

信任白皮书

2026

目录

CEO 致辞	01
引言	
文件定位与适用范围	04
信任体系的结构性支柱	05
风控与风险治理体系	
风险治理理念	08
风险管理框架总览	09
风险识别与量化：以数据驱动的风险测量体系	10
业务线风控机制：以场景化控制替代“一刀切”规则	11
实时监控与事件响应：从预警到处置的系统化流程	12
风险报告与持续透明度	13
合规和监管基础	
全球牌照体系	16
AML/KYC 信任框架	20

安全架构与资产保护体系	
系统安全架构	28
密钥管理与资产保护机制	33
安全事件监控与防御体系	35
外部安全评估与第三方验证	37
员工安全培训与安全文化	39
安全作为信任的基石	40
审计与鉴证体系	
ISO 国际标准审计体系	43
SOC 第三方独立鉴证	44
年度财务审计	45
内部审计机制	46
业务线级审计与透明度验证	47
多层审计体系	49
结语	51
术语表	53

CEO致辞

在数字资产行业，信任从来不是由一次承诺或一次审计建立的。它更多来自长期、持续的制度选择——在市场波动与不确定性面前，是否能够坚持清晰的风险边界；在增长压力之下，是否仍然遵循既定的规则；在问题出现时，是否以清晰、可追溯的方式对外沟通。

过去几年，行业经历了多轮深刻调整。这些过程反复提醒我们，技术本身并不能自动带来信任。真正影响结果的，往往是治理结构是否稳健、风险管理是否具备前瞻性，以及信息披露机制是否能够经受住时间与周期的检验。

BIT¹自成立以来，在业务发展与战略选择中始终高度重视风险管理与基础设施能力。我们始终认为，数字资产并不意味着可以降低对安全、合规与透明度的要求；相反，在一个高度不确定的行业中，这些要求只会更加重要。

基于这一判断，BIT 在业务发展过程中持续坚持以下原则：

第一，安全是系统与资产运行的前提条件，而非附加选项；

第二，合规是业务边界的起点，而不是事后补充；

第三，透明意味着对关键治理与控制安排进行清晰披露；

第四，可验证性要求所有重要结论能够经受第三方与时间的检验。

¹ BIT 于 2026 年 3 月完成品牌更名，在此之前以 Matrixport 名称开展业务。除非另有明确说明，本文所述内容均追溯适用于品牌更名前的 Matrixport。

围绕上述原则，BIT 已在合规牌照、托管架构等关键基础设施层面形成持续运行的制度安排。在信息披露层面，我们坚持以事实为基础、以责任为导向，并在适用法律与合规框架下，通过官方渠道对重要事项进行说明，确保相关信息具备清晰性与可追溯性。

本《信任白皮书》并非对未来的承诺清单，而是对 BIT 当前已经建立并运行的制度、流程与第三方验证安排的系统性呈现。所有内容均基于可公开范围内的事实，旨在为机构客户、监管机构及合作伙伴提供可理解、可参考、可核验的尽职调查基础。

我们并不认为信任可以被快速建立，但认为它可以通过持续、可验证的方式被证明。这也是 BIT 选择以制度化方式，对外披露自身信任基础的原因。



John Ge

联合创始人兼首席执行官, BIT



引言

在数字资产与技术驱动的金融服务环境中，信任相关安排通常涉及安全、合规、透明度与可验证性等多重制度与技术要素，需要在制度层面进行系统性理解与评估。随着市场结构、监管环境及业务复杂度的不断演进，单一承诺、单次审计或孤立的技术方案，已难以满足机构级业务对稳定性与可核查性的要求。

本《信任白皮书》以安全、合规、透明度与可验证性作为分析框架，对 BIT 当前已建立并运行的相关制度、流程及第三方验证安排进行结构化说明。内容涵盖数字资产托管与安全架构、风险治理与合规体系，以及审计与鉴证机制等关键领域，重点聚焦于治理结构、控制环境与验证机制的设计与运行方式，旨在为机构客户、监管机构及生态合作伙伴提供可理解、可对照、可核验的尽职调查参考。

一、文件定位与适用范围

本白皮书并非对单一产品或个别能力的展示，也不构成对任何结果的保证或前瞻性承诺，而是对 BIT 整体信任相关基础设施的结构化呈现。所有内容均基于当前可公开范围内已落地并持续运行的制度、流程与第三方验证安排，亦不等同于对风险的转移或责任的单方面承担。

二、信任体系的结构性支柱

从整体结构上看，BIT 的信任体系围绕以下三个相互支撑的层级构建：

1. 合规与监管基础

通过多司法辖区的牌照与注册安排、AML/KYC 合规框架及持续的合规治理，明确法律边界与监管适用范围，为业务运营提供监管可验证性基础。

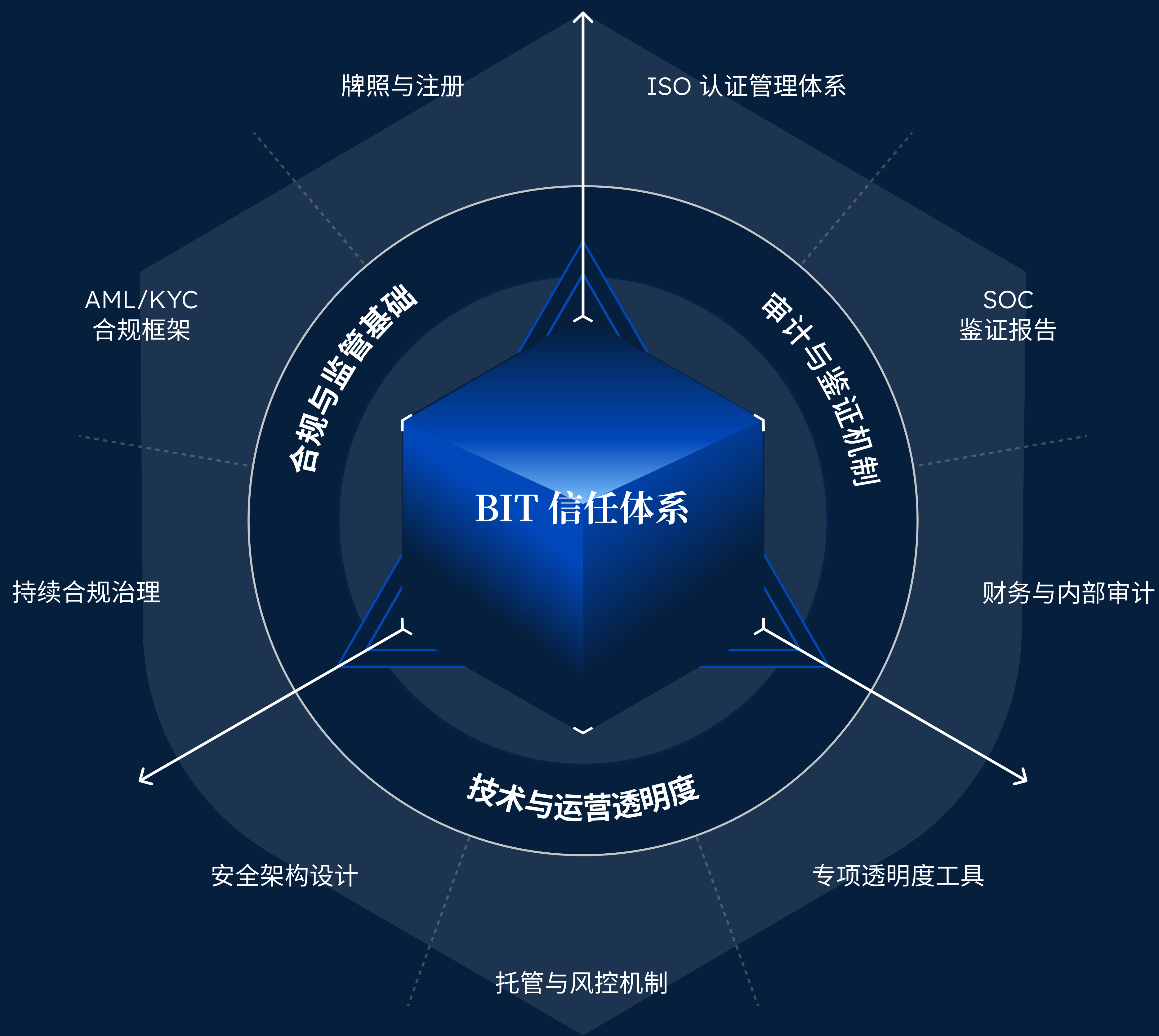
2. 独立审计与鉴证机制

通过 ISO 管理体系、SOC 独立鉴证、年度财务审计及内部审计安排，构建多层次、互补型的第三方验证结构，支持对关键控制环境的独立评估，并避免对单一审计或认证的依赖。

