 数据隐私检查（GDPR）
- 

## Q138：若发现历史客户资料不完整，需要全部重新做 KYC 吗？

视风险等级而定：

- 高风险客户 → 必须重新验证
- 中风险 → 补齐缺失资料
- 低风险 → 定期更新时核查即可

不可忽视旧客户 KYC 风险。

---

## Q139：是否需要为高风险客户执行“人工复核”？

是的。

人工复核包括：

- 人工比对资料
- MLRO 审查链上行为
- 交叉认证交易路径
- 核查资金来源
- 判断是否 STR

不能完全依赖自动化。

---

## Q140：仁港永胜如何帮助项目搭建希腊版 AML/KYC 框架？

我们通常提供：

1. Full AML/KYC Documentation Pack（50–200 页）
2. 链上监控架构设计（含工具集成）
3. KYC/KYT 系统联动方案
4. EDD 模板（企业 & 高净值）
5. STR 提交流程模板
6. Travel Rule + Unhosted Wallet 管理框架
7. 年度 AML 培训材料
8. MLRO 面谈训练
9. AML 风险评估模型（BRA/IRA）

适用于希腊 MiCA 审查 + 欧盟跨境业务。

---

# 第 6 章 | Safeguarding 客户资产隔离、托管 Custody 与钱包管理（Q141–Q180 | 希腊版）

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

## Q141：在希腊 CASP 监管中，什么是 Safeguarding？为什么这么重要？

A：

Safeguarding 的核心是：

“确保客户资产永远与平台自有资产分离，任何人不能随意动用。”

在希腊 MiCA 框架下，监管极度关注三点：

1. 客户资产与自有资产分账、分账户、分记录；
2. 私钥与访问权限有严格控制，避免内部人滥用；
3. 无论平台破产、清盘、被攻击，客户资产都能被识别、提取、归还。

一句话：Safeguarding 是“客户资产的防火墙”，是托管类 CASP 能不能获牌的最关键模块之一。

---

## Q142：在希腊持牌 CASP，客户资产必须如何“与公司资产隔离”？

至少要做到三层隔离：

1. 法律层面（Legal Segregation）
  - 客户资产在法律上明确归客户所有；

- 公司只作为托管方（Custodian）或名义持有人；
- 在客户协议 / 条款中写明资产属于客户。

## 2. 账务层面（Accounting Segregation）

- 分别记录“客户资产”和“公司资产”；
- 客户资产永不计入公司自有资产；
- 财报/账簿中有单独项目表示。

## 3. 技术层面（Technical Segregation）

- 链上地址专门用于客户资产；
- 冷/热钱包明确标记归属；
- 系统内账与链上记录可一一对应。

---

## Q143: Safeguarding 和“简单托管 Custody”有什么区别？

- **Custody:** 更偏向“代持保管”功能——你持有客户资产的私钥；
- **Safeguarding:** 更偏向“保护客户在破产 / 运营风险下的权利”。

MiCA + 希腊实施法要求：

只要你提供 **Custody**，就必须有一整套 **Safeguarding** 机制。

---

## Q144: 在希腊 CASP，如果我只提供“技术托管”，是否也算 Custody？

看关键问题：

“你是否有能力单方面移动客户资产？”

- 如果你只是部署软件/硬件，完全不持有密钥 / 不参与签名 → 可能只是技术服务；
- 如果你的任何一片密钥、单一服务器或单一权限足以发起转账 → 在监管眼中就是 Custody。

绝大多数所谓“技术托管”在监管眼中都是实质 **Custody**。

---

## Q145: 希腊监管对 Custody 服务的最低要求是什么？（高维度）

1. 明确托管关系与责任（合同层面）；
2. 有完整的钱包管理政策（Wallet Management Policy）；
3. 有多层级授权与签名机制；
4. 有有效的冷/热钱包架构；
5. 有灾备、备份与恢复机制；
6. 有定期对账与审计；
7. 有客户资产隔离的完整执行链；
8. 有应对黑客/丢失密钥的应急方案（Incident Response）。

---

## Q146: 冷钱包（Cold Wallet）与热钱包（Hot Wallet）在希腊 MiCA 实务中如何区分？

- **冷钱包（Cold Wallet）:**
  - 私钥不接触互联网；
  - 物理隔离；
  - 多数用于长期储存客户大额资产；
- **热钱包（Hot Wallet）:**
  - 连接互联网；
  - 用于日常提款与交易结算；
  - 容易成为攻击目标。

监管更欣赏“少量热钱包 + 大部分冷钱包”的结构。

## Q147：冷/热钱包比例如何设置比较监管友好？

常见实践（可写入 Policy）：

- **80–95%** 客户资产放在冷钱包；
- **5–20%** 客户资产用于热钱包流动性；
- 热钱包余额超过某个阈值时自动转入冷钱包（Auto Sweep）；
- 定期审查比例的合理性（由风险委员会/董事会审阅）。

具体比例视业务类型和交易频率而定，但一定要有**内部明确规则**。

---

## Q148：什么是“多签 Multi-Sig”和“MPC（多方计算）”？监管如何看待？

- **多签（Multi-Signature）**：交易需多个私钥共同签署才能生效（例如 2-of-3）；
- **MPC（Multi-Party Computation）**：不再使用完整私钥，而是将密钥拆成多份碎片，多个节点共同参与计算签名；
- 相比经典单一私钥，MPC 在云环境下更灵活，也更方便实现“无单点失效”。

希腊监管通常接受 Multi-Sig 和 MPC，只要：

- 有清晰的技术描述；
  - 有详尽权限控制；
  - 有第三方安全审计报告；
  - 有密钥备份策略。
- 

## Q149：使用 MPC 或 HSM，是否可以不再提交传统私钥管理政策？

不可以。

无论使用 Multi-Sig / MPC / HSM：

- 都需要一套 **“Wallet & Key Management Policy”**；
- 阐述密钥生成、分发、使用、备份、废止、恢复等全流程；
- 解释谁有权调用；
- 说明如何防止单点故障和内部滥用。

技术越复杂，文档越要清晰。

---

## Q150：钱包管理政策（Wallet Management Policy）一般需要涵盖哪些内容？

至少包括：

1. 钱包类型（冷/热/温）定义与用途；
  2. 钱包生成与密钥生成流程；
  3. 多签/MPC/HSM 架构说明；
  4. 密钥备份和存储位置；
  5. 权限与角色分工（谁能发起、谁能批准）；
  6. 交易审批流程（限额 / 多人审批）；
  7. 冷/热钱包资金迁移规则；
  8. 风险事件响应流程；
  9. 日常对账与审计机制；
  10. 升级与变更管理流程。
- 

## Q151：谁负责客户资产的 Safeguarding？可以外包吗？

最终责任永远在持牌 CASP 身上。

可以外包：

- 部分技术运维；
- HSM/MPC 方案供应商；
- 数据中心托管；

不能外包：

- 对客户资产负责的法律責任；
- 决定是否冻结/释放资产；
- 决定是否阻止可疑交易。

监管要求持牌 CASP 保持对 Safeguarding 的“最终控制权”。

---

## Q152：在希腊 CASP 中，Who can sign（谁可以签名）是如何被监管看待的？

监管重点关注：

- 有多少人具备“单人发起转账”的权限？
- 是否存在单一管理员可以“绕过多签/MPC”？
- 权限分离是否合理？
- 是否有多因素认证（MFA）；
- 是否记录所有签名行为的日志并可审计。

监管不希望看到：

“一个超级管理员就能把几千万资产转走。”

---

## Q153：是否必须为不同业务设置独立的钱包地址？

强烈建议，也是加分项。

例如：

- 客户存款地址池（Deposit Addresses）；
- 自有资产运营地址；
- 手续费收入地址；
- 冷存储主地址；
- 热钱包流动资金地址。

这样可以：

- 客户资产与公司资产在链上清晰可见；
  - Audit / FIU / 监管未来检查更轻松；
  - 出事时能迅速识别受影响资金范围。
- 

## Q154：如何实现“客户资产+公司资产”的链上对账？

一般做法：

1. 为客户生成独立地址或子账户；
2. 每日导出链上余额快照；
3. 与系统内账（Ledger）自动对比；
4. 差异由专人调查并记录；
5. 由财务/风控/内审定期审查。

文件中必须呈现“日对账 + 月/季/年抽查”的机制。

---

## Q155：是否需要外部审计公司对 Custody / Safeguarding 做专项审计？



中大型平台 → **强烈建议**，并可能成为监管预期。

可由：

- Big4 或专门做加密审计的机构  
出具：
- “钱包余额证明（Proof-of-Reserves 风格）”；
- 内控测试报告（SOC1/SOC2 风格）；
- 安全评估报告。

这些报告可在申请阶段或运营阶段提供给监管。

---

## Q156：在希腊，如果平台破产，客户的加密资产会怎样处理？

在合规设计正确的前提下：

- 客户资产应从破产财产中剥离；
- 管理人/清算人需依据客户名义进行返还；
- 这是 Safeguarding 机制的首要目标。

因此 Policy 中需要明确：

- 客户资产的法律性质；
  - 托管协议中客户的权利；
  - 平台不得将客户资产质押或另作他用。
- 

## Q157：是否允许平台用客户资产进行质押 / 借贷 / 再抵押（Rehypothecation）？

**极高风险，监管高度敏感。**

如涉及：

- 必须在 Terms & Conditions 中明示；
- 必须提供退出机制和风险警示；
- 必须取得客户明确同意；
- 必须保持足够的流动性与保障。

大多数监管审查中，对“客户资产再利用”会提出大量问题，  
很多项目最终选择 **不再利用** 以简化审查。

---

## Q158：在希腊 CASP 中，是否可以提供 Staking / Earn / Lending 产品？

可以，但需特别管理：

- 必须明确区分“托管中的基础资产”和“参与 Staking/Lending 的资产”；
- 必须说明收益与风险；
- 可能触及 MiFID 或其他投资产品框架；
- 资产损失责任如何划分需在合同中说明清楚。

这类产品属于监管“高风险关注点”。

---

## Q159：如何向监管说明“托管资产不会被内部员工擅自挪用”？

可以通过以下组合证明：

1. 权限分离（Segregation of Duties）：
  - 发起人、审批人、签名人角色分离；
2. 多签/MPC 结构：
  - 无任何一人单独完成交易；

3. 多因素认证与物理安全控制；
  4. 交易审批限额（内部限额表）；
  5. 日志记录 & 内审抽查；
  6. 内部政策中明确“违规零容忍 + 法律责任”。
- 

## Q160：是否必须针对钱包安全制定 Incident Response Plan（事件响应预案）？

必须。

应覆盖：

- 黑客攻击事件
- 私钥泄露
- 部分节点失效（MPC 节点宕机）
- 钱包系统故障
- 链上重大异常（如主链分叉）

预案包括：

- 紧急停止所有提款
  - 将热钱包资金立即转冷钱包
  - 启动相应级别的应急小组
  - 通知监管与客户（视事件严重程度）
  - 与安全供应商配合调查
  - 形成事后报告（Post-mortem）
- 

## Q161：是否必须为钱包系统购买保险（Crypto Custody Insurance）？

法律上不一定强制，但监管会问：

“你如何减轻托管风险？”

若能提供：

- 托管保险（Crime Insurance / Custody Insurance）；
- 安全漏洞保险（Cyber Insurance）；

会是非常重要的加分项。

如暂未购买，必须在风险评估中说明替代控制措施。

---

## Q162：可以把 Custody 完全外包给第三方托管机构吗？

可以，但要注意：

1. 外包方必须本身受监管（例如持有其他欧盟金融牌照）；
2. 外包协议必须非常详细；
3. 你仍然对客户资产负最终责任；
4. 你必须随时可审计外包方的操作；
5. 客户协议中需明示外包关系及相关风险。

监管会重点审查：外包后你是否仍保有“控制权 + 审查权”。

---

## Q163：如果只做“第三方托管集成”（例如对接外部托管银行/托管所），是否还算 Custody？

若你不持有密钥、不触碰客户资产、不能指令托管方转账，  
而只是技术集成 / 前端 → 可视为“非托管”。

但需证明：

- 资金流完全在第三方托管机构；
- 客户与托管机构直接建立法律关系；
- 你只负责界面与指令传递。

如你能直接控制资金/代客户发出指令，则仍被视为 Custody。

---

## Q164：如何展示钱包架构设计，才符合希腊监管审查预期？

建议准备：

1. 架构图 (Architecture Diagram)
    - 冷/热/温钱包位置
    - MPC 节点分布
    - HSM/硬件钱包位置
    - 外部托管接口
  2. 数据流图 (Data Flow Diagram)
    - 从客户发起提款 → 审核 → 签名 → 广播全流程
  3. 权限矩阵 (Access Matrix)
    - 哪个岗位可以做什么操作
  4. 风控与监控点 (Control Points)
    - 在每一步如何防止越权、欺诈与错误操作。
- 

## Q165：密钥备份 (Key Backup) 如何设计才不会产生“第二个安全隐患”？

常见原则：

- 使用 Shamir Secret Sharing 或 MPC 的方式分片存储；
- 备份存储在不同地理位置与机构；
- 每个备份片单独无效；
- 需要多人协同才能恢复；
- 恢复时有完整的审批流程与记录。

“一个人拿着一张纸上写私钥”是监管眼中严重反面示范。

---

## Q166：是否需要对钱包系统做渗透测试和安全审计？频率如何？

必须进行。

- 上线前进行一次全面渗透测试；
- 每年至少一次定期渗透测试；
- 对重大升级进行专项测试；
- 保留测试报告与整改记录。

监管可能要求查看报告摘要。

---

## Q167：如何处理“链上资产与系统内账不匹配”的情况？

必须有：

1. 差异发现机制 (对账)；
2. 差异调查流程 (由合规/风控/财务牵头)；
3. 差异解决责任人 (Responsible Person)；
4. 对重大差异事件上报流程 (报管理层/监管)。

差异不可被“随意补平”，必须找到原因。

---

## Q168：是否允许在一个钱包中混合存放多个客户资产？（Omnibus Wallet）

监管允许使用 Omnibus Wallet，但必须确保：

- 系统内账能准确识别每个客户的“份额”；
- 对账机制精确；
- 破产/清算时可区分归属；
- Terms & Conditions 中明确说明；
- 有防止滥用与挪用的控制措施。

如有条件，基于客户规模和技术能力，独立地址模型更友好。

---

## Q169：如何验证冷钱包的持有权和余额？

常见方法：

1. 签名验证：平台在监管/审计要求下，对冷钱包地址发起签名证明；
2. 点对点验证：通过广播小额交易证明控制权；
3. 定期出具第三方审计报告；
4. 与系统内账定期对账。

申请阶段可以在文件中写明这种 Proof-of-Control 机制。

---

## Q170：是否需要为客户提供“Proof-of-Reserves”透明度披露？

不是法律强制，但对提高透明度非常有效：

- 定期公布“链上总资产地址”和“客户总负债”；
- 使用 Zero-Knowledge 技术防止暴露客户隐私（如选择）；
- 用第三方机构审计并披露摘要。

监管会将此视为“良好实践（Best Practice）”。

---

## Q171：若发生黑客入侵导致客户资产损失，希腊监管会怎么看？

关键看三个问题：

1. 事前是否采取了“合理且符合行业标准的防护措施”？
2. 事后是否按预案迅速响应（冻结、通报、调查、报告）？
3. 是否有赔付机制或保险支持？

完全没有 Policy、没有预案、没有审计 → 责任极重；

有充分控制但仍被高阶攻击 → 监管会更宽容。

---

## Q172：是否可以让单一云服务商掌握所有钱包相关关键资源？

极大风险。

监管希望看到：

- 至少在关键环节有“多云或混合部署”；
- 关键节点的控制不全堆叠在同一云环境；
- 你对云服务商有退出与切换计划（Exit Plan）。

文件中必须提到这一点。

---

## Q173：钱包管理与 AML/KYC 之间应如何联动？

必须做到：

- 每一个链上地址都对应到一个明确客户 ID；
- 交易监控系统可根据地址直接找到客户信息；
- 怀疑某地址高风险时，AML 系统能立刻冻结/限制客户操作；
- 所有钱包操作在 AML Risk Score 中有体现。

这也是为什么 Wallet Policy 需要与 AML Policy 一起设计。

---

## Q174：是否需要为托管服务设计单独的客户协议（Custody Agreement）？

**强烈建议。**

Custody Agreement 中应包括：

- 资产归属（仍属于客户）；
- 平台的职责与免责边界；
- 客户义务（如不得共享账号等）；
- 资产利用规则（若有 Staking/Lending）；
- 保险与赔付条款；
- 终止关系与资产提取流程。

监管会查看该协议内容。

---

## Q175：如何向监管说明“客户资产可以在平台破产情况下被优先返还”？

你需要：

1. 法律意见书（Legal Opinion）：
  - 说明客户资产不属于破产财团；
  - 阐明托管结构下的财产权安排；
2. 运营流程文件：
  - 一旦破产，如何验证每个客户的资产；
  - 如何与清算人协调；
3. 案例模拟：
  - 以简单数字演示“破产时资产分配流程”。

这部分通常由律师 + 合规顾问共同设计。

---

## Q176：在希腊 CASP 中，如果采用 DeFi 协议作为托管底层，会有什么监管问题？

主要问题有：

- 托管资产受链上智能合约风险支配；
- 无传统意义上的“托管人”；
- 智能合约是否经过审计；
- 是否存在管理员权限（Admin Key）；
- 如何确保资产可随时赎回。

若要在此框架下获批，须提交：

- 智能合约审计报告；
  - 风险披露文件；
  - 紧急暂停/升级机制说明；
  - 对“合约黑天鹅事件”的处理方案。
- 

## Q177：是否可以允许客户使用自托管钱包（Non-Custodial）却依然使用平台服务？

可以，但需区分：

- **Non-Custodial 场景：**
  - 平台不控制私钥；
  - 仅提供撮合／路由／信息服务；
- **Custodial 场景：**
  - 平台控制私钥；
  - 属于托管服务。

政策与 Terms 中要写清楚区分及风险。

---

## Q178：如何解释“我们是 Non-Custodial 平台”才能令希腊监管接受？

必须满足：

1. 平台完全不控制私钥；
2. 不代表客户执行链上交易（客户自己签名）；
3. 不集中管理客户资产；
4. 不代客托管资产或进行质押；
5. 技术架构图中能证明“无单一节点有能力移动客户资产”。

如果实际业务里有“代为签名”“一键授权”，很可能被否定为 Non-Custodial。

---

## Q179：在申请文件中，Safeguarding 章节应如何结构化呈现？

建议结构：

1. 客户资产法律归属说明；
2. 客户资产与自有资产分离机制；
3. 钱包架构与密钥管理；
4. 日常对账与审计；
5. 破产/清算情景下的资产保护流程；
6. 外包托管安排（如有）；
7. 保险与赔付机制；
8. 重大事件响应与客户沟通。

这样呈现，监管一目了然。

---

## Q180：仁港永胜在 Safeguarding / Custody / Wallet 管理模块中，可提供哪些具体协助？

我们通常会提供一整套 “Wallet & Safeguarding Pack”，包括：

1. **Wallet Management Policy**（冷/热/MPC/HSM 全覆盖）
2. **Safeguarding Policy & Procedure**（客户资产隔离全流程）
3. **Wallet Architecture 图 + Data Flow 图**
4. **Access Control Matrix**（权限矩阵）
5. **Incident Response Playbook**（钱包安全事件应急预案）
6. **Custody Agreement 模板**（客户托管协议）
7. **Proof-of-Reserves & 对账机制设计说明**
8. 第三方托管 / 技术供应商外包框架
9. 与 AML/KYC 系统的联动设计
10. 针对监管面谈的 **Custody 专题 Q&A 脚本**

