



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

保加利亚电子货币机构（EMI）牌照申请注册指南

本文内容由仁港永胜唐生提供讲解，这是一份面向实操的《保加利亚电子货币机构（EMI）牌照申请注册指南》——覆盖：牌照概览、法律依据、可开展业务、申请条件与人员配置、董事/股东适格性、申请流程与时间表、后续维护与年检/续牌、官方收费与全周期预算、常见问题（FAQ）等。

一、牌照概览（Regulatory Snapshot）

- 主管机关：**保加利亚国家银行 **BNB**（Bulgarian National Bank）。电子货币与支付服务在《支付服务与支付系统法》（**PSPSA**）下监管，具体许可流程与持续义务由 **BNB 第16号条例（Ordinance No.16）** 细化。
- 牌照性质：**EMI为无限期许可（非固定年限），但须持续满足资本充足与合规要求；不满足可被撤销。
- 最低注册资本 / 初始资本：****BGN 700,000**（约合**EUR 350,000**），且自有资金不得低于监管口径的计算结果（欧盟 EMD2/本地法承接）。
- 公共登记：**获批的支付机构与EMI须载入BNB公共注册，并同步进 **EBA 中央注册**（便于通行与透明）。
- 欧盟护照：**作为欧盟成员国许可的EMI，可按欧盟规则进行跨境护照至EEA其它成员国（设立分支/自由提供服务）。

二、法律依据与监管框架

- 主法规：**
 - 《支付服务与支付系统法》（PSPSA）——许可、拒发、撤销、报告、注册、公示等总则。
 - BNB 第16号条例（Ordinance No.16）**——许可申请材料清单、代理/分支注册、外包、报告、审计等实施细则。
 - BNB 第40号条例（Ordinance No.40）**——年度监管成本费的计费方法学（风险、业务类型与规模指标驱动，而非统一定额）。
- 资本金门槛：**本地承接欧盟EMD2，对EMI最低初始资本**EUR 350,000**（保加利亚法规以**BGN 700,000**体现）。
- 许可地域要件：**申请人注册地在保加利亚；BNB对注册地、经营地与实际管理（mind & management）实质审查。

三、业务范围（获批后可开展）

- 发行电子货币、开立电子钱包/账户；
- 收付与转账（卡/转账/直接借记等）及相关支付服务；
- 代理网络/分支机构开展业务（境内/跨境）须按 BNB 登记与通知流程办理。

注：EMI不得吸收存款或发放贷款（区别于银行业）；可按PSPSA条款使用**代理（agents）与外包**，但须满足风险管理、监督与信息通报要求。

四、申请门槛与人员要求（含董事/股东“适格性”）

4.1 实体与资本

- 公司形态：**通常为有限责任公司（**OOD**）或股份公司（**AD**），在保加利亚注册。
- 最低初始资本：****BGN 700,000**（≈**EUR 350,000**），须为高质量资本（股东真实缴付、来源清晰可证）。

4.2 董事/高管配置

- 至少两名日常管理者 (four-eyes principle 实质把关)，良好声誉与胜任能力 (金融/支付/科技/风险/合规经验)。
- 关键岗位：合规负责人/MLRO、风险管理、内部审计 (可内设或合规外包，但须证明有效独立与监管可见)。

4.3 股东与实控人 (fit & proper)

- 资金来源可追溯、未涉及金融犯罪或严重不当记录；控制结构透明、避免不当复杂性；BNB可要求穿透核查。

4.4 实体“实质”与场地

- 保加利亚本地办公场所 (租约/产权证明)，虚拟地址不可接受；本地人员与运营能力需与商业计划匹配。

五、申请文件清单 (核心要点)

BNB会按 Ordinance No.16 审查完整性与充分性，通常包括：

1. **商业计划** (3-5年财务与营收模型、风险评估、KPIs、护照计划)；
2. **资本证明与资金来源** (出资凭证、银行对账单、KYC/KYB链条)；
3. **治理架构** (组织图、岗位职责、独立性与问责机制)；
4. **政策与制度**: AML/CFT、制裁筛查、客户尽调、可疑交易报告、投诉处理、外包管理、业务连续性/灾备、操作风险、IT/网络安全 (DORA 对齐思路可一并阐述)；
5. **技术与运营**: 系统架构、APS/接口、密钥/加密、日志稽核、变更管理、渗透测试节奏、数据保护 (GDPR/DPO)；
6. **客户资金隔离与 Safeguarding 方案** (银行专用保障账户或保险/担保安排；意向函、流程图与对账机制)。

六、标准申请流程与办理时间

阶段A — 策划与设立 (4-8周)

- 选定治理与股权结构、注册公司、开户 (运营+保障账户意向)、准备首轮制度文档与技术说明。

阶段B — 预沟通/预审材料 (2-6周)

- 与BNB进行非正式沟通 (如有)；补足关键立场文件 (资本、外包、IT与Safeguarding)。

阶段C — 正式申报与问答 (3-6个月常见)

- 递交完整申请包 → BNB形式审查 → 实质性问答 (1-3轮) → 许可决定。PSPSA 许可为无限期；若12个月内未开业，BNB可撤销。

提示：BNB 年报披露每年有若干新批与拒绝个案，问答质量与材料完整性直接影响周期。

七、后续维护、报告与欧盟护照

- **年度审计报表**：经注册会计师审计后，于次年6月30日前报送BNB；BNB可要求临时/专项报表。
- **资本与自有资金监控**：持续符合初始资本+自有资金口径的较高者；低于阈值须立即报告。
- **代理/分支与外包**：新增、变更、跨境设点须按规定事前报备/登记。
- **公共登记信息维护**：名称、地址、网站、联系人、许可编号等更新登记。
- **护照**：获批后可通过EBA注册与欧盟程序办理跨境通行 (通知-生效机制)。

八、官方收费与持续监管费用

- **一次性受理/评估费**：市场实践常见为 **BGN 10,000** (咨询机构披露，供预算参考；以BNB当期收费为准)。
- **年度监管成本费**：按 **BNB 第40号条例的方法学**计取 (基于风险、业务类型与规模指标)，非统一金额，年度会有测算与缴纳。

建议：申报前向BNB确认当期收费口径与计算基数，并在商业计划中预留“监管费”科目。以上报价未含服务费用，具体金额以仁港永胜业务顾问报价为准。

九、全周期费用与预算（区间参考，EUR）

以下为实务区间（不含增值税），具体以项目体量、外包深度、IT复杂度与BNB问答轮次为准：

- **注册资本：≥350,000**（法定最低）
 - **法律与许可顾问：80,000–200,000**（起）
 - **政策与制度编制（AML/风控/外包/IT/BCP等）：40,000–120,000**
 - **IT合规与安评（渗透/代码审计/日志与SIEM/备份）：30,000–120,000**
 - **Safeguarding 专户开户与银行函件：3,000–10,000**（银行端合规流程与函件制作成本）
 - **本地实体与办公（12个月）：20,000–60,000**（租金/设施/会计）
 - **关键人员（首年薪酬包）：合规/MLRO、风控、财务、IT安全合计 180,000–400,000**
 - **外包内审/数据保护官（DPO/GDPR）：15,000–60,000**
 - **BNB一次性受理费：约 BGN 10,000**（≈ EUR 5,100）
 - **年度监管费（BNB）：按 Ordinance 40 方法学测算（请在财务模型单列“Regulatory Levy”科目）**
 - 以上报价未含服务费用，具体金额以仁港永胜业务顾问报价为准。
-

十、续牌/年审与变更

- **续牌：**许可为无限期，无“换证”概念；核心在**年度审计、资本充足、治理有效性与重大变更报备的持续合规**。
 - **人员/实控变更：**董事、RO/MLRO、重要外包与控股结构发生变化，须依 Ordinance No.16 向BNB报批/报备。
 - **不合规后果：**可被处以纠正措施、罚款，严重者撤销许可。
-

