BIT

Bridge Into Tomorrow

Trust Whitepaper

2026

Trust Whitepaper BIT

Table of Contents

Message from the CEO

In the digital asset industry, ***trust has never been established through a single promise or one-off audit***. It is formed through sustained and consistent institutional choices: whether clear risk boundaries are maintained in times of market volatility and uncertainty; whether established rules continue to be followed under growth pressure; and whether issues, when they arise, are communicated externally in a clear and traceable manner.

Over recent years, the industry has undergone multiple periods of significant adjustment. These cycles have repeatedly demonstrated ***that technology alone does not automatically generate trust***. Outcomes are shaped instead by the robustness of governance structures, the forward-looking nature of risk management, and the ability of disclosure mechanisms to withstand scrutiny over time and across market cycles.

Since its establishment, ***BIT***[1] has placed a high priority on risk management and foundational infrastructure in both business development and strategic decision-making. We have consistently held the view that digital assets do not justify lower standards for security, compliance, or transparency. On the contrary, in a highly uncertain industry, these requirements become even more critical.

Based on this understanding, BIT has consistently adhered to the following principles in the development of its business:

1. ***Security*** is a prerequisite for the operation of systems and the protection of assets, not an optional add-on.
2. ***Compliance*** defines the starting point of business boundaries, rather than serving as an after-the-fact supplement.
3. ***Transparency*** requires clear disclosure of key governance and control arrangements.
4. ***Verifiability*** requires that material conclusions be capable of independent review and demonstrate resilience over time.

Guided by these principles, BIT has established and continues to operate institutional arrangements across key foundational areas, including regulatory licensing and custody infrastructure. In terms of disclosure, we adhere to a fact-based and responsibility-oriented approach. Within applicable legal and compliance frameworks, material matters are communicated through official channels to ensure clarity and traceability of information.

This Trust Whitepaper is not a catalogue of future commitments. Rather, it provides a structured presentation of the systems, processes, and third-party verification arrangements that BIT has already established and currently operates. All content is based on publicly disclosable facts and is intended to provide institutional clients, regulators, and partners with a referenceable and verifiable basis for due diligence.

We do not believe that trust can be established quickly. ***We do believe, however, that it can be demonstrated through sustained and verifiable practice***. This conviction underlies BIT's decision to disclose its trust framework in an institutional and systematic manner.

John Ge

Co-Founder & CEO, BIT

[1] *BIT* previously operated under the name Matrixport until March 2026, when it was formally rebranded as BIT. Unless otherwise stated, all content herein applies retrospectively to Matrixport prior to the March 2026 rebranding.

Trust Whitepaper BIT

Introduction

In digital-asset and technology-driven financial services environments, trust-related arrangements typically involve multiple institutional and technical elements, including ***security, compliance, transparency, and verifiability***. These elements require systematic understanding and assessment at an institutional level. As market structures, regulatory environments, and business complexity continue to evolve, isolated commitments, one-off audits, or standalone technical solutions are no longer sufficient to meet the stability and verifiability requirements expected of institutional-grade business operations.

This ***Trust Whitepaper*** adopts security, compliance, transparency, and verifiability as its analytical framework and provides a structured description of the systems, processes, and third-party verification arrangements that BIT has established and currently operates. The scope of the paper covers key areas including ***digital-asset custody and security architecture, risk governance and compliance frameworks***, as well as audit and assurance mechanisms. It focuses in particular on the design and operation of governance structures, control environments, and verification mechanisms, and is intended to serve as a due diligence reference that is ***understandable, comparable, and verifiable*** for institutional clients, regulators, and ecosystem partners.

I. Document Positioning and Scope

This Whitepaper is neither a presentation of any single product or individual capability, nor does it constitute a guarantee of outcomes or a forward-looking commitment. Rather, it provides a structured representation of ***BIT's trust-related infrastructure*** as a whole.

All content is based on systems, processes, and third-party verification arrangements that have been implemented and are in continuous operation within the scope of what is currently publicly disclosable. Nothing herein should be interpreted as a transfer of risk or a unilateral assumption of responsibility by BIT.

II. Structural Pillars of the Trust Framework

From an overall structural perspective, BIT's Trust Framework is built around the following three mutually reinforcing pillars:

1. Compliance and Regulatory Foundations

Through multi-jurisdictional licensing and registration arrangements, ***BIT 's AML/KYC compliance framework*** and ongoing compliance governance define applicable legal boundaries and regulatory scope, providing a foundation to support regulatory oversight in connection with its business operations.

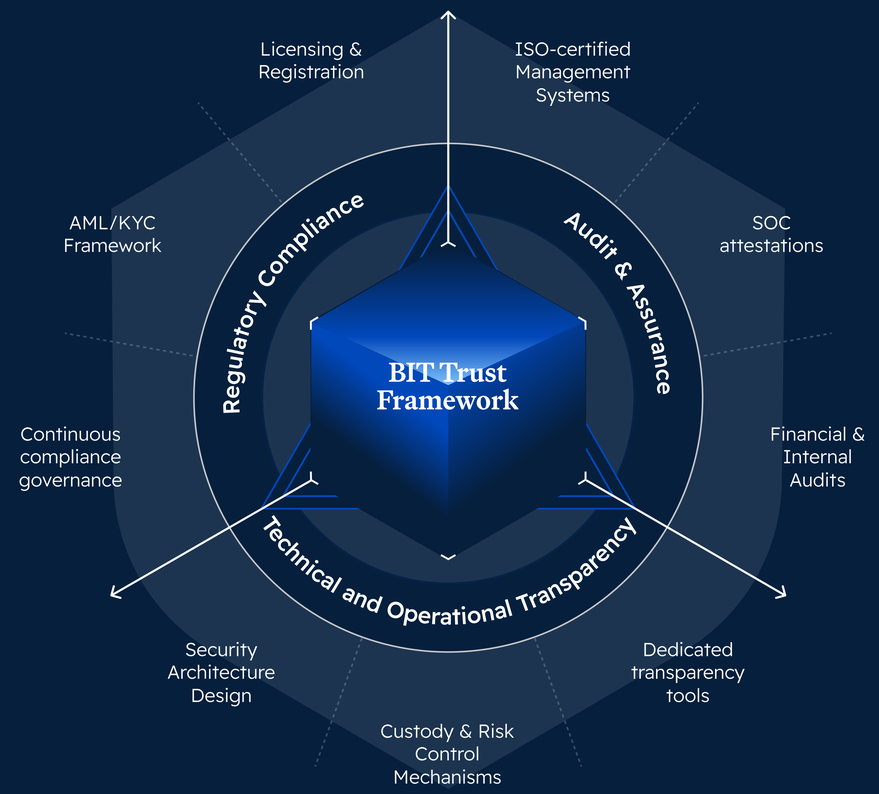
2. Independent Audit and Assurance Mechanisms