仁港永胜帮助你在希腊 MiCA 审查中，将“托管 + Safeguarding”这一最敏感环节一次性说清楚、做扎实。

---

# 第 7 章 | 外包 (Outsourcing)、IT & Cybersecurity、数据保护 GDPR (Q181–Q220 | 希腊版)

本文由 仁港永胜 (香港) 有限公司 拟定, 并由 唐生 提供专业讲解。

## (A) 外包 Outsourcing 模块 (Q181–Q200)

### Q181: 希腊 CASP 是否允许外包关键职能? 有哪些限制?

**A:** 允许外包, 但必须“可控、可审计、可替代”。  
不得外包核心监管责任, 例如:

- 治理 (董事会职责)
- AML 最终责任
- Safeguarding 客户资产最终责任
- 关键风险与合规决策权

可以外包:

- 技术开发
- IT 维护
- 云服务器托管
- 客服/后台支持
- 安全监测
- KYC/链上分析工具 (工具可外包, 但判断责任仍在你)

监管对外包非常敏感, 因为:

- 外包 ≠ 放弃责任。
- 外包后风险更高, 审查“加倍严格”。

### Q182: 哪些外包属于“重要外包 (Critical Outsourcing)”?

一旦某项外包满足以下其中一点, 就属于 **Critical**:

- 若失败会导致 CASP 无法继续运营
- 与客户资产安全相关 (钱包、密钥、存储、签名)
- 与 AML/KYC 核心流程相关
- 与交易撮合、订单处理核心模块相关
- 与业务连续性管理 (BCM) 相关
- 涉及敏感客户数据 (跨境数据流)

Critical 外包需要:

- 更严格的审查
- 更详细的外包合同
- 更完整的风险管理方案
- 报告义务更重

### Q183: 外包是否必须向监管 (HCMC) 申报?

是的, 重要外包必须申报。  
通常包括:

- 外包前的风险评估
- 外包方尽调报告
- 外包协议草案
- 监控机制说明
- 退出方案 (Exit Plan)
- 业务连续性与备援方案

轻型外包可备案，但 Critical 外包必须提前书面告知或报批（视最终希腊实施法细节）。

---

## Q184：如何判断某个外包是否“不可接受（Not Allowed）”？

监管会拒绝外包以下事项：

1. 导致 **CASP** 对自身业务失去控制权
  2. 外包方位于高风险司法辖区（**FATF** 黑名单）
  3. 外包方可单方面移动客户资产（这是致命问题）
  4. 外包 **AML** 判断权（KYC 工具允许，但判断不能外包）
  5. 外包关键管理岗位（**CEO/MLRO/Compliance Officer**）
- 

## Q185：外包协议（Outsourcing Agreement）必须包含哪些条款？

至少包括：

- 外包服务描述（Scope）
- 服务等级协议 SLA
- 数据保护条款（GDPR）
- 审计与访问权（Audit & Access Rights）
- 业务连续性要求
- 安全控制措施（Cybersecurity Controls）
- 变更管理流程
- 退出方案（Exit Plan）
- 分包限制（Sub-outsourcing）
- 监管可直接联系外包方的条款

仁港永胜会提供一套标准 MiCA 外包协议模板。

---

## Q186：云服务（AWS / Azure / GCP）算外包吗？是否必须申报？

是的，云服务属于外包。

如果承载：

- 核心交易系统
- 用户数据
- 钱包/密钥管理相关节点
- AML 系统

则属于 **Critical Outsourcing**。

需要：

- 云风险评估报告
  - 数据存储位置说明
  - 访问控制机制
  - 加密机制
  - 退出机制（Cloud Exit Plan）
-



## Q187：外包方可以不在欧盟境内吗？例如美国、新加坡？

可以，但必须满足严格条件：

- 司法辖区必须符合 GDPR 的跨境传输要求
- 外包方需接受监管审计
- 外包对 CASP 的关键控制权不可削弱
- 不能是 FATF 高风险地区
- 外包方必须能证明其安全管理与合规能力

对非欧盟外包，文档必须非常完整。

---

## Q188：外包方必须具备哪些资质？需要监管牌照吗？

视外包业务性质而定：

- **托管（Custody）相关外包** → 需金融牌照或已被监管
- **AML 工具供应商** → 需展示 AML 资质与合规能力
- **IT 安全供应商** → 需安全认证（如 ISO 27001）
- **云服务商** → 需安全认证和审计（SOC2 Type II）

外包方无相关资质 → 审查难度倍增。

---

## Q189：外包后是否需要持续监控外包方的表现？如何证明？

必须持续监控（Ongoing Monitoring）。

需要：

- KPI / SLA 报表
  - 外包风险季度评估
  - 年度外包方绩效审查
  - 现场/远程审计
  - 董事会年度外包报告
  - 如果发现问题，必须记录整改措施（Remediation）
- 

## Q190：是否可以外包给母公司或关联公司（Group Outsourcing）？

可以，但必须满足：

- 不削弱本地实体的自主决策权
- 外包协议与第三方外包一样详细
- 有价格透明度
- 不能因集团安排导致监管信息不透明

若集团总部在希腊以外，监管会更关注控制链条和数据安全。

---

## Q191：如何解释“外包 ≠ 转移风险”？

监管逻辑：

- 外包执行
- 风险仍归你承担

因此所有外包文件中必须写明：

“The CASP retains full responsibility for all outsourced functions.”

---

## Q192：客户需不需要被告知你使用了外包服务？

对 Critical 外包 → 必须披露。

特别是以下情况：

- 云托管客户数据
- 外包 KYC
- 外包钱包技术
- 外包客服接触客户资料

披露方式：

- 客户协议 (Terms)
  - 网站/隐私政策
  - 风险披露文件
- 

## Q193：外包服务商是否可以再继续外包 (Sub-outsourcing) ？

可以，但条件非常严格：

- 需要 CASP 同意
- 对 Critical 功能必须监管同意
- Sub-outsourcing 不得削弱 SLA
- 必须明确责任链
- 必须允许监管追踪到“最底层外包者”

这是最容易被忽略的审查点之一。

---

## Q194：是否必须准备 Outsourcing Policy？内容应包括哪些？

必须。

应包含：

- 外包定义与分类
- 外包风险评估方法
- 外包流程（前期尽调、合同、监控）
- 终止与退出机制
- 分包规则
- 董事会责任
- 外包年度报告模板
- Outsourcing Register（监管清单）

仁港永胜会为客户拟定 MiCA 标准版文档。

---

## Q195：监管如何判断贵司“对外包商是否保持足够控制权”？

关键问题：

1. 能否随时获得数据？
2. 外包方出问题，你能否独立继续运行？
3. 能否随时替换外包方？
4. 是否有监管访问权？
5. 是否有内部能力监控外包方？

缺少其中任何一项，补件风险极高。

---

## Q196：如果外包方出现数据泄露，CASP 是否要承担责任？

是的。

外包方泄露数据 ≠ 外包方承担全部责任。

监管会问：

- 是否事前进行了安全尽调？
- 是否有监控 SLA？
- 是否有 Incident Response Plan？

CASP 永远是第一责任人。

---

## Q197：是否必须维持 Outsourcing Register（外包登记册）？

必须。

内容包括：

- 外包方名称
- 外包功能描述
- 重要性等级（Critical / Non-critical）
- 服务期限
- 风险分类
- 合同日期
- 监控机制
- 退出计划
- Sub-outsourcing（如有）

监管可要求随时提交。

---

## Q198：可以将整个交易系统交易核心（Matching Engine）外包？

可以，但属于 **Critical Outsourcing**，审查极严格。

必须提供：

- 交易系统架构图
- 交易引擎的 SLA
- 冗余与高可用设计
- 外包方安全资质
- Backtesting 与风控机制
- 出问题后手动/自动切换方案

若引擎与钱包托管皆外包 → 审查强度会显著提高。

---

## Q199：如何向监管证明外包对客户“透明且可控”？

你需要提交：

- Outsourcing Policy
  - Outsourcing Register
  - 外包协议摘要
  - 数据流图
  - 权限矩阵
  - 风险评估报告
  - 董事会外包审查会议纪要
-

## Q200：仁港永胜能否协助客户完成 Outsourcing 全套文件？

是的，我们提供：

- Outsourcing Policy
- Outsourcing Register
- SLA 模板
- 外包尽调（Vendor Due Diligence）模板
- 外包协议法律条款建议
- 外包风险评估模型
- Outsourcing Governance 业务流程说明图

确保一次性通过审查。

---

## (B) IT & Cybersecurity 模块（Q201–Q210）

---

### Q201：MiCA 与希腊监管对 IT 安全总体要求是什么？

简而言之：

**“零信任 + 最小权限 + 可审计 + 多层防护 + 高可用。”**

必须构建：

- IT Governance Framework
  - 信息安全管理（ISO 27001 级别）
  - 渗透测试
  - 变更管理
  - 事件响应流程
  - 网络安全策略
  - 日志监控
  - 访问权限控制
  - 灾备与业务连续性
- 

### Q202：是否必须提交 IT Security Policy？

必须。

通常包含：

- 网络安全架构
  - 身份与访问管理（IAM）
  - 密码策略
  - 加密要求
  - 数据存储要求（含云安全）
  - 日志与监控
  - 开发/测试/生产环境隔离
  - 补丁与漏洞管理
  - 备份策略
- 

### Q203：必须做渗透测试（Penetration Testing）吗？频率如何？

必须。

- 上线前全面测试

- 每年至少一次
  - 系统重大修改后专项测试
  - 需保留整改记录与报告
- 

## Q204：是否必须建立“变更管理流程（Change Management）”？

是的。

监管关注：

- 谁提出变更？
- 谁批准？
- 如何记录？
- 如何测试？
- 是否可回滚？
- 是否有版本管理？

Change Management Failures 是监管常见“补件点”。

---

## Q205：是否必须使用 MFA（多因素认证）保护后台系统？

必须。

适用于：

- 所有管理账号
  - 所有钱包相关系统
  - 所有云控制台（AWS / GCP / Azure）
  - 所有支持操作人员
- 

## Q206：如何实现日志管理（Logging）以满足审计要求？

必须确保：

- 记录所有关键操作（登录、交易、审批、转账、变更）
  - 记录不可被篡改（WORM / Immutable Logs）
  - 日志可保存至少 5 年
  - 有自动告警
  - 每月审计日志（由 IT/内审审核）
- 

## Q207：是否必须准备 Business Continuity Plan（BCP）？

必须。

需涵盖：

- 服务器故障
- 云平台停机
- DDoS
- 软件漏洞
- 数据库损坏
- 关键供应商不可用
- 办公场地无法使用

BCP 必须附带：

- RTO（恢复时间）
- RPO（数据恢复点）

- 负责人
  - 演练记录
- 

## Q208: 是否必须准备 Disaster Recovery Plan (DRP) ?

必须。

内容包括：

- 热备 / 冷备节点
  - 多区部署
  - 数据库备份策略
  - 恢复流程
  - 联络机制
  - 灾备切换测试报告
- 

## Q209: 是否必须对员工进行网络安全培训?

是的，包括：

- 钓鱼攻击识别
- 密码管理
- 风险事件报告流程
- 隐私保护
- 远程办公安全

监管会抽查培训记录。

---

## Q210: 仁港永胜是否提供 IT & Cybersecurity 文档?

是的，包括：

- IT Security Policy
  - Cybersecurity Policy
  - Incident Response Policy
  - BCP/DRP
  - Access Control Matrix
  - Security Architecture Diagram
  - Penetration Test Scope 模板
- 

## (C) GDPR + 数据保护模块 (Q211–Q220)

---

### Q211: 希腊 CASP 是否必须完全遵守 GDPR?

必须遵守。

MiCA + GDPR 双重框架适用，包括：

- 数据收集合法性
  - 数据最小化原则
  - 跨境传输要求
  - 数据主体权利（删除 / 更正 / 访问）
  - DPIA（数据影响评估）
  - 安全泄露通知流程
-

## Q212: GDPR 中, CASP 是 Data Controller 还是 Data Processor?

通常:

- CASP = **Data Controller**
- 外包服务商 (如 KYC 提供商) = Data Processor

必须签署 **DPA (Data Processing Agreement)**。

---

## Q213: 客户数据可以在欧盟外存储吗? (如 AWS 新加坡)

可以, 但条件非常严格:

- 必须满足 GDPR 第 46 条
- 必须使用 Standard Contractual Clauses (SCC)
- 必须进行 Transfer Impact Assessment (TIA)
- 必须确保云供应商符合法律要求

高风险国家不适合存储客户数据。

---

## Q214: 客户能请求删除 KYC 数据吗? (Right to Erasure)

KYC 数据不能随意删除, 因为 AML 法律要求保存:

- **5 年 (基本)**
- 某些高风险可延长至 7-10 年

必须向客户解释“AML 法律优先于 GDPR 删除权”。

---

## Q215: 是否必须设立 DPO (Data Protection Officer) ?

取决于:

- 是否处理大规模敏感数据
- 是否大量监控客户行为
- 是否跨境数据传输

大多数 CASP → **建议设立 DPO** (内部或外包均可)。

---

## Q216: 是否必须准备 Data Protection Policy?

必须。

内容包括:

- 数据分类
  - 数据存储期限
  - 跨境传输机制
  - 访问权限控制
  - 数据泄露通知流程 (72 小时规则)
  - 数据主体权利处理流程
- 

## Q217: 如果发生数据泄露, 是否必须通报监管?

是的, GDPR 要求:

- **72 小时内**向监管机构报告
- 在严重影响数据主体权利时, 需通知客户

- 记录泄露原因与补救措施

MiCA 可能要求同时通知 HCMC。

---

## Q218：是否可以将客户数据用于营销？

可以，但条件非常严格：

- 必须获得客户明确同意（Opt-in）
- 必须允许客户随时撤销
- 必须保持业务必要性的原则

不能将 AML/KYC 数据用于营销。

---

## Q219：是否必须做 DPIA（数据保护影响评估）？

如果满足以下任一情况 → 必须做：

- 大规模处理个人数据
- 处理敏感数据（如生物特征识别）
- 数据跨境传输
- 使用 AI 自动决策
- 监控用户行为

大多数 CASP → 必须进行 DPIA。

---

## Q220：仁港永胜能否提供 GDPR 全套模板？

可以，包含：

- GDPR Policy
- DPA（数据处理协议）
- SCC（标准合同条款）
- DPIA 模板
- 隐私政策（Privacy Notice）
- 客户权益说明
- 数据泄露流程（Breach Notification）

确保一次性满足 MiCA + GDPR 的监管要求。

---

# 第 8 章 | 业务模式与资本金、流动性、财务与审计要求

（Q221–Q260 | 希腊 Greece（MiCA）CASP 版）

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

## （A）业务模式与收入结构（Business Model & Revenue Streams）

---

### Q221：在希腊申请 MiCA-CASP 牌照时，业务模式（Business Model）需要写到多细？

**A：** 原则是——写到监管可以“画出一张业务流程图”为止。

至少要包含：

1. 客户群体（Target Clients）
  - 零售 / 专业投资者 / 机构
  - 欧盟 or 非欧盟
  - 是否含高风险司法辖区



## 2. 产品与服务 (Services & Products)

- 托管 Custody
- 交易平台 Exchange
- 经纪 / 代理
- 投资建议
- Staking、Earn、借贷等增值服务（如有）

## 3. 资金 & 资产流向 (Flow of Funds & Assets)

- 客户如何入金、出金
- 法币与加密之间如何转换
- 参与哪些链 / 交易对
- 是否对接其他 VASP、银行或支付机构

## 4. 收入来源 (Revenue Streams)

- 手续费
- 价差收益
- 托管费
- 订阅费 / 技术服务费
- 其他（如市场营销返佣等）

写到监管看完之后，可以清楚知道：

“你靠什么赚钱、给谁服务、用什么系统做、承担什么风险。”

---

## Q222：在 Business Plan 中，是否必须提供 3–5 年的财务预测？

**A：**基本标配是 3 年预测，很多国家（包括希腊）更倾向于看到 3–5 年。

包括：

- 预计客户数量
- 交易量 (Volume)
- Fee Rate 假设
- 收入 (Revenue)
- 运营成本 (OPEX)
- 人员成本
- IT & 外包成本
- 资本支出 (CAPEX)
- 税前 / 税后利润

关键不是“精准”，而是“逻辑合理 + 假设清楚 + 一致性”。

---

## Q223：监管最不喜欢看到什么样的“业务预测”？

典型踩雷模式：

1. 第一年的预测就非常激进（例如：上来就数十万客户）；
2. 完全没有分解假设（市场规模、转化率、费率、流失率等）；
3. 成本严重低估（特别是合规 & IT 安全成本）；
4. 人员配置明显不够（3 个人要做完全部业务）；
5. 数字好看但与实际资源投入完全不匹配。

**建议：**宁愿保守、渐进式，也不要“PPT 式暴涨”。

---

## Q224：是否需要在商业计划中对“目标市场 (Market Analysis)”做分析？

**A：**必须要有。

包括：

- 欧盟整体市场情况
- 希腊本地市场（如有）
- 竞争对手类型（本地 + 跨境）
- 目标客户群（Retail / Pro / HNWI / Family Office / Web3 项目方等）
- 自身差异化竞争优势（USP）

监管不会要求你做投行级别报告，但必须能说明：

“为什么你在这个时间点来希腊做 CASP，是有商业逻辑的。”

---

## Q225：在产品设计上，是否可以直接复制国外成熟交易所模式？

可以参考，但绝对不能“生搬硬套”。

必须结合：

- MiCA 对不同服务的分类
- 希腊本地对投资者保护的要求
- AML / Sanctions 风控能力
- 本地市场的支付通路 / 法币流转情况

监管非常敏感的问题是：

“你是在复制一个海外高风险平台模式，还是在本地重构一个合规版？”

---

## Q226：业务模式中是否可以设计“自营交易（Proprietary Trading）”？

这是高风险点。

如你同时经营：

- 客户经纪/撮合业务
- 自营盘（Principal Trading）

必须注意：

- 利益冲突（Conflict of Interest）
- 价格操纵 / 市场滥用风险
- 是否构成 MiFID 投资机构活动
- 自营盘是否会动用客户资产（绝对不允许）

大多数初期 CASP 项目会选择：不做自营盘或非常有限地自营。

---

## Q227：是否需要在 Business Plan 中单独写“风险因素（Risk Factors）”？

强烈建议。

包括：

- 市场风险（价格波动）
- 流动性风险
- 对手方风险
- 技术 / 黑客风险
- 监管变更风险
- 税务不确定性
- 商业模式可行性风险

监管希望你对风险有“自知之明”，而不是只写好处。

---

## Q228：是否必须写清楚“退出策略（Exit Strategy）”？

越来越多监管机构会问：

“如果你业务失败，客户怎么办？”

建议在文件中备注：

- 在无法持续经营时的客户资产返还流程；
- 是否有清算计划；
- 是否有第三方托管人可协助迁移资产；
- 如何通知客户与监管。

---

## Q229：希腊 CASP 项目中，是否可以采用“轻资产 + 重技术 + 外包”模式？

可以，但必须解决好：

- 外包风险（见上一章 Outsourcing）；
- 本地实质（Substance）要求：必须有核心管理与合规在希腊；
- 客户资产与数据的管控权。

简言之：**不反对轻资产，但不能是“空壳 + 完全远程操控”。**

---

## Q230：仁港永胜可以帮助怎样梳理 Business Model？

通常会提供：

1. 商业模式梳理 Workshop
2. 业务流程图（Process Flow）+ 资产/资金流转图（Flow of Funds）
3. 完整商业计划书（BP – Regulator Version）
4. 收入模型（Fee Model）+ 审慎假设说明
5. 风险因素章节
6. 结合 MiCA 服务类型匹配业务模式