十一、实操时间线（保守预估）

- **端到端：6–12个月**较常见（复杂IT/跨境护照/多轮问答可延长）。
 - **关键里程碑：**立项→公司设立与方案冻结（1–2月）→材料打磨与预沟通（1–1.5月）→受理与问答（3–8月）→获批与上线（≤12个月内必须开业，否则可能撤销）。
-

十二、常见问题（FAQ）

Q1：保加利亚是否有“小型EMI（Small EMI）”？

A：欧盟框架允许成员国设“小型”制度，但各国落地不同。保加利亚主流路径为“完全授权EMI”（EUR 350k 初始资本）。如考虑“小型/限额”路径，请以BNB口径为准，且跨境护照通常受限。

Q2：资本一定要一次性到位吗？来源如何证明？

A：实务上要求**到位且可验证**，资金需为高质量资本（股东实缴、合法来源、留存收益等）。

Q3：护照到欧盟其它国要多久？

A：按PSD2/EMD2 护照机制，通过本国监管向他国监管**通知**；时长依目的国监管与业务复杂度，通常数周至数月。参考EBA中央注册与本地登记要求。

Q4：客户资金如何“隔离/保障”（Safeguarding）？

A：开设**专用保障账户**或获取等效保障（保险/担保），并建立**对账与差错处理流程**；银行出具函件常见有**3,000–10,000**费用。

Q5：审计与报告节奏？

A：年度经审计财报最迟次年**6月30日**报送；BNB可要求临时报告或专项信息（如保障账户开立7日内通知）。

Q6：若许可被拒，多久可重报？

A：PSPSA规定被拒后**6个月内**一般不可重报（以法条具体表述与BNB实际执行为准）。

Q7：若获批后迟迟不开业？

A：自许可日起**12个月内**未开业可触发撤销。

十三、申报材料打磨与合规要点清单（精简版）

- 资本与股权：≥BGN 700,000、穿透至自然人实控，资金来源佐证齐全。
- 人员与治理：两名以上实际管理者、MLRO/合规/风险/内审职责清晰、独立性证明。
- IT与运营：系统拓扑、密钥与加密、日志留存、变更与发布、备份与灾备、渗透测试计划、第三方/外包治理。
- 客户资金保障：专户银行函+流程与对账；异常与补偿机制。
- 报告与持续义务：年度审计/临时报送、代理/外包注册、登记信息维护、监管费预算。

结语 | 给你的落地建议

1. 先做可行性-差距评估（Gap Assessment）：资本-人员-IT-外包-银行端Safeguarding 接入可行性；
2. 与目标托管银行尽早沟通保障账户函与对账接口；
3. 将BNB第40号条例监管费纳入财务模型；
4. 准备两轮以上问答的时间与人力冗余；
5. 规划护照节奏与目的国本地化差异（KYC、语言、客服时区、费用条款）。

十四、申请材料总表（Checklist | 可按此建文件夹）

建议以下目录创建资料夹：01-公司注册与股权、02-资本与资金来源、03-治理与人员、04-制度与政策、05-IT与安全、06-Safeguarding、07-外包与代理、08-商业计划与财模、09-审计与报送、10-护照与分支

模块	关键文件	负责人	形式	证明/附件	状态
公司与股权	公司注册证、章程、股东名册、UBO穿透图	法务	PDF/原件	翻译与公证	<input type="checkbox"/>
资本与来源	≥BGN 700,000实缴证明、出资流水、KYC/KYB链条	财务	PDF/XLS	银行对账单、资金来源说明	<input type="checkbox"/>
董监高	简历、学历/资质、无犯罪/破产证明、推荐信、Fit&Proper表	HR/合规	PDF	近3个月内开具	<input type="checkbox"/>
治理与组织	组织结构图、岗位说明书、独立性声明（合规/风控/内审）	合规	PDF	董事会批准决议	<input type="checkbox"/>
政策制度	AML/CFT、制裁与筛查、客户尽调、投诉处理、外包、IT/BCP/DR、风险管理、内部审计章程、薪酬政策	合规/风控/IT	PDF/Word	版本控制页	<input type="checkbox"/>
IT与安全	架构图、访问控制矩阵、密钥管理、变更发布、备份/灾备、渗透测试计划、日志保留策略	IT安全	PDF/PNG	年度测试计划	<input type="checkbox"/>
Safeguarding	保障专户银行意向函/确认函、日内/日终对账流程、差错处理SOP	财务/合规	PDF	银行联络人	<input type="checkbox"/>
外包与代理	外包框架协议、尽调报告、KPI/SLA、退出计划；代理登记清单	业务/合规	PDF	审核打分表	<input type="checkbox"/>
商业计划	3-5年业务计划、EEA护照路线、KPI、客户画像、市场与合规成本模型	战略/财务	PPT/XLS	敏感性分析	<input type="checkbox"/>
审计与报送	审计师聘任函、年报时间表、监管报送清单	财务	PDF	审计计划	<input type="checkbox"/>

十五、制度文档模板索引（提纲+落地要点）

1) AML/CFT政策（含制裁）

- 风险评估方法（国别/客户/产品/渠道/交易）；KYC/KYB分层（S/DD）；PEP/制裁筛查频率；持续尽调；STR提交流程与门槛；样本表单与话术。

2) 客户资金保障（Safeguarding）制度

- 专户结构、T+0/T+1对账、差错补足机制、利息/费用处理原则、备付金比例监控、异常阈值与升级路径。

3) 外包管理政策

- 尽调评分卡、关键/非关键外包划分、KPI/SLA标准、审计权、数据驻留、可用性保障、退出与转移（Exit Plan）。

4) IT安全与变更管理（对齐DORA思路）

- 访问控制与最小权限、密钥/加密、日志（不可抵赖）、代码/变更发布、备份与演练、渗透测试/红队频率、重大事件通报窗口。

5) 业务连续性与灾备（BCP/DR）

- RTO/RPO指标、同城/异地冗余、演练计划与记录、第三方依赖清单。

6) 投诉处理与客户保护

- 受理渠道、SLA（受理/反馈/结案）、赔偿与恢复、上报触发点、模板回函。

7) 风险管理与内部审计

- 风险分类库、KRI、限额与预警阈值；内审年度计划、独立性、报告至审计委员会/董事会。

8) 薪酬与利益冲突

- 以合规为导向的薪酬约束、可变薪限制、冲突申报与回避、礼品/招待登记。

十六、董监高资料包（Fit & Proper模板）

A. 信息披露表（节选）

- 个人信息、居住史（10年）、就业史（10年）、资格证书、监管/刑事/民事/破产业务记录、金融机构任职记录、关联方交易披露。
- 声明：真实完整、可供BNB与他国主管机关共享；签字+日期。

B. 附件清单

- 无犯罪记录证明、资信/破产证明、学历与资格公证件、推荐信（2封以上）、过往雇主证明信、住址与税务居留证明。

C. 能力说明（胜任力Narrative）

- 与岗位相关的实务案例（合规、风险、IT、支付运营），对监管框架认识与过往问责经历，首年工作计划要点。

十七、股东/UBO 尽调与资金来源证明（清单）

- 身份与地址证明（经认证/公证）、税务居民声明、资金来源说明（股息/经营收入/资产处置等）与佐证流水、银行资信证明。
- 股权链与控制结构（至自然人UBO）、一致行动协议、否定控制与表决安排说明。
- 适当性声明：无制裁/无重大诉讼/非PEP或PEP风险缓释措施。