3. 技术与运营透明度

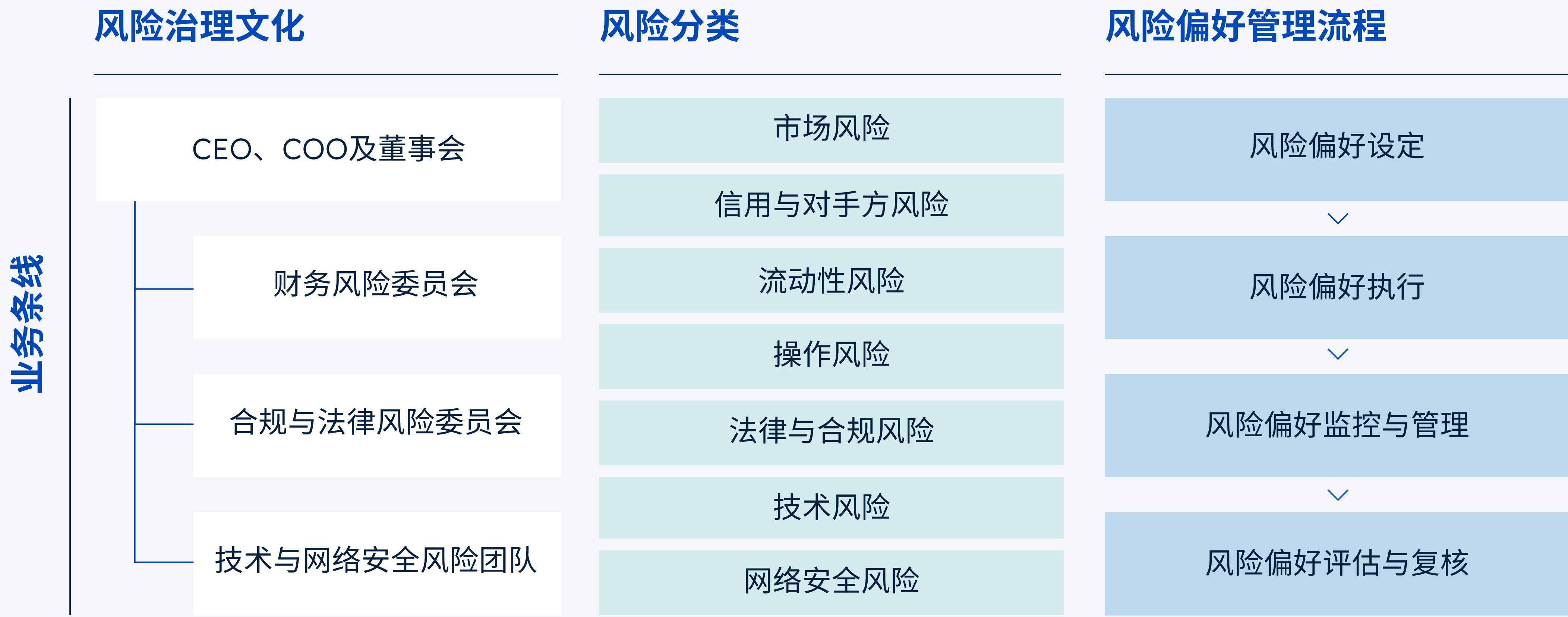
通过安全架构设计、风险控制系统、资产托管机制及特定业务场景下的透明度工具，提升关键运行与控制安排的可解释性与可验证性。

信任体系三大支柱总览





风控与风险治理体系



该图概述了 BIT 的风险管理与治理框架，展示治理机构、风险类别以及风险偏好从设定、实施到监控与审查的完整管理流程。

一、风险治理理念

在数字资产相关的金融服务环境中，风险并非异常状态，而是业务运行的常态背景。BIT 将风险管理视为一项制度性能力，并通过《风控与风险治理体系》加以实施，而非将其作为事后控制工具，其核心目标是在业务创新、资本效率与客户保护之间建立长期可持续的平衡。

BIT 的风险治理体系以清晰的风险分类、明确的风险偏好与严格的组织治理结构为基础，覆盖公司在各类业务场景中所面临的关键风险类型，包括：市场风险、信用风险、操作风险、流动性风险、法律与合规风险，以及技术与网络安全风险。在操作风险管理方面，BIT 通过内部控制框架、标准化操作流程（SOP）、独立保障机制（包括 SOC 审计）以及持续监测机制进行综合缓释。

在治理层面，BIT 设有由董事会任命的风控委员会，由风险政策负责人及业务负责人组成，对业务活动以及资本与流动性规划提供风险监督。管理层通过明确风险偏好，确保所有风险承担行为与公司整体战略保持一致，并在组织内部持续强化风险文化。

二、风险管理框架总览

BIT 的风险管理并非集中于单一控制点，而是嵌入在业务全生命周期中，从交易前评估、交易中监控到交易后处置，形成闭环管理机制。



三、风险识别与量化：以数据驱动的风险测量体系

在风险识别与量化层面，BIT 采用多维度、可量化的测量方法，对不同风险类型进行持续评估：

市场风险	信用与对手方风险	资本与流动性风险
通过组合层面的 VaR（ 99% 置 信 区 间）、压力测试、流 动 性 风 险（ 买 卖 价 差）及集中度风险监 测进行管理。	实施超额抵押、尽职 调查流程、信用额度 管理及产品与对手方 层面的风险分散。	通过资产负债管理与 压力测试，确保充足 的资本与流动性缓 冲。

这些风险指标并非孤立存在，而是被持续输入至内部风险引擎，用于支持实时监控与决策。

四、业务线风控机制：以场景化控制替代“一刀切”规则

BIT 在不同业务线中实施差异化、场景化的风险控制机制。

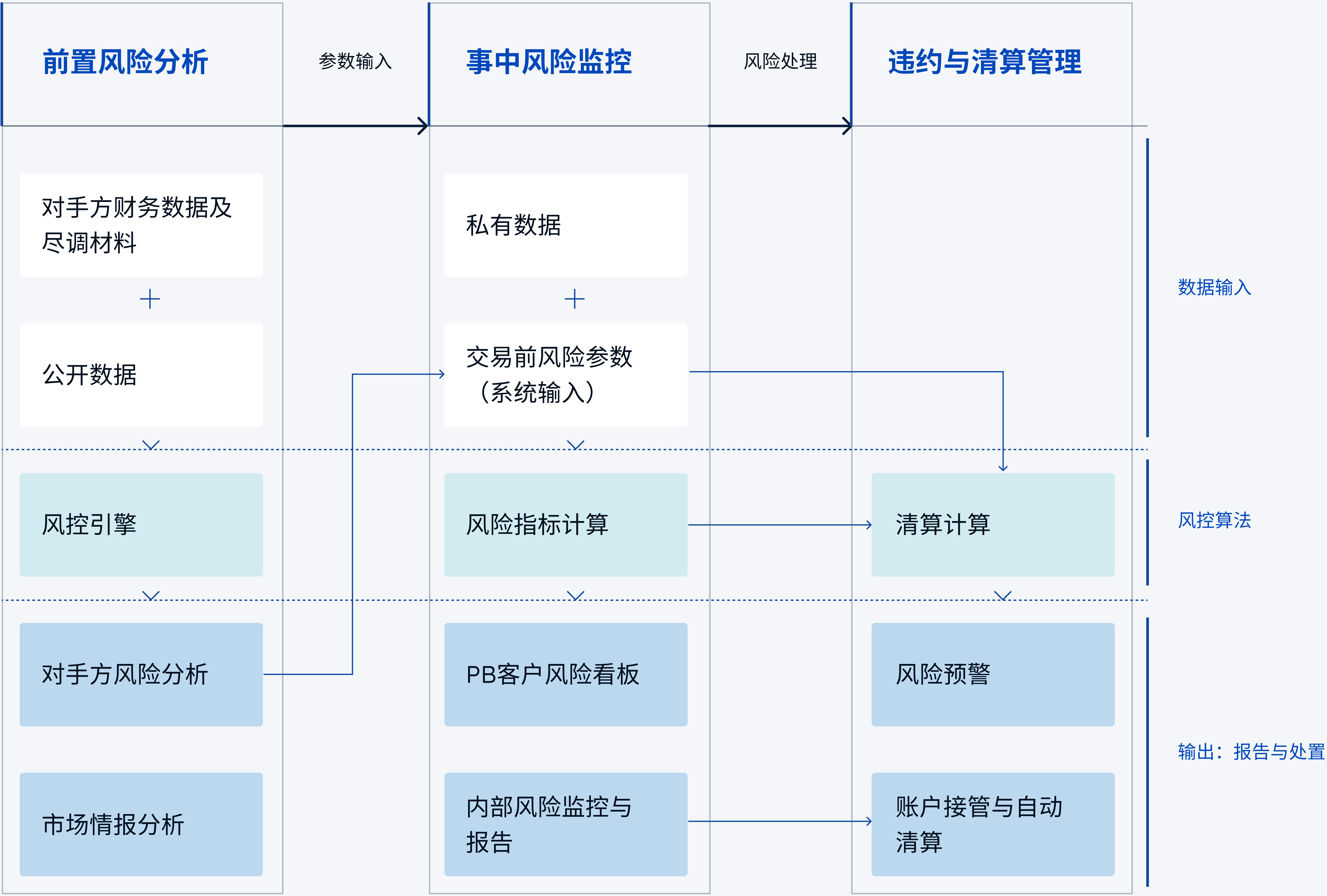
以配资与抵押类业务为例，风险控制从交易前即开始：客户需完成尽职调查问卷，涵盖客户背景、交易策略、既有风险控制措施及历史业绩表现。相关信息将结合分析工具进行初步评估，并由风控团队与客户进行尽职调查沟通，在内部讨论后，为该笔业务设定定制化风险参数，包括杠杆比例、净敞口及最大回撤等。业务仅在双方确认参数后方可启动。