做到：

一份 BP 能同时给：监管 + 银行 + 股东/投资人 看。

---

## （B）资本金（Capital Requirements）与流动性（Liquidity）

---

### Q231：希腊 MiCA-CASP 的最低资本金要求是多少？

MiCA 对不同类型服务规定了不同的初始资本要求（例如：只做咨询的最低要求与做托管、交易平台的不同），希腊实施法会在此基础上细化。

一般思路：

- 仅提供“投资建议型服务”的 CASP → 较低资本要求
- 提供托管 / 交易平台 / 执行订单类服务 → 较高资本要求
- 多服务叠加时 → 通常取“最高标准”或一定叠加逻辑

实务中，我们建议准备的**实缴资本**会高于法定最低要求，以体现稳健性与抗风险能力。

---

### Q232：资本金可以分期缴付吗？是否必须在申请前全部到位？

通常：

- 正式获牌前，资本必须全部到位；
- 在提交申请前，建议至少先注入一部分（如 50–70%）以显示诚意；
- 监管在最终发牌前，会检查银行证明，确认资本已到位。

**资本金必须是真金白银（Paid-up Capital），不能只是账面承诺。**

---

### Q233：资本金可以通过借款或股东贷款形式注入吗？

监管更偏好：

- 资本金来源为：股东自有资金（Equity），而非高负债注入；
- 股东贷款可以存在，但不能被视为核心监管资本。

如果资本主要来自股东贷款，监管会怀疑：

“公司是否有足够的‘风险自留’能力？”

---

### Q234：资本金是否可以投资其他项目或用于自营加密资产投资？

监管希望看到：

- 监管资本主要用于支持 **CASP** 自身运营与风险缓冲；
- 不应被大量用于投机性投资（特别是高波动加密资产）；
- 不得用客户资产来弥补自营损失。

如要投资，需要：

- 在 Risk Appetite 中明确；
  - 建立限额与审批机制；
  - 确保不会侵蚀监管要求的最低资本。
- 

### Q235：什么是“持续资本充足（Ongoing Capital Adequacy）”要求？

不是“一次性存够资本就完事”，而是：

- 持续满足监管最低资本；
- 定期对业务风险进行评估，判断是否需要追加资本；
- 将资本充足性纳入董事会风险报告。

如业务大幅扩张、风险提高，监管可能期望你**增加资本金**。

---

### Q236：流动性（Liquidity）与资本金有什么不同？

- **资本金**：长期风险缓冲，偏“净资产层面”；
- **流动性**：短期支付能力，偏“现金流层面”。

监管希望：

- 你不仅“账面上有资本”，
  - 还要“随时有现金”支付运营成本、突发事件和合法债务。
- 

### Q237：希腊 CASP 是否需要设置“流动性备付金（Liquidity Buffer）”？

实务建议：

- 为 3–6 个月运营成本设立流动性储备（现金或等价物）；
- 在内部 Policy 中写明：不得随意挪用该部分资金；
- 定期向董事会报告“现金储备 vs 运营成本”的比例。

这是获得监管信任的重要信号。

---

### Q238：资本金可以以加密资产形式存放吗？

监管普遍只认可“法币资本”。

- 加密资产波动性太高，不适合作为监管资本；
- 即便公司持有大量加密资产，监管仍要求“资本金以货币形态计入、存放银行”。

---

### Q239：资本金与客户资产可以存放在同一个银行账户吗？

绝对不可以。

必须至少设置：

- 公司自有运营账户（公司银行账户）
- 客户钱款专用账户（Client Money Account，若涉及法币）
- 税款 / 工资等支付账户（视情况）

混存 = 监管红线。

---

### Q240：是否需要编制 ICAAP/ICARA 类似的“内部资本评估文件”？

MiCA 未必要求完全照搬银行标准的 ICAAP，但越来越多监管（包括希腊）期望：

- 至少有一份“内部资本充足性评估报告”；
- 评估业务风险与所需资本之间的匹配程度；
- 提交给董事会审批；
- 每年至少更新一次。

仁港永胜可按“轻量版 ICAAP”思路为 CASP 编制。

---

### Q241：若公司出现持续亏损，会影响牌照吗？

监管关心：

- 是否仍符合最低资本要求；
- 亏损是否短期可控；
- 股东是否有明确计划继续支持；
- 是否有合理的扭亏计划。

持续亏损 ≠ 一定被吊销牌照，  
但必须持续证明“没有侵蚀监管资本”。

---

### Q242：仁港永胜如何协助设计资本 & 流动性结构？

我们一般会：

1. 根据业务类型 + 服务范围，测算监管资本需求区间；
  2. 帮你设计“股权+资本金+流动性储备”组合；
  3. 在 Business Plan 中嵌入资本充足逻辑；
  4. 设计内部 Capital & Liquidity Policy；
  5. 为董事会准备“资本监控报表模板”。
- 

## (C) 财务报告、监管报表与审计 (Financial Reporting & Audit)

---

### Q243：希腊 CASP 是否必须按 IFRS 编制财务报表？

通常：

- 若为中/大型公司或集团一部分 → 建议采用 IFRS；
- 小公司在本地 GAAP 下编报，但需确保能转换为监管需要的口径。

监管最看重的是：

- 报表真实、完整、可对比；
  - 客户资产与公司资产清晰分列。
-

## Q244：财务年度（Financial Year）可以自选吗？

在设立阶段可选择，但建议：

- 与集团保持一致（如有集团）；
- 若未来计划引入投资人/上市，尽量使用常见年结（月末为 12 月 31 日）。

一旦确定，变更财年需向监管说明理由。

---

## Q245：是否必须指定外部审计师（External Auditor）？

必须有审计师。

审计师职责包括：

- 审核年度财报；
- 出具审计意见（Unqualified / Qualified 等）；
- 对客户资产隔离情况进行检查（特别是 Custody 业务）；
- 必要时向监管报告重大问题。

选择审计师时，尽量选择有加密资产经验的事务所。

---

## Q246：审计师是否会对 Custody / Safeguarding 做专项审计？

越来越常见。

审计师可能会：

- 检查冷/热钱包余额；
- 对账链上记录与系统内账；
- 审查钱包管理控制；
- 检查客户资产与自有资产分离情况。

审计范围可在 Engagement Letter 中事先约定。

---

## Q247：是否有周期性的监管报表（Regulatory Reporting）义务？

一般包括：

- 年度报告（Annual Report）
- 半年度 / 季度报告（视情况）
- AML 专题报告
- 客户投诉汇总
- 重大事件报告（Incident Reports）
- 外包汇总报告

具体格式由 HCMC 或相关监管细则确定。

---

## Q248：出现哪些情况时必须“即时报告（Ad-hoc Reporting）”？

典型触发事件：

- 重大安全事故（例如钱包被黑）
- 严重资本金不足
- 董事 / MLRO / Compliance 突然离任
- 公司结构重大变更（股东重大变动、控制权变更）
- 重大法律诉讼
- 重大客户资产损失事件

文件中应有“重大事件报告政策（Incident & Regulatory Notification Policy）”。

---

## Q249：是否需要编制管理层报告（Management Accounts）？频率如何？

建议至少：

- 每月 / 季度编制管理层内部报表；
- 包括经营损益、资本与流动性指标、风险事件统计。

监管在检查时，会问：

“董事会是如何、以什么数据管理公司的？”

管理层报告是最好的证明。

---

## Q250：是否需要单独披露“客户资金报表（Client Money / Client Assets Report）”？

托管 / 接收客户资金的 CASP → 强烈建议编制：

- 期初余额
- 期间变动（入金/出金/内部转移）
- 期末余额
- 分银行账户 / 分钱包的分布
- 与账目差异说明

有些监管框架甚至会要求由审计师出具“Client Assets Assurance Report”。

---

## Q251：税务（Corporate Tax）在 MiCA 审查中会被问到吗？

税率本身不是 MiCA 的重点，但监管会关注：

- 你是否有合规报税；
- 业务模式是否设计“避税结构”影响合规性；
- 跨境结构是否涉及恶意税务筹划。

在 BP 中简单说明税务假设是加分项。

---

## Q252：仁港永胜是否提供“财务+合规一体化报表模板”？

是的，我们会：

- 提供适用于监管 + 董事会的财报模板；
  - 嵌入资本金、流动性、客户资产等专栏；
  - 配套“Regulatory Reporting Calendar（监管报送日历）”；
  - 提供“重大事件报告模板”。
- 

## （D）成本结构、费用预算与项目实操经验（Cost & Budgeting / Practical Tips）

---

### Q253：在申请阶段，监管会不会质疑“成本预算太低”？

会，而且经常会。

典型问题：

- 你说要做全国性 / 欧盟范围平台，却只预算了很少 IT / 安全支出；
- AML 团队规模与客户数不匹配；
- 外包成本严重低估。

合理的预算是证明“你真的打算长期经营，而不是短期套利”的关键。

---

### Q254：一个典型希腊 CASP 项目，主要成本有哪些？

大致包括：

- 人员成本（管理层、合规、AML、IT、运营）
- 办公与行政成本
- IT 系统开发 / 采购 / 维护
- 云 / 安全 / 钱包服务成本
- 外部顾问（法律、合规、税务）
- 审计与会计费用
- 外包服务费用
- 牌照申请与官方收费
- 监管年费（如有）

Business Plan 中要有清晰拆分。

---

## Q255：是否可以在申请阶段使用“最低/精简版”团队，获牌后再扩张？

可以，但需注意：

- 申请时团队必须满足“最低监管标准”；
- 不可夸张承诺“未来会招聘很多人”来弥补当前明显不足；
- 可以列出“人员扩张计划（Hiring Plan）”，与业务增长挂钩。

监管关注的是“你现在能不能安全运营”，不是“未来画饼”。

---

## Q256：项目资金不足（Runway < 12 个月）会影响审查吗？

会。

监管会问：

- 是否有股东承诺追加资金？
- 是否有备用授信？
- 你预期何时盈亏平衡？

实务建议：

申请时最好能证明“至少有 18–24 个月运营资金”。

---

## Q257：若公司计划同时在多个欧盟国家申请牌照，监管在资本上会怎么看？

MiCA 理论上是单一国获牌 + 护照通行，但很多项目考虑多国布局。

监管会关注：

- 是否造成资源分散；
- 股东是否有足够资本支持多地运营；
- 是否存在监管套利倾向。

在希腊申请时，最好清晰说明：

“希腊实体的定位、资源与独立性。”

---

## Q258：对初创团队来说，“资本投入越多越好吗”？

不一定。

- 资本太少 → 监管觉得你抗风险弱；
- 资本太多 → 衍生出更多监管期望（例如希望你做更多业务 / 增强风控）。

关键是：

- 与业务规模匹配；



- 与股东承受风险能力匹配；
- 与商业计划中“渐进发展”逻辑匹配。

**Q259：如果后续引入新股东或追加资本，是否需要监管批准？**

对于“重大持股变更”：

- 持股比例超过一定门槛（例如 10%、20%、33%、50%）；
- 控制权发生变化；

通常都需要 **事先通知 / 获得监管批准**。  
具体门槛由 MiCA + 希腊实施细则确定。

**Q260：仁港永胜在“业务模式 + 资本 + 财务 + 审计”模块可以提供一站式什么服务？**

我们一般为希腊 MiCA-CASP 客户做：

1. 完整 **Business Plan**（监管版本）
2. 详细 **3–5 年财务模型**（财务预测 + 场景分析）
3. 资本结构与流动性方案设计
4. **Regulatory Reporting & Governance** 模板套装
5. 与审计师、会计师协同对接方案
6. 配合银行开户 & 客户资产账户结构设计
7. 给董事会使用的“合规+财务”月度/季度报告模板

仁港永胜帮助项目方从“想法阶段”直接进化为“可落地、可被监管接受的结构化方案”。

**第 9 章 | 监管沟通、RFI 补件与面谈机制（希腊版 Q261–Q300）**

这是希腊 *HCMC* 监管沟通风格 + *MiCA* 官方审查流程 + 欧盟跨境展业监管习惯综合而成的深度实操版本。  
本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐生** 提供专业讲解。

**(A) 监管沟通机制：流程、节奏、策略（Q261–Q275）**

**Q261：希腊 MiCA-CASP 审查中，“监管沟通”通常在什么时候开始？**

一般在 **正式提交申请后 1–3 周内**，监管会：

- 分配 Case Officer
- 要求补充文件（RFI Round 1）
- 对申请内容做初步合规性评估

若申请材料结构完整、逻辑清晰，沟通会更顺畅。

**Q262：希腊监管是否像德国 BaFin 一样会提出大量 RFI？**

不会像德国那样极端（一次百条），但：

- RFI 通常 20–60 条
- 若申请复杂（含交易平台、托管、多国运营），可能超过 100 条
- 问题深度不亚于 BaFin

希腊 HCMC 更关注：

- 实质经营（Substance）
- AML 控制
- 风险管理与治理

- 客户资产保护
  - 技术安全（Cybersecurity）
  - Outsourcing 风险
- 

## Q263: HCMC 第一次 RFI 通常问的是什么？

第一轮问题一般集中在：

1. 组织架构与治理（Governance）
2. 实质经营（办公室、人员、本地决策权）
3. 股东背景（尤其是资金来源）
4. 商业模式的风险点
5. 客户资产隔离机制
6. AML/CFT（重点）
7. IT 系统与钱包管理

建议：第一轮回复质量决定后续审查节奏。

---

## Q264: 是否可以在第一次 RFI 中“边答边补充文件”？

可以，而且建议：

- RFI 文本回答
- - 附加补充材料（Policy、流程图、截图、Proof）
- - 表格形式的 Cross-Reference（让监管快速找到你回答的位置）

监管最怕的是：申请人光说不证实。  
附文件，才有公信力。

---

## Q265: 希腊 HCMC 比较看重什么风格的回复？

三大原则：

### ① 切题（Direct Answer）

每个问题必须逐字、逐点回答。

### ② 有证据（Evidence-based）

最好附上：

- 政策文件
- 程序流程
- 操作截图
- 控制措施证明
- 板块组织图
- 钱包架构说明
- 资金流向图
- 审计/监控报表样本

### ③ 一致性（Consistency）

你的回答必须与：

- Business Plan
- AML Manual
- Risk Register

- Outsourcing Agreement
- 技术架构文档
- 公司治理结构

保持一致。

---

## Q266：监管最讨厌看到怎样的 RFI 回答？

典型雷区：

- “我们稍后会制定...”
- “未来计划是...”
- “我们打算聘请某某外包处理...”
- “会根据监管要求调整...”

翻译：你现在还没准备好。

MiCA 监管喜欢：

“你已经准备好了，我来确认你是否合规。”

---

## Q267：若不理解监管问题，可以直接问监管吗？

可以问，但必须专业且不显得无准备。

正确问法示例：

“为了确保我们按监管意图准确答复，是否可确认本问题中您指的是（A）客户资金隔离逻辑，或（B）内部账簿与区块链 reconciliation 的技术要求？”

错误问法：

“我们不明白您想问什么，请解释。”

---

## Q268：RFI 回应的典型周期是多久？

通常：

- 第一轮 2–4 周
- 第二轮 2–3 周
- 第三轮如有，1–2 周  
（取决于申请人的准备程度）

提交快但答得马虎 = 对你不利。

高质量答复永远比“快速但敷衍”更重要。

---

## Q269：可以向监管申请延期提交 RFI 吗？

可以，但须注意：

- 一般只能延期 1 次
- 延期理由必须正当（例如大量新增信息需要董事会批准）
- 建议延期不超过 1–2 周
- 监管会评估你的项目管理能力

避免频繁延期，会降低监管对你的信任。

---

## Q270：监管是否会要求提供“补充证明文件”例如银行账户流水？

可能要求：

- 股东资金来源证明

- 客户资产独立账户证明
- 钱包地址 Ownership 证明
- 服务供应商资质证明
- 外包 SLA
- SOC2 / ISO27001 认证
- IT 架构图
- Third-party penetration test（如适用）

若是托管 / 交易所模式，会更严格。

---

### Q271：希腊监管是否会要求“控股股东面谈”？

可能。

特别是：

- 股东为海外公司
- 股东结构复杂
- 股东资金来源说明不充分
- 存在高风险司法管辖区关联

监管面谈重点：

- 资金实力
  - 业务背景
  - 公司战略
  - 风险承受能力
  - 对 MiCA 监管框架的理解
- 

### Q272：是否会出现“监管反问监管”的情况？

有时监管会反向问：

- 你为什么选择希腊？
- 为什么不在你主要业务所在国申请？
- 为什么业务主要在海外，却将牌照设在希腊？

必须准备一份：

**Country Choice Rationale（选择希腊的理由）**

仁港永胜会协助编写。

---

### Q273：是否可提前模拟 RFI？

是的，这也是仁港永胜的强项。

我们会：

- 提供 300 条 MiCA-EU 通用 RFI
- 按希腊风格定制 60–120 条本地化问题
- 模拟监管面谈
- 检查回答一致性
- 给出改进建议

100% 客户反馈：

“提前模拟一次，正式 RFI 容易一倍。”

---

### Q274：监管沟通中是否可以“隐藏”敏感信息？

不可以。

包括：

- 高风险司法辖区关联
- 历史违规记录
- 技术外包风险
- 系统漏洞
- 资金来源不透明
- 关联交易

监管迟早会发现。

正确做法：

提前解释 + 风险缓释措施。

---

## Q275：RFI 是谁负责？CEO？MLRO？合规总监？外部顾问？

最佳结构是：

- 合规（主导起草）
- AML（负责 AML 章节）
- CTO（技术、钱包、系统安全）
- MLRO（制裁、监控、STR 流程）
- 法律（检查一致性）
- 仁港永胜（总体架构、监管语言、文件打磨）
- 董事会（最终审核）

绝对不能：

- 把所有 RFI 回答丢给一个人  
或
  - 完全依赖外包（监管不信任）
- 

## （B）监管面谈（Interview）机制（Q276–Q290）

---

### Q276：希腊是否一定会进行面谈？

视情况而定：

- 若业务简单（如仅投资咨询）→ 不一定
  - 若涉及托管 / 交易 / 关键外包 → 几乎必面谈
  - 若股东结构复杂 → 必面谈
  - 若 AML 风险高 → 必面谈
  - 若申请材料不清晰 → 必面谈
- 

### Q277：面谈级别有哪些？

一般分三个层级：

1. 初步沟通会议（Intro Call）
  - 介绍公司
  - 介绍团队
  - 监管澄清若干问题
2. 深入技术 / 风险面谈（Technical & Risk Interview）
  - CTO / 合规负责人 / MLRO 参与
  - 钱包、风控、链上监控、STR 等细节
3. 董事会与股东面谈（Governance Interview）

- 评估管理层是否“适合与适当 (Fit & Proper)”
  - 评估决策能力与风险文化
- 

## Q278：监管面谈的风格是尖锐还是友好？

希腊监管风格偏理性、专业、中等强度。

不像德国 BaFin 那样“咄咄逼人”，  
也不像法国 AMF 那样“逻辑严密到零容错”。  
但若准备不足，也会迅速暴露。

---

## Q279：技术面谈一般问什么？

重点包括：

- 钱包架构（热/冷分层、MPC、多签）
- 存取流程（Deposit/Withdraw）
- 私钥管理（HSM、权限分级、MFA）
- 区块链监控（Chain Analysis、AML Risk Scoring）
- 系统高可用（HA）
- 事件响应（Incident Response）
- 数据安全（备份、恢复、加密）

监管要判断：

“你是真的懂技术，还是只是讲 PPT。”

---

## Q280：合规 / AML 面谈重点是什么？

常见考点：

- KYC / KYB 流程
  - 风险评级模型
  - 不同客户群体的差异化尽调
  - 交易监控算法（RBA）
  - STR 提交流程
  - Sanctions Screening
  - 黑名单管理
  - Travel Rule 的落地方式
  - 高风险国家客户的限制措施
- 

## Q281：董事会面谈重点是什么？

重点不在技术，而在：

- 战略（Strategy）
- 资本实力（Capital Backing）
- 风险文化（Risk Appetite）
- 业务可持续性（Sustainability）
- 对监管框架的理解
- 合规承诺（Compliance Commitment）