Through ISO management systems, SOC independent assurance reports, annual financial audits, and internal audit arrangements, BIT establishes a ***multi-layered and complementary third-party verification structure***. This supports independent assessment of key control environments while avoiding reliance on any single audit or certification.

3. Technical and Operational Transparency

Through security architecture design, risk-control systems, asset-custody mechanisms, and transparency tools applied in specific business scenarios, BIT enhances the ***interpretability and verifiability*** of key operational and control arrangements.

Overview of the Three-Pillar Trust Framework



Risk Management and Risk Governance Framework

This illustration summarizes BIT's Risk Management and Governance Framework across governance bodies, risk categories, and the risk-appetite lifecycle. It shows how senior management and specialized committees oversee different types of risk while setting, implementing, monitoring, and reviewing risk appetite across business lines in a continuous loop.

I. Risk Governance Approach

In digital-asset-related financial services environments, risk is an inherent feature of business operations. BIT therefore treats risk management as an institutional capability, implemented through its ***Risk Management and Governance Framework*** (the "***Framework***"), rather than as a post-event control function. The objective of the Framework is to support a sustainable balance between ***business development, capital efficiency, and client protection***.

The Framework is built on clear risk classification, a defined risk appetite, and a structured organizational governance arrangement. It addresses the principal risk categories arising across BIT's business activities, including market risk, credit risk, operational risk, liquidity risk, legal and compliance risk, as well as technology and cybersecurity risk. Operational risks are mitigated through a combination of internal control frameworks, standardized operational procedures (SOPs), independent assurance mechanisms (including SOC audits), and ongoing monitoring processes.

At the governance level, BIT has established a ***Risk Committee*** appointed by the Board of Directors. The Committee comprises the risk policy lead and relevant business representatives, and provides oversight of business activities as well as capital and liquidity planning. Management defines and maintains the firm's risk appetite to ensure that risk-taking activities remain aligned with BIT's overall strategic objectives, while reinforcing a risk-aware operating culture across the organization.

II. Overview of the Risk Management Framework

Under the ***Risk Management and Governance Framework***, risk management is not centralized around a single control point. Instead, risk controls are embedded across the full business lifecycle, including pre-transaction assessment, in-transaction monitoring, and post-transaction handling, forming a closed-loop risk management mechanism.

Risk Management Framework

Credit and counterparty risk	Market/portfolio risk	Capital Liquidity risk	Operational risk
Client due diligence process	Calculate market based margin parameters (e.g. LTV, margin level, liquidation level)	Asset liability management to mitigate duration risk	Crypto Asset Storage
Credit scoring the counterparty and decide the credit limit based on the margin parameters (e.g. LTV, margin call level and liquidation level for collateralised lending)	Real-time risk monitoring and automated alert notification	Capital reserve for loan loss and liquidation gap	Safety and security on transactions (e.g. approval process)
Advise on the commercial terms based on the "risk-adjusted" analysis	Automated liquidation procedure		Enterprise level security policy (e.g. 2FA/Ukey access)

This diagram provides a high-level view of how BIT's RMGF maps credit and counterparty risk, market risk, capital and liquidity risk, and operational risk to specific business controls and system capabilities.

III. Risk Identification and Quantification: A Data-Driven Risk Measurement Framework

As part of the Risk Management and Governance Framework, BIT applies ***multi-dimensional and quantifiable measurement methodologies*** to continuously assess different categories of risk:

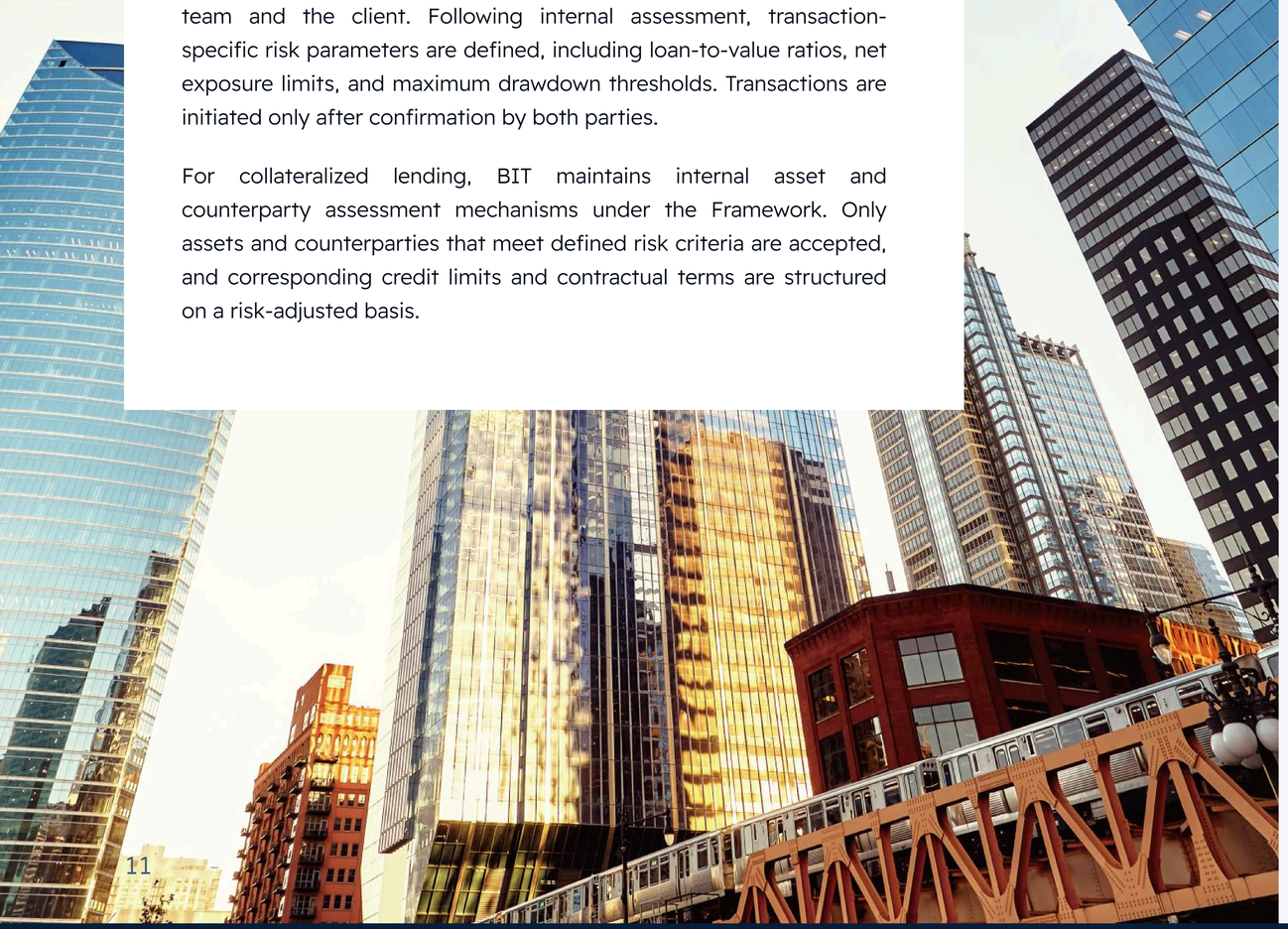
Market Risk	Credit and Counterparty Risk	Capital and Liquidity Risk
Managed through portfolio-level Value at Risk (VaR) calculations (99% confidence interval), stress testing, liquidity risk indicators (such as bid-ask spreads), and concentration risk monitoring.	Addressed through over-collateralization requirements, due diligence review processes, credit-limit management, and risk diversification across products and counterparties.	Managed through asset-liability management and stress testing to maintain appropriate capital and liquidity buffers.

These risk indicators are continuously integrated into BIT's internal risk engine to support real-time monitoring and decision-making under the Framework.

IV. Business-Line Risk Control Mechanisms: Scenario-Based Controls in Place of Uniform Rules

Within the Risk Management and Governance Framework, BIT implements differentiated and scenario-specific risk control mechanisms across its various business lines. Using margin lending as an example, risk control begins prior to transaction execution. Clients are required to complete due diligence questionnaires covering background information, trading strategies, existing risk-control measures, and historical performance. Relevant information is assessed using analytical tools and, where appropriate, supplemented by direct due diligence discussions between the risk management team and the client. Following internal assessment, transaction-specific risk parameters are defined, including loan-to-value ratios, net exposure limits, and maximum drawdown thresholds. Transactions are initiated only after confirmation by both parties.

For collateralized lending, BIT maintains internal asset and counterparty assessment mechanisms under the Framework. Only assets and counterparties that meet defined risk criteria are accepted, and corresponding credit limits and contractual terms are structured on a risk-adjusted basis.



V. Real-Time Monitoring and Incident Response: From Alert to Resolution

After the transaction is executed, the Risk Management and Governance Framework enables real-time risk visibility, automated alerting, and analytical capabilities. When risk parameters deviate from defined ranges or approach established thresholds, alerts are triggered and escalated in accordance with predefined procedures. Relevant teams respond in line with comprehensive *Standard Operating Procedures (SOPs)* designed to manage operational incidents and control operational risk, and apply tiered response measures as appropriate.

Risk Management Process Flow

This diagram illustrates the end-to-end process from pre-transaction risk analysis, through in-transaction monitoring, to default management and liquidation.

VI. Risk Reporting and Ongoing Transparency

As part of the Framework's governance and oversight arrangements, BIT operates a periodic risk reporting mechanism. Under normal market conditions, risk reports are generally produced on a weekly basis and cover market volatility, potential liquidation price ranges, and stress-testing results. During periods of elevated market volatility, reporting frequency and level of detail are increased to support timely decision-making by management and business teams.