对于抵押借贷业务，BIT 设有内部的代币与对手方评级机制，仅接受达到既定风险等级的资产与对手方，并基于风险调整分析设计相应的信用额度与条款。

五、实时监控与事件响应：从预警到处置的系统化流程

在交易执行阶段，BIT 的风险系统提供实时风险展示、自动化预警与分析能力。当风险参数出现偏离或接近既定阈值时，系统将触发相应告警，并按照既定流程进行升级处理。相关团队依据标准操作流程（SOP）开展处置，以管理潜在操作事件并控制操作风险，并根据具体情况采取分级响应措施。

风险管理流程



该图用于展示从交易前风险分析、交易中监控到违约与清算管理的完整链路。

六、风险报告与持续透明度

在信息披露与内部监督层面，BIT 设有周期性风险报告机制。风险报告通常按周生成，涵盖市场波动情况、潜在清算价格区间及压力测试结果。在市场波动显著加剧时，报告频率将相应提高，以支持管理层与业务团队的及时决策。



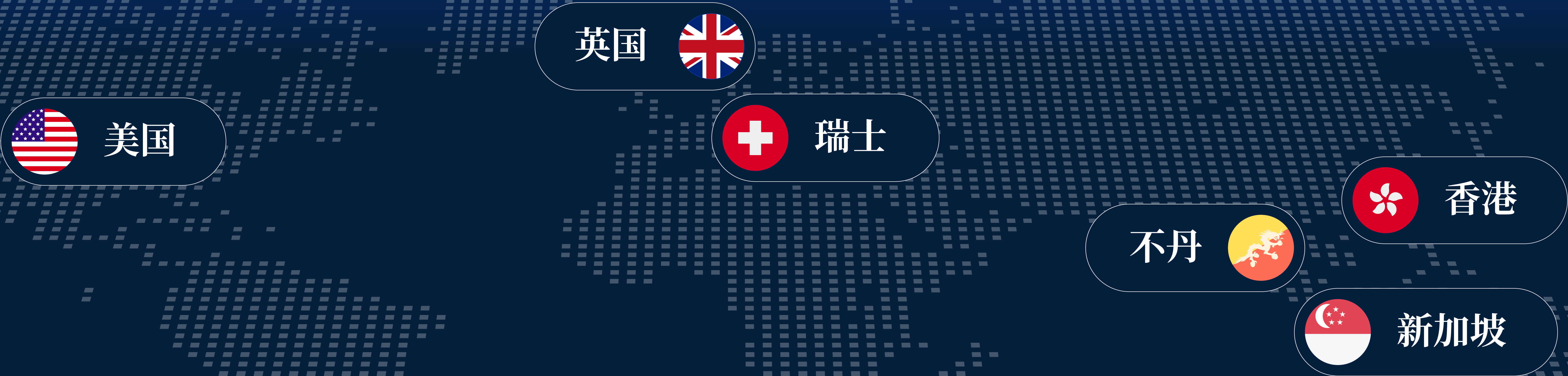
合规和监管基础

BIT 的全球合规体系建立在经监管验证的法律实体结构、跨司法辖区的牌照布局、合规标准以及系统化的 AML/KYC 框架之上。该体系在适用法律与许可范围内，覆盖托管、资产管理、数字资产相关服务、贵金属处理、支付及金融中介等关键业务领域，用于披露集团层面的合规安排与监管基础。

一、全球牌照体系

BIT 通过在多个司法辖区取得相应监管许可，为其托管、资产管理、数字资产相关服务、贵金属处理、支付及金融中介等业务建立合规法律基础。以下信息仅涉及已正式取得、且可公开披露的牌照与注册资质，并仅适用于对应法律实体、司法辖区及许可范围内的业务活动。

司法辖区	监管实体	发牌机构
 香港	Matrix Trust Company Limited	牌照类型：TCSP（Trust or Company Service Provider） 发牌机构：公司注册处（Companies Registry, CR）
	Matrix Port Technologies (Hong Kong) Limited	牌照类型：放债人牌照（Money Lender License） 发牌机构：放债人牌照法庭（Licensing Court）



各司法辖区的监管与持牌情况

司法辖区	监管实体	发牌机构
 香港	Flying Hippo (Custody) Limited	牌照类型： TCSP 发牌机构：公司注册处
	Matrix Infinitus (Hong Kong) Limited	牌照类型： DPMS Category A (Dealer in Precious Metals and Stones) 注册/反洗钱监管机构：香港海关 (Customs and Excise Department, C&ED)
 不丹	Matrix Gelephu Pte Ltd	牌照类型： Financial Services License 发牌/监管机构：格勒普金融服务办公室 (Gelephu Financial Services Office)，格勒普市 (Gelephu Mindfulness City, GMC)
	Matrix Bhutan Pte Ltd	牌照类型： Financial Services License 发牌/监管机构：格勒普金融服务办公室 (Gelephu Financial Services Office)，格勒普市 (Gelephu Mindfulness City, GMC)
 新加坡	Fly Wing Technologies Pte. Ltd.	牌照类型： Major Payment Institution – Digital Payment Token Service 监管机构：新加坡金融管理局 (Monetary Authority of Singapore, MAS)

司法辖区	监管实体	发牌机构
 瑞士	ChainTech AG	牌照类型：自律组织成员 (SRO) 监管机构：金融服务标准协会 (VQF)
	Matrixport Asset Management AG	牌照类型：Managers of Collective Assets 监管机构：瑞士金融市场监管局 (FINMA)
 英国	Matrixport Advisors Limited	监管状态：指定代表 (Appointed Representative, AR) 监管机构：英国金融行为监管局 (FCA)
 美国	Matrixport Inc	牌照类型： Money Services Business (MSB)
		注册机构：美国金融犯罪执法网络 (Financial Crimes Enforcement Network, FinCEN)

监管状态免责声明

上述所列牌照、注册及监管状态，均由相关监管机构就特定受监管活动授予或维护。该等状态不构成任何监管机构对本集团或其服务的认可、批准或推荐，亦不代表本集团获授权在相关牌照范围或司法辖区之外开展任何活动。