十八、Safeguarding 银行确认函（草稿范本）

（英文模板，可双语随附）

[Bank Letterhead] Date: [●] To: Bulgarian National Bank (BNB) Re: Client Money Safeguarding Account - [Company Legal Name], E-money Institution Applicant We hereby confirm that [Bank Name] maintains a designated safeguarding account: Account Name: [Company Name - Client Safeguarding] IBAN: [●] | BIC: [●] The account is ring-fenced for safeguarding clients' funds under applicable law and cannot be used to set-off any obligations of [Company Name] to the Bank. Withdrawals are limited to (i) returning funds to customers, or (ii) transfers in accordance with safeguarding rules. Contact: [Bank Officer, Title, Email, Phone] Signed, [Name], [Title] [Bank Name]

要点：专户命名、用途限制、不可抵销、联系人、唯一标识（IBAN/BIC）。

十九、EEA护照（Passporting）通知文件包（示例）

- 母国通知函：致BNB说明拟护照国家/业务方式（自由提供服务或设立分支）、产品范围、投诉/语言/客服安排、当地联络。
- 目的国信息包：本地消费者保护信息披露、客服语言、争议解决、广告审阅机制。
- 时间轴：母国受理→转报目的国→生效日期→官网更新与客户沟通。

二十、外包框架协议关键条款（SLA样例）

- 服务范围：KYC外包、客服、IT托管、云服务等，定义可衡量交付物。
- KPI/SLA：KYC周转≤24h、命中复核≤4h、系统可用性≥99.9%、关键事件响应≤30min。
- 监管权利：BNB/公司内审进入权；数据与日志可得性。
- 数据保护：加密、驻留、跨境传输限制、分包审批。
- 退出计划：30–90日平稳迁移、数据返还格式与验收清单。
- 违约与赔偿：服务积分/罚金、持续违约解约权。

二十一、IT与DORA控件映射清单（简版）

- ICT风险管理：资产清单、风险评估、供应链风险、变更管理。
- 事件通报：分级（重大/高/中/低）、T+0内部预警、T+1外部沟通草案。

- **数字运营韧性测试**: 年度渗透/红队、场景化演练（系统中断/数据泄露/第三方中断）。
 - **第三方风险**: 关键ICT服务识别、合同化控制、退出测试。
 - **记录与证据**: 日志留存≥12–24个月，时间同步，审计跟踪。
-

二十二、客户协议与信息披露关键条款

- **电子货币性质说明**（非存款、无存款保险）；
 - **费用表**（发行/充值/提现/兑换/不活跃费/汇率）；
 - **资金保障说明**（Safeguarding机制与异常处理时限）；
 - **客户尽调义务与资料真实性承诺**；
 - **投诉与争议解决**（SLA与申诉渠道）；
 - **隐私与数据处理**（GDPR权利与联系渠道）；
 - **变更通知与生效机制；冻结/终止情形**。
-

二十三、首年合规工作计划（月度节奏）

- **M1–M2**: 员工合规培训1/4、政策发布与宣导、KYC外包商审核与上线前评估。
 - **M3**: 首轮渗透测试/修复；投诉通道上线演练。
 - **M4–M5**: 内部审计季度巡检（KYC抽样、日志抽测）；风险评审会（更新KRI）。
 - **M6**: 年度中期资本充足与Safeguarding压力测试；培训2/4。
 - **M7–M8**: 外包年度再评估（SLA对标、整改计划）；客户条款年中复核。
 - **M9**: BCP/DR全量演练；董事会报告1次。
 - **M10–M11**: 年度审计预备、样本锁定；培训3/4。
 - **M12**: 年终合规报告、来年计划与预算、培训4/4。
-

二十四、监管问答（RFI/RFP）高频点与示范答复要点

- **资本来源**: 提供实缴凭证、流水、税务/股息/资产处置证明，阐明非债性、不附带担保或回购安排。
 - **Safeguarding**: 银行确认函+对账流程图+差错补足时限（例如T+1前补足）。
 - **外包安排**: 尽调报告（含分包链）、KPI/SLA、审计权条款、退出计划PDF。
 - **IT与安全**: 访问矩阵、渗透报告摘要、关键漏洞修复清单与复测证据。
 - **治理与独立性**: 合规/风险/内审的直线汇报至董事会的机制与冲突回避举措。
-

二十五、费用与预算细化（建议Excel科目）

- **一次性**: 法律与顾问、制度编制、IT评测、Safeguarding开户与函件、公证翻译、BNB受理费。
- **经常性**: 合规/MLRO/风险/IT安全薪酬、外包SLA费用、云与安全订阅、年度审计、监管费。
- **缓冲**: 监管问答追加成本、目的国护照本地化成本（翻译、客服、投诉处理）。

Excel建议字段：科目、一次性/经常性、币种、基线、低/高情景、付款里程碑、负责人。

二十六、项目实施RACI（示例）

任务	R (负责)	A (签核)	C (协商)	I (知会)
资本到位与证明	财务	CFO	法务/合规	董事会
制度文档编制	合规	CCO	风控/IT/业务	全员
IT与渗透测试	IT安全	CTO	外包商	合规
Safeguarding开户	财务	CFO	合规/银行	董事会
申请包提交	法务	CEO	合规/顾问	董事会
监管问答	合规	CCO	法务/IT/财务	董事会

二十七、审计与监管报送日历（模板）

- **年度经审计财报**: 次年6月30日前提交。
- **重大事项** (董事/高管变更、UBO/外包/代理变更、名称/地址变更): 事前报批/报备。
- **Safeguarding开户/变更**: 取得银行确认后于规定窗口内通知。
- **外包年度复核**: 每12个月一次; 关键外包半年度复核。

二十八、风险登记册（Risk Register）样表

风险ID	类别	场景	影响/概率	KRI/阈值	控制措施	负责人	下次评审
R-EMI-001	操作	对账失败导致差错	M/H	T+1未对平	双人复核+自动比对	财务	2025-12
R-IT-003	信息安全	凭证泄露	H/M	异常登录次数	MFA+密钥轮换	IT	2025-11
R-AML-005	合规	高风险客户渗透	H/M	PEP命中率↑	强化EDD+二线复核	合规	2025-10

二十九、STR（可疑交易报告）流程与范文（要点）

流程：一线发现→合规初审→二线复核→MLRO决定→提交STR→保存记录与保密管理。

叙述要点：客户背景、触发信号（金额/频次/地域/结构化）、已采取的KYC/EDD、异常之合理怀疑、无通知客户声明、后续监控计划。

三十、培训计划与测评题库（示例）

- **季度主题**: Q1 AML基础与制裁、Q2 Safeguarding与客户保护、Q3 事件通报与BCP、Q4 外包与数据保护。
- **考题示例（单选）**:
 1. 发现客户分拆交易迹象，第一步应当？ A. 通知客户 B. 记录并报MLRO (✓) C. 直接销户
 2. Safeguarding差额补足最迟应在？ A. T+3 B. T+1 (✓) C. 次周一

三十一、董事会/股东会决议模板（可直接落章）

A. 董事会决议（申请EMI许可）

Board Resolution Company: [●] AD/OOD Date: [●] 1. RESOLVED that the Company shall apply to the Bulgarian National Bank (BNB) for authorization as an Electronic Money Institution under PSPSA. 2. RESOLVED to approve the capital of BGN 700,000 (or above) fully paid-in, and to evidence lawful sources of funds. 3. RESOLVED to appoint [Name, Title] and [Name, Title] as persons effectively directing the business (four-eyes). 4. RESOLVED to adopt the following policies: AML/CFT, Outsourcing, Safeguarding, IT & Cybersecurity, Risk Management, Complaints Handling, BCP/DR. 5. RESOLVED to designate [Bank Name] for safeguarding accounts and authorize signatories: [●], [●]. 6. RESOLVED to appoint MLRO: [Full Name], Deputy MLRO: [Full Name]. 7. RESOLVED to appoint external auditor: [Firm, Reg. No.]. 8. RESOLVED to authorize [CEO/CCO] to execute and submit all application documents and respond to BNB inquiries. Chairperson: [Signature] Secretary: [Signature]