监管关注：

“董事会是否真的在管理公司，而不是挂名？”

---

## Q282：面谈是否会失败？

会。

常见失败原因：

- 关键人员水平不达标
  - 董事会不了解业务
  - 技术负责人无法解释关键流程
  - MLRO 不熟悉 AML 制度
  - 与申请文件内容不一致
  - 回答含糊、避重就轻
  - 承认信息不真实或准备不足
- 

### Q283：面谈能否提前准备？

当然，这也是仁港永胜的核心服务内容。

我们会：

- 提供 **100 题面谈库（希腊版）**
- 逐题模拟监管对话
- 纠正用词、逻辑、表达方式
- 模拟突发提问
- 检查“文件与回答是否一致”

客户反馈：

“模拟一次，相当于通过一半审查。”

---

### Q284：是否需要准备面谈 PPT？

不强制，但我们建议准备：

- 组织架构
- 钱包管理
- 客户资产隔离机制
- 风险管理架构
- AML 流程图
- 技术架构图
- Outsourcing Map
- 业务流程图

监管喜欢“清晰可视化”。

---

### Q285：在面谈中可以反问监管吗？

可以，但必须：

- 简洁
- 不反驳
- 不显得质疑监管立场
- 不显得没有准备

适当反问可显示专业和成熟。

---

### Q286：面谈前需要向监管提交材料吗？

通常需要提交：

- PPT
- 最新人员名单

- 技术架构
- AML 政策最新修订版
- 外包服务清单
- Flow of Funds / Flow of Assets

监管越清楚你的准备，面谈越顺畅。

---

### Q287：面谈后通常多久会收到下一轮 RFI？

一般 1–3 周。

说明监管在：

- 记录回答
  - 要求支持性证据
  - 要求进一步澄清
  - 核查内部一致性
- 

### Q288：面谈结束是否代表“快要发牌”？

不一定。

面谈意味着：

- 已进入审查深水区
- 监管认为你值得继续评估
- 但仍可能进入
  - RFI 3
  - 文件补正
  - 人员补充
  - 操作测试（如托管业务）

只有当监管已确认：

- 人员合格
- 资本充足
- 系统稳健
- 风险控制合规
- AML 有效
- 审计机制清晰

才会准备最终批准。

---

### Q289：如果关键人员在审查期间离职，会发生什么？

这是致命事件之一。

监管可能要求：

- 暂停审查
- 提供替代人员简历
- 重新面谈
- 重新审查 Fit & Proper
- 更新组织架构
- 更新 Policies

严重时申请可能被终止。

---

### Q290：仁港永胜如何协助“面谈准备”？



我们会：

1. 模拟面谈官
2. 逐人训练 CEO / CTO / CCO / MLRO
3. 检查回答一致性
4. 提供标准答案框架
5. 整理面谈资料包
6. 准备 PPT 套件
7. 通过案例让管理层理解监管思维

---

## (C) 补件 (RFI) 深度拆解 (Q291–Q300)

---

### Q291: 补件失败的典型原因有哪些？

5 大致命错误：

1. 回答含糊、不具体
2. 回复没有证据，没有附件
3. 回答与原申报文件自相矛盾
4. 避重就轻，让监管再次追问
5. 使用“未来会如何”代替“现在如何”

---

### Q292: HCMC 的 RFI 通常最严的部分是什么？

三大模块：

- AML
- 客户资产保护
- 技术安全 (Cybersecurity)

特别是托管业务，极其严格。

---

### Q293: RFI 中的 AML 问题深度如何？

深度极高，例如：

- 如何识别 DeFi 风险？
- 如何识别 Mixing / Privacy Coins？
- 对 Tornado Cash 历史交易如何处理？
- 你的地址风险评分模型是什么？
- 是否使用 Chainalysis / Elliptic？
- 对 OFAC 关联地址如何处理？

MLRO 必须能回答得“专业且自信”。

---

### Q294: RFI 中的“客户资产保护”问题一般有哪些？

- 钱包分层结构
- MPC / Multi-signature 流程
- 冷钱包隔离
- 客户与公司资产分账方式
- 私钥权限管理
- Withdraw 审批机制
- Reconciliation (链上与账面一致性)
- 事故恢复 (DR) 与 BCP

这些必须在文件中写到“可操作级别”。

---

## Q295: RFI 关于“外包 (Outsourcing)”会问什么?

重点如下:

- 外包是否涉及关键功能?
- 供应商是否有监管资质?
- SLA 内容?
- 数据存储地?
- 风险分类?
- 退出机制?
- 第三方风险监控?

若外包过多, 会被质疑“空壳公司”。

---

## Q296: 审查过程中发现申请文件不一致, 会怎样?

监管会立即问:

“你是否真正理解自己的业务?”

最严重情况下:

- 要求重新提交
- 要求补充分析
- 甚至拒绝申请 (极端情况)

仁港永胜的核心服务就是 保证文件一致性。

---

## Q297: 在 RFI 中是否可以“修复错误”?

可以, 但要注意:

- 必须诚实承认“为了确保一致性, 我们已更新文件”
  - 必须附“修订版”
  - 必须解释为什么修订
  - 必须更新所有相关文件 (避免连锁矛盾)
- 

## Q298: RFI 最终审查通过后, 是否还会有“License Conditions (附带条件)”?

有可能。

例如:

- 6 个月内补充新人员
- 定期提交 AML 报告
- 降低某类高风险客户比例
- 增加强制冷备份
- 限制部分产品先不开放 (如 Earn)

附带条件并不代表你不合格, 而是监管“谨慎许可”。

---

## Q299: 获得批准后, 多久会正式发牌?

通常:

- 批准通知 (Approval Letter) 后
- 完成资本金最终验证
- 完成某些技术合规证明

- 完成公司注册登记更新
- 最终确认后即可发牌

一般 2–6 周内完成。

---

### Q300：仁港永胜在 RFI、面谈、补件全流程中提供什么级别协助？

我们提供：

#### 一级服务：监管沟通总包

- 撰写全部 RFI 回答
- 附件准备
- 文件一致性审查
- 时间节点管理
- 监管邮件往来草拟
- 所有文件的监管语言优化

#### 二级服务：面谈总包

- 100 题模拟面谈
- 董事会培训
- MLRO/CTO 一对一训练
- 面谈资料包整理
- 技术架构图重绘
- 场景式突发提问模拟

#### 三级服务：全套政策文件修订

- AML Manual
- Risk Register
- Governance Manual
- Outsourcing Policy
- Cybersecurity Manual
- Client Asset Protection Rules

你只需要准备人员与真实业务，我们仁港永胜负责让文件成为“监管会接受的版本”。

---

## 第 10 章 | 跨境护照、分支机构、集团结构与多牌照布局

(Q301–Q320 | 希腊 Greece (MiCA) CASP 版)

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

### (A) MiCA 护照 (Passporting) + 跨境展业机制

---

#### Q301：在希腊拿到 MiCA-CASP 牌照后，是否可以在整个欧盟/EEA 30 国展业？

可以。

- MiCA 采用“单一授权 + 护照机制 (Single License + Passporting)”；
- 在希腊取得 CASP 授权后，可以向其他 EU/EEA 监管机构做 跨境通报 (Notification)，在当地合法提供同类服务；
- 前提是：你只能在境外提供 与希腊获批范围一致的服务类型，不能超范围经营。

---

#### Q302：护照机制下，是否需要在每个成员国再申请本地牌照？

不用重新申请牌照，但需要履行“通知 + 本地要求”：

- 不需要再拿第二张 MiCA-CASP 牌照；
- 但需向目标成员国监管机构做 **Passport Notification**；
- 配合当地在消费者保护、税务、广告、语言披露等方面的额外要求。

---

### Q303：护照机制下，业务模式可以在不同国家“差异化设计”吗？

可以有差异，但必须注意：

1. 不得超出希腊获牌范围；
2. 若在某国开展新的服务类型（希腊未获批），可能构成违法；
3. 本地广告、语言、适当性评估要兼顾当地规则（有些国家更保守）。

建议：

先在希腊拿到完整服务范围，再往外护照扩展。

---

### Q304：护照通知（Passport Notification）的大致流程是怎样的？

典型步骤：

1. 向希腊监管（Home State）提交跨境展业计划；
2. 说明目标国家、目标客户群、拟提供服务类型；
3. 附商业计划概要 / 风险评估 / 本地联络安排；
4. 由希腊监管转发至目标国监管（Host State）；
5. 一定等待期后，即可在目标国开始提供服务（具体时间视 MiCA 实务细则）。

---

### Q305：护照业务是否需要在目标国设立办公室或人员？

跨境提供服务（Cross-border）：

- 通常可在无本地实体情况下远程提供服务；
- 但需满足本地消费者保护、语言披露等要求。

设立分支机构（Branch）：

- 若在当地设立常设机构，则会被视为“分行/分支”；
- 需满足额外的治理与合规要求。

两种模式都在 MiCA 框架下，但监管期望不同。

---

### Q306：选择希腊作为 MiCA-CASP Home State，有什么跨境布局上的优势？

常见优势逻辑：

- 社会成本与薪酬水平相对部分西欧国家更可控；
- 金融与法律体系成熟、受欧盟框架约束；
- 监管态度总体开放，但专业；
- 适合作为 “南欧枢纽 + 地中海+中东连接点”；
- 有利于后续与塞浦路斯、马耳他等地区形成多点布局。

仁港永胜可以帮你整理一份 “Why Greece” 专门说明，用于 BP 和与监管沟通。

---

### Q307：护照机制下，如何管理“多国监管期望不同”的问题？

实务上要做：

1. **Home vs Host Requirements Mapping**（监管要求对照）；
2. 为每个重点目标国编制简要合规备忘录（广告、销售规则、投资者保护等）；
3. 内部设立 **EU Passporting Coordinator** 角色，专门跟踪多国监管变更；

### Q308：护照扩展业务前，是否需要更新内部政策和程序？

需要。

例如：

- Complaints Handling Policy 需覆盖新国家；
- KYC/客户适当性评估需考虑本地法律与风险；
- 市场推广与广告政策需适应当地要求；
- 税务处理与发票开具方式可能不同。

简单说：

每扩一个国家，至少要做一次“Country Add-On Compliance Review”。

---

### Q309：对于非欧盟/EEA 客户，护照机制是否仍然适用？

不适用。

MiCA 护照只在 EU/EEA 30 国有效。

对非欧盟客户：

- 需遵守相应国家的本地金规/虚拟资产规制；
  - 可能需要取得本地牌照或设立实体；
  - 或采取限制性服务模式（只接收“主动来访”客户等）。
- 

### Q310：如果在某成员国遇到监管调查或处罚，是否会影响整个 EU 护照？

很可能影响。

- 主国（希腊）监管会被通知；
- 可能要求解释整改；
- 情节严重时，甚至会影响主牌照（Home License）本身。

因此跨境展业不能把某些国家当作“监管洼地”去冒险。

---

## （B）分支机构（Branch）与子公司（Subsidiary）结构

---

### Q311：在 MiCA 框架下，什么情况下建议设立分支机构（Branch）？

通常在以下情形：

- 某个国家业务量大、客户多；
- 需要本地团队面对面服务（如机构客户、家族办公室）；
- 当地监管文化偏好“有本地存在”；
- 需要本地语言与法律支持。

分支机构是 Home State 牌照的延伸，本身不是单独法人。

---

### Q312：分支机构与子公司在监管上的差别是什么？

- **Branch（分支机构）**
  - 没有独立法人资格；
  - 由希腊 CASP 直接负责；
  - 监管责任主要仍在主国（希腊）；
  - 更便于统一管理 with 资本使用。
- **Subsidiary（子公司）**

- 独立法人；
- 通常需要本国监管授权；
- 在各自国家承担独立监管义务；
- 适合大型集团结构、多牌照布局。

---

### Q313：作为希腊 CASP，在其他国家设立子公司是否会削弱 MiCA 护照意义？

不会削弱，但模式不同：

- 护照：一张牌照 + 多国服务 → 管理集中，合规统一；
- 多子公司：多国本地化牌照 → 管理分散，但贴近本地市场。

很多大型集团会采用“希腊 MiCA-CASP + 若干本地子公司牌照”混合模式。

---

### Q314：分支机构的管理结构一般怎样设计比较合理？

常见做法：

- 本地 Branch Manager（负责当地运营与合规落实）；
- AML Local Contact（与本地 FIU 通信）；
- 定期向希腊总部报告（包括客户投诉、重大事件、KPI）；
- 所有关键政策与制度仍由希腊总公司统一制定。

---

### Q315：分支机构必须有本地实体办公室吗？

大多数情况下，有实体办公室更符合监管预期：

- 作为客户沟通点；
- 体现实质经营；
- 内部会议场所；
- 存档某些本地必要文件。

极端“纯虚拟办公室”模式容易引起监管疑虑。

---

### Q316：集团结构复杂（多层控股、信托、离岸公司）会增加获牌难度吗？

会明显增加难度。

监管会担心：

- 穿透股权后，无法明确最终实益拥有人（UBO）；
- 存在避税/规避制裁/洗钱风险；
- 控制权实际掌握在不透明主体手中。

实务建议：

尽量用清晰、透明的股权结构去申请 MiCA-CASP，  
避免过多离岸与信托叠加。

---

### Q317：集团内部是否可以有多个 CASP 牌照（不同国家）？

可以，但需注意：

- 不同实体之间的业务分工；
- 避免在客户面前混淆身份（谁是合同相对方）；
- 避免“选择监管较松的一方去接风险较高的业务”；
- 内部需有集团层面的风险与合规协调机制。

---

### Q318：如果集团在其他国家已有虚拟资产牌照，是否对希腊 MiCA 审查有帮助？

有，一方面：

- 说明团队有实务经验；
- 可提供他国监管同意 / 无异议证明；
- 提升可信度。

另一方面：

- 监管也会审查“在其他国家有无处罚记录”；
- 需要诚实披露，并说明整改。

---

**Q319：是否可以在集团层面统一配置 AML / Risk / IT 安全部门？**

可以，但需满足：

1. 本地实体（希腊 CASP）仍保留关键合规与决策权；
2. 集团层面与本地层面职责划分清晰；
3. 不得因集团集权导致本地主体沦为“执行点”；
4. 监管需要看到“希腊本地有足够管理能力”。

这在文档中一般通过 **Matrix Structure（矩阵汇报线）** 来呈现。

---

**Q320：仁港永胜在“希腊 Home + 多国布局”结构设计方面可以做什么？**

我们会：

- 帮你评估哪国适合作为 MiCA Home State；
- 设计集团结构（股权、实体分工、牌照组合）；
- 设计 EU Passporting 路线图；
- 为每个目标国出具简要合规分析；
- 设计 Branch / Subsidiary 管理模型；
- 准备“Why Greece + EU Strategy”说明部分，便利你向监管/股东/银行解释布局逻辑。

---

# 第 11 章 | 客户保护（Client Protection）、投诉机制、营销宣传（Marketing）与透明度要求（Q321–Q360 | 希腊版）

这是 *MiCA + 希腊 HCMC* 的结合版实操指南，深度适用于申牌、内部合规建设及日后监管沟通。  
本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

## （A）客户保护与投资者保障（Client Protection）

---

**Q321：MiCA 对客户保护的核心原则是什么？（希腊监管特别强调）**

三个监管永恒原则：

1. 透明性（Transparency）
  - 所有费用、风险、执行方式、资产性质必须提前披露。
2. 适当性（Appropriateness）
  - 不得向风险承受能力不足的客户 提供复杂/高风险产品。
3. 公平性（Fair Treatment）
  - 不得误导、不得隐瞒、不得通过复杂机制“掩盖风险”。

希腊监管尤其强调 “消费者保护优先于商业目标”。

**Q322：哪些客户必须做适当性评估？**

MiCA 要求对所有使用下列服务的客户进行适当性评估（Appropriateness Test）：

- 虚拟资产交易
- 虚拟资产接收与传送
- 投资建议
- 投资组合管理
- 订单执行
- 托管服务

判定要素包括：

- 财务状况
- 风险偏好
- 投资经验
- 知识水平
- 可承受损失能力

---

**Q323：适当性评估是否需要“自动评分系统”？**

不强制，但强烈鼓励。

最佳配置：

- 自动评分（System Scoring）
- - 人工复核（Manual Review）
- - 存档（Audit Trail）

监管会检查评分算法逻辑，是否有“风险触发机制（Trigger Rules）”。

---

**Q324：哪些客户应被视为“高风险客户”？**

典型包括：

- 身处或与 **FATF 高风险地区** 有关联
- 使用混币服务、DeFi 路径复杂
- 大额交易且无合理解释
- 过度杠杆/高频投机型操作
- 通过隐私币（Monero、Zcash 等）进行操作
- 经常跨境大额转入
- 投资经验不足但交易非常活跃

若客户被识别为高风险，必须强化 KYC/EDD 与持续监控。

---

**Q325：MiCA 是否要求提供风险警告？**

必须提供。

风险披露包括：

- 市场波动风险
- 技术风险（钱包、系统、链上风险）
- 对手方风险
- 法律风险
- 资产可能归零的风险
- 无担保、无存款保险（特别必须强调）



- 黑客攻击与系统漏洞风险

希腊监管特别强调文案要“清晰易懂，避免技术性掩盖风险”。

---

### Q326：是否允许向所有客户提供“高风险产品”？

允许，但需满足：

- 完整适当性评估
- 额外风险警告
- 关键风险指标展示
- 对新手或不适格客户要限制访问（如限制开仓规模）

MiCA 不鼓励“激进分销”，特别是没有经验的客户。

---

### Q327：是否允许销售“复杂结构化虚拟资产产品”？

如果产品涉及：

- 收益承诺
- 算法收益
- 自动再质押
- DeFi liquidity mining
- Derivatives-like 结构

监管会视为“复杂产品”，需要额外控制，包括：

- 额外披露
  - 风险问卷升级
  - 客户签署高风险确认书
  - 强制冷静期（Cooling-off）
- 

## （B）客户资金与资产保护（Safeguarding）

---

### Q328：MiCA 要求客户资产与公司自有资产隔离吗？（希腊极度重视）

绝对必须隔离（Segregation）。

涉及：

- 钱包层级隔离（On-chain segregation 或 Ledger segregation）
- 内部账簿隔离
- 资金流隔离
- 客户资产不得被抵押、质押、借贷
- 公司不得将客户资产用于运营或对冲

希腊监管在审查此项几乎是“零容忍”。

---

### Q329：客户资产消失时（如黑客攻击），CASP 是否要赔偿？

MiCA 强调：

若因 CASP 的管理、技术、或安全失误导致资产损失，CASP 需承担全额责任。

不允许将责任强行转嫁给客户。

也不能在 Terms 中写“我们不负责任”这类条款。

---

### Q330：是否必须提供客户资产对账（Reconciliation）？

必须每日进行：

- Blockchain vs internal ledger
- Hot wallet vs cold wallet
- Fiat safeguarding account vs ledger

需记录：

- 差异原因
- 调整步骤
- 审核人
- 风险报告

监管会抽查记录。

---

### Q331：是否必须设置客户专用 Safeguarding 账户？

如果公司涉及法币业务：

- 必须设立客户专用账户（Client Money Account）
- 账户必须在受监管金融机构开立
- 公司不得混用（混同 = 严重违规）

虚拟资产对应链上钱包也必须隔离。

---

### Q332：是否需要“客户资产政策（Client Asset Protection Policy）”？

需要，内容包括：

- 钱包架构及控制
- 权限分工
- 交易审批流程
- 冷热钱包管理
- Reconciliation 流程
- 客户资金隔离
- 灾备计划（DR）
- 安全事件应对流程