二、AML/KYC 信任框架

在复杂且跨多个司法辖区的监管环境下开展业务，BIT 的控制体系与其业务所在地区适用的法律法规、监管要求及国际标准保持一致。BIT 致力于防范洗钱（ML）和恐怖融资（TF）活动，并遵守适用的反洗钱（AML）、反恐怖融资（CFT）及相关制裁制度。这些义务连同相关监管指引，共同构成了 BIT 反洗钱/反恐怖融资（AML/CFT）计划的基础。

BIT 的 AML/CFT 框架基于风险为本的方法，并适用于其开展业务的所有司法管辖区。该框架通过建立治理结构、政策体系、操作流程及内部控制机制，以识别、评估并降低金融犯罪风险，包括与防扩散融资及制裁合规相关的风险。

1. 反洗钱/打击资助恐怖主义政策

反洗钱/打击资助恐怖主义政策规定了BIT 必须遵守的基本标准。这包括:

- 1.1 书面政策、程序和内部控制，以确保遵守适用的反洗钱法律和法规；
- 1.2 职责分工: 任命一位负责反洗钱计划的专合规官 (MLRO) 以及指定的合规官，负责日常合规工作的有效执行；
- 1.3 治理框架: 制定健全的治理框架，确保高层管理人员对反洗钱计划进行监督；
- 1.4 客户尽职调查 (CDD): 对客户、授权代表以及（如适用）受益人的身份进行识别和核实；在开户时获取账户用途、预期交易活动、资金来源，以及在适当情况下的财富来源信息；
- 1.5 风险评估: 客户、产品、服务、交易、交付渠道及地域风险评估；
- 1.6 强化尽职调查 (EDD): 适用于高风险关系（例如：政治公众人物（PEP）、高风险行业/司法管辖区、负面媒体报道、以及来自 KYT/交易监控(TM) 的高风险因素）；

- 1.7 制裁合规：筛查与控制符合相关制裁制度要求，包括与防扩散融资相关的义务；
- 1.8 上报与通报：内部上报流程及并及时向相关监管部门提交可疑交易/活动报告；
- 1.9 持续尽职调查：定期审查（PRs），基于风险等级及触发事件执行；
- 1.10 培训: 所有员工在入职时及每年必须参加反洗钱/反恐怖融资（AML/CFT）及制裁培训；
- 1.11 独立审查/测试：定期、独立审计/评估计划的有效性；
- 1.12 记录保存：依照适用法律法规要求保留记录；
- 1.13 汇款信息传递规定（适用时）：传递必要的汇款人/收款人信息。



2. 严禁的账户用途、客户，及业务类型

2.1 禁止建立的业务关系

BIT 不会在其合规框架下，与存在以下高风险或受限情形的相关方建立或维持业务关系：

- 2.1.1 受 BIT 持牌所在地相关监管机构制裁的个人或实体，或列入国际制裁名单的个人或实体（例如：联合国安全理事会、美国海外资产控制办公室（OFAC）、欧盟、英国财政部及新加坡金融管理局等制裁名单）
- 2.1.2 已知或有合理理由推定参与恐怖融资或严重犯罪活动，或属于/支持此类组织的个人或企业
- 2.1.3 空壳银行，即在其注册地没有实际办公场所的银行
- 2.1.4 使用虚假姓名或化名进行经营的客户
- 2.1.5 从事武器、军火制造或军火贸易的客户
- 2.1.6 从事烟草贸易的客户
- 2.1.7 从事成人娱乐行业的客户
- 2.1.8 从事赌场、赌博或类似行业的客户



2.2 严禁的资产种类

BIT 严禁任何经其客户尽职调查（KYC）或交易监测（KYT）识别为来源于犯罪活动、涉及恐怖主义融资，或与犯罪组织相关的资金在其体系内流转。对于涉及上述情形的相关方，BIT 不会建立或继续任何业务关系，无论相关违法或犯罪行为发生于何种司法辖区。

2.3 限制地区和国家

BIT 在其官方网站上维护并定期更新受限制司法辖区清单。根据其反洗钱与反恐融资（AML/CFT）计划，BIT 不会与来自受到全面制裁或存在严重 AML/CFT 缺陷的司法辖区的相关方建立业务关系。

3. BIT 的 KYT

BIT 严禁其体系被用于任何非法活动，包括但不限于洗钱、恐怖主义融资或其他违法交易行为。BIT 通过持续性的交易监测与了解交易（KYT）机制，对相关交易活动进行实时与持续监控。如监测过程中识别出涉嫌非法或可疑活动，BIT 可根据适用法律、监管要求及合同约定，采取包括但不限于以下措施：拒绝或退回相关资金、发出信息请求（RFI）、冻结账户、暂停或终止相关账户或业务关系，以及在适用法律和《条款与条件》允许的情况下，向有关主管机关报告可疑活动。BIT 保留依据适用法律及合同约定所享有的一切权利。

4. 禁止活动

在 BIT 的合规框架下，以下活动被明确禁止，包括但不限于：

- 4.1 可能违反或导致 BIT 违反适用经济制裁的交易，包括但不限于由美国财政部海外资产控制办公室（OFAC）、美国国务院、联合国安全理事会、欧盟成员国、英国财政部及新加坡金融管理局实施或执行的制裁。这并非详尽列表，也包括 BIT 运营所在司法管辖区的其他适用制裁计划措施；
- 4.2 与非法活动相关的交易，包括欺诈、诈骗、被盗资金、勒索软件及恶意软件相关交易；
- 4.3 涉及混币服务/加密货币搅拌机、暗网市场或其他混淆服务的交易；
- 4.4 与赌场、赌博或类似行业相关的交易；
- 4.5 交易模式异常、罕见或无合理商业解释的交易。

安全架构与资产保护体系

在数字资产与技术驱动的金融服务环境中，安全并非附加能力，而是信任得以建立的基础条件。BIT 从成立第一天起就将“安全优先”确立为公司级原则，通过端到端的安全防护设计、全球分布式基础设施及与业务场景相匹配的安全工程能力，构建了覆盖资产、系统、业务、人员与流程的安全体系，以支持平台的长期安全稳健运行。

一、系统安全架构

BIT 的系统安全架构以零信任（Zero Trust）为核心，采用纵深防御（Defense-in-Depth）分层控制，并贯彻最小攻击面（attack surface minimization）与最小权限原则，从管理、流程与技术三个层面形成相互支撑的安全闭环。

以 Cactus Custody 为例，以下参考架构图用于说明在机构级托管与数字资产管理场景中，安全控制、权限治理、审计可追溯性与风险防控机制如何被系统性地嵌入核心架构之中。