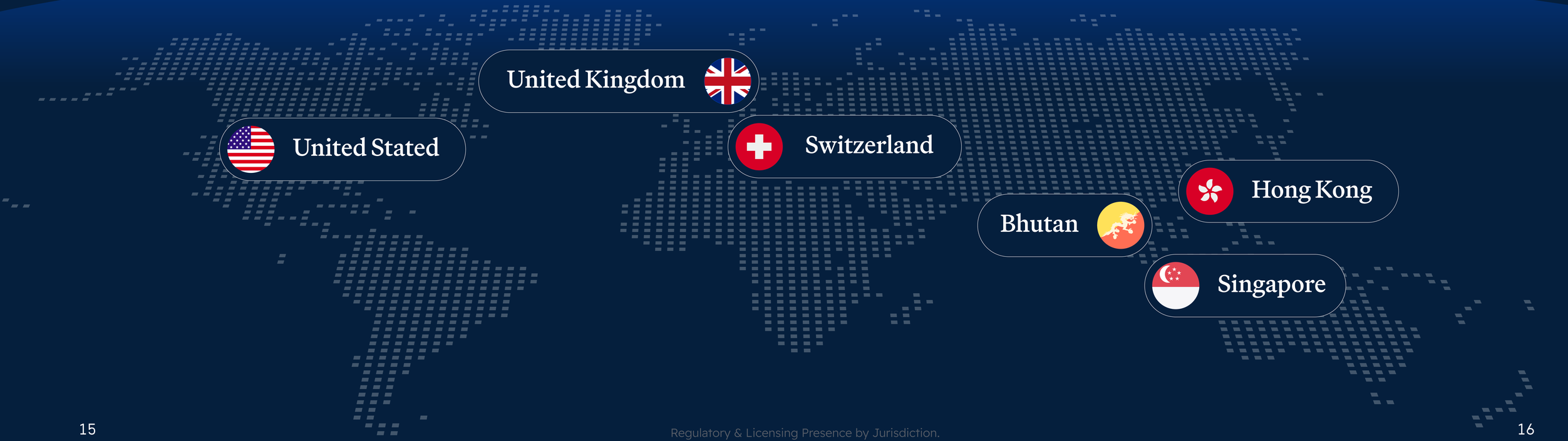
Compliance and Regulatory Framework

Over the years, BIT has built a geographically distributed operating footprint to support its global client base and evolving regulatory obligations. With regulated legal entities incorporated and licenses obtained across ***multiple jurisdictions***, BIT has established a global compliance architecture built on standardized policies and an integrated anti-money-laundering and know-your-customer ***(AML/KYC) framework***. This architecture forms the legal and compliance basis for its principal lines of business, including custody, asset management, digital-asset services, precious-metals handling, payment services, and intermediation, providing clients with transparent visibility into the Group's regulatory standing and compliance practices.

I. Global Licensing Infrastructure

The following information lists licences and registrations pertaining to BIT and its affiliated legal entities that have been duly granted and publicly announced. Each licence applies solely to the specified legal entity, jurisdiction, and permitted activities, as in effect at the time of publication.

Jurisdiction	Regulatory Status	Licensing authority
Hong Kong	Matrix Trust Company Limited	License type: TCSP (Trust or Company Service Provider) Licensing authority: Companies Registry (CR)
	Matrix Port Technologies (Hong Kong) Limited	License type: Money Lender License Licensing authority: Licensing Court



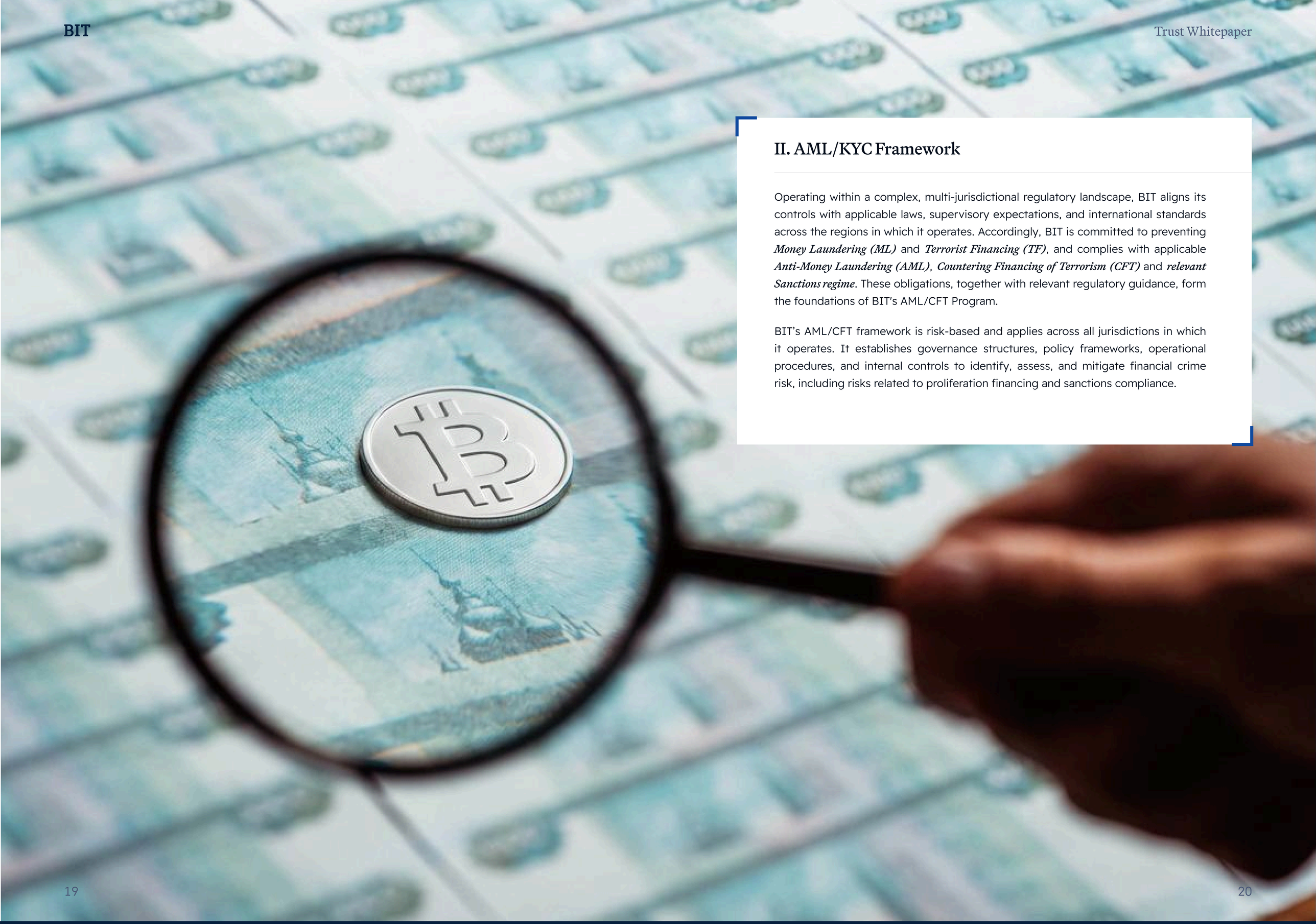
Regulatory & Licensing Presence by Jurisdiction.