仁港永胜提供完整模板。

---

### Q333：是否可以对客户资产进行“借贷、质押、收益增强”等操作？

MiCA 明确禁止：

- 未经客户明确授权，不得挪用客户资产
- 不得为了收益而借出客户资产
- 若允许“收益产品”，必须独立结构、完全透明、风险披露充分

希腊监管对这类业务格外谨慎。

---

## (C) 客户投诉（Complaints Handling）

---

### Q334：MiCA 是否要求设立正式投诉机制？

必须设立 Complaints Handling Framework，包括：

- 投诉程序
- 受理渠道
- 投诉登记册（Complaints Register）

- 内部升级机制
- 回复期限（通常 ≤15–30 天）
- 年度投诉分析报告

监管会抽查投诉记录与结案证明。

---

### Q335：投诉是否必须用客户本国语言回复？

不强制，但必须满足：

- 客户能读懂；
- 语言不得造成误导；
- 对欧盟主要语言（EN/FR/DE/ES/IT/EL）至少提供英文回复。

希腊监管允许英文作为主要沟通语言，但若业务针对某国，应考虑本地语言。

---

### Q336：是否必须有“投诉专员”？

需要，但不一定是专职，可以由：

- 合规负责人
- 客服主管
- 运营主管

但必须独立于销售部门。

---

### Q337：是否需要每年向董事会报告投诉情况？

需要，内容包括：

- 投诉数量
- 分类
- 根本原因（Root cause）
- 整改计划
- 预防措施

监管非常重视消费者保护文化。

---

### Q338：客户不满意内部回复是否可以升级到监管机构？

可以。MiCA 框架允许：

- 国家监管机构（希腊 HCMC）
- 消费者保护机构
- 金融仲裁机制（如 ADR/ODR 平台）

因此内部投诉处理必须专业且充分。

---

## （D）市场推广（Marketing）与广告合规

---

### Q339：MiCA 对虚拟资产广告有何核心要求？

必须遵守：

- 公平
- 清晰
- 不误导
- 风险警告显著

- 不夸大收益
- 不隐藏重大风险
- 不允许未经授权使用“监管背书”语言

广告也必须在内部政策下逐条审查。

---

### Q340：线上广告（Facebook、Google、TikTok）需要额外遵守要求吗？

是的，包括：

- 再营销（Retargeting）限制
- 禁止针对弱势群体（如未成年人）
- 清晰展示风险警告
- 存档广告版本与发布日期（Audit Trail）
- 透明说明费用与潜在损失

监管会要求你证明广告未误导。

---

### Q341：是否可以用“我们受监管”“我们安全可靠”等字眼？

可以，但要非常谨慎：

禁止：

- “Guaranteed return”（保证回报）
- “Safe investment”（安全投资）
- “Zero risk”（零风险）
- “Government-backed”（政府担保）

可以：

- “Licensed under MiCA by the HCMC”
  - “Regulated CASP in the EU”  
（条件是真有牌照才能写）
- 

### Q342：是否需要对每一条营销内容做内部审批？

MiCA 要求：

- 所有市场推广内容必须经过合规部门审批；
  - 必须保存营销审批记录；
  - 必须保存广告的最终版本与投放时间；
  - 必须保留“风险评估文件”（证明广告不会误导）。
- 

### Q343：是否允许网红（KOL）推广？

可以，但必须：

- KOL 明确披露“这是广告”；
  - KOL 不得夸大收益；
  - KOL 不得暗示 CASP 提供“投资建议”；
  - CASP 必须监督 KOL 文章/视频内容；
  - 必须保留所有合作记录与审查证据。
- 

### Q344：是否允许“活动奖励”“推广赠金”类营销？

可以，但条件严格：

- 不得误导客户认为可获得稳定收益；

- 不得诱导客户承担不适当的投资风险；
- 必须披露所有条款条件；
- 不得向不适格客户推广高风险产品。

---

### Q345：是否禁止“推荐好友”计划？

未禁止，但需确保：

- 不得构成“诱导性交易”
- 不得对新手客户造成不当风险
- 必须明确披露奖励条件与风险

许多国家（如法国/荷兰）对此类行为更严格，护照业务需格外留意。

---

### Q346：是否必须有“Marketing Policy”？

必须。

内容包括：

- 广告审批流程
- 风险评估规则
- 禁用词（Banned words）
- 风险警告模板
- 合规检查清单
- 存档与记录保留机制
- 第三方推广（KOL/代理）的要求

仁港永胜可提供完整模板。

---

## （E）透明度（Disclosure）与 Terms of Service

---

### Q347：MiCA 对披露要求有哪些？

必须公开披露：

- 公司信息
- 服务范围
- 风险披露
- 手续费结构
- 托管机制
- 客户资产隔离方式
- 清算与结算方式
- 投诉机制
- 费用变更通知机制

必须清晰、易懂、可下载。

---

### Q348：Terms of Service 是否必须每次更新都告知客户？

是的，但可采用：

- 邮件通知；
- 客户中心通知；
- App 内提醒；
- 更新日志（Changelog）。

必须给予客户合理时间审阅。

---

### Q349: 是否可以在 Terms 中加入免责条款？

可以，但不能：

- 免除 CASP 的监管义务；
- 转嫁安全疏忽的责任；
- 转嫁非客户过失造成的损失；
- 免除客户资产保护责任。

若 Terms 过度偏向 CASP，监管会要求修改。

---

### Q350: 是否需要提供“费用一览表”(Fee Schedule)？

必须。

包括：

- 交易费
- 提现费
- 充值费
- 保管费
- 未活跃账户费用（如适用）
- 其他隐含费用

费用不可“隐藏在多页条款深处”。

---

## (A) 系统安全与网络风险 (Cybersecurity)

---

### Q351: MiCA 要求 CASP 至少采用哪些 IT 安全基线？是否必须对标国际标准？

是的，MiCA 要求 CASP 必须使用“行业公认标准”。

希腊监管期望采用：

- **ISO 27001** 信息安全管理体系
- **NIST Cybersecurity Framework**
- **ENISA**（欧盟网络安全局）指南
- **EBA ICT & Security Guidelines**（银行标准，用于 MiCA 参照）

最低必须具备：

1. 访问控制 (IAM / RBAC)
2. 日志监控 (SIEM)
3. 网络隔离 (Network Segmentation)
4. 加密 (Encryption at Rest / in Transit)
5. 多因素认证 (MFA)
6. 漏洞扫描 (Vulnerability Scan)

如果 CASP 无法证明对标这些国际标准 → 基本无法获牌。

---

### Q352: MiCA 是否要求 CASP 设立专门的网络安全负责人 (CISO)？

不一定要“CISO Title”，但必须：

- 任命 **IT Security Responsible Officer**
- 拥有网络安全背景
- 具备管理密钥与钱包经验优先

- 不得与 CTO 完全重叠（避免利益冲突）
- 必须可直接向董事会报告

MiCA 关键原则：

“安全职能必须独立，不能只由开发团队负责。”

**Q353：是否必须实施渗透测试（Penetration Test）与漏洞扫描（Vulnerability Assessment）？频率是什么？**

必须实施，并且要求 外部独立团队 执行。

频率：

类别	要求
渗透测试（Pen Test）	每 12 个月 1 次（黑盒为主）
漏洞扫描（VA）	每季度一次
重大系统变更后	必须进行专项安全测试

测试内容必须包含：

- API 安全
- 钱包系统
- 后台管理系统
- 用户端（Mobile / Web）
- 身份认证（IAM）
- DDoS 与流量攻击模拟

## （B）业务连续性计划（BCP）与灾难恢复（DRP）

**Q354：CASP 是否必须提供业务连续性计划（BCP）？最少要求什么？**

必须提供 BCP，包含：

1. 关键业务流程清单（Critical Functions）
2. RTO（恢复时间目标）
3. RPO（数据恢复点目标）
4. 备份策略（Offsite Backup / Cloud Backup）
5. 备用运营地点（Alternate Site）
6. 人员应急通讯机制
7. 危机管理团队（Crisis Management Team）

MiCA 的期望与银行监管一致：

“即使遭受重大事故，也必须保证客户资产与基本功能不受影响。”

**Q355：是否必须实施灾难恢复演练（DR Drill）？频率是什么？**

必须实施灾难恢复演练，并记录：

- 演练计划
- 演练脚本
- 参与人员
- 恢复时间
- 改进点（Post-Mortem）

频率：

- 每年至少一次全面演练
- 关键系统建议半年一次

# (C) 热钱包 (Hot Wallet)、冷钱包 (Cold Wallet) 架构与合规要求

## Q356: MiCA 是否要求 CASP 必须维持冷钱包比例？是否必须披露？

MiCA 未硬性规定比例，但监管普遍期望：

- 冷钱包 ≥ 70–90% (Custody Service)
- 热钱包用于小额流动性

希腊监管偏向传统 EU Custody 框架，倾向：

“越多冷存储 → 客户资产保护越强。”

CASP 必须披露：

- 热/冷钱包比例
- 钱包地址（如可公开）
- 密钥控制方式（MPC / HSM）
- 第三方托管情况

## Q357: 热钱包必须具备哪些安全控制？

必须具备：

- MPC / 多签 (Multi-Sig) 机制
- 限额管理 (Withdrawal Limits)
- 白名单 (Address Whitelisting)
- 实时监控 (24/7)
- 异常交易冻结机制 (Freeze Function)
- 地理风险控制 (Geo-risk)

监管重点：

“热钱包必须减少攻击面，并具备立即响应机制。”

# (D) 密钥管理 (Key Management) 要求

## Q358: MiCA 对密钥管理的核心要求是什么？

MiCA 要求采用“银行级别 (Bank-Grade)”密钥管理：

- 密钥不可单点控制 (No Single Person Control)
- 必须分散化 (Threshold Signing)
- 必须加密存储 (Encrypted Key Shards)
- 必须有灾备流程 (Key Recovery Plan)
- 必须有访问审计 (Audit Trail)
- 必须限制可疑 IP 或地理位置

监管不接受“单一设备、单人掌控私钥”的做法。

## Q359: 密钥必须使用 HSM (硬件安全模块) 或 MPC 吗？



强烈建议使用：

- **HSM (Hardware Security Module)**
- **MPC (Multi-Party Computation)**

监管者通常不接受：

- 本地电脑存储密钥
- 单人保管私钥
- 未加密的密钥明文
- 共享密钥的做法

最安全且被监管高度认可的架构：

MPC + HSM 混合模式。

---

**Q360：是否必须制定“密钥泄露 / 受损应急响应计划”？内容包括什么？**

必须制定，并包括：

1. 密钥泄露检测机制
2. 立即冻结热钱包机制
3. 广播新地址 / 更换密钥
4. 链上追踪与通知用户
5. 监管报告（24 小时内初报）
6. 客户补偿机制
7. 事件复盘与改进措施

MiCA 与希腊监管机构规定：

“密钥事件 = 重大事故 (Major Incident) → 必须在 24h 内通报监管机构。”

---

## 第 12 章 | 技术运营 (Tech Ops)、链上分析 (On-Chain Analytics)、市场滥用防范 (Market Abuse)、Travel Rule (资金链追踪)

(Q361–Q420 | 希腊版)

本章为 MiCA + 希腊 HCMC 技术/AML 实操最重要章节之一。  
本文由 仁港永胜 (香港) 有限公司 拟定，并由 唐生 提供专业讲解。

---

### (A) 交易系统与技术运营 (Tech Operations)

**Q361：MiCA 对交易系统有什么总体要求？**

核心要求包括：

1. 稳定性 (Stability)
2. 高可用 (HA)
3. 可审计 (Auditability)
4. 可控风险 (Controlled Risk)
5. 事件响应能力 (Incident Response)
6. 防止市场滥用 (Abuse Prevention)

HCMC 会要求 CASP 提供：

- 系统架构图
  - 日志机制
  - 权限管理矩阵
  - 安全审计（PenTest）
  - SLA / 冗余策略
- 

### Q362：交易平台是否必须提供“实时监控系统”？

强烈建议使用实时监控工具，包括：

- 撮合延迟监控
- 系统压力监控
- 异常行为预警
- API 滥用侦测
- 交易量激增报警

监管关注：

“平台是否能提前识别异常情况，而不是事后解释。”

---

### Q363：后台管理系统必须具有哪些控制？

最低要求：

- MFA 登录
- RBAC 权限模型
- 交易审批
- 冻结账户
- 日志记录（不可篡改）
- API 管理
- 操作留痕（谁、何时、做了什么）

若无法实现全部监管要求 → 申请基本上不可能通过。

---

### Q364：是否必须提供交易系统的“压力测试”(Load Test) 结果？

MiCA 对大型平台是强制的，但小型平台通常也被要求提交：

- TPS（每秒交易量）测试
  - 撮合速度测试
  - API 并发处理能力
  - 高峰期吞吐分析
  - 节假日和重大行情下的系统表现预测
- 

### Q365：是否允许将交易引擎完全外包？

可以，但属于 **Critical Outsourcing**。需要：

- 外包尽调
- SLA（包含 uptime、latency）
- 冗余节点
- 安全审计
- 监管访问权
- Exit Plan（退出机制）

监管非常关注“可替代性”。

---

### Q366: MiCA 是否要求交易平台提供“自动暂停交易机制”(Circuit Breaker) ?

不是强制，但监管鼓励部署：

- 价格异常波动暂停
- 成交量异常暂停
- 单一账户异常交易暂停

HCMC 特别强调：

“CASP 必须防止市场被操控。”

---

### Q367: 是否必须有“市场风险管理功能”？

需要至少具备：

- 交易限额
- 强制平仓规则（如适用）
- 风险敞口监测
- 资产风险评级
- 异常价格/交易监控

MiCA 对风险管理要求接近传统金融。

---

## (B) 链上分析 (On-Chain Analytics) 与地址风险评分

---

### Q368: MiCA 是否要求使用链上分析工具 (Chainalysis / Elliptic 等) ?

严格来说：

- MiCA 不强制“必须使用某品牌工具”，
- 但 必须具备链上风险分析能力。

监管非常清楚：

没有专业链上监控的 CASP = AML 风险不可接受。

---

### Q369: 链上分析必须涵盖哪些内容？

最基本包括：

- 地址风险评分 (Risk Score)
  - 是否接触 Sanctioned 地址
  - 是否接触 Mixer
  - 是否接触黑市、诈骗、勒索地址
  - 交易路径追踪 (Transaction Pathway)
  - UTXO 分析 (Bitcoin类)
  - Counterparty 风险评估
- 

### Q370: 是否必须记录链上分析的“证据链”(Audit Trail) ?

必须。

包括：

- 风险评分截图
- 链路追踪图
- 分析时间
- 分析人员

- 系统自动记录（若有）

监管会抽查几份真实案例。

---

### Q371：链上分析是否必须与客户风险评级（KYC Risk Rating）整合？

必须整合。

KYC + 链上分析 两者不一致时：

- 必须人工复检
- 必须记录原因
- 必须更新风险等级

例如：

- 客户 KYC 评分 = 低
- 链上分析评分 = 高

这类客户需要升级为 **EDD**（增强尽调）。

---

### Q372：隐私币（Monero、Zcash）是否允许交易？

希腊倾向于与欧盟主流监管一致：

- 允许上市/交易，但 AML 风控必须更严格
- 必须有 **链上风险替代方案**（如交易模式、地址行为分析）
- 若无法监控链上风险 → 监管可能要求下架

这类业务通常要特别解释。

---

### Q373：是否必须拒绝来自 Mixer（混币器）的资产？

监管预期如下：

1. 若来自 **已制裁 Mixer** → 必须拒绝
2. 若来自 **高风险 Mixer 或“拆分隐匿”行为** →
  - 自动冻结
  - 人工调查
  - STR（可疑交易报告）

作为 CASP，必须证明“你能识别并阻断混币风险”。

---

### Q374：链上分析结果出现“风险未知（Unknown）”时怎么办？

监管逻辑：

“Unknown” = 高风险。

必须执行：

- 人工审核
  - 额外证明资金来源
  - 冻结出入金（如必要）
  - 记录调查过程
- 

## （C）市场滥用防范（Market Abuse Prevention）

（MiCA 要求 CASP 遵守类似传统金融的 Market Abuse Rules）

---

### Q375: CASP 是否必须监控市场操纵行为?

必须。

常见操纵行为包括：

- Wash Trading
- Pump & Dump
- Spoofing / Layering
- Insider Trading
- Price Manipulation
- Cross-exchange manipulation

MiCA 明确要求 CASP 配备 **Market Abuse Monitoring Framework**。

---

### Q376: 是否必须进行交易行为监控 (Trade Surveillance) ?

需要。

交易监控系统应能检测：

- 异常订单行为
- 定价异常
- 大额集中度
- 高频策略异常
- 可疑账户协同行为
- 内部员工异常交易

大型 CASP 通常部署专用系统。

中小型 CASP 需要提交监控规则清单。

---

### Q377: 是否必须制定 Market Abuse Policy?

必须，内容包括：

- 禁止行为列表
- 内部员工交易限制
- 监控方法
- 触发机制
- 调查流程
- 内部升级与报告
- 通知监管的义务

仁港永胜可提供可直接提交监管的版本。

---

### Q378: 员工是否允许在平台内自交易? (员工交易政策)

可以，但必须：

- 事前申报
- 禁止利用内部信息
- 设定冷静期 (Blackout Period)
- 限制短期频繁交易
- 记录留存日志

监管对“内部交易风险”非常敏感。

---

### Q379: 是否必须检测跨平台操纵行为?

如果 CASP 确认：

- 客户在多个平台交易

- 行为可构成操纵

则必须：

- 纳入 Market Abuse 监控
  - 必要时向监管提交报告
  - 冻结账户（合理情况下）
- 

### Q380：是否必须有“内部举报人保护机制”（Whistleblowing）？

MiCA 建议设立；希腊监管更倾向要求。

须包括：

- 匿名举报渠道
  - 内部调查机制
  - 承诺不报复举报人
  - 书面政策
- 

## （D）Travel Rule（TR）与资金链追踪（Fund Flow）

---

### Q381：MiCA 是否要求 CASP 强制执行 Travel Rule？

是的，完全强制。

欧盟 2024 年法规已明确：

- 所有虚拟资产转账
- 超过 **0 欧元**（不是 1,000）  
→ 均必须收集与传输 Originator 与 Beneficiary 信息。

MiCA 与 TFR（Transfer of Funds Regulation）结合执行。

---

### Q382：Travel Rule 实施必须实时（Real-time）吗？

必须 **在转账前完成** 发送与接收信息验证。

不能：

- 事后发送
- 延迟补传
- 用截图代替 TR 消息

必须使用 TR 协议（IVMS-101 或兼容格式）。

---

### Q383：如果对方 VASP 不支持 Travel Rule 怎么办？

欧盟监管明确：

- **不得自动发起转账**
- 必须执行风险评估
- 可能要求人工审核
- 如对方在高风险地区 → 建议拒绝

可以采用：

- “Unhosted Wallet Procedure”（自管钱包流程）
- 

### Q384：个人钱包（Unhosted Wallet）如何执行 Travel Rule？

流程必须包括：

1. 验证地址所有权（Signing / Satoshi test / Proof-of-control）
2. 收集用户声明（地址属于本人）
3. 监测链上行为
4. 高风险地址禁止提现