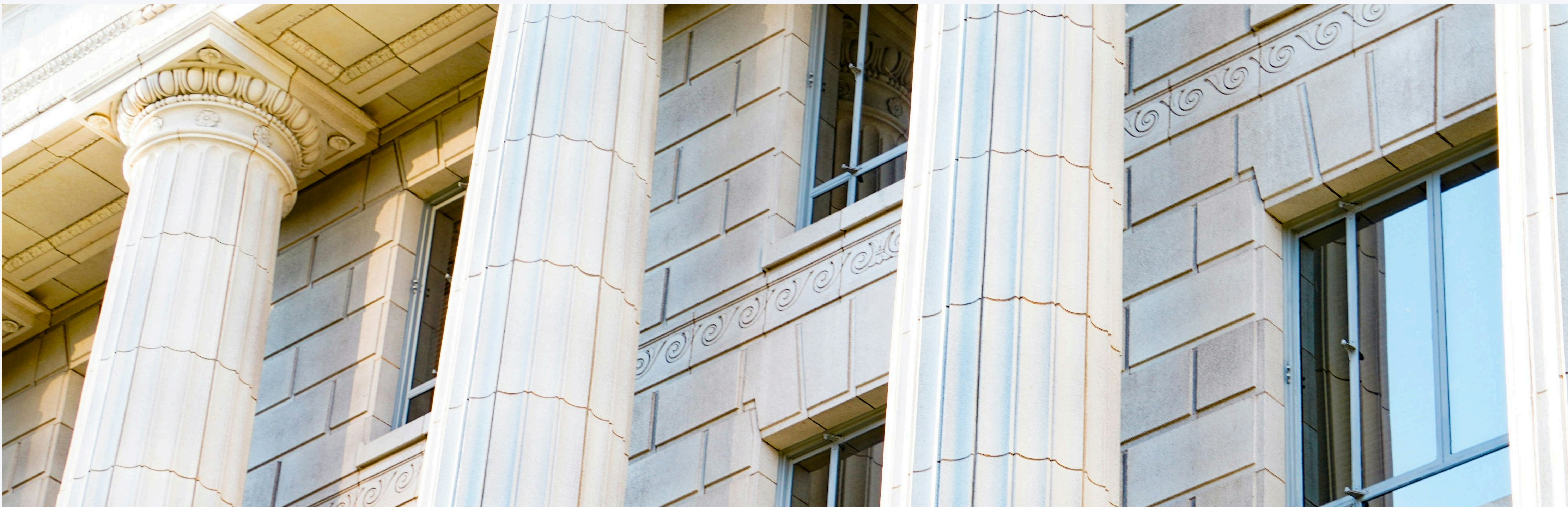
机构级数字资产托管安全架构



1. 管理层面：制度化的安全治理

有效的安全始于治理。在数字资产相关业务中，若缺乏明确的权责归属、规范化的决策机制以及可执行的问责体系，单一的技术控制措施本身并不足以支撑稳健的安全管理。

BIT 通过建立正式的安全治理框架，将安全要求制度化嵌入组织运行之中，明确组织内部的授权边界、责任分工及风险升级路径。通过将安全嵌入管理结构与运营流程，BIT 确保风险得到持续监督，关键决策接受独立审视，且安全标准能够在不同产品、系统及各类业务活动中保持一致适用。



1.1 安全责任制度化

安全治理由具备金融与网络安全背景的管理层及专业团队共同承担。公司通过制度化的安全责任分配与配套管理提醒机制，明确安全职责的落实路径与内部问责边界。

1.2 安全一票否决权

安全团队具备一票否决权。当发现产品方案、需求、架构或上线变更存在重大安全风险，或不符合公司安全基线和合规要求时，安全团队有权直接叫停相关活动，并要求整改与复核通过后方可继续推进或发布。

1.3 最小权限与分权原则

遵照零信任原则，员工仅被授予履行其职责所必需的系统访问权限，并动态调整，以降低权限滥用与内部风险。

1.4 四眼原则

所有关键操作均需至少两名授权人员共同参与，以形成内部制衡机制，降低单点失误与内部操作风险。该原则适用于包括资产转移在内的各类高风险或关键操作场景，如涉及账户安全、权限变更、交易指令生成与审核等环节。通过多方参与与相互制衡，进一步强化操作安全性与整体风险控制能力。

2. 流程层面：安全嵌入业务全生命周期

2.1 安全软件开发生命周期（S-SDLC）

安全要求贯穿系统设计、开发、测试、部署与运维阶段，并作为与功能和性能并列的基础质量考量因素。

2.2 持续监控与响应机制

参考 Identify-Protect-Detect-Respond-Recover（IPDRR）安全框架，对系统与业务运行状态进行持续监测与响应。

2.3 威胁情报与风险监测

持续关注潜在威胁来源与新型攻击手法，及时识别并响应可能影响平台稳定性与资产安全的风险。

3. 技术层面：工程化的安全防护能力

3.1 行业级安全工具与解决方案

采用经过验证的安全技术，覆盖身份管理、访问控制、入侵防御与异常行为检测。

3.2 全链路安全规范

制定并执行覆盖系统设计、编码、测试与运维的统一安全标准，在组织范围内强制落实。

3.3 安全最佳实践沉淀

通过对安全工程实践的持续复盘与标准化沉淀，支持安全控制在不同系统与业务场景中的一致性应用。

二、密钥管理与资产保护机制

数字资产安全并不局限于软件与密码学层面，而是延伸至物理世界。设施环境、硬件基础条件及访问控制构成整体威胁面的关键组成部分，尤其是在冷钱包基础设施场景中更为重要。BIT 通过实施严格的物理与环境控制措施，保护关键系统与敏感信息，确保核心资产能够有效抵御未经授权的访问、环境风险以及运营中断等威胁：

1. 冷热钱包分离与动态资产管理

大部分资产存放于冷钱包；
热钱包仅用于满足必要的日常流动性需求；
该策略有助于降低网络攻击暴露面，减少在线资产风险。

2. 冷钱包环境与物理安全

冷钱包存储地址严格保密；
采用隔离网络与受控环境；
配备多重物理安保措施；
上述安排旨在降低冷钱包相关操作在物理层面与环境层面的风险暴露。

3. 私钥安全与硬件保护

私钥存储于 FIPS 140-3 Level 3 级别的硬件安全模块（HSM）；
私钥在任何情况下均不可明文访问或导出；
HSM 部署于具备严格物理访问控制与环境安全要求的受控基础设施环境中，其安全标准与金融行业及关键基础设施的通行实践保持一致。
该等级的 HSM 广泛应用于对密钥安全要求极高的金融与基础设施场景。

三、安全事件监控与防御体系

1. 强制多重身份验证（Multi-Factor Authentication）

账户登录与关键操作均需通过多重身份验证机制完成；

支持 UKey、Passkey、身份验证器等方式；

所有关键操作（如提币、修改安全设置）均需二次验证；

此外，用户可选择使用生物识别（指纹 / 人脸）简化验证流程，在不降低安全性的前提下提升体验。

2. 24 小时动态风控与异常预警

现代数字资产平台持续运行，长期暴露于不断演变的欺诈风险与账户接管风险之中。有效的安全防护因此不仅依赖于事后审查或静态规则，而有赖于对用户行为与交易活动的实时可见性，并结合能够对异常情况即时响应的自动化控制机制。

BIT 建立持续的风险监测与动态预警机制，对可疑行为在其发生过程中进行识别与分析，从而支持及时干预、分层验证及用户通知，降低未经授权访问或资产损失的发生概率：

- 实时监测账户行为；
- 自动识别异常登录、异常设备、异常提币等高风险行为；
- 根据风险等级触发预警、延迟或人工审核；
- 通过邮件等方式提醒用户。

3. 高等级加密与访问控制

数据保密性、系统完整性与运行隔离性构成防止未经授权活动、并限制潜在安全事件影响范围的基础要素。BIT 在采用高强度加密标准的同时，实施精细化的访问控制机制，确保敏感信息持续受保护、权限范围受到严格限定、系统边界得到有效落实，从而构成应对外部威胁与内部滥用风险的核心防御层：

- BIT 全站服务采用保障数据传输安全的行业通用标准 HTTPS；
- 敏感信息使用高强度加密算法存储；
- 细粒度身份认证与权限控制；
- 不同角色、用户与系统模块之间严格隔离；
- 提现白名单机制降低误操作与攻击风险。

4. 防钓鱼与用户安全保护机制

- **官方渠道验证:** 用户可通过安全中心核验官方沟通渠道、员工身份及公告信息，从而降低与冒充人员或欺诈性联系互动的风险。
- **全平台钓鱼监测:** BIT 持续对钓鱼网站、仿冒应用程序及品牌冒用行为开展监测。一旦发现欺诈性站点，将主动启动下架流程并向用户发出相应安全提醒。
- **漏洞与钓鱼情报激励计划:** BIT 设立正式的漏洞激励计划，鼓励负责任地披露安全漏洞。经核实的安全问题可获得最高 100,000 USD 的奖励，通过社区参与持续提升平台整体安全韧性。
- **安全事件与可疑活动上报：**与平台相关的安全问题、漏洞报告或可疑活动，可通过指定的安全事件上报渠道进行反馈，为安全研究人员及用户提供直达 BIT 安全响应中心的沟通路径。

四、外部安全评估与第三方验证

在数字资产托管领域，内部控制体系需要通过符合国际公认标准的独立验证予以强化。外部认证与鉴证报告能够对治理结构、安全控制、隐私保护及运营质量框架提供客观验证，为客户及相关方提供衡量机构成熟度的依据。基于此，BIT 持续对标国际通行标准，并对关键系统与流程开展定期的第三方审计与鉴证，确保安全实践不仅在设计层面具备有效性，也能够在实际运行环境中持续接受测试与验证。

秉持对既有国际标准与最佳实践的持续遵循，BIT 旗下的机构级数字托管品牌 Cactus Custody 就其安全与管理体系，已取得以下国际认可的认证及独立鉴证报告：