Jurisdiction	Regulatory Status	Licensing authority
Hong Kong	Flying Hippo (Custody) Limited	License type: TCSP Licensing authority: Companies Registry (CR)
	Matrix Infinitus (Hong Kong) Limited	License type: DPMS Category A (Dealer in Precious Metals and Stones) Registration/AML supervisory authority: Customs and Excise Department (C&ED)
Bhutan	Matrix Gelephu Pte Ltd	License type: Financial Services License Licensing/Regulatory authority: Gelephu Financial Services Office, Gelephu Mindfulness City (GMC)
	Matrix Bhutan Pte Ltd	License type: Financial Services License Licensing/Regulatory authority: Gelephu Financial Services Office, Gelephu Mindfulness City (GMC)
Singapore	Fly Wing Technologies Pte. Ltd.	License type: Major Payment Institution – Digital Payment Token Service Regulator: Monetary Authority of Singapore (MAS)

Jurisdiction	Regulatory Status	Licensing authority
Switzerland	ChainTech AG	License type: Member of Self-Regulatory Organization (SRO) Regulatory authority: Financial Services Standards Association (VQF)
	Matrixport Asset Management AG	License type: Managers of Collective Assets Supervisory authority: FINMA
United Kingdom	Matrixport Advisors Limited	Regulatory status: Appointed Representative (AR) Regulatory authority: Financial Conduct Authority (FCA)
United States	Matrixport Inc	License type: Money Services Business (MSB) Registration authority: Financial Crimes Enforcement Network (FinCEN)

Regulatory Status Disclaimer

All licenses, registrations, and regulatory statuses listed above are granted or maintained by the relevant authorities for specific regulated activities only. They do not constitute an endorsement, approval, or recommendation of BIT or its services by any regulator, nor do they authorize the conduct of activities outside the approved scope or beyond the relevant jurisdictions.



II. AML/KYC Framework

Operating within a complex, multi-jurisdictional regulatory landscape, BIT aligns its controls with applicable laws, supervisory expectations, and international standards across the regions in which it operates. Accordingly, BIT is committed to preventing ***Money Laundering (ML)*** and ***Terrorist Financing (TF)***, and complies with applicable ***Anti-Money Laundering (AML)***, ***Countering Financing of Terrorism (CFT)*** and ***relevant Sanctions regime***. These obligations, together with relevant regulatory guidance, form the foundations of BIT's AML/CFT Program.

BIT's AML/CFT framework is risk-based and applies across all jurisdictions in which it operates. It establishes governance structures, policy frameworks, operational procedures, and internal controls to identify, assess, and mitigate financial crime risk, including risks related to proliferation financing and sanctions compliance.

Trust Whitepaper BIT

1. AML/CFT Policy

The AML/CFT Policy sets minimum standards that apply across BIT and includes:

1.1 ***Written policies, procedures, and internal controls*** to ensure compliance with applicable AML/CFT and sanctions laws.

1.2 ***Accountability:*** Appointment of a Money Laundering Reporting Officer (MLRO) for oversight and control effectiveness.

1.3 ***Governance:*** A robust AML/CFT framework with Senior Management oversight.

1.4 ***Customer Due Diligence (CDD):*** Due diligence is performed on customers, authorized representatives, connected parties and beneficial owners.

1.5 ***Risk Assessment:*** Customer, country, product, service, transaction, and delivery channel risk assessments.

1.6 ***Enhanced Due Diligence (EDD):*** Applied to higher-risk relationships (including but not limited to clients with PEP nexus, clients from high-risk industries/jurisdictions, adverse media, elevated risk factors from Know Your Transaction (KYT)/transaction monitoring (TM)).

1.7 ***Sanctions Compliance:*** Screening and controls consistent with applicable sanctions regimes, including but not limited to obligations related to proliferation financing.

1.8 ***Ongoing Due Diligence and Monitoring:*** Periodic reviews (PRs) on clients based on risk rating and trigger events. KYT conducted for real-time transaction screening and TM for post-transaction review to analyze patterns and behavior over time to detect suspicious activity.

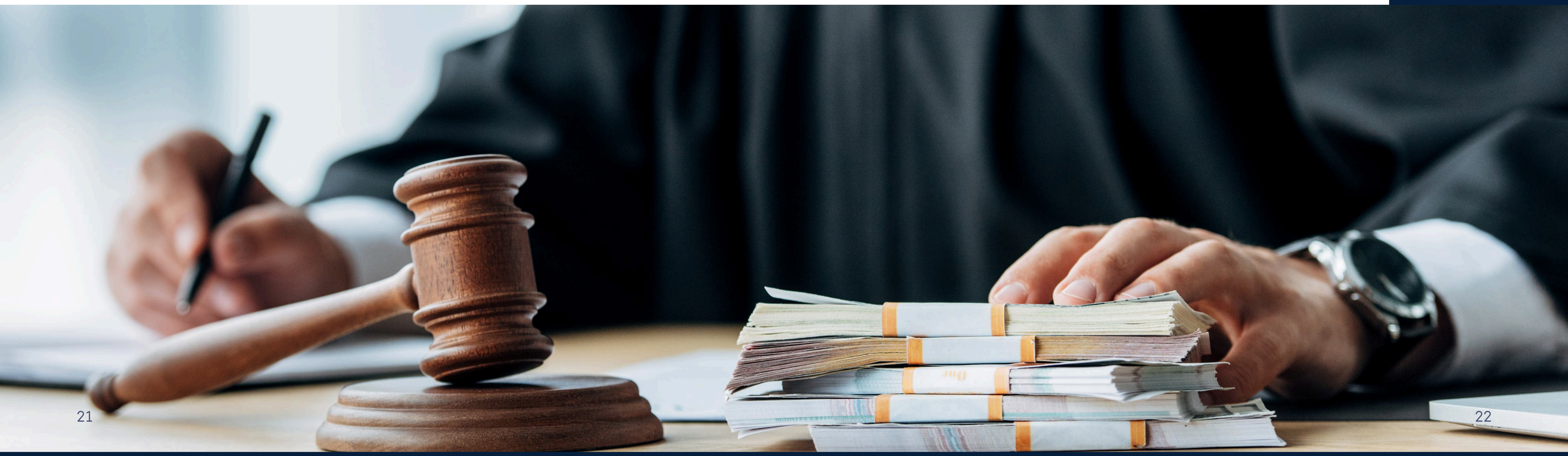
1.9 ***Escalation & Reporting:*** Internal escalation and timely filing of suspicious transaction/activity reports with the relevant authorities.