MiCA 特别强调“自有钱包风险必须降低至可控”。

---

### Q385：是否必须保留全部 Travel Rule 记录？

必须至少保存 **5 年**，包括：

- TR 消息（JSON/XML 流）
- 审核记录
- 例外处理
- 错误处理
- 地址关联证明

监管随时可要求抽查。

---

### Q386：平台必须集成哪类 Travel Rule 技术？

常见方案：

- Notabene
- Sumsb TR
- Sygna Bridge
- VerifyVASP
- TRP（Travel Rule Protocol）

监管不指定供应商，但要求：

1. 实时
  2. 可验证
  3. 可审计
  4. 可整合 AML 风险评分
- 

### Q387：Travel Rule 与链上分析必须整合吗？

必须整合，流程如下：

1. 提现 → Travel Rule 验证 →
2. 若通过 → 链上分析自动评分
3. 若分数高 → 冻结 / 人工复核
4. 最终执行或拒绝

监管重点检查“TR + On-chain Analytics”一致性。

---

### Q388：跨境转账是否也受 MiCA Travel Rule 监管？

是的，只要：

- 发起方在 EU  
或
- 接收方在 EU

即可触发 Travel Rule。

---

### Q389：Travel Rule 是否适用于 NFT 或稳定币？

适用于 任何可转移的加密资产 (Crypto-Assets)：

- NFT
- 稳定币
- Utility Token
- Exchange Token
- Wrapped Token

MiCA 不区分资产类型，统一监管。

**Q390：仁港永胜能否协助建立 Travel Rule 全套机制？**

可以，我们提供：

- TR Policy
- Unhosted Wallet Procedure
- Risk Appetite Matrix (资金链风险矩阵)
- TR System Mapping
- AML + TR Workflow 图
- 实操文档 (SOP)
- TR 合规声明模板

**第 13 章 | 内部治理 (Governance)、审计 (Audit)、合规监控 (Compliance Monitoring)、年度报告与重大事件通报 (Incident Reporting)**

(Q391–Q440 | 希腊版)

本章是 MiCA 审查的重心之一，也是监管最关注“真实运营与风险文化”的关键判断点。  
本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

**(A) 内部治理 (Governance Structure)**

**Q391：MiCA 对 CASP 的内部治理结构总体要求是什么？**

必须满足 “三层治理”模型：

- 1. 董事会 (Board)
  - 制定战略、文化、风险偏好
  - 对合规、AML、IT 安全承担最终责任
- 2. 高级管理层 (Senior Management)
  - 负责日常运营、资源管理
  - 负责落实政策、确保执行到位
- 3. 三道防线 (Three Lines of Defence)
  - 业务部门 (风险承担者)
  - 合规与风险管理部门 (监督者)
  - 内部审计部门 (独立检查者)

希腊监管非常强调治理的独立性与实质性 (Substance)。

**Q392：董事会成员需要在希腊居住吗？**

不是强制，但 MiCA+希腊监管鼓励：



- 至少 1 名居住在希腊或欧盟的董事
- 董事会召集必须能即时参与
- 对当地法律、监管、合规有基本理解

如果董事全在第三国，往往会被认为缺乏“本地实质”。

---

### Q393：董事会必须包含哪些专业能力？

MiCA 要求具备以下知识结构：

- 风险管理
- 反洗钱 AML
- IT 安全 & Cyber Risk
- 金融/虚拟资产市场
- 企业治理
- 法律/监管合规

至少要有 1-2 名成员具备强合规/AML 背景，否则审查很难过。

---

### Q394：董事会会议（BoD Meeting）频率有什么要求？

通常：

- 每季度至少一次
- 遇重大风险事件时需临时会议
- 必须保存会议记录（Minutes）
- 记录需体现“审查 + 决策 + 追踪” (Not rubber stamping)

监管喜欢看到“董事会真正在管理公司”。

---

### Q395：董事会会议必须覆盖哪些内容？

包括：

- 经营进度
- 风险分析
- AML 报告
- IT/网络安全报告
- Outsourcing 监控
- 客户投诉统计
- 内审结果
- 资本状况
- 新业务审批
- 市场风险

若会议记录过于空泛 → 监管会视为“治理不足”。

---

### Q396：是否需要设立专门委员会（如风险委员会）？

对于中大型 CASP，强烈鼓励设置：

- 风险委员会（Risk Committee）
- 审计委员会（Audit Committee）
- 合规委员会（Compliance Committee）

小型 CASP 则可将这些职能整合在董事会层面。

---

### Q397：MiCA 是否要求“适合与适当（Fit & Proper）”审查？

是的，监管关注：

- 1. 诚信 (Honesty)
- 2. 能力 (Competence)
- 3. 经验 (Experience)
- 4. 声誉 (Reputation)
- 5. 无犯罪记录 (尤其 AML/金融犯罪)
- 6. 无严重监管处罚历史

通常需提交：

- 简历
- 资格证明
- 无犯罪记录
- 反洗钱背景调查 (如有)

---

**Q398：管理层是否可以兼职？**

可以，但不能出现：

- CEO = MLRO (禁止)
- CTO = 内审负责人 (禁止)
- CFO 兼任风险负责人 (不建议)

MiCA 强调关键职能之间要“适当分离 (Segregation of Duties)”。

---

**Q399：CASP 是否必须有实体办公室与本地团队？**

必须有 **实体运营能力**，包括：

- 办公室地址
- 部分全职员工在希腊
- 关键岗位 (MLRO/合规/运营) 在当地或欧盟境内

如果团队全在第三国，监管很难批准。

---

**(B) 合规职能 (Compliance Function)**

---

**Q400：CASP 是否必须设立独立合规部门？**

必须，即使是小型机构，也必须：

- 有一名独立合规负责人 (可兼职，但不能冲突)
- 向董事会定期报告
- 负责监督政策执行
- 定期进行合规监控 (Monitoring)

---

**Q401：合规负责人 (Compliance Officer) 必须具备什么资格？**

监管期待：

- 欧盟/希腊合规经验
- 虚拟资产合规背景 (加分)
- 熟悉 MiCA 与 AML 规则
- 熟悉 Travel Rule 与链上分析
- 能参与监管沟通

若完全无经验 → 很难通过 Fit & Proper。

---

#### Q402: 是否必须制定“合规监控计划 (Compliance Monitoring Plan)”?

必须，内容包括：

- 每月检查要点
- 每季度重点监控
- 高风险业务专项检查
- 抽样检查流程
- 合规 KPI 指标
- 年度计划

监管会要求提供样本。

---

#### Q403: 是否必须定期向监管提交合规报告?

MiCA 要求：

- 年度合规报告
- 年度 AML 报告
- 风险管理报告
- 技术/安全年度审核
- 客户资产审查报告

希腊监管未来可能要求额外的本地报告义务。

---

## (C) 风险管理 (Risk Management)

---

#### Q404: 风险管理职能是否必须独立?

必须，与合规、运营、业务相分离。

监管期望 Risk Officer 可以：

- 独立评估风险
  - 反对不合理业务拓展
  - 独立报告给董事会
  - 定期出具风险评估报告
- 

#### Q405: MiCA 要求的主要风险类型有哪些?

至少要覆盖：

1. 市场风险
  2. 信用风险
  3. 流动性风险
  4. 操作风险
  5. 技术/网络安全风险
  6. Outsourcing 风险
  7. 洗钱/制裁风险
  8. 声誉风险
  9. 客户集中度风险
  10. 法律风险
- 

#### Q406: 是否必须管理“流动性风险”? (Crypto 也需要?)

是的，MiCA 认为：

虚拟资产价格剧烈波动 → 更需要流动性管理。

需建立：

- Stress Test（压力测试）
- Scenario Analysis（情景模拟）
- Liquidity Monitoring（流动性指标监控）

---

**Q407：是否必须有“风险登记册（Risk Register）”？**

必须。

内容包括：

- 风险类别
- 风险评分（Impact × Likelihood）
- 风险缓释措施
- 控制措施
- 责任人
- 审查频率

仁港永胜可提供 MiCA 适用版模板。

---

## （D）内部审计（Internal Audit）

---

**Q408：MiCA 是否要求 CASP 必须设内部审计（IA）？**

是的，必须具备 独立审计职能。

形式可以是：

- 内部审计团队（大型 CASP）
- 外包给独立审计机构（中小 CASP）

---

**Q409：内部审计必须审查哪些领域？**

至少包含：

- AML
- 风险管理
- 客户资产保护
- IT 安全
- Outsourcing
- 市场滥用监控
- 行为规范
- 客户投诉
- 业务连续性（BCP/DRP）

---

**Q410：内部审计报告必须提交给谁？**

三层提交：

1. 董事会
2. 审计委员会（如有）
3. 监管机构（视 MiCA 执行细则）

**Q411：内部审计的频率是什么？**

一般：

- 全面审计：每年一次
- 高风险领域：每 6-12 个月
- 特定专题审计：根据风险事件需要

---

## (E) 重大事件报告 (Incident Reporting)

---

**Q412：哪些事件必须向监管机构通报？**

包括但不限于：

- 客户资产损失
- 系统安全漏洞
- 黑客攻击
- 数据泄露 (GDPR 72 小时规则)
- 服务中断
- 钱包私钥损害
- 高风险 AML / STR 事件
- Market Abuse 重大事件
- Outsourcing 失败

---

**Q413：通报监管的时间要求是什么？**

MiCA 一般要求：

- 重大事件：24 小时内初报 (Initial Notification)
- 72 小时内补充报告 (Detailed Follow-up)

GDPR 数据泄露遵循 72 小时规则。

---

**Q414：通报内容一般包括什么？**

包括：

- 事件描述
- 影响评估
- 涉及客户数量
- 财务影响
- 技术原因
- 风险评估
- 暂时性措施
- 永久性整改措施
- 避免再次发生的计划

监管非常关注：

“你是否从事件中学习并改进。”

---

**Q415：是否必须建立 Incident Response Policy？**

必须。

内容应包括：

- 事件等级分类（Severity Level）
- 响应团队（IRT）
- 通报监管流程
- 暂停交易机制
- 通知客户机制
- 内部升级流程
- Post-Mortem 分析模板

仁港永胜提供全套模板。

---

#### Q416：重大事件是否必须通知客户？

是的，例如：

- 资产可能受影响
- 数据泄露
- 系统长时间无法使用
- 服务遭受攻击
- 提现受阻

通知方式：

- E-mail
  - App 内通知
  - 官方公告
- 

#### Q417：是否必须记录所有事件（即使未造成损害）？

必须。

需保存：

- 事件日志
- 处理记录
- 原因分析
- 改进措施

监管会抽查事件管理能力。

---

#### Q418：如果平台失误导致客户资产暂时无法提现，是否构成“重大事件”？

多数情况下构成。

监管认为：

“客户无法提取资产 = 严重风险。”

必须通报监管。

---

#### Q419：是否必须向监管提供年度“事件总结报告”？

必须提供，包括：

- 所有事件分类统计
  - 影响分析
  - 已完成整改
  - 待改进事项
  - 风险趋势图
- 

#### Q420：仁港永胜是否可以协助建立治理、审计、风险、事件报告体系？

可以，我们提供：

- Governance Manual
- Compliance Monitoring Plan
- Risk Register（MiCA 版）
- Audit Charter（内部审计章程）
- Incident Response Policy
- Annual Report Templates
- Board Reporting Package 模板

让治理架构达到可直接通过监管审查的水平。

## 第 14 章 | 外部审计、年度审查（Annual Review）、监管报送（Regulatory Reporting）、会计与税务（Accounting & Tax）

（Q421–Q460 | 希腊版）

本章属于 *MiCA 持牌运营后持续监管义务* 的关键部分，希腊监管机构（HCMC + Bank of Greece）通常会比其他国家更关注财务透明度、客户资产独立性、审计可验证性与报表质量。

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

### （A）外部审计 External Audit 要求

#### Q421: MiCA 是否要求 CASP 必须聘请外部审计师？

是的，必须聘请 独立注册会计师（Statutory Auditor）负责：

- 年度财务审计
- 客户资产分离与托管审计
- 技术/系统控制审计（如适用）
- 反洗钱 AML 程序审计
- 审查内部控制有效性

希腊监管极度重视“客户资产保护（Asset Safeguarding）”的审计质量。

#### Q422: 外部审计师是否必须位于希腊？

一般必须是：

- 希腊认可的审计机构 或
- 欧盟境内具备跨境审计执业资格的事务所

非欧盟审计公司通常不被接受。

#### Q423: 审计报告提交给谁？

必须提交：

1. HCMC（主要监管）
2. 希腊税务局（Tax Authority）
3. 公司股东/董事会

MiCA 框架文件也可能要求上传至 ESA 监管平台。

#### Q424: 年度审计报告包含哪些核心内容？

至少包括：

- 财务报表
- 内控测试 (Internal Control Testing)
- 客户资产保护独立审查
- 风险管理有效性评估
- AML 程序执行情况
- Outsourcing 控制有效性
- 系统与数据安全

审计师必须提供“有保留/无保留”意见。

---

#### **Q425：是否必须提供“客户资产保障报告 (Safeguarding Audit Report)”？**

必须。

内容包括：

- 客户资产与公司自有资产分离情况
- 第三方托管审查
- 钱包密钥管理审查
- 链上资产核对程序
- 对账机制 (Reconciliation) 有效性

MiCA 将“客户资产保护”视为监管核心。

---

#### **Q426：CASP 若资产较少，审计要求会减少吗？**

不会。

MiCA 采取“活动风险导向”，而非规模导向。

只要涉及：

- 客户资产
- 虚拟资产钱包
- 交易执行 或
- 돈 handling (资金收付)

就必须履行全套审计义务。

---

#### **Q427：审计周期是什么？**

- 财务年度结束后 **6 个月内** 必须提交完整审计报告
  - 若发现重大问题，审计师必须在 **72 小时内** 通报监管机构
- 

## **(B) 年度审查 Annual Review 要求**

---

#### **Q428：MiCA 是否要求年度 AML/风险审查？**

是的，至少包括：

- 年度 AML 独立审查 (Independent AML Review)
- 年度风险管理审查 (Annual Risk Assessment)
- 年度 IT 安全测试 (Pen Test / Vulnerability Scan)
- 年度 Outsourcing 供应商审查
- 年度政策更新审查

希腊监管比其他国家更强调 AML 执行力度。

---



**Q429：年度 AML 报告必须包含哪些内容？**

一般包括：

- STR 报告数量与类型
- 客户风险分类数据（High/Medium/Low）
- 是否发生高风险国家（HRC）交易
- 交易监测系统有效性评估
- 政策更新
- 资源配置与培训情况
- AML 控制缺陷与整改

**Q430：年度风险评估（ARA）必须覆盖哪些风险？**

至少包括：

- 市场风险
- 流动性风险
- 网络安全风险
- 交易执行风险
- 洗钱风险
- 托管风险
- 行为风险
- 操作风险

必须提供评分模型和矩阵。

**Q431：年度 IT 安全审查是否必须外包？**

对于大多数 CASP，答案为 是。

监管偏好：

- 外部 Penetration Test（黑盒渗透测试）
- 外部 Vulnerability Assessment（漏洞扫描）

内部团队自行测试通常不会被视为“足够独立”。

**Q432：是否必须制定年度合规培训计划？**

必须，包括：

- AML / CFT
- MiCA 行为规则
- 市场滥用 Market Abuse
- Sanction 制裁
- 客户资产保护
- Outsourcing 政策
- Cybersecurity Awareness

监管最看重：

“是否每年提供并记录培训（Training Log）。”

**(C) 监管报送（Regulatory Reporting）**

**Q433：MiCA CASP 必须向监管机构定期报送哪些内容？**

包括但不限于：

1. 资本充足率报告 (Capital Requirement Report)
  2. 客户资产余额 & 独立托管报告
  3. 交易量与业务统计
  4. 市场滥用监控报告 (如适用)
  5. 年度合规报告
  6. 年度风险管理报告
  7. 年度审计报告
  8. 重大事件报告 (Incident Report)
- 

#### Q434：监管报送的频率是什么？

- 季度：运营与风险报表
  - 半年：资本充足性
  - 年度：审计与合规报告
  - 即时：重大事件通报 (24-72 小时)
- 

#### Q435：是否必须通过监管平台 (Portal) 提交？

是的，希腊正在使用：

- HCMC 电子监管报送系统
- 未来将对接 ESMA MiCA 统一监管平台

企业必须完成系统接入与上线测试。

---

#### Q436：监管报送是否包括链上数据？

对于涉及托管、交易执行、订单簿业务的 CASP，通常包括：

- 钱包地址
- 交易总量
- 热/冷钱包分布
- 存取款流向
- 链上监测风险 Exposure

部分国家已要求提供链上分析工具 (Chainalysis/LexisNexis)。

---

## (D) 会计与税务 (Accounting & Tax)

---

#### Q437：CASP 在希腊必须采用哪种会计准则？

必须采用：

- Greek GAAP (ΕΛΠ) 或
- IFRS (国际财务报告准则)

多数 CASP 选择 IFRS，便于跨境集团合并报表。

---

#### Q438：虚拟资产在会计处理上如何分类？

通常按 IFRS：

- 客户虚拟资产：不计入本公司资产 (Off-Balance)
- 公司自营虚拟资产：按 Intangible Asset 或 Inventory (若为做市业务)

- 手续费收入：按服务收益确认

MiCA 强调必须 **彻底区分自有资产与客户资产**。

---

### Q439：希腊 CASP 的企业所得税是多少？

希腊公司税率约：

- **22% 企业税 Corporate Tax**
- 股息分红税约 **5%–10%**（视结构）

如设置控股公司可进一步降低税负。

---

### Q440：虚拟资产交易收益是否需要缴税？

针对 **公司层面（非客户）**：

- 若是自营交易，需缴纳企业所得税
- 若是手续费收入，则按业务收入征税

MiCA 不负责税务，但税务机构会严格审查。

---

### Q441：是否可以将研发支出（如区块链技术）申请税务抵扣？

可以，希腊提供：

- **R&D Tax Credit**（最高可达 **20–30%**）
  - 可抵扣研发成本
  - 适用于软件、合规系统、智能合约开发等领域
- 

### Q442：希腊是否允许 CASP 在其他欧盟国家设分公司？

可以，但必须：

- 保持“总部实质”在希腊
  - 符合理当地 MiCA 护照通报流程
  - 更新组织结构与人力配置
- 

### Q443：是否必须建立会计政策手册（Accounting Manual）？

必须，包括：

- 收入确认
- 虚拟资产估值
- 客户资金处理
- 汇率风险
- 合规成本资本化
- 折旧与摊销政策

监管可能抽查。

---

### Q444：是否需要准备“税务合规包（Tax Compliance Pack）”？

建议准备，包括：

- Transfer Pricing 文件
- 关联方交易说明
- 税务风险评估
- 税务申报流程

- 交易数据对账

对于跨境运营尤其重要。

---

#### **Q445：审计中最常被问到的问题是什么？**

1. 你们如何证明客户资产与公司自有资产完全分离？
  2. 钱包私钥管理流程如何？
  3. 你们如何进行链上对账？
  4. 是否进行了充分的 AML 监控？
  5. Outsourcing 是否可控？
  6. 是否存在未记录的风险事件？
- 

#### **Q446：集团公司是否可以提供共享服务（Shared Service）？**

可以，但必须：

- 签订 SLA
- 说明权限与风险
- 保证不影响独立性
- 具备可审计性

否则审计师会挑战。

---

#### **Q447：是否有监管罚款与审计意见相关联？**

是的，如果出现：

- 审计意见带保留
- 重大内部控制缺陷
- 客户资产保护不到位
- 多次不提交报表

监管可能：

- 限制业务
  - 暂停某项服务
  - 吊销牌照
  - 处以高额罚款
- 

#### **Q448：未按时报送监管报表会发生什么？**

可能后果：

- 行政罚款
  - 启动“加强监管周期”
  - 要求 CEO/RO/MLRO 面谈
  - 多次延迟可能导致撤牌
- 

#### **Q449：仁港永胜是否可以协助搭建财务、审计与报表体系？**

可以，提供：

- MiCA 财务政策手册
- 客户资产分离会计处理模板
- 审计准备文件清单
- 年度监管报送模板

- 风险/合规/AML 年度报告模板

确保企业在审计与监管报送环节没有短板。

---

## Q450: MiCA 会计/审计部分为什么难?

因为虚拟资产涉及：

- 未实现市值波动
- 跨链对账
- 钱包/密钥管理
- 客户资产保护
- 交易数据海量
- 自营与客户端数据分离

很多公司因为会计流程不清晰 → 审计无法通过 → 牌照受阻。

---

# (A) 外部审计要求补充 (Extended Audit Requirements)

## Q451: MiCA 是否要求针对“客户资产保护 (Safeguarding of Client Assets)”进行独立专项审计?

是的。

MiCA 明确要求 **客户资产保护必须经独立审计验证**，希腊监管更强调：

1. 客户资产与公司资产彻底分离 (Ring-fencing)
2. 链上资产对账机制是否真实运行
3. 钱包管理 (Key Management) 流程是否符合可审计性
4. 第三方托管机构的风险可控性 (Fireblocks、Coinbase Custody 等)
5. 客户提款延迟是否有日志、解释、补偿政策