1. SOC 1 Type 2 / SOC 2 Type 2

由第三方对内部控制与安全控制有效性进行独立鉴证。



2. ISO/IEC 27001:2022

信息安全管理体系，确保资产机密性、安全性与可用性。



3. ISO/IEC 27701:2019

隐私信息管理体系，符合数据保护与隐私法规要求。

4. ISO 9001:2015

质量管理体系，体现持续改进能力。

上述评估共同构成可验证的外部安全信任基础。

CONTRACT
AGREEMENT

五、员工安全培训与安全文化

仅依赖技术与控制措施，无法在缺乏具备安全意识且承担明确责任的人员参与下，充分保障数字资产安全。人员行为仍是防范安全事件的关键因素，尤其是在涉及高价值资产的运行环境中更为重要。基于此，BIT 通过体系化的培训机制、持续的安全意识建设以及明确的职责划分，培育以安全为先的组织文化，确保安全原则被嵌入日常运营流程，并在组织内部落实至个人层面的责任与问责。

“安全第一”是 BIT 的核心文化之一，并贯穿于组织全生命周期：

- 招聘阶段进行背景调查
- 新员工必须完成安全培训与考试
- 定期进行钓鱼演练
- 年度全员网络安全考试
- 针对不同岗位定制差异化安全要求
- 严格的网络安全奖惩制度
- 持续强化员工对安全事件与风险的识别能力

通过制度、培训与实践的结合，确保安全意识从“流程要求”转化为“组织习惯”。

六、安全作为信任的基石

BIT 的安全体系并非由单一技术或孤立控制构成，而是一套贯穿治理、流程与工程实践的制度化信任基础设施。通过持续演进的安全架构、嵌入式的风险控制机制以及可被独立验证的外部评估，安全能力被系统性地融入平台的日常运营与长期发展之中。

该安全体系与合规与审计安排共同构成 BIT 信任框架的重要支柱，使其不仅能够应对当前的安全与风险挑战，也具备在业务规模、技术环境与监管要求不断变化的背景下，持续维护资产安全与客户信任的能力。



审计与鉴证体系

BIT 的机构级审计与鉴证框架用于整合不同类型、相互独立的审计与鉴证机制，对外披露与托管服务安全性、财务信息可靠性及关键控制环境相关的可验证信息，以支持机构客户、监管机构及生态合作伙伴的尽职调查需求，而非依赖单一审计或认证作为信任基础。

整体审计与鉴证体系由以下四个相互补充的结构化层级构成：

- 国际标准化体系审计（ISO）
- 第三方独立鉴证（SOC）
- 年度财务审计
- 内部审计

注

所有 ISO 与 SOC 审计仅覆盖 Cactus Custody，不构成对 BIT 集团其他实体或业务线的统一覆盖。

一、ISO 国际标准审计体系

在当前可公开披露的范围内，Cactus Custody 的托管服务运营体系已接受多项国际通行的 ISO 管理体系标准的第三方审计与认证。相关审计范围、控制目标及适用性均以经批准的**适用性声明文件**（Statement of Applicability, SoA）为准。

ISO 管理体系审计用于验证 Cactus Custody 在数字资产托管服务的系统设计、开发、交付与运营过程中，已建立并运行符合相关国际标准要求的管理与控制机制，构成其外部安全与管理能力验证体系的重要组成部分。

在可公开范围内，已通过审计并持续维护的主要标准包括：



1. ISO 9001 – 质量管理体系（Quality Management System）

覆盖数字资产托管服务的设计、开发、提供与运营流程。

2. ISO 27001 – 信息安全管理 体系（Information Security Management System）

覆盖用于向客户提供数字资产托管服务的信息安全管理体系，审计范围基于已批准的适用性声明。

3. ISO 27701 – 隐私信息管理体系（Privacy Information Management System）

在 ISO 27001 的基础上扩展隐私管理要求，覆盖内部运营中的数据控制者角色及客户信息处理相关的合规责任。

ISO 审计频率为每年一次，具体审计报告内容、详细控制清单及审计结论仅在适用的合规与保密框架下提供，不作为公开披露内容。



二、SOC 第三方独立鉴证（AICPA Attestation Reports）

在 ISO 管理体系之外，Cactus Custody 亦接受 SOC 鉴证，用于对其托管服务相关控制环境进行第三方独立评估。

目前，Cactus Custody 已取得以下 SOC 鉴证报告：



1. SOC 1 Type 2

针对与用户单位财务报告相关的内部控制，在一定期间内对控制设计的合理性及运行有效性进行鉴证。

2. SOC 2 Type 2

围绕托管服务相关的 IT 环境，对安全性、可用性与机密性等信任服务准则下的控制进行鉴证。

相关 SOC 鉴证均由国际认可的独立会计师事务所执行，用于向机构客户与合作方提供关于其控制环境成熟度与可持续性的独立验证。

三、年度财务审计

在前述安排基础上，BIT 及其相关附属实体依据各自适用司法辖区的监管及法定要求，于每一财务年度开展独立的外部财务审计。年度财务审计的范围通常包括：

- 评估财务报表的准确性与完整性
- 评估关键财务控制的有效性
- 审查主要会计政策与适用会计准则的一致性

所有审计意见均由外部审计机构在符合适用审计准则的前提下，基于其专业判断独立形成并出具。

四、内部审计机制

在内部治理层面，BIT 建立内部审计相关安排，包括：

- 风险识别与评估
- 控制性测试
- 审计报告与沟通
- 整改跟进与优化提升

内部审计作为对外部审计与鉴证的补充层，支持持续改进并保持与国际标准体系的一致性。

五、业务线级审计与透明度验证

1. Cactus Custody

托管业务相关的审计与鉴证已纳入 ISO 管理体系与 SOC 鉴证框架之中，相关内容不再重复披露。



2. Matrixdock (RWA)

在现实世界资产（Real-World Asset, RWA）场景中，尤其是涉及贵金属等实物资产的代币化产品时，相关信任要求并不仅限于链上控制或智能合约本身，而是依赖于覆盖发行、托管及持续运营环节的结构化运营治理安排、信息披露机制与核验框架。

在 RWA 相关业务中，BIT 旗下 RWA 平台 Matrixdock 并不将信任建立在单一主体或单一技术组件之上，而是通过治理安排、技术控制及第三方参与所构成的多层保障机制，为资产透明度与可验证性提供支持。主要包括：

2.1 实物资产托管与信息披露安排

在涉及实物资产的 RWA 场景中，相关资产通常由具备相应资质的第三方托管机构进行保管。Matrixdock 依据既定的托管与信息披露框架，在约定范围内支持对资产托管状态、数量及相关属性的核查，相关信息基于托管机构及审计方所提供的报告与核验结果进行呈现。

2.2 链上透明度与可查询机制

Matrixdock 利用区块链基础设施的公开性与可审计特性，使代币的发行、流通及代币与底层资产之间的对应关系能够被独立查询与验证，从而为用户及合作方提供可审阅、可核查的技术基础。

2.3 第三方机构的参与与支持

RWA 场景中的信任依托多方参与形成，包括托管机构、审计机构及其他验证服务提供方的独立参与，有助于在链上与链下组件之间形成相对清晰的责任边界。

上述资产层面的透明度与可核查安排，与系统层面已建立的控制、审计与合规机制协同运作，用以回应链上与链下信任交汇所产生的特定验证需求。



六、多层审计体系

从整体架构来看，BIT 对外披露的审计与鉴证安排体现了一套多层级审计与鉴证框架，其总体设计遵循“三道防线”模型的基本原则。

第一层：运营与管理体系（ISO）

支持运营流程、数据治理与安全管理符合国际标准化要求。

第二层：独立控制验证（SOC/External Audit）

通过第三方鉴证与财务审计，对控制环境的设计与运行情况提供独立验证。

第三层：资产层面透明度与可核查机制（RWA/Matrixdock）

结合链下托管安排与链上可验证机制，为现实世界资产代币化相关场景提供补充性的透明度与可核查机制。

通过构建由国际标准化体系审计、第三方独立鉴证、年度财务审计及内部审计机制组成的多层审计与鉴证框架，BIT 旨在在不同业务与风险层面建立结构化、可验证且具备明确适用边界的信任基础。

该框架强调不同鉴证机制之间的相互独立与功能互补，避免将信任建立在单一审计或认证之上，并通过对披露范围与适用边界的明确界定，支持机构参与方、监管机构及生态合作伙伴开展基于事实的尽职评估。