1.10 ***Training:*** Mandatory AML/CFT and sanctions training for all employees at onboarding and annually thereafter.

1.11 ***Independent Testing:*** Periodic, independent audit/review of program effectiveness.

1.12 ***Recordkeeping:*** Retention of records for the periods required by applicable law and regulations.

1.13 ***Travel Rule (where applicable):*** Transmission of required originator/ beneficiary information between VASPs/financial institutions.



2. Prohibited Business Relationships

2.1 In accordance with the AML/CFT framework, certain uses, customers, and business relationships are prohibited. These include relationships or activities involving the following parties:

2.1.1 Sanctioned individuals and entities by local regulatory authorities which BIT holds licenses or under International Sanctions lists (e.g., United Nations Security Council, United States Office of Foreign Asset Control (OFAC), EU Sanctions, His Majesty's Treasury of the United Kingdom, Monetary Authority of Singapore lists, etc.)

2.1.2 Persons or enterprises known or reasonably presumed to be involved in terrorist financing or serious criminal activity, or that belong to/support such organizations

2.1.3 Shell banks which have no physical presence at their place of incorporation

2.1.4 Clients operating under fictitious names or pseudonyms

2.1.5 Clients that are in Weapons, Armament Manufacturers, and Armament Trading

2.1.6 Clients involved in Tobacco trading

2.1.7 Clients involved in Adult Entertainment

2.1.8 Clients involved in Casinos, Gambling or similar industries

2.2 Prohibited Assets

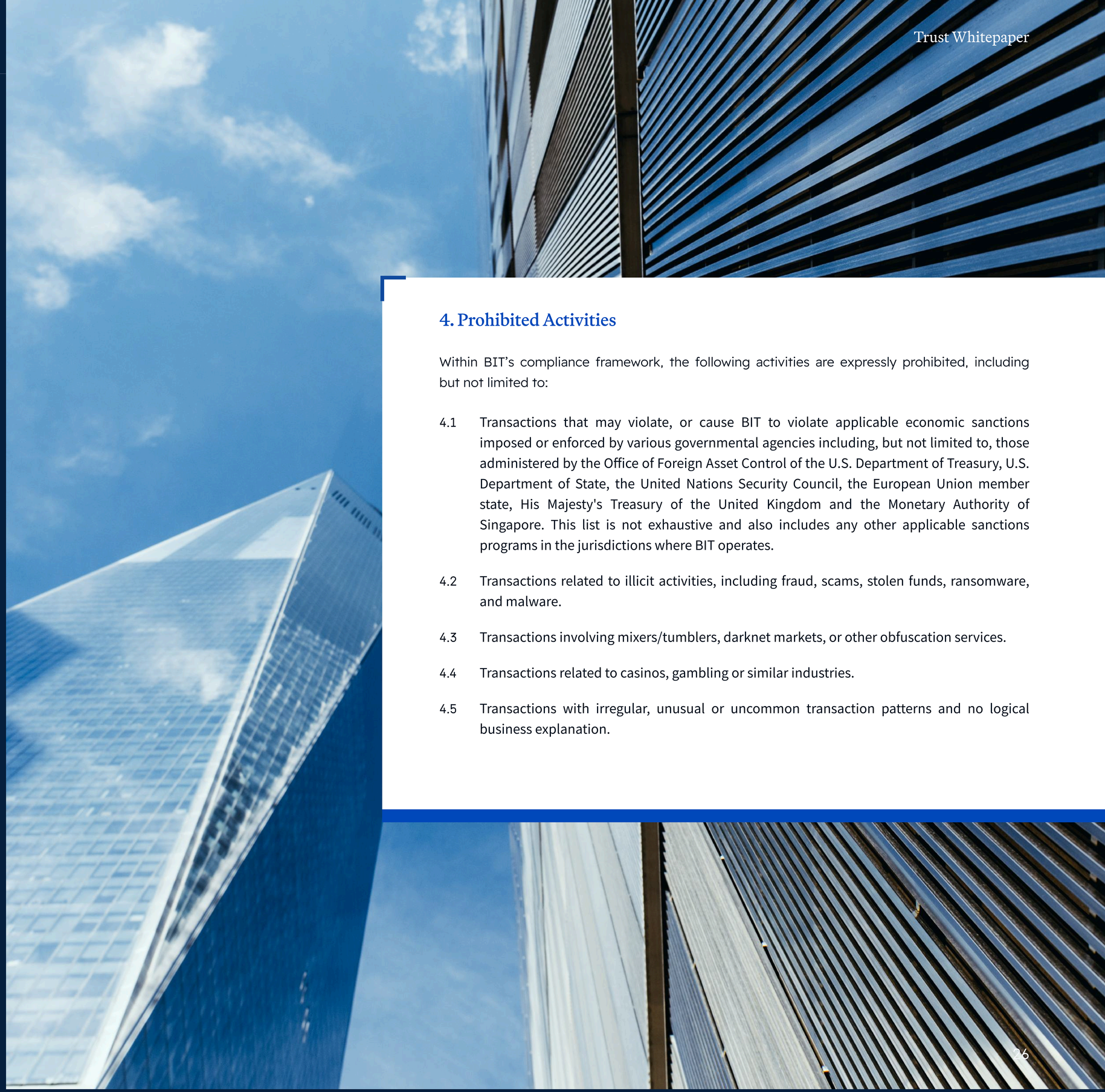
BIT prohibits funds that are identified through customer due diligence (KYC) or transaction monitoring (KYT) as originating from criminal activities, involving terrorist financing, or linked to criminal organizations from entering or remaining within its systems. BIT will not establish or continue any business relationship involving such circumstances, regardless of the jurisdiction in which the underlying illegal or criminal activity occurred.