专项审计报告通常包含：

- 钱包配置、地址清单
- 对账频率与结果
- 控制缺陷与整改计划

监管会以此判断：

“平台是否真正具备保护客户资产的能力。”

---

## Q452: 审计师是否必须检查 CASP 的风险管理 (Risk Management) 制度运行情况?

是的。

MiCA 认为风险管理体系是 CASP 的 **核心运营能力之一**，外部审计必须检查：

- 风险评估模型是否有效
- 是否有独立的风险管理职能
- 风险登记册 (Risk Register) 是否保持更新
- 风险限额 (Risk Limits) 是否实际执行
- 是否有重大风险事件未报告

审计师会要求查看：

- 会议记录
- 风险监控日志
- 内部限额触发记录
- 改进措施执行情况

Q453：审计师是否必须对 Outsourcing（外包）进行独立审查？

必须。  
希腊监管非常强调外包风险控制，例如：

- KYC 供应商
- 第三方钱包托管
- 云服务（AWS / GCP）
- 交易监控系统（Chainalysis / Elliptic）
- 市场监控系统（Eventus、Solidus）

审计师必须确认：

- 是否有完整 SLA
- 是否有退出机制（Exit Plan）
- 是否经过尽职调查
- 是否存在单点失败（Single Point of Failure）

Q454：年度审计是否必须包含 IT Controls（IT 控制测试）？

是的，必须包含：

1. 身份与访问管理（IAM）
2. 系统权限矩阵
3. 日志完整性（Log Integrity）
4. 数据备份测试
5. 渗透测试报告
6. 钱包系统访问控制
7. 应急恢复演练结果

MiCA 强调“技术可验证性（Technical Verifiability）”。

Q455：年度审计报告未通过，会影响 MiCA 牌照吗？

会。  
例如：

审计意见	监管影响
无保留意见	正常运营
保留意见	启动整改、监管可能介入
否定意见	高风险，可能影响继续持牌
无法表示意见	被视为严重内控缺陷

一旦连续两年审计意见不佳，监管可：

- 限制 CASP 部分业务
- 强制更换管理层
- 在极端情况下吊销牌照

(B) 监管报送（Regulatory Reporting）补充 FAQ

Q456：MiCA 是否要求 CASP 定期报送“运营关键指标（KPI Reporting）”？

是的，典型 KPI 包括：

- 日均交易量
- 月活客户数
- 高风险国家交易占比

- STR / STR-M 报告数量
- 技术系统可用性 (Uptime)
- 提现延迟情况
- 冲销/纠错交易数量
- 客户资产变动总额

这些数据可用于监管判断业务风险是否上升。

---

### Q457: 监管机构对“数据质量 (Data Quality)”有什么要求?

MiCA 要求报送的数据必须:

- 准确 (Accurate)
- 完整 (Complete)
- 可追踪 (Traceable)
- 可验证 (Verifiable)

常见问题 (也是监管拒绝的理由):

- 数据不一致 (报表 vs 链上不匹配)
- 缺乏对账机制
- 无法解释异常峰值
- 财务数据与风险数据矛盾

希腊监管特别重视“链上 vs 内部系统”一致性。

---

### Q458: MiCA 是否要求 CASP 报送“服务中断 (Service Outage)”相关数据?

是的, 必须在两部分进行报送:

1. 即时通报 (24–72 小时)
  - 重大宕机
  - 交易中断
  - 提现受阻
2. 季度报告
  - 系统可用性
  - 故障原因
  - 恢复时间
  - 长期改善计划

MiCA 要求 CASP 系统的 可用性必须达到  $\geq 99\%$ 。

---

### Q459: 对于链上资产, 是否必须提交独立的“链上证明 (On-chain Evidence)”?

是的, 监管要求:

- 钱包余额
- 对账截图
- 区块链浏览器证明
- 第三方托管报告
- 地址白名单 (如适用)
- 多签 / MPC 架构证明

监管机构会对比链上数据与内部账本数据, 确保无差异。

这是 MiCA 与传统金融监管的最大差异之一。

---

## (C) 会计与税务补充 (Accounting & Tax)

**Q460：CASP 是否必须对虚拟资产进行“减值测试（Impairment Test）”？**

必须。  
适用于：

- 公司自有虚拟资产
- 库存资产（如做市库存）

采用 IFRS 或 Greek GAAP 时必须：

- 每年至少进行一次
- 市场价格暴跌时必须额外测试
- 根据“公允价值”制定会计处理

监管关注：

- 是否合理分类
- 是否避免隐藏亏损
- 是否及时披露风险

**第 15 章 | 市场滥用（Market Abuse）防范、内幕交易（Insider Trading）、价格透明度、利益冲突（Conflict of Interest）制度**

（Q461–Q500 | 希腊版）

本章内容高度专业，是 MiCA 审查和希腊监管机构（HCMC）最关注的重点领域之一。  
虚拟资产市场波动大、信息不透明、操纵风险高，因此 MiCA 特别设置专章要求 CASP 提供完整的市场行为规范和监控机制。  
本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

**（A）市场滥用（Market Abuse）防范要求**

**Q461：MiCA 是否要求 CASP 建立市场滥用（Market Abuse）防范制度？**

是的，所有 CASP 都必须建立：

1. 市场操纵（Market Manipulation）监控制度
2. 内幕信息监测与隔离制度（Inside Information Controls）
3. 可疑交易报告 STR-M（Suspicious Market Abuse Report）制度
4. 公平透明的交易执行政策（Best Execution Policy）

这是 MiCA 与传统欧盟金融监管（如MAR）接轨的核心部分。

**Q462：市场操纵风险在虚拟资产中为何特别严重？**

因为：

- 流动性不均衡
- 假量、刷量普遍
- 订单簿易操纵
- 大户集中度高
- 链上数据透明但易误导
- 部分交易发生在未受监管的第三国交易所

因此监管要求 CASP 必须具备“适当、有效、可证明”的防操纵机制。



## Q463: CASP 必须监控哪些类型的市场操纵行为？（MiCA 指定）

包括但不限于：

1. **Pump & Dump**（拉高出货）
2. **Wash Trading**（自买自卖）
3. **Spoofing**（虚假挂单）
4. **Layering**（层叠式挂单操纵）
5. **Quote Stuffing**（大量无意义挂单扰乱市场）
6. **Marking the Close**（收盘前操纵价格）
7. **Cross-platform Manipulation**（跨平台价格操纵）
8. **Coordinated behaviour**（协同行为操纵）

MiCA 认为虚拟资产更容易发生操纵，因此审查极严格。

---

## Q464: 是否必须部署自动化市场监控系统（Market Surveillance Tool）？

强烈推荐，监管倾向：

- 自动监控（Automated Monitoring）
- 可疑行为识别（Pattern Recognition）
- 多平台价格对比（Cross-Exchange Price Analysis）
- 异常成交提醒（Alerts）

如果仅依靠人工监控，审查几乎不可能通过。

常用方案如：

- Solidus Labs
- Chainalysis Market Surveillance
- Eventus Systems
- Elliptic（部分功能）

仁港永胜可协助规划实施。

---

## Q465: 是否必须制定 Market Abuse Policy?

必须，包括：

- 定义与风险分类
- 监控技术方法
- 警报触发机制
- 调查流程
- 报告义务（STR-M）
- 纪律行动
- 记录保存

MiCA 会要求查看完整政策文本。

---

# （B）内幕交易（Insider Trading）防范

---

## Q466: 虚拟资产也适用“内幕信息 Insider Information”的规定吗？

是的，MiCA 规定：

任何对资产价格有重大影响、尚未公开的信息，都属于“内幕信息”。

包括：

- 上市计划 (Listing)
  - 重大合作/公告
  - 技术漏洞
  - 内部治理变动
  - 清算/暂停业务
  - 大额投资或撤资
  - 链上安全事件
- 

#### **Q467: CASP 必须采取哪些措施防止内幕交易?**

至少包含:

1. **Insider List** (内幕名单) 制度
  2. 信息隔离墙 (**Chinese Wall**)
  3. 限制特定员工交易 (**Restricted Trading List**)
  4. 重大事件处理制度 (**Material Event Handling**)
  5. 员工交易申报 (**Employee Trade Reporting**)
- 

#### **Q468: 员工是否允许在平台上交易虚拟资产?**

可允许, 但必须:

- 事先申报 (Pre-clearance)
- 设立观察期 (Cooling-off)
- 禁止在重大事件前后交易
- 受到最低 Holding Period
- 由合规部门审批

否则构成重大监管违规。

---

#### **Q469: 内幕名单 (Insider List) 如何维护?**

必须包括:

- 姓名、职位
- 获取内幕信息的时间
- 获取方式
- 参与事件
- 职责说明
- 离开内幕名单的时间

必须可随时提供给希腊监管机构 (HCMC)。

---

#### **Q470: 是否必须进行员工 Market Abuse 相关的合规培训?**

必须, 每年至少一次。

内容包括:

- 市场滥用类型
- 内幕交易禁止
- 员工交易限制
- 信息隔离墙
- 职责冲突识别
- 提交 STR-M 的责任

培训未落实 → 牌照无法通过。

---

# (C) 价格透明度 (Pricing Transparency) 与公平交易 (Fair Trading)

---

## Q471: MiCA 对交易所/经纪商的价格透明度要求有哪些？

必须：

- 公布实时价格
  - 定期公布价差 (Spread)
  - 公布手续费
  - 公布成交深度 (如适用)
  - 提供订单执行情况说明
  - 不得误导客户关于价格与成本
- 

## Q472: 是否必须提供“最佳执行政策”(Best Execution Policy) ？

是的，适用于：

- 经纪服务 (Brokerage)
- 接收/传递指令
- 交易执行

政策内容包括：

- 执行场所选择
- 执行速度
- 成交价格
- 市场影响
- 成交概率

MiCA 强调 CASP 必须确保客户获得“可实现的最佳结果”。

---

## Q473: 是否必须提供执行质量报告 (Execution Quality Report) ？

是的，至少每年一次。

必须包括：

- 订单执行场所
- 成交速度
- 成交滑点
- 订单拒绝率
- 执行质量统计对比

监管机构会抽查数据真实性。

---

## Q474: CASP 是否可以自营交易 (Proprietary Trading) ？

可以，但风险极大，必须满足：

- 完整披露
- 不得与客户利益冲突
- 必须有独立流动性政策
- 不得利用客户订单信息
- 必须有严格的风险限额

很多国家（包括希腊）对自营业务审查极严。

---

**Q475: CASP 是否必须披露“平台如何定价虚拟资产”？**

必须披露：

- 定价来源（Oracle / 第三方报价）
- 多平台价格加权方法（VWAP）
- 订单簿价格机制
- 流动性提供者（LP）清单（若适用）
- 手续费和价差结构

透明度不足 → 监管会质疑“价格可操纵性”。

---

**（D）利益冲突（Conflict of Interest）管理制度**

---

**Q476: MiCA 是否要求 CASP 必须有利益冲突政策？**

必须，包括：

- 利益冲突识别
- 利益冲突登记册（COI Register）
- 回避措施
- 披露机制
- 外部监察
- 员工私人账户（PA）交易限制

利益冲突管理是 MiCA 和希腊监管的强项领域之一。

---

**Q477: 哪些行为属于 CASP 常见利益冲突？**

例如：

1. 自营交易 vs 客户交易
  2. 员工交易 vs 客户交易
  3. 上市审核 vs 收费关系
  4. 做市 vs 客户订单流（Order Flow）
  5. 推广项目 vs 风险披露不充分
  6. 推荐资产 vs 持仓利益
- 

**Q478: 是否可以接受“上市费 / Listing Fee”？**

可以，但必须：

- 公布收费模式
- 不得影响风险评估结果
- 不得承诺价格上涨
- 不得与项目方共谋操纵市场

最重要的是：

上市评审委员会必须独立、透明、可记录。

---

**Q479: 利益冲突登记册（COI Register）应包含哪些内容？**

包括：

- 潜在冲突描述
- 相关人员

- 风险评分
- 采取的缓释措施
- 监控频率
- 状态（已解决/持续/升级）

监管可能随时要求提供。

**Q480：是否必须向客户披露利益冲突？**

必须披露：

- 传统金融同级标准
- 书面披露文件（COI Disclosure Form）
- 可能造成损害的情形
- 如何缓解冲突
- 是否收取隐藏费用

**（E）可疑市场行为报告（STR-M）制度**

**Q481：什么是 STR-M？与 AML 中的 STR 有何区别？**

- **STR（Suspicious Transaction Report）**：反洗钱可疑交易
- **STR-M（Suspicious Market Abuse Report）**：市场操纵或内幕交易可疑行为报告

两者不同：

类型	监管机构	关注点
STR	FIU（金融情报单位）	洗钱/恐怖融资
STR-M	HCMC（资本市场监管）	市场操纵/内幕交易

**Q482：哪些情况必须报告 STR-M？**

例如：

- 异常挂单或撤单
- 短时间内大量反向交易
- 多账户协同交易
- 大户突然清仓导致价格异常
- 非公开信息导致价格剧震
- 价格明显偏离市场

必须在“无需达到完整证据”的前提下报告。

**Q483：STR-M 的报告时限是多少？**

MiCA 要求：

- **立即（Without Delay）**
- 通常必须在 **24 小时内** 提交

必须可追踪、完整、可审计。

**Q484：员工是否可匿名提交市场滥用线索？**

必须提供匿名举报渠道（Whistleblowing Channel）。

可以匿名向：

- 合规部门

- 审计委员会
- 监管机构（HCMC）

提交举报。

# (F) 监管期望与实例

## Q485：如果 CASP 未能监测到明显操纵行为，是否会被处罚？

可能被视为：

- 内控无效
- Market Abuse Surveillance Failure
- 误导客户
- 未尽合理注意义务

后果：

- 行政罚款
- 牌照限制
- 业务暂停
- 监管接管

## Q486：员工若构成内幕交易，CASP 是否承担责任？

通常承担 管理责任与制度责任，除非：

- 有完善制度
- 有培训记录
- 有监控措施
- 有及时制止

否则监管会认为公司“未尽管理义务”。

## Q487：监管机构最不喜欢 CASP 的哪类行为？

1. 上市收费但缺乏独立评审
2. 做市与交易执行同团队
3. 未披露利益冲突
4. 价格严重偏离但未告知客户
5. 放任刷量
6. 允许员工随意交易
7. 未及时报告 STR-M

## Q488：如何证明监控系统有效性？

包括：

- 告警样本
- 调查记录
- Escalation 记录
- 系统测试报告
- 监控范围文档
- KPI / Threshold 文档

监管会要求这些证据。

## Q489：仁港永胜是否可提供市场滥用监控、政策与制度模板？

可以，我们提供：

- Market Abuse Policy（MiCA 版）
- Insider Trading Policy
- Best Execution Policy
- Conflict of Interest Policy
- Market Surveillance Rulebook
- 上市评审标准（Listing Review Framework）

可直接用于注册申请。

---

## Q490：MiCA 与传统金融的 Market Abuse 规则有什么不同？

相似点：核心原则一致（公平、透明、无操纵）。

不同点：

- 虚拟资产波动更大
- 数据来源更复杂
- 链上交易增加监控难度
- 高集中度钱包影响价格
- 跨链与跨平台操纵更常见

监管预期更高。

---

## Q491：是否必须对上市（Listing）过程进行“市场滥用风险评估”？

必须，包括：

- 项目方持仓分布
- 首发/解锁时间表
- Smart Contract 风险
- 团队集中度
- 三方审计报告
- Tokenomics 稳定性

这是申请 MiCA 牌照时最被问到的部分之一。

---

## Q492：是否必须将上市前的信息保密？

必须：

- 保密协议
- 内幕名单
- 信息隔离墙
- 禁止提前交易

否则容易导向内幕交易案例。

---

## Q493：是否必须建立“公开透明的 Listing 规则”？

MiCA 要求：

- 客观（Objective）
- 可验证（Verifiable）
- 不歧视（Non-discriminatory）
- 明确收费标准

监管会要求提供完整流程。

---

#### Q494：如何管理外部做市商（Market Maker）？

必须有：

- 书面协议
- 价差与量化参数
- 风险限额
- 监控机制
- 不得操纵市场
- 必须遵守透明度要求

否则 CASP 可能承担责任。

---

#### Q495：是否必须监控员工是否参与“社群操纵活动”？

必须监控，包括：

- Discord/Telegram Pump 群
- 非公开拉群行为
- 员工参与市场操纵讨论

若员工参与该类活动属于重大合规问题。

---

#### Q496：是否可以向客户提供交易推荐？

可以，但：

- 必须符合“适当性评估”(Suitability)
- 必须避免误导
- 必须披露利益冲突
- 不得暗示“保本”或“稳定增值”

违规属于“市场行为违规”。

---

#### Q497：是否可以给予客户手续费返佣？

可以，但必须遵守：

- 不得鼓励过度交易
- 必须公开披露
- 必须纳入利益冲突政策
- 不得对高风险客户采用激进激励

MiCA 对此监管较严。

---

#### Q498：平台如何证明价格透明？

需提供：

- 挂牌资产价格来源
  - 成交深度截图
  - 定价机制文档
  - Fee Schedule
  - 流动性来源说明
- 

#### Q499：是否必须定期向监管机构提交 Market Abuse Monitoring Report？

是的，至少：



- 每年一次正式报告
- 监管可要求季度报告
- 必须包括监控结果、告警数量、调查结果、整改措施

---

### Q500：仁港永胜是否可以提供完整的 Market Abuse 监管合规体系？

可以，包括：

- Market Abuse Policy
- Insider Trading Policy
- Best Execution Policy
- Conflict of Interest Policy
- Listing Committee Framework
- Market Surveillance System Requirements
- STR-M 模板
- 告警调查流程（Alert Investigation SOP）

确保能满足希腊监管对 MiCA 的严格审查。

---

## 第 16 章 | 客户投诉（Complaints Handling）制度、信息披露（Disclosure）、客户风险评级（Risk Profiling）与适当性评估（Suitability Assessment）

（Q501–Q550 | 希腊版）

本章是 MiCA 对“消费者保护（Investor & Consumer Protection）”核心要求之一，也是希腊监管最关注的领域之一。

若投诉机制不健全、披露不足、风险评级不合理或适当性制度缺失 → 牌照无法通过。

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

---

### （A）客户投诉处理制度（Complaints Handling）

---

#### Q501：MiCA 是否要求 CASP 必须有正式的客户投诉处理制度？

是的，所有 CASP 必须建立：

1. 投诉政策（Complaints Handling Policy）
2. 投诉登记册（Complaints Register）
3. 投诉调查流程（Investigation Process）
4. 客户回复机制（Customer Response）
5. 监管通报机制（Regulator Notification）
6. 年度投诉报告（Annual Complaints Report）

这是 MiCA 监管中最有可能导致罚款的领域之一。

---

#### Q502：投诉处理必须满足哪些具体要求？

必须满足：

- 公平（Fair）
- 透明（Transparent）
- 可追踪（Traceable）
- 及时回复（Timely）
- 可审计（Auditable）
- 无歧视（Non-discriminatory）