在此基础上，系统级控制与资产层面透明度机制协同运作，使审计与鉴证不仅构成合规治理的重要组成部分，也成为平台长期稳健运行与持续治理能力的重要支撑。

结语

本《信任白皮书》围绕安全、合规、透明度与可验证性，对 BIT 当前已建立并持续运行的信任相关制度、治理结构、控制环境与第三方验证安排进行了系统性呈现。通过对风险治理、合规与监管基础、安全架构与资产保护机制，以及审计与鉴证体系等关键领域的结构化说明，白皮书旨在为机构客户、监管机构及生态合作伙伴提供一个可理解、可对照、可核验的尽职调查参考框架。

在数字资产与技术驱动的金融服务环境中，信任并非单一措施或孤立机制的产物，而是多层制度安排长期协同运行的结果。BIT 的实践表明，稳定的信任基础需要在治理层面明确责任与边界，在流程层面嵌入风险识别与控制机制，在技术层面落实可执行的安全与监控能力，并通过独立审计与鉴证形成外部验证。这些要素相互依存、彼此制衡，共同构成能够随业务规模、技术环境与监管要求变化而持续运行的制度性基础。

从风险治理角度看，BIT 将风险管理视为一项制度性能力，而非事后控制工具。通过清晰的风险分类、风险偏好设定及组织治理结构，将风险识别、量化、监控与处置嵌入业务全生命周期，支持业务创新、资本效率与客户保护之间的长期平衡。这一治理理念为信任体系提供了上位框架，使具体控制与技术措施能够在一致的风险边界内发挥作用。

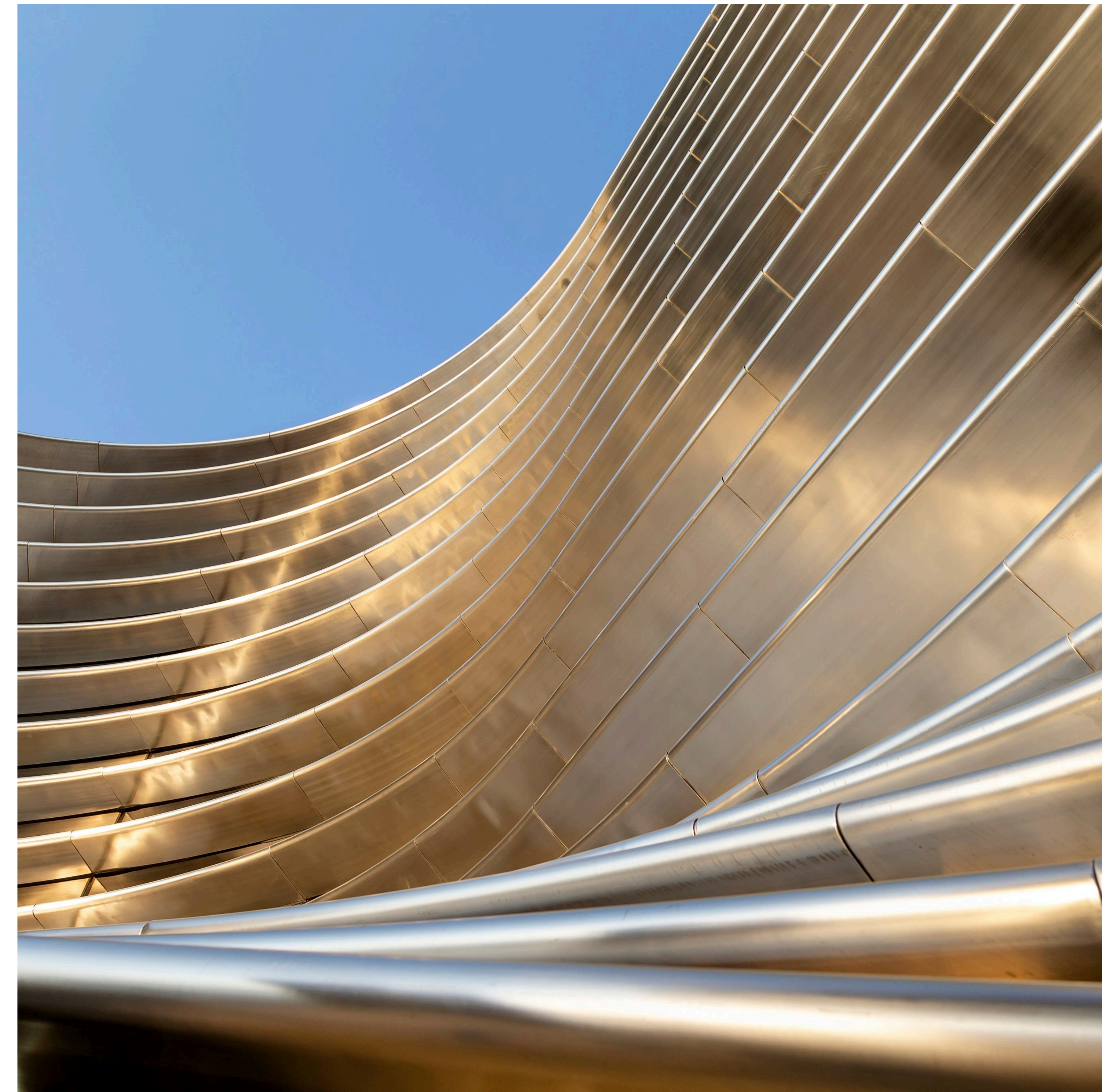
在合规与监管层面，BIT 通过多司法辖区的合规布局、AML/KYC 框架及持续的合规治理，明确业务活动的法律边界与监管适用范围，并在客户准入、交易监控与持续尽职调查等关键环节采用风险为本的方法。这些安排不仅用于满足合规要求，也为机构客户与合作伙伴提供监管可验证性的基础条件。

在安全与资产保护层面，BIT 将安全能力系统性地嵌入治理、流程与工程实践之中。通过零信任、纵深防御等架构原则，结合密钥管理、资产托管、防御监控、用户安全机制与安全文化建设，形成多层防护结构。这一安全体系并非静态配置，而是通过制度化与工程化方式持续演进，以应对不断变化的技术风险与威胁环境。

在审计与鉴证层面，BIT 采用多层级、互补型的验证结构，通过 ISO 管理体系审计、SOC 独立鉴证、年度财务审计及内部审计机制的组合，避免将信任建立在单一审计或认证之上，并通过明确披露范围与适用边界，支持基于事实的尽职调查。在 RWA 等链上链下协同的业务场景中，资产托管与信息披露安排、链上可查询机制及第三方参与，为资产层面的透明度与可核查性提供补充，使系统级控制与资产级验证形成协同。

如前文所述，BIT 对“信任”的构建以治理结构、风险管理、安全工程及外部鉴证的协同对齐为基础，形成一套具备韧性的机构级框架，旨在保障客户资产安全，并在不利的市场或运营环境下保持稳健运行。

随着市场环境、监管框架与技术条件的持续演进，相关制度、控制与验证机制亦将不断完善。本白皮书所呈现的，并非终点状态，而是一套可持续运行、可被审视、并具备演进能力的制度性信任基础。BIT 将在适用法律与合规框架下，持续通过治理、控制与独立验证机制，对其信任基础进行更新与维护。



免责声明

本《信任白皮书》旨在对公司在安全、合规、透明度及可验证性方面所采取的措施进行概述说明。其内容不构成对任何结果、资产安全或风险水平的保证，亦不应被视为承诺或担保文件。本文件仅作为向机构客户、监管机构及生态合作伙伴提供的结构化、可核验的参考资料使用。