B. 股东会决议（增资/结构与授权）

- 批准实缴增资与资金来源说明；
- 确认UBO穿透结构、授权董事会办理护照与外包重大事项；
- 批准关键岗位聘任与薪酬框架（合规导向）。

三十二、授权书（POA）与声明模板

POA（提交/领证/问答）

POWER OF ATTORNEY Grantor: [Company] Attorney-in-fact: [Local Counsel/Officer, ID/Address] Scope: Filing, collecting documents, making submissions and receiving notices before BNB and other authorities in relation to EMI authorization and passporting matters. Term: Until revoked. Signature: [●] Company Seal: [●]

声明类：资金来源声明、无关联贷款/回购安排声明、外包不构成未经许可的转授权声明、数据跨境合规模块声明（GDPR）。

三十三、翻译、公证与认证清单（保加利亚实务版）

- 宣誓翻译：保语↔英/中（章程、决议、无犯罪记录、资信证明、学历与资格等）。
- 公证：境外文件先公证/海牙认证（Apostille）后入保使用。
- 时间预估：宣誓翻译2-7个工作日/件；Apostille 3-10个工作日/件（视国家而定）。

- 版式规范：每份文件统一编号+版本（例如：POL-AML-v1.2-2025-09-24）。
-

三十四、KYC/AML 表单套件（可直接发客户/代理）

1. **个人客户KYC表**：身份/地址/税号、职业与收入、资金来源、PEP/制裁声明、风险分层同意。
 2. **企业客户KYB表**：注册信息、股权链至UBO、受益安排、董事与授权签字人、财务与交易目的。
 3. **SOW/SOF问卷**：来源类别（工资/股息/资产出售/贷款等）与证明清单。
 4. **风险评分矩阵**：国家/行业/产品/渠道/行为（阈值可配置）。
 5. **EDD清单**：高风险/PEP/复杂结构所需的补充材料与频率。
-

三十五、客户协议与费用/限额政策（示范条款）

- **费率表**（可放可配置表）：发行费/充值费/提现费/赎回费/兑换费/不活跃费/卡片（如适用）。
 - **限额策略**：单笔/日/月度交易与余额上限；分层KYC对应限额；异常触发**人工复核**。
 - **货币与汇兑**：FX成本构成与加点披露、极端波动应急。
 - **清算与到账时间**：T+0/T+1；节假日例外。
 - **冻结/终止**：触发条件、客户告知机制、申诉途径与时限。
-

三十六、财务模型假设库（Excel建议字段）

- **驱动**：注册用户、活跃率、ARPU、充值/提现/兑换量、资金在途天数。
 - **收入**：费率（阶梯/分层）、FX加点、浮存资金利息（若适用，合规披露）。
 - **成本**：支付通道费、KYC/筛查SaaS、云与安全订阅、外包SLA、审计与监管费。
 - **合规缓冲**：年度监管费（方法学）、渗透测试与整改预算、护照本地化成本。
 - **场景**：基线/乐观/保守，输出现金流表、监管资本缓冲曲线。
-

三十七、交易监测规则库（初始版本）

- **结构化交易**：多笔小额接近阈值；**24/72小时**窗口累计超阈。
- **快速资金循环**：充值→短时赎回/提现；黑名单商户往来。
- **地理异常**：高风险辖区IP/设备变换；代理/VPN特征。
- **速度/频率**：新开账户在短期高频操作；夜间异常活动。
- **名单命中**：制裁/PEP命中二次复核；同名/近似名处理SOP。

每条规则包含：**触发条件、阈值、处置SLA、证据留存**。

三十八、投诉与争议处理包

- **流程图**：受理→分级→答复→整改→关闭→董事会季度合规汇报。
 - **登记样表**：编号、客户ID、类别、收件时间、承诺SLA、实际结案、补偿（如有）、根因分类。
 - **模板回函**：确认受理、预期时限、材料清单、二次申诉通道。
-

三十九、运营SOP（关键流程）

- **开户**：身份核验→名单筛查→风险评分→限额分配。
 - **充值/提现/赎回**：资金路径、对账节点、异常差额**T+1补足**。
 - **退款与拒付**（如有发卡/收单）：证据包、时限与责任分配。
 - **休眠/销户**：不活跃阈值、费用与通知、资金退回路径。
 - **数据留存**：KYC与交易记录≥规定年限；取证与审计可用性。
-

四十、营销与信息披露合规指南

- 禁止性表述：不得将电子货币宣传为“银行存款/受存款保险保护”。
- 风险披露：资金性质、费用、限额、退款/赎回规则、客户权利。
- 广告审批：四眼复核、法务合规盖章、留存样证（截图/外链）。
- KPI：误导性投诉比率、审核前置时长、素材抽检覆盖率。

四十一、供应商与云尽调问卷（VDDQ）

- 一般合规：牌照/认证（ISO27001、PCI-DSS等）、审计报告可用性。
- 安全：加密、密钥管理、访问控制、日志、备份与RTO/RPO。
- 数据：位置/跨境传输、子处理者（sub-processor）名录与通知机制。
- 合同：审计权、退出计划、SLA与违约条款。
- 连续性：容量与弹性、重大事件通报窗口与演练记录。

四十二、事件管理与通报（重大事件报告包）

- 分级与SLA：重大（即时内通报管理层，外部通报按法规时限）；高/中/低优先级。
- 必备字段：事件概述、影响范围（客户/金额/地域）、根因、即刻缓解、长期整改、证据清单。
- 对外模板：致BNB的初报/续报/结案报告格式；客户通知话术与FAQ。

四十三、数据保护合规模块（GDPR实操）

- ROPA（处理活动记录）字段：目的、法定基础、数据主体、类别、接收方、存储期限、技术与组织措施（TOMs）。
- DPIA模板：场景、风险、影响评估、缓释措施、残余风险评估与批准意见。
- 数据主体请求（DSR）：接收→验证→检索→答复→留档SOP（30天内）。
- 隐私政策/饼干政策：可复用骨架，支持多语言与护照国本地化条款。

四十四、员工手册的合规章节（要点+模板）

- 行为准则/利益冲突：申报、回避、礼品与招待阈值。
- 举报（Whistleblowing）：匿名渠道、免于报复声明、调查流程。
- 信息安全：MFA、口令策略、便携设备与远程办公规范。
- 培训与考核：入职、岗位变更、年度与临时培训；测评与缺考补训。

四十五、合规KPI / OKR看板（季度滚动）

- AML：STR提交及时率、EDD完成率、名单误报率、规则命中处置SLA。
- 运营：对账差额率、T+1补足率、系统可用性、客户投诉SLA达标率。
- 治理：政策年审覆盖率、内审整改关闭率、供应商再评估完成率。
- 人力：强制培训完成率、关键岗位备份覆盖率。

四十六、年度审计与证据目录（示例）

- 财务：经审计报表、银行函证、Safeguarding对账包、资金差错台账。
- 合规：KYC抽样、EDD证据、STR样本、外包尽调档案、培训记录。
- IT：渗透测试报告（含复测）、变更记录、权限审计、备份演练截图。
- 治理：董事会与合规委员会会议记录、政策年审记录。

四十七、护照项目包 (Per Country Pack)

- 本地化：客服语言、投诉机制、广告法规、费用与税务提示。
- 通知材料：服务模式 (FOS/Branch)、联系人、服务清单。
- 上线清单：网站本地化、条款差异、隐私与Cookie、客服SLA。

四十八、代理 (Agent) 网络管理政策与合同要点

- 准入：资质/区域/渠道合规，KYC能力评估与培训。
- 合同：职责边界、不得再授权、KPI/SLA、佣金与费用披露、合规违约退出。
- 监督：抽样复核、神秘客、投诉回溯、季度合规打分与整改。