2.3 Restricted Jurisdictions

BIT maintains and periodically updates a list of restricted jurisdictions on its official website. In accordance with its AML/CFT programme, BIT does not establish business relationships with parties from jurisdictions subject to comprehensive sanctions or exhibiting severe AML/CFT deficiencies.

3. BIT's Know Your Transaction (KYT)

BIT strictly prohibits the use of its platforms for any illegal activity, including but not limited to money laundering, terrorist financing, or unlawful commerce. Through continuous transaction monitoring and its Know Your Transaction (KYT) mechanisms, BIT conducts real-time and ongoing monitoring of relevant transaction activities. Where monitoring identifies suspected illegal activity, BIT may take action, including rejecting or refunding funds, issuing requests for information (RFIs), freezing accounts, suspending or terminating access or relationships, and/or reporting suspicious activity to the relevant authorities, where permitted by applicable law or our Terms and Conditions. BIT reserves all rights under applicable law and its contractual arrangements.



4. Prohibited Activities

Within BIT's compliance framework, the following activities are expressly prohibited, including but not limited to:

4.1 Transactions that may violate, or cause BIT to violate applicable economic sanctions imposed or enforced by various governmental agencies including, but not limited to, those administered by the Office of Foreign Asset Control of the U.S. Department of Treasury, U.S. Department of State, the United Nations Security Council, the European Union member state, His Majesty's Treasury of the United Kingdom and the Monetary Authority of Singapore. This list is not exhaustive and also includes any other applicable sanctions programs in the jurisdictions where BIT operates.

4.2 Transactions related to illicit activities, including fraud, scams, stolen funds, ransomware, and malware.

4.3 Transactions involving mixers/tumblers, darknet markets, or other obfuscation services.

4.4 Transactions related to casinos, gambling or similar industries.

4.5 Transactions with irregular, unusual or uncommon transaction patterns and no logical business explanation.

Security Architecture and Asset Protection Framework

In digital-asset and technology-driven financial services environments, security is not an auxiliary capability but a foundational condition for establishing trust. From its inception, BIT has treated security as a company-level principle. Through end-to-end security-by-design, globally distributed infrastructure, and security engineering capabilities aligned with specific business scenarios, BIT has established a security framework covering assets, systems, business operations, personnel, and processes. This framework supports the platform's long-term security, stability, and resilience.

I. System Security Architecture

BIT's system security architecture is built on a ***Zero Trust*** model and applies a ***Defense-in-Depth*** approach through layered controls. In parallel, BIT implements the principles of ***attack surface minimization*** and ***least privilege***, forming mutually reinforcing security layers across management, process, and technology.

Using ***Cactus Custody*** as an illustrative example, the reference architecture below demonstrates how security controls, access governance, audit traceability, and risk-mitigation mechanisms are systematically embedded into the core architecture for institutional-grade digital asset custody scenarios.

Institutional-Grade Digital Asset Custody Security Architecture

<table>
<tr><td rowspan="4">Wallet Utility Layer</td><td colspan="5">Institutional Wallet Ecosystem</td></tr>
<tr><td colspan="2">Multi-user control</td><td colspan="2">Fiat custody</td><td>Crypto custody</td></tr>
<tr><td colspan="2">RWA asset management</td><td colspan="2">Role-based access control</td><td>Whitelist & limit management</td></tr>
<tr><td colspan="2">Audit logs & asset reports</td><td colspan="2">Customisable security levels</td><td>Mobile approval tools</td></tr>
<tr><td rowspan="4">Digital Asset Layer</td><td colspan="3">DeFi Ecosystem</td><td colspan="2">CeFi Ecosystem</td></tr>
<tr><td>Native ETH collateral</td><td>Safe{Wallet} access control</td><td>Pre-execution of transactions</td><td>Custodied OTC & internal trading</td><td>Digital asset trust services</td></tr>
<tr><td>Whitelisted contract/spender addresses</td><td>Custom tokens</td><td>Custom RPC nodes</td><td colspan="2">Trusted third-party escrow</td></tr>
<tr><td colspan="2">Message signing & contract approval policies</td><td>Cactus Link (DeFi Connector)</td><td colspan="2">Cactus Oasis (off-exchange settlement)</td></tr>
</table>

Trust Whitepaper
BIT

1. Governance Layer: Institutionalized Security Governance

Effective security begins with governance. In digital-asset-related operations, the absence of clear authority ownership, formal decision-making mechanisms, and accountable execution structures cannot be compensated for by technical controls alone.

BIT has established a formal security governance framework that embeds security requirements into organizational operations. This framework defines ***internal authorization boundaries, accountability structures, and escalation pathways***. By integrating security into management structures and operational processes, BIT ensures continuous oversight of risk, independent review of critical decisions, and consistent application of security standards across products, systems, and business activities.