监管会抽查投诉处理的完整记录（从提交到回复）。

---

**Q503: CASP 必须在多少时间内回复客户投诉？**

一般规则为：

- 首次确认：48 小时内
  - 正式回复：15 个工作日内（MiCA 与 PSD2 对齐）
  - 如果案件复杂：最迟不超过 35 个工作日，需告知客户延迟原因。
- 

**Q504: 投诉登记册（Complaints Register）必须记录哪些内容？**

包括：

- 投诉编号
  - 投诉日期
  - 客户姓名或编号
  - 投诉内容摘要
  - 涉及资产/交易
  - 调查过程与证据
  - 责任部门
  - 最终处理结果
  - 回复客户内容
  - 是否升级（Escalation）
- 

监管机构可随时要求调阅登记册。

---

**Q505: 客户可以通过哪些渠道提交投诉？**

必须至少提供：

- Email
  - Web 表单（Portal）
  - 电话（Call Centre）
  - 邮寄地址
  - 移动 App 内投诉入口
- 

MiCA 强调“可被所有客户公平使用”。

---

**Q506: 是否必须设立专门的投诉处理负责人？**

是的，需要：

- Complaints Officer（可由合规部门兼任）
  - 不能与业务部门存在利益冲突
  - 必须可独立调查投诉
- 

**Q507: 投诉处理流程必须包括哪些步骤？**

一般 6 步：

1. 接收（Acknowledgement）
2. 登记（Registering）
3. 初步调查（Preliminary Review）
4. 深度调查（Full Investigation）
5. 结论形成（Outcome Assessment）
6. 客户回复（Response）

MiCA 要求“流程必须书面化，可审计”。

---

**Q508：是否需要向监管机构报告重大投诉？**

是的，包括：

- 金额巨大
- 客户资产损失
- 涉及市场滥用
- 涉及内幕信息
- 重大系统故障导致投诉高峰
- 涉嫌误导销售（Mis-selling）

必须在 **24–72 小时内** 报告。

---

**Q509：是否必须向监管机构提交年度投诉报告？**

必须，内容包括：

- 投诉数量
- 类型
- 已解决/未解决
- 处理时间
- 根本原因分析（Root Cause Analysis）
- 改进措施

监管会根据该报告评估机构的“消费者保护能力”。

---

**Q510：投诉处理记录必须保存多久？**

MiCA 要求至少 **5 年** 保存。  
希腊金融监管一般要求保存 **7 年**，建议采用更严格标准。

---

## **（B）客户信息披露（Disclosure Obligations）**

---

**Q511：CASP 必须向客户披露哪些关键信息？**

至少包括：

- 公司信息（地址、牌照号、监管机构）
- 风险披露（Risk Disclosure）
- 费用披露（Fee Schedule）
- 交易执行政策（Best Execution）
- 利益冲突披露
- 客户资产保护说明
- 冷/热钱包分布比例
- 停服与暂停交易规则
- 赔偿制度（若有）

披露不足属于“重大违规”。

---

**Q512：费用披露必须包含哪些细项？**

必须包括：

- 交易手续费

- 上市费用（如向客户收费）
- 存取款费用
- 钱包托管费用
- 网络 Gas 费用
- 点差（Spread）
- 做市费用（若适用）

MiCA 明确禁止“隐藏费用”。

---

### Q513：适合普通客户的“风险披露声明”必须包括什么？

至少包括：

- 虚拟资产波动风险
- 清算风险
- 技术风险（智能合约漏洞）
- 网络安全风险
- 第三方托管风险
- 监管政策风险
- 流动性不足风险
- 停牌风险
- 市场滥用风险

MiCA 强调“必须易于理解（Clear & Non-Technical）”。

---

### Q514：CASP 是否必须披露托管方式？

必须披露：

- 私钥管理方式（MPC / HSM / Cold Wallet）
- 托管比例（如 80% 冷 20% 热）
- 第三方托管机构（如 Fireblocks / Coinbase Custody）
- 客户资产独立性

不透明 → 监管会质疑客户资产保护能力。

---

### Q515：是否必须通知客户重大事件？

是的，包括：

- 系统中断
- 钱包安全事件
- 资产暂无法提取
- 重大市场操纵事件
- 合规违规

必须以 Email / App 通知。

---

### Q516：是否可以向客户宣传投资回报？

不可以。

MiCA 明确禁止：

- 暗示保证收益
- 暗示低风险
- 不合理夸大收益
- 推荐热点资产但不披露风险

该类行为属于“误导性营销（Misleading Marketing）”。

---

## (C) 客户风险评级（Risk Profiling）制度

---

### Q517：MiCA 是否要求 CASP 必须对客户进行风险评估？

必须。

客户必须完成：

- 1. 风险承受能力评估
- 2. 财务状况问卷
- 3. 投资经验评估
- 4. 目标用途评估
- 5. 虚拟资产知识评估

否则不得向其提供复杂产品服务。

---

### Q518：风险评级模型应如何设计？

必须包括：

- 客户资金来源
- 投资目的
- 投资期限
- 可承受的最大损失比例
- 风险偏好（保守 / 中等 / 激进）
- 过往经验
- 对杠杆/衍生品的理解（如提供此类服务）

MiCA 更强调整体画像，而非只看问卷结果。

---

### Q519：风险评级结果如何使用？

必须结合：

- 产品适当性（Suitability）
- 产品匹配程度
- 是否限制高风险资产
- 是否限制杠杆交易
- 是否限制复杂产品

监管审查重点：

“你是否根据风险评级对客户销售做了限制？”

---

### Q520：风险评级结果是否必须定期更新？

必须：

- 至少每 12 个月 更新一次
  - 在客户资产规模快速增长时提前更新
  - 在客户请求时更新
- 

### Q521：是否可以自动化风险评估？（如 API / App 问卷）

可以，但必须满足：

- 可追踪
- 可审计
- 记录保存
- 不得诱导客户填写
- 清晰解释问题含义

---

## (D) 适当性评估 (Suitability Assessment) 制度

---

### Q522: MiCA 是否要求适当性评估 (Suitability) ?

是的, 适用于:

- 投资建议 (Investment Advice)
- 组合管理 (Portfolio Management)
- 高风险资产销售
- 复杂结构化代币
- 衍生品交易 (如提供)

核心原则:

“客户是否理解风险? 产品是否符合其风险等级?”

---

### Q523: 适当性评估必须包含哪些内容?

包括:

1. 客户经验 (Experience)
2. 财务状况 (Financial Situation)
3. 投资目标 (Objectives)
4. 风险承受能力 (Risk Capacity)
5. 知识水平 (Knowledge Test)
6. 产品复杂程度 (Product Complexity)

---

### Q524: 是否需要为每次交易进行“适当性检查”?

视产品类型而定:

- 普通现货 Crypto: 一般无需
- 高风险产品 (杠杆、衍生品、收益类): 必须进行

---

### Q525: 如果产品不适合客户, CASP 是否必须禁止交易?

MiCA 规定:

- 若风险极度不匹配 → 必须 **拒绝交易**
- 若存在部分风险不匹配 → 必须 **发出风险警告**

警告必须可记录, 如:

- App 弹窗
- Email
- 屏幕提示

---

### Q526: 适当性报告 (Suitability Report) 是否必须提供给客户?

若提供投资建议 → 必须提供。

内容包括：

- 为什么推荐该资产
- 风险与复杂度
- 如何与客户风险等级匹配

这是 MiCA 新增的重要义务。

**Q527：是否必须保存适当性评估记录？**

必须保存 **5–7 年**。

**Q528：客户拒绝提供风险信息时如何处理？**

MiCA 规定：

- 若为普通现货交易：可以允许，但必须警告
- 若为复杂产品：**必须拒绝提供服务**

必须记录“客户拒绝提供信息”。

**Q529：是否可以根据客户交易历史自动调整风险等级？**

可以，但必须：

- 客户知情
- 不得隐形更改
- 保留完整记录
- 合规部门审查机制

**Q530：合规部门在适当性评估中的角色是什么？**

包括：

- 检查模型合理性
- 审查问卷质量
- 随机抽查客户记录
- 监督警告机制
- 向董事会报告

**(E) 透明度与客户沟通**

**Q531：CASP 是否必须使用简明语言与客户沟通？**

必须。

MiCA 要求：

- Clear（清晰）
- Fair（公平）
- Not Misleading（不误导）

尤其是：

- 风险披露
- 营销材料
- 适当性警告

**Q532：是否必须向客户显示“费用明细”？**

是的，包括：

- 每笔交易费用
- 总费用
- 点差
- 网络费用
- 托管费

必须“逐笔可视化”。

---

**Q533：CASP 是否必须提供年度对账单（Annual Statement）？**

必须，包括：

- 客户资产余额
  - 历史交易
  - 手续费总额
  - 市场估值变化
  - 风险提示
- 

**Q534：是否必须提前向客户通知政策变更？**

必须至少提前 **30 天**。

---

**Q535：如果平台暂停服务（如维护），是否必须告知客户？**

是的，必须：

- 公告
- Email
- App 通知

且必须说明原因和预计恢复时间。

---

**Q536：客户投诉与风险披露之间的关系是什么？**

监管会检查：

- 是否因缺乏披露导致投诉
- 是否存在误导销售
- 是否出现大量类似投诉

如果投诉集中在“亏损误导”，监管会质疑平台销售行为。

---

**Q537：如何证明客户已阅读风险披露？**

可采用：

- 勾选确认
- 强制滚动阅读页面
- 视频/图文说明
- 交易前弹窗确认
- 电子签名（Strong）

必须可记录存档。

---

**Q538：是否必须提供客户教育内容？**



建议提供，包括：

- 风险指南
- 投资知识
- 如何防诈骗
- 链上安全说明
- 市场操纵案例

MiCA 越来越强调“投资者教育（Investor Education）”。

---

## (F) 监管期望与常见风险

---

### Q539：监管机构最关注客户适当性制度的哪些问题？

1. 问卷内容太简单
  2. 客户随便填写也能通过
  3. 未真正根据风险评级限制交易
  4. 没有强制警告机制
  5. 无记录可证明行为
- 

### Q540：是否必须禁止未成年人使用 CASP 服务？

必须禁止。

必须通过：

- KYC
- 身份证件验证
- 年龄验证

否则属于严重监管违规。

---

### Q541：风险评级过度宽松会导致什么后果？

监管会认为：

- 故意忽略风险
- 误导客户
- 诱导交易
- 违反消费者保护原则

可能被罚款并限制业务。

---

### Q542：是否必须在网站上公开客户投诉流程？

必须公开：

- 投诉渠道
  - 处理时间
  - 升级机制
  - 监管机构联系方式
- 

### Q543：客户是否可以要求复查其风险等级？

可以，必须提供复查机制。

---

### Q544：是否必须提供“退出机制”，允许客户注销账户？

必须提供清晰流程。

**Q545：平台是否必须提供客户存取款日志？**

必须提供可下载记录（CSV / PDF）。

**Q546：是否必须在年度报告中总结投诉与适当性问题？**

必须。

**Q547：交易过度（Excessive Trading）是否属于消费者保护问题？**

是的，监管认为：

“过度交易 = 可能被激励不当、平台鼓励频繁交易”

CASP 必须监控。

**Q548：是否可以利用算法向客户推送投顾内容？**

不可以提供“自动化投资建议”，除非：

- 完整遵守 MiCA 投资建议规则
- 完成适当性评估
- 有记录
- 有解释义务

否则违反 MiCA。

**Q549：仁港永胜是否可以提供投诉处理制度、适当性制度与风险评估体系？**

可以，我们提供：

- Complaints Handling Policy
- Customer Disclosure Policy
- Risk Profiling Questionnaire
- Suitability Assessment Framework
- Customer Communication Templates
- 投诉登记册模板
- 风险评级系统设计指引

所有内容均符合 MiCA + 希腊监管要求。

**Q550：本章中最容易导致监管拒牌的情况是什么？**

三大致命问题：

1. 未进行适当性评估→误导销售
2. 投诉记录不完整→被判定内部控制失效
3. 风险披露不足→客户损失→大量投诉→监管介入

MiCA 审查中有超过 40% 的拒牌案例与本章直接相关。

**第 18 章 | 仁港永胜（Rengang Yongsheng）对申请希腊 / 欧盟 MiCA-CASP 牌照的专业建议**

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

# 一、仁港永胜对申请人的务实建议（来自真实监管经验总结）

MiCA 是欧盟历史上对虚拟资产监管最全面、最严格的框架之一。  
希腊监管机构（HCMC · Bank of Greece）风格谨慎、审查节奏偏实质执行（Substance over Form）。  
结合我们为大量企业筹备 MiCA 申请的经验，给出以下非常关键的“实战建议”：

## 建议 1：不要低估 MiCA 的合规深度，它已经接近传统金融牌照要求

MiCA 不是“填表格+写政策”即可获批的简单牌照，而是：

- AML/KYC → 要求达到传统银行级别
- IT 安全 → 需要链上监控、热冷钱包控制
- 市场滥用监控 → 必须实时监测操纵行为
- 客户资产保护 → 监管要求可证明与可核查
- 治理结构 → 董事会、MLRO、RO 必须真实可履职

MiCA 的逻辑：

“你要开展业务，必须具备经营一家金融机构的能力。”

## 建议 2：最常导致申请失败的不是商业模式，而是“团队能力不足”

监管最关注：

- 董事会经验
- MLRO / Compliance Officer 专业能力
- IT 安全负责人是否足够资深
- 是否存在第三国团队占比过高
- 是否具备本地实质运营（Substance）

仁港永胜经常帮助客户：

- 补齐关键岗位
- 重建管治结构
- 重新梳理合规报告线
- 重写监管面谈问答

团队能力是决定能否获批的核心变量。

## 建议 3：不要试图提交“模板式申请”——MiCA 会直接否决

监管者偏好：

- 风险评估有真实逻辑
- 产品说明与流程图完整
- 客户资产托管方案可执行
- IT 架构真实存在而非 PPT
- 市场滥用监控规则可运行

我们协助过多家被拒项目进行二次整改，发现：

**80% 被拒原因是内容空洞或缺乏实操性。**

## 建议 4：尽早准备“监管补件（RFI）”的应对方案

MiCA 审查至少会出现：

- 30~120 条 RFI（补件）
- 1~3 次监管面谈

- 技术、安全、AML 独立质询

如果没有事先准备完整 Q&A 框架，企业往往：

- 回答不一致
- 内容与政策不匹配
- 缺乏证明文件
- 时间被拖延

仁港永胜已经为多国申请人整理出：

- **300 条 RFI 题库**（可直接填写）
- **监管面谈全套问答脚本**
- **IT、AML、Market Abuse 各模块答复模板**

让企业从被动应对 → 主动提前准备。

---

## **建议 5：MiCA 是欧盟 30 国护照的核心，不要把它当“单一国家牌照”**

获批后可：

- 全欧盟 27 国展业
- 全 EEA 3 国展业（冰岛、列支敦士登、挪威）
- 无需逐国申请
- 可在欧盟设立运营中心、上链项目、注册结构化产品
- 大幅提升估值与融资能力

MiCA 的本质是：

“一次申请 → 欧洲市场全部打开。”

---

## **二、为什么选择仁港永胜？（七大核心优势）**

---

### **优势 1：我们拥有全球最多“MiCA 实操经验”之一**

我们的团队长期深耕：

- MiCA 制度
- 欧盟金融法规
- AML / Sanction
- Crypto Market Abuse
- 审计与客户资产保护
- IT 安全与风险管理

我们为客户提供的文件包都是：

- 实操可用
- 监管认可
- 结构成熟
- 案例丰富

不是模板，是“真正能过监管的内容”。

---

### **优势 2：我们在希腊、塞浦路斯、爱沙尼亚、立陶宛、马耳他等国拥有本地专业网络**

包括：

- 当地律师
- 合规官（RO/MLRO）

- 会计师与审计师
- IT 安全公司
- 托管服务商
- 监管沟通顾问

让客户可以：

“不需要自己搭建完整团队，我们替你整合最好的资源。”

---

### 优势 3：提供 MiCA 所有必备的 60+ 份合规文件全集

例如：

- AML Manual（欧盟版）
- Risk Assessment（资产、客户、技术）
- Conflicts of Interest Policy
- Market Abuse Monitoring Rulebook
- Incident Response Plan
- IT Security Framework（含钱包管理）
- Outsourcing Policy
- Business Plan（监管版）
- Governance Manual
- Customer Asset Safeguarding Framework

文件一次交付即可用于：

- 申请
  - 监管面谈
  - 审计
  - 银行开户
  - 内部合规体系搭建
- 

### 优势 4：监管面谈（Interview）一对一培训

我们提供：

- 监管最常问的 150~200 条问题
- 风险类、AML 类、IT 类、市场滥用类答复
- 面谈模拟（Mock Interview）
- 逐句纠正回答逻辑

确保：

“你说的话 → 与提交的文件一致 → 与监管期望一致。”

---

### 优势 5：全程可托管式服务（Full Outsourcing Model）

客户可以选择：

- 我们作为合规顾问
- 我们提供外部 MLRO
- 我们提供外部 RO
- 我们协助搭建本地团队
- 我们提供监管报送支持

适合 Web3、交易所、钱包、托管商、RWA 项目方等。

---

### 优势 6：我们能协助企业同时规划欧洲架构（公司+税务+运营）

如：

- 荷兰控股公司
- 卢森堡基金结构
- 爱沙尼亚技术中心
- 希腊 / 塞浦路斯运营中心
- EEA 全境护照计划

让企业不仅能拿牌，也能真正建立欧洲市场能力。

优势 7：交付速度快、监管沟通能力强

我们擅长：

- 在 30-60 天内提交完整申请
- 在 RFI 阶段做到快速响应
- 保持与监管机构良好沟通
- 降低审查周期
- 提高成功率

仁港永胜常被客户称为：

“最懂 MiCA 的合规顾问团队之一。”

三、关于仁港永胜（Rengang Yongsheng）

仁港永胜（香港）有限公司  
**Rengang Yongsheng (Hong Kong) Limited**  
是一家深耕以下领域的全球合规服务机构：

- 欧盟 MiCA / CASP / EMI / PI 牌照
- DIFC / VARA（迪拜）虚拟资产牌照
- 香港 SFC / HKMA / MSO 持牌架构
- 新加坡 MAS 牌照
- 加拿大 MSB / 美国 MTL 架构
- 全球银行牌照、支付牌照咨询
- 企业数字银行 / 钱包 / 托管系统整体方案
- RWA、交易所、托管、支付平台合规模块搭建
- 跨境集团结构（法律 + 税务 + 运营）咨询

我们不只是提供文档，而是提供 可快速落地、可通过监管审核、可长期运营的合规体系。

四、联系方式

联系人：唐生（Tang Shangyong）  
仁港永胜（香港）有限公司 | 业务经理

合规咨询与全球金融服务专家

- 官网：[www.jrp-hk.com](http://www.jrp-hk.com)
- 香港：852-92984213（WhatsApp）
- 深圳：15920002080（微信同号）

办公地址：

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

- 香港环球贸易广场86楼

如需咨询：

- 希腊 (MiCA) CASP 牌照
- 欧盟任意国家 CASP/EMI/PI 牌照
- 香港 SFC / MSO / SVF
- 迪拜 VARA
- 加拿大 MSB
- 美国 MTL
- 数字银行系统
- 完整合规体系搭建

欢迎随时与我们联系。

---

## 五、结束语

MiCA 时代已经开始。

未来的虚拟资产市场属于 **合规化、透明化、可监管化** 的机构。

若您希望在欧盟 30 国开启业务，MiCA 是唯一合法且可持续的道路。

仁港永胜愿成为您在全球监管框架中的长期战略伙伴。

我们不只是顾问，而是协助您真正落地持牌业务的全流程运营伙伴。

---

© 2025 仁港永胜（香港）有限公司 | Rengangyongsheng Compliance & Financial Licensing Solutions

由 仁港永胜 唐生 提供专业讲解。