四十九、(可选) 现金与ATM相关业务控制

如开展现金充值/ATM提现相关服务：

- 现金限额与轨迹、视频/柜员双人确认、异常金额T+0上报；
- 与合作机构接口对账SOP；现金差额调查与保全链条。

五十、有序退出/应急计划 (Wind-Down Plan)

- 触发：资本不足/重大违规/关键供应商失败/持续性事件。
- 步骤：新开户冻结→交易限额→通知客户与监管→资金妥善赎回/退回→数据与记录保全→合同退出。
- 治理：专项工作组、每日仪表盘、顾问与审计参与、里程碑验收。

五十一、对外递交通函 (Cover Letter) 与目录 (Submission Index)

A. 递交通函 (英文示范，可平行出保语版)

[Company Letterhead] Date: [●] To: Licensing and Supervision Department Bulgarian National Bank (BNB) Re: Application for Authorization as an Electronic Money Institution (EMI) Dear Sir/Madam, We hereby submit our application for authorization as an Electronic Money Institution under the PSPSA, including all supporting documents per Ordinance No.16. The persons effectively directing the business are [Full Name] and [Full Name]. The appointed MLRO is [Full Name]. The initial capital of BGN [$\geq 700,000$] has been fully paid in. Please find enclosed the Submission Index and signed declarations. We remain at your disposal for any clarifications. Sincerely, [Name, Title] [Company Legal Name] Email: [●] Tel: [●]

B. 提交目录 (映射条例条款的“索引”)

序号	文档名称	法规映射	版本/日期	备注
1	公司注册与章程	PSPSA §... / Ord.16 §...	v1.0 / 2025-09-24	认证译本
2	资本与资金来源证据	PSPSA §...	v1.0	实缴证明、流水
3	实际管理人任命与简历	Ord.16 §...	v1.0	两名以上
4	AML/CFT政策与风险评估	Ord.16 §...	v1.0	含制裁模块
5	Safeguarding制度+银行函	Ord.16 §...	v1.0	专户/保险
6	IT与网络安全/BCP/DR	Ord.16 §...	v1.0	含渗透计划
7	外包管理与尽调包	Ord.16 §...	v1.0	关键/非关键
8	商业计划与财务模型	Ord.16 §...	v1.0	3-5年
9	审计师聘任与报送日历	Ord.16 §...	v1.0	年度安排
10	代理与分支登记计划	PSPSA §...	v1.0	跨境护照

注：把每份文件封面右上角标注“法规映射”，BNB问答时能快速定位。

五十二、监管面谈 (Interview) 与书面问答题库 (精选20题)

- 请解释你们Safeguarding专户的对账频率与差额补足时限。
- 两位“实际管理人”如何落实four-eyes在产品、风控、资金上的制衡？
- 外包商子处理者 (sub-processor) 出现重大事件时，你们如何行使审计权？

4. 如何保证客户资金与自有资金不被混同（含费用扣减）？
5. 高风险客户进入的审批阈值与EDD证据清单？
6. 多币种账户的汇兑与费率披露如何执行？
7. 渗透测试频率、修复SLA与复测证据管理。
8. 投诉分级与SLA，以及向BNB通报触发条件。
9. IT变更的审批-测试-发布闭环如何记录？
10. 停机/灾备演练RTO/RPO与年度计划。
11. 如何识别并阻断结构化交易与快速资金循环？
12. 名单筛查：来自UN/EU/OFAC的同步机制与误报处理。
13. 护照到他国后的客服语言/争议解决安排。
14. 营销合规避免“存款/保险”误导的流程。
15. 资金来源（SOF/SOW）证据不足时的处置。
16. 董事会治理：合规/风控/内审直线汇报机制。
17. 资本充足监控与预警阈值、补资本动作表。
18. 数据主体请求（GDPR）30日内响应机制。
19. 代理（Agent）管理：准入、抽检、退出。
20. 有序退出计划触发条件与客户资金返还路线。

每题准备1页“要点弹药”，附上制度/流程页码与索引。

五十三、项目甘特图（里程碑与责任人清单）

里程碑	起止（周）	负责人	关键产出
组建与Gap评估	W1-W2	CCO	差距报告、时间/预算版
资本与结构冻结	W2-W4	CFO	实缴凭证、UBO穿透图
制度与IT材料	W3-W8	合规/CTO	政策全集、架构与渗透计划
Safeguarding开户	W4-W7	CFO	银行函+对账SOP
外包尽调与合同	W5-W8	采购/合规	VDDQ、SLA/退出条款
申报与受理	W9	法务	封面信+索引
监管问答轮1	W10-W14	CCO	答复包v1
监管问答轮2	W15-W18	CCO	答复包v2
许可与上线准备	W19-W24	PMO	UAT、培训、公告
护照与本地化	W25-W32	PMO	目的国包

五十四、Safeguarding 对账SOP（T+0/T+1）

目标：确保客户资金专户日终=客户账面余额。

流程：

1. 日内实时对账（T+0）：网关入账→中台账→专户入账；异常阈值触发预警。
2. 日终对账（T+0 23:30前）：账面余额与银行对账单核对。
3. 差额补足（T+1 11:00前）：财务出具补足回执；异常报告存档。
4. 月度抽审：内审/合规抽样核验10%日样本。

记录：留存CSV/报表、责任人签名、差异原因与整改。

五十五、交易监测规则（参数化“起步集”）

规则	触发条件（示例）	处置SLA	证据
结构化	24h内≥5笔接近KYC层级阈值的充值	4h初审/24h结案	明细+图形
快速循环	24h内≥80%资金在充入后≤2h赎回	4h	通道票据
地理异常	同日跨高风险国IP/设备指纹切换≥3次	4h	设备指纹
黑名单可疑	命中制裁/PEP近似名且KYC异常	2h	筛查截图
异常商户	某商户退款/拒付率>行业基线*2	48h	对账与证据

阈值可随基线/季节性动态调整，保留版本变更记录。

五十六、外包与云合同“合规模块条款”(可摘入合同)

- 审计与访问权：BNB/内审进入、样本与日志可得性。
- **SLA**：可用性≥99.9%；重大事件T+0初报30分钟内；修复SLA分级。
- 数据与保密：加密（在传/在存）、驻留与跨境约束、子处理者名单变动通知。
- 退出：最短30–90日迁移窗口、数据返还格式（CSV/JSON/DB dump）、验收清单。
- 监管优先条款：监管要求优先于其他合同条款，供应商配合义务。

五十七、客户条款（T&C）关键披露段落（中英对照）

电子货币性质 / Nature of E-Money

- 中文：电子货币并非银行存款，不适用存款保险。我们通过受监管的**资金保障机制（Safeguarding）**保护您的资金。
- EN: E-money is not a bank deposit and is not protected by deposit guarantee schemes. Your funds are protected via safeguarding arrangements.

费用与汇率 / Fees & FX

- 中文：我们将透明披露费用与汇率加点；任何变更将提前[●]日通知。
- EN: We disclose fees and FX mark-ups transparently; changes will be notified [●] days in advance.

赎回规则 / Redemption

- 中文：在适用限额内，您可按条款赎回电子货币，通常T+0/T+1到账。
- EN: You may redeem e-money within applicable limits; crediting is typically T+0/T+1.