术语表

A

AICPA Attestation Reports（AICPA 鉴证报告）

依据美国注册会计师协会（AICPA）鉴证标准出具的独立保障报告，包括 SOC 系列报告。

AML（Anti-Money Laundering，反洗钱）

用于预防、识别和报告洗钱及相关金融犯罪的监管与合规框架。

Annual Financial Audit（年度财务审计）

由独立审计机构按照适用监管要求与审计标准，对财务报表进行评估并出具审计意见的年度审计。

AR（Appointed Representative，指定代表）

英国监管体系下的一种监管身份，指在英国金融行为监管局（FCA）监管框架下作为授权机构代表开展业务的公司。

B

Bid-Ask Spread（买卖价差）

买方愿意购买资产的价格与卖方愿意出售资产的价格之间的差额。

Bug Bounty Programme（漏洞赏金计划）

一种正式的漏洞披露机制，对被验证的安全漏洞提供奖励。

C

C&ED（Customs and Excise Department，香港海关）

香港负责贵金属及宝石交易商（DPMS Category A）注册及反洗钱监管的机构。

Cactus Custody

BIT 旗下机构级数字资产托管平台，为数字资产提供安全托管基础设施。

CDD（Customer Due Diligence，客户尽职调查）

在 AML/CFT 框架下，对客户、授权代表、关联方及受益所有人进行的尽职调查。

CFT（Countering the Financing of Terrorism，反恐融资）

用于识别、预防和报告恐怖主义融资行为的控制措施。

Cold Wallet（冷钱包）

离线存储数字资产的钱包。由于不连接互联网，可降低网络攻击风险，通常用于长期资产存储。

Concentration Risk Monitoring（集中度风险监测）

作为市场风险测量的一部分，对风险集中度进行监测，通常结合 VaR、压力测试及流动性指标使用。

D

Defense-in-Depth（纵深防御）

一种分层安全策略，通过多重安全控制而非单一防护机制提供保护。

DPMS Category A（贵金属及宝石交易商 A 类）

香港针对贵金属及宝石交易商设立的注册类别。

DPT Service（Digital Payment Token Service，数字支付代币服务）

新加坡《支付服务法》下针对涉及数字支付代币服务的受监管业务类别。

E

EDD（Enhanced Due Diligence，强化尽职调查）

针对高风险客户或关系实施的额外尽职调查程序，例如涉及政治公众人物（PEP）、高风险司法辖区、不利媒体信息或高交易风险等情形。

F

FCA（Financial Conduct Authority，英国金融行为监管局）

英国负责监管金融服务机构与金融市场的监管机构。

FINMA（Swiss Financial Market Supervisory Authority，瑞士金融市场监管局）

瑞士金融市场监管局，负责监管金融机构及资产管理机构。

FinCEN（Financial Crimes Enforcement Network，美国金融犯罪执法网络）

美国负责监管和监督货币服务业务（MSB）的机构。

FIPS 140-3 Level 3

用于保护敏感信息的密码模块安全标准。

Four-Eyes Principle（四眼原则）

一种控制原则，要求至少两名授权人员参与关键操作，以减少单点错误和内部操作风险。

G

GMC（Gelephu Mindfulness City）

不丹正在建设的特殊行政及金融中心项目，与金融创新及数字资产监管相关。

H

HSM（Hardware Security Module，硬件安全模块）

用于安全生成、存储和管理加密密钥的专用硬件设备。

HTTPS（Hypertext Transfer Protocol Secure）

一种用于在互联网系统之间加密数据传输的安全通信协议。

I

Independent Testing（独立测试）

通过定期独立审查或审计评估 AML/CFT 项目及相关控制机制的有效性。

Internal Audit Framework（内部审计框架）

用于通过审计活动和持续监控评估风险管理、内部控制及运营流程的内部治理体系。

ISO 9001（质量管理体系，QMS）

适用于数字资产托管服务设计、开发、交付及运营流程的质量管理体系标准。

ISO 27001（信息安全管理体​​系，ISMS）

适用于托管服务信息安全管理​​的标准，具体范围由适用性声明（SoA）确定。

ISO 27701（隐私信息管理体系，PIMS）

在 ISO 27001 基础上扩展的隐私管理标准，用于规范数据控制者职责及客户信息处理合规要求。

K

KYC（Know Your Customer，了解你的客户）

根据监管要求对客户身份进行验证并评估其风险状况的客户尽职调查程序。

KYT（Know Your Transaction，了解你的交易）

对交易活动进行筛查和分析的监测流程，用于识别可疑交易模式及潜在金融犯罪风险。

L

Least Privilege（最小权限原则）

一种安全原则，仅授予用户完成其职责所需的最低访问权限。

Liquidity Risk Indicators（流动性风险指标）

用于监测流动性风险的指标，例如买卖价差等。

L

Loan-to-Value（LTV，抵押杠杆）

用于衡量贷款金额相对于抵押资产价值比例的指标，反映抵押资产对应的融资杠杆水平。

M

MAS（Monetary Authority of Singapore，新加坡金融管理局）

新加坡中央银行及金融监管机构。

Matrixdock

BIT 旗下现实世界资产（RWA）平台，通过治理安排、技术控制及第三方验证支持代币化资产的发行与透明度。

MFA（Multi-Factor Authentication，多因素认证）

通过多种认证因素验证账户登录或关键操作的身份认证机制，例如 UKey、Passkey 或认证器验证。

ML（Money Laundering，洗钱）

通过掩盖非法资金来源使其看似合法的金融犯罪行为。

MLRO（Money Laundering Reporting Officer，反洗钱报告官）

负责监督 AML/CFT 合规并在必要时向监管机构报告可疑交易的负责人。

MSB（Money Services Business，货币服务业务）

美国对从事资金转移或相关金融服务活动机构的一种监管分类。

N

Net Exposure Limit（净敞口限额）

用于限制借贷或交易活动可能产生总风险敞口的风险管理参数。

O

Operational Risk（操作风险）

由于内部流程、系统、人为因素或外部事件不足或失效导致损失的风险。

P

Passkey（密钥式认证）

一种无需密码的身份验证方式，通过加密密钥验证用户身份。

PEP（Politically Exposed Person，政治公众人物）

因其公共职务或影响力而可能面临较高洗钱或腐败风险的个人或相关人员。

Proliferation Financing（大规模杀伤性武器扩散融资）

用于支持大规模杀伤性武器扩散活动的资金或金融服务。

R

Risk Appetite（风险偏好）

组织在实现战略目标过程中愿意承担的风险水平与类型。

Risk Committee（风险委员会）

由董事会任命的治理机构，负责监督业务活动及资本与流动性规划。

S

Sanctions Compliance（制裁合规）

在 AML/CFT 框架下，根据适用制裁制度实施的筛查与控制机制。

SoA（Statement of Applicability，适用性声明）

ISO 27001 信息安全管理体系中用于说明适用安全控制及其实施状态的文件。

SOC 1 Type 2 Report

对与用户财务报告相关的内部控制设计与运行有效性进行评估的独立鉴证报告。

SOC 2 Type 2 Report

针对托管相关 IT 环境控制（安全性、可用性、保密性等）进行评估的独立鉴证报告。

S

SOP（Standard Operating Procedure，标准操作流程）

用于规范运营或风险管理场景中标准流程和操作步骤的文件。

SRO（Self-Regulatory Organization，自律组织）

被授权在其管辖范围内监督某些金融服务机构的行业自律机构。

Stress Testing（压力测试）

在极端但合理的不利情景下评估投资组合或金融系统韧性的风险管理方法。

T

TCSP（Trust or Company Service Provider，信托或公司服务提供商）

香港针对提供信托或公司设立与管理服务机构的牌照制度。

TF（Terrorist Financing，恐怖主义融资）

为支持恐怖活动或组织提供或筹集资金的行为。

TM（Transaction Monitoring，交易监测）

通过持续分析交易活动识别可疑模式或潜在金融犯罪风险的流程。

Travel Rule（旅行规则）

要求金融机构或虚拟资产服务提供商在转账时传递必要的交易发起人与受益人信息的监管要求。

Trust Services Criteria（信任服务标准）

SOC 2 审计中用于评估安全性、可用性、保密性、处理完整性及隐私控制的标准。

U

UKey

一种用于多因素认证的硬件身份验证设备。

V

VaR（Value at Risk，风险价值）

用于估计在给定时间范围和置信水平下投资组合潜在损失的风险测量指标。

VQF（Financial Services Standards Association）

瑞士经 FINMA 认可的自律组织，负责监督金融中介机构遵守瑞士反洗钱法规。

W

Whitelisting Mechanism（白名单机制）

一种安全控制机制，仅允许预先批准的地址、用户或操作执行。

Z

Zero Trust（零信任架构）

一种网络安全架构理念，基于默认不信任任何用户或系统的原则。

The background features a repeating pattern of interlocking cubes, creating a three-dimensional optical illusion. This pattern is rendered in a dark blue color. A horizontal band of a slightly lighter shade of blue runs across the center of the image, providing a backdrop for the text.

BIT

WWW.BIT.COM