五十八、审计与合规证据“打包清单”(交付给审计师)

- 资本与专户：实缴凭证、银行函、月末对账单与差额台账。
- AML：风险评估、规则库、命中样本、STR记录。
- IT：渗透报告、重大事件记录、权限审计与变更单。
- 外包：尽调问卷、SLA、季度服务报表、退出演练记录。
- 治理：董事会/合规委员会会议记录、政策年审单、培训签到与测评。

五十九、监管报告模板（初报/续报/结案）

初报关键字段：时间、影响（客户数/金额/地域）、系统/流程、已采取措施、下一步与时限、联系人。

续报：新增事实、修复进度、残余风险、临时控制。

结案：根因、永久修复、复盘与改进、证据。

六十、护照（Passporting）目的国“本地化清单”

- 语言：客户支持/条款/隐私与广告合规的语言版本。
- 投诉：本地监管/仲裁通道与SLA；披露在网站“Complaints”页。
- 营销：本地禁限表述与行业自律规范。
- KYC差异：本地身份证明、住址证明常用文件与等价性。
- 税务：如涉预扣/间接税的说明与票据交付路径。

六十一、内部审计章程（精简版模板）

使命：对治理、风险管理与控制有效性提供独立保证。

权责：不受限制访问记录/人员/场所；直接向审计委员会/董事会报告。

频率：年度计划+临时审计；重大事件后专项审计。

独立性：不得承担被审计活动的经营职责。

报告：评级、发现、整改计划与复核时间点。

六十二、MLRO年度报告（结构化提纲）

- 1. 法规与执法趋势回顾；2) 企业风险评估（更新）；
- 2. KYC/EDD与交易监测指标；4) STR统计与案例；
- 3. 名单筛查有效性（误报/漏报）；6) 培训与文化；
- 4. 外包KYC质量评估；8) 改进行动与时间表。

六十三、HR与人员合规（背景核查SOP）

- 入职前：身份与学历核验、无犯罪/破产、雇佣证明。
- 敏感岗位：财务/MLRO/IT安全需加强背景审查与年复核。
- 离任与交接：权限回收、设备/资料返还、保密延续条款。
- 培训：入职/年度/临时三类；缺考补训机制。

六十四、网站“合规披露”页面结构（可直接上线）

- Licensing & Company Info**: 公司名、注册地址、BNB许可信息、联系渠道。
- Fees & Limits**: 清晰表格（可下载PDF）。
- Safeguarding**: 机制概述与客户权利说明。
- Complaints**: 流程、SLA、升级与外部机构链接。
- Legal**: T&C、Privacy、Cookie、AML告知、营销限制。
- Status**: 系统可用性/重大事件历史（可选，提升信任）。

六十五、有序退出（Wind-Down）“运行手册”（Runbook）

- T-3天：冻结新开与营销、限额降档、公告预告。
- T-2天：通知合作方与供应商、锁定数据备份、开通专线客服。
- T-1天：发送赎回引导、网站/APL置顶提示、报BNB进度。
- T日：停止入金、仅保留赎回通道、资金清算。
- T+1~T+30：遗留对账、未领资金公示、证据与档案封存。

六十六、KRI（关键风险指标）与阈值（示例表）

KRI	阈值	预警	违规	责任人
日终对账差额率	0%	>0%	>0.01%	财务
结构化交易命中率	基线	>基线*1.5	>基线*2	合规
渗透高危未修复>7天	0	1	>2	CTO
培训完成率	100%	<98%	<95%	HR
投诉SLA达标率	≥98%	95-98%	<95%	客服

六十七、GDPR文档快速包（可直接起草）

- ROPA**表头：处理目的/法定基础/数据主体/类别/接收方/保留期/TOMs。
- DPIA**模板：高风险场景（KYC、监测、跨境云），列明残余风险与批准意见。
- DSRSOP**：身份验证清单、检索脚本、标准回函模板。
- 处理者合同附件**：TOMs清单、分包商名录、事件通报时限。

六十八、培训方案（微课+测验）

- 微课**：每节10-12分钟，题库5题；季度滚动主题（AML、Safeguarding、事件管理、外包）。
- 追踪**：学习平台导出证据（完成率、成绩、时间戳）。

- 纠偏：连续两次不合格→部门负责人一对一面谈与补训。
-

六十九、客户常见问题（FAQ）成品段落（可上官网）

- 电子货币安全吗？我们不吸收存款；您的资金在专用保障账户中隔离保管。
 - 赎回多久到账？按T&C通常T+0/T+1；遇节假日可能顺延。
 - 为什么需要这么多资料？为遵守反洗钱与制裁法律。
 - 如何投诉？在“Complaints”页提交，我们在2个工作日内回复。
 - 账户冻结了怎么办？我们会告知原因与需要的材料，核验通过后尽快解冻。
-

七十、上线清单（Go-Live Checklist）

- 生产变更审批与回滚方案
 - 网站/APP合规披露上线复核
 - 客服知识库与FAQ同步
 - STR提交流程演练记录
 - Safeguarding试运行对账与模拟补足
 - 目的国护照国家本地化材料核对
-

保加利亚电子货币机构（EMI）牌照申请注册指南常见问题解答

本文内容由仁港永胜提供讲解，这是一份面向实操的《保加利亚EMI常见问题解答（FAQ全集）》。结构按申请前→材料准备→审批过程→技术与合规→运营与持续义务→变更与护照→费用与预算→风控与退出八大类，便于检索与内训。

七十一、申请前（资格与路径）

Q1：EMI与支付机构（PI）有什么本质区别？

A：EMI可发行电子货币并提供支付服务；PI只能提供支付服务，不得发行电子货币。EMI对资本、Safeguarding、治理与IT要求更高。

Q2：是否存在“小型EMI/过渡许可”？

A：保加利亚主流为完全授权EMI路径（最低初始资本≈EUR 350k）。若考虑限额/过渡安排，须以BNB当期口径为准，并通常不具跨境护照资格。

Q3：境外股东能否申请？是否必须当地团队？

A：可以有境外股东，但注册地与实质管理需在保加利亚；需配置**本地实际管理人（至少两名）**与可核验的办公场所。

Q4：银行牌照和EMI牌照能同时持有吗？

A：可由不同法人分别持有；单一实体同时持有两类牌照在治理与资本要求上复杂度极高，实务上少见。

Q5：申请周期通常多久？

A：常见6-12个月（材料成熟度、IT复杂度、问答轮次决定节奏）。获批后12个月内须开业，否则存在撤销风险。

七十二、材料准备（资本、股东与董监高）

Q6：最低资本与到位形式？

A：最低初始资本≥BGN 700,000 (≈EUR 350,000)，需实缴、来源可追溯且为高质量资本（非债性、无回购安排）。

Q7：资金来源（SOF/SOW）如何证明更稳妥？

A：提供股息/经营收入/资产处置等来源证明+银行流水+税单/审计报告；避免循环转账与短期资金占用迹象。

Q8：实际管理人（four-eyes）必须具备什么背景？

A：支付、风控、合规、IT/运营多维经验；能展示对Safeguarding、AML、外包与IT安全的实操能力与治理机制。

Q9：MLRO与合规负责人可以同人兼任吗？

A：小型团队可兼任，但需证明资源充足、独立性与冲突回避；建议配备副MLRO以保障连续性。

Q10：外部顾问能否充当“实际管理人”？

A：不宜。实际管理人应为公司核心管理层、持续在岗并驻地，顾问可辅助但难以满足“有效管理”与持续在场要求。

七十三、审批过程（流程、问答与审查要点）

Q11：BNB更关注哪些“致命项”？

A: ①资本来源与所有权结构透明；②Safeguarding闭环（专户/保险、对账、补足SLA）；③IT与外包可控与可审计；④AML/CFT风险评估与交易监测有效性；⑤治理独立性。

Q12：预沟通是否必要？

A: 强烈建议。可就Safeguarding模式、外包边界、IT韧性等关键立场先行对齐，降低后续问答成本。

Q13：问答通常几轮？如何提效？

A: 1-3轮常见。以**“法规映射索引”**回应，逐条引用政策页码/流程图/证据附件，避免叙述型长文无证据。

Q14：被拒后多久可重报？

A: 通常有冷却期（以当期规则为准）。实务建议先完成差距整改与预审沟通再重启。

Q15：是否需要现场核查或面谈？

A: 视情形。准备办公室与系统演示、关键岗位面谈要点与证据包（权限审计、对账报表、日志样例）。

七十四、技术与合规（IT、外包、数据与Safeguarding）

Q16：客户资金“Safeguarding”有哪些合规做法？

A: ①专用保障账户（银行函明确用途限制、不可抵销）；②保险/担保等等效保障；配套T+0/T+1对账与差额T+1前补足。

Q17：能否把KYC/客服完全外包？

A: 可外包，但责任不可外包。需尽调评分卡、KPI/SLA、审计权、退出计划与子处理者管理；关键外包定期年度复评。

Q18：云上部署合规点？

A: 访问控制、加密、日志、事件通报、数据驻留/跨境安排、备份与演练（RTO/RPO）、合同化审计权与退出条款，并与DORA思路对齐。

Q19：渗透测试频率与证据？

A: 至少年度一次（重大变更/事件后加测），保存报告、修复单与复测证据，把高危>7天未修复列为KRI红线。

Q20：GDPR如何落地？

A: 建立ROPA、DPIA、DSR处理SOP；处理者合同写入TOMs、分包商名录与事件通报时限；隐私政策清晰披露。

七十五、运营与持续义务（报告、审计、投诉与营销）

Q21：年度审计与监管报送节奏？

A: 年度经审计报表次年6月30日前提交；重大事项（董事/UBO/外包/地址等）按规定报批/报备；保留差异与补足台账。

Q22：投诉处理的监管关注点？

A: 受理渠道、分级与SLA、证据与回溯、根因与整改闭环；官网“Complaints”页公开流程与升级路径。

Q23：营销有哪些禁忌？

A: 禁止将电子货币描述为“银行存款/受存款保险”；费用与FX加点须透明披露；广告素材需四眼复核与留存。

Q24：费用与限额如何管理？

A: 建立费率表与限额策略（按KYC层级与风险分层），重大调整提前告知；系统校验与手工复核并行。

Q25：如何证明持续资本充足？

A: 按监管口径计算自有资金/运营规模，设置预警阈值与补资本流程；董事会定期审阅资本与KRI仪表盘。

七十六、变更、护照与集团协同

Q26：董事/MLRO变更流程？

A: 提前报批/报备并提交适格性材料与过渡安排；确保职责交接与权限回收有记录。

Q27：跨境护照如何推进？

A: 走母国通知→目的国生效流程；准备目的国语言、投诉、广告差异与客服SLA；网站与T&C同步本地化。

Q28：集团里多实体协同会被质疑吗？

A: 可协同，但需防范监管套利与风险外溢；明示服务边界、数据与资金隔离、关联交易定价与披露。

Q29：能否通过代理（Agent）扩张？

A: 可，但需准入尽调、培训、合规条款与抽检；严禁未经批准的再授权链条。

Q30：更换Safeguarding银行要注意什么？

A: 先开后换，确保并行期对账无缝；取得新银行确认函并在规定时限内通知监管与更新内部SOP。

七十七、费用、预算与时间表

Q31：总预算如何抓大头？

A：三大块：人力（合规/风控/IT）、IT与安全与外包SLA、法务与审计及监管费；一次性项目（制度编制、渗透与整改、Safeguarding开户）需单列。

Q32：监管收费是固定值吗？

A：一次性受理费通常有参考区间；年度监管费多按方法学（风险/业务规模）测算，非统一金额，建议在模型中单列“Regulatory Levy”。

Q33：节省成本的同时如何不踩雷？

A：能外包但不可外放责任；核心控件（对账、名单筛查、日志与审计权）应自控+可审计；对低价供应商强化退出演练与备援。

Q34：时间表如何控风险？

A：预留两轮问答冗余；将银行函、渗透测试、外包合同安排在正式申报前完成；设置关键路径里程碑与决策闸口。

七十八、风险、执法与退出（Wind-Down）

Q35：最常见的撤销/处罚触发？

A：未按期开业、Safeguarding失当（混同/差额未补）、高危漏洞长期未修复、重大变更不报备、反洗钱机制失效。

Q36：应急/退出计划何时启动？

A：资本跌破阈值、关键外包连续失败、重大事件影响客户资金安全等触发；按冻结新开→限额→客户赎回→清算→封存路线执行，并全程报监管。

Q37：重大事件如何通报？

A：内部分级与T+0初报机制；外部按法规时限初报/续报/结案；对客户透明披露影响与补救路径。

Q38：如何降低合规黑天鹅？

A：建立KRI阈值与看板、季度红队/演练、关键外包备援、董事会直达的合规通道与“停止按钮”。

七十九、加分项与落地建议

Q39：哪些“证据型材料”最打动监管？

A：①Safeguarding银行确认函+月度对账与差额台账；②渗透测试报告+复测证据；③外包SLA与退出演练记录；④投诉台账与改进闭环；⑤董事会会议纪要与政策年审记录。

Q40：如何把FAQ用于内训与面谈？

A：将每一问映射到制度条款与流程编号，制作“一页纸要点弹药”；面谈前进行情景演练（如对账差额、名单误报、云服务中断）。

Q41：第一周应该先做什么？（7天起步包）

Day1-2：Gap评估；Day3：Safeguarding银行筛选与接触；Day4：组织架构与角色冻结；Day5：外包清单与尽调问卷发出；Day6：政策目录与法规映射表定稿；Day7：项目里程碑与风控KRI卡。

八十、申请包“目录树”与归档规则（可复制）

/BNB-EMI-Submission/ 00-Cover-Index/ 001-Cover-Letter.docx 002-Submission-Index.xlsx 01-Corporate-Gov/ 011-COI-Articles-CN-EN-BG.pdf 012-Shareholder-Register.pdf 013-UBO-Structure-Chart.pdf 014-Board-Resolutions-EMI-Authorization.docx 02-Capital-SOF/ 021-Paid-in-Capital-Certificates.pdf 022-Bank-Statements.pdf 023-Source-of-Funds-Pack.zip 03-Fit-and-Proper/ 031-Directors-CVs.zip 032-Police-Clearance.pdf 033-Bankruptcy-Certificates.pdf 04-Policies/ AML-Policy-v1.2.docx Safeguarding-Policy-v1.1.docx Outsourcing-Policy-v1.0.docx IT-Security-Policy-v1.3.docx BCP-DR-Policy-v1.1.docx Complaints-Handling-Policy-v1.0.docx 05-IT-Architecture/ 051-System-Topology.pptx 052-Access-Matrix.xlsx 053-Logging-Spec.docx 06-Safeguarding/ 061-Bank-Letter.pdf 062-Reconciliation-SOP.docx 063-Daily-Match-Reports-Samples.zip 07-Outsourcing-Agents/ 071-Vendor-DueDiligence.xlsx 072-Standard-SLA.docx 073-Exit-Plan.docx 08-Business-Plan/ 081-BizPlan-5Y.pptx 082-Financial-Model.xlsx 09-Audit-Reporting/ 091-Auditor-Engagement.pdf 092-Reporting-Calendar.xlsx 10-Passporting/ 101-Home-Notice.docx 102-Host-Country-Pack.zip

版本规则：文档名-版本号-日期（如 Safeguarding-Policy-v1.1-2025-09-24.docx）；只增不改，旧版移入/Archive/并保留变更记录。

八十一、法规映射索引（示例字段）

文档	条款/法规	要求摘要	文档页码/段落	证据/附件
Safeguarding Policy	PSPSA §... / Ord.16 §...	专户、对账、T+1补足	p.3-7	银行函、对账样表
Outsourcing Policy	Ord.16 §... / DORA框架	尽调、SLA、审计权、退出	p.2-6	VDDQ、SLA条款
IT Security Policy	Ord.16 §... / GDPR	访问控制、日志、事件	p.4-10	渗透报告、事件模板

八十二、文件命名与版本控制政策（精简版）

- **语法:** <主题>-<子模块>-v<主次版>-YYYY-MM-DD-<作者缩写>
- **版序:** 主版变更（策略/流程修改）+0.1；次版（修字/排版）+0.0.1。
- **审批:** 草拟（D）→复核（R）→批准（A）；封面列出 D/R/A 与日期。
- **受控发放:** 只发PDF受控版；源文件仅限合规库访问。

八十三、获批后“前100天”稳定运行计划（100-Day Plan）

- **D1-D7:** 资金对账“演练→实战”，名单筛查阈值投产复核；客服FAQ上线。
- **W2-W4:** 首轮内审抽样（KYC 50份、交易100笔、对账10日样本）；修复闭环。
- **W5-W8:** 供应商再评估、退出演练；KRI看板周更→双周更。
- **W9-W12:** 护照首批国家上线（FOS模式优先）；投诉机制复盘与话术库更新。

八十四、银行与支付通道合规模块（若涉卡/收单）

- **PCI DSS范围界定:** Token化/不落敏感数据优先；选择 **SAQ A/A-EP/D** 路径。
- **拒付/争议SOP:** 证据包清单、提交时限、胜诉率KPI（≥65%起步）。
- **商户尽调（如有收单）:** 行业白/灰/黑名单、退款率阈值、冻结机制与解冻SLA。

八十五、费用变更与客户通知SOP

- **前置评审:** 法务合规与董事会授权阈值；影响评估（NPS/投诉风险）。
- **通知机制:** 提前 **≥30日**（示例），多渠道（站内、邮件、APP推送），保留送达证据。
- **申诉例外:** 弱势客户保护与过渡期；官网FAQ同步。

八十六、业务连续性“场景库”（演练脚本）

场景	触发	目标	RTO/RPO	成功判据
银行专户对账失败	银行对账系统中断	T+1前补足	4h/0	差额=0、记录完整
云区域故障	区域性宕机	业务无感切换	1h/15m	交易不中断
数据泄露疑虑	日志异常	识别/隔离/通报	2h/15m	法定时限通报

八十七、董事会与合规委员会年度议程（要点）

- **季度:** KRI仪表盘、资本充足、审计整改闭环、外包/供应商报告。
- **半年:** 政策年审、渗透测试、Safeguarding抽审、客户保护专题。
- **年度:** 战略与护照路线、预算与监管费预计、MLRO年度报告。

八十八、监管联络函模板库（节选）

- **重大变更报备函**（董事/MLRO/地址/外包）
- **护照通知函**（FOS/Branch）
- **事件初报/续报/结案模板**
- **Safeguarding银行更换通知**

每份函件：抬头、事实与时间线、合规条款引用、附件索引、联系人。

八十九、数据字典（KPI/报送用核心字段）

主题	字段	类型	说明
客户	kyc_level	enum	L1/L2/L3
交易	txn_type/amount/currency/timestamp	mixed	充/赎/转/兑
监测	rule_id/hit_score/outcome	int/decimal	命中与处置
对账	ledger_balance/bank_balance/diff	decimal	T+0/T+1

主题	字段	类型	说明
投诉	cat/open_ts/close_ts/sla_flag	mixed	SLA达标

九十、访问控制与职责分离 (RBAC/SoD矩阵)

职能	查看	提交	审批	复核
财务 (对账)	√	√		√ (二线)
合规/MLRO	√	STR提交		√
IT运维	系统日志	变更申请	变更批准 (CAB)	
业务运营	客诉资料	工单		合规抽查

红线：同一人不得同时“创建交易+对账复核”；变更实施与批准隔离。

九十一、漏洞管理与渗透测试流程 (全生命周期)

- 识别 (扫描/渗透/情报) → 2) 评估 (CVSS/业务影响) →
- 修复计划 (优先级与SLA: 高危≤7天、中危≤30天) →
- 复测与关闭 (证据) → 5) 月报与趋势分析 (董事会可视化)。

九十二、API与审计日志规范 (字段清单)

- 请求: req_id、user_id、ip、device_fingerprint、endpoint、payload_hash、ts。
- 响应: status、latency_ms、error_code、error_msg。
- 审计: actor、action (create/update/delete/approve)、object_id、before/after、ts、sig。
- 留存: ≥12-24个月；时间同步 (NTP)；篡改防护 (WORM/签名)。

九十三、数据保留与销毁矩阵 (示例)

文档/数据	保留期	法规依据	介质	销毁方式
KYC档案	≥5年 (自关系结束)	AML框架	加密存储	粉碎/安全擦写
交易记录	≥5年	支付法规	数据库/归档	脚本彻底删除
日志	12-24月	安全/取证	SIEM/对象存储	生命周期策略

九十四、营销素材审批表 (带签核)

素材编号	渠道	关键信息	风险用语自检	合规复核	法务复核	最终批准
MKT-2025-001	网站Banner	费率0.x%、Safeguarding说明	已剔除“存款/保险”	CCO签名	Legal签名	CMO签名

九十五、供应商分级与评分卡 (VDDQ打分)

维度	权重	指标	满分	备注
合规资质	25%	ISO/审计报告/监管历史	100	
安全控制	25%	加密/访问/日志/事件	100	
运营韧性	20%	可用性/备援/RTO/RPO	100	
合同条款	15%	审计权/退出/SLA	100	
价格与服务	15%	成本/响应/SLA履约	100	
分级: ≥85 A级 (关键供应商可用), 70-84 B级 (限用途), <70 需整改或更换。				

九十六、企业风险评估方法 (评分模型简版)

风险评分 = 影响 (1-5) × 概率 (1-5) × 控制成熟度系数 (0.6-1.2)

- 影响维度: 客户资金、合规处罚、声誉、经营中断。
 - 概率维度: 历史事件、行业情报、技术脆弱性、外包依赖度。
 - 成熟度系数: 内控/审计/自动化水平；外包为+0.1 风险加权。
- 阈值: ≥16 红色、9-15 橙色、4-8 黄色、≤3 绿色；红/橙需董事会跟踪。

九十七、客户适当性与限额（如开展特定高风险功能）

- **适当性问卷：**资金来源稳定性、经验与风险承受力、用途与频率。
- **限额联动：**适当性等级与KYC层级绑定，异常提升需二线审批与冷静期。

九十八、合同“合规优先”条款（摘录，可入框架协议）

“在不影响双方其他权利义务的前提下，如本协议与适用法律、监管机构的指导/要求或公司内部政策存在冲突，以监管要求及公司合规政策为先，供应商应予以无条件配合。”

九十九、项目收尾与复盘模板（Post-Mortem）

- **事件/项目概述：**范围、目标、时间线。
- **指标达成：**KPI/KRI 对比、偏差分析。
- **问题与根因：**技术/流程/组织/外包。
- **改进计划：**责任人、时限、验收标准。
- **知识沉淀：**文件与脚本入库、培训更新。

注：本文中的文档/附件原件可向仁港永胜索取电子档]

提示：以上是仁港永胜对保加利亚电子货币机构（EMI）牌照申请的详细内容讲解，旨在帮助您更加清晰地理解相关流程与监管要求，更好地开展未来的申请与合规管理工作。选择一间专业专注的合规服务商协助牌照申请及后续维护及合规指导尤为重要，在此推荐选择仁港永胜。

如需进一步协助，包括申请/收购、合规指导及后续维护服务，请随时联系仁港永胜 www.jrp-hk.com 手机:15920002080
(深圳/微信同号) 852-92984213 (Hongkong/WhatsApp) 获取帮助，以确保业务合法合规！