1.1 Institutional Security Accountability

Security governance responsibilities are jointly borne by management personnel with financial and cybersecurity expertise and dedicated professional teams. Through formalised responsibility allocation and management reporting mechanisms, BIT clearly defines execution pathways and internal accountability boundaries for security responsibilities.

1.2 Security Veto Authority

The security function holds veto authority. Where product designs, business requirements, architectural changes, or production deployments present material security risks or fail to meet BIT's security baseline or compliance requirements, the security team is authorised to suspend relevant activities and require remediation and re-review before continuation or release.

1.3 Least Privilege and Segregation of Duties

In line with Zero Trust principles, employees are granted only the system access necessary for their roles, with dynamic adjustment to reduce the risk of privilege misuse and internal exposure.

1.4 "Four-Eyes" Principle

All critical operations require the participation of at least two authorized individuals, establishing internal checks and balances to reduce single-point failure and operational risk. This principle applies to high-risk or sensitive actions, including asset transfers, account security changes, privilege modifications, and transaction approvals.

2. Process Layer: Security Embedded Across the Full Business Lifecycle

2.1 Secure Software Development Lifecycle (S-SDLC)

The Secure Software Development Lifecycle (S-SDLC) embeds security requirements across system design, development, testing, deployment, and operations, and treats security as a baseline quality requirement alongside functionality and performance.

2.2 Continuous Monitoring and Response

BIT applies the *Identify-Protect-Detect-Respond-Recover (IPDRR)* security framework to continuously monitor and respond to system and business operations.

2.3 Threat Intelligence and Risk Monitoring

BIT continuously monitors emerging threat sources and new attack techniques, enabling timely identification and response to risks that may affect platform stability or asset security.

3. Technical Layer: Engineering Security Controls

3.1 Industry-Standard Security Tools and Solutions

BIT applies proven security technologies covering identity management, access control, intrusion prevention, and anomalous behaviour detection.

3.2 End-to-End Security Standards

Unified security standards are defined and enforced across system design, development, testing, and operations to ensure consistent implementation across the organization.

3.3 Best-Practice Security Baselines

Security control baselines are continuously refined and standardised to support consistent application across systems and business scenarios.

II. Key Management and Asset Protection Mechanisms

Digital asset security extends beyond software and cryptography into the physical and environmental layers of infrastructure. This is particularly critical in cold-wallet custody scenarios. BIT applies stringent physical and environmental controls to protect critical systems and sensitive information from unauthorised access, environmental risk, and operational disruption.

1. Cold and Hot Wallet Segregation

- The majority of assets are stored in cold wallets.
- Hot wallets are used only to meet necessary day-to-day liquidity requirements.

This approach reduces online exposure and limits the attack surface.

2. Cold Wallet Environment and Physical Security

- Cold wallet storage locations are strictly confidential.
- Isolated networks and controlled environments are used.
- Multiple layers of physical security protections are implemented.

This approach reduces online exposure and limits the attack surface.

3. Private Key Security and Hardware Protection

Private keys are stored using ***FIPS 140-3 Level 3*** certified Hardware Security Modules (HSMs).

Private keys are never exposed in plaintext form under any circumstances.

HSMs are deployed in controlled environments with stringent physical and environmental security requirements consistent with financial-grade and critical infrastructure standards.

Trust Whitepaper BIT

III. Security Incident Monitoring and Defence Framework

1. Multi-Factor Authentication (MFA)

BIT applies a multi-factor authentication framework to prevent unauthorized access. Key operations remain protected even if a single authentication factor is compromised.

- MFA is required for account login and critical operations.
- Supported methods include UKey, passkeys, and authenticator-based verification.
- All critical actions (e.g., withdrawals, security setting changes) require secondary verification.

Optional biometric verification (fingerprint/facial recognition) may be used to enhance user experience without reducing security standards.

2. 24-Hour Risk Monitoring and Anomaly Alerts

BIT maintains continuous monitoring of user behaviour and transaction activity. Automated controls provide real-time visibility and response capabilities.

- Real-time monitoring of account activity
- Automated detection of anomalous logins, devices, and withdrawal behaviour
- Risk-based alerts triggering delays or manual review
- User notifications via email and other channels

3. Advanced Encryption & Access Control

BIT applies industry-standard encryption and granular access control mechanisms to ensure data confidentiality, system integrity, and operational isolation.

- HTTPS is used across all services to protect data in transit
- Strong encryption algorithms applied to sensitive data at rest
- Fine-grained identity and access management
- Strict segregation between roles, users, and system modules
- Whitelisting mechanisms to reduce operational and attack risk

4. Anti-Phishing & User Security Protection

- ***Official Channel Verification:*** Users may verify official communication channels, employee identities, and announcements through the Security Center.
- ***Platform-Wide Monitoring:*** BIT monitors phishing websites, malicious applications, and brand misuse; fraudulent sites are taken down, and users are notified.
- ***Bug Bounty Programme:*** BIT operates a formal vulnerability disclosure programme, offering rewards of up to USD 100,000 for validated security findings.
- ***Security Incident Reporting:*** Dedicated reporting channels allow security researchers and users to report vulnerabilities or suspicious activity directly to BIT's security response teams.

IV. External Security Assessments and Third-Party Assurance

In the context of digital asset custody, internal controls are strengthened through independent verification against internationally recognised standards. External assurance provides objective validation of governance structures, security controls, privacy protections, and operational quality.

BIT conducts periodic third-party audits and assessments of key systems and processes to evaluate the effectiveness of security controls in both design and operation. These assessments are intended to support transparency, accountability, and ongoing improvement of the security framework.

BIT's digital asset custody platform, *Cactus Custody*, has obtained the following internationally recognised certifications and assurance reports:

1. SOC 1 Type II/SOC 2 Type II

Independent assurance reports evaluating the design and operating effectiveness of internal controls and security measures over an extended assessment period.

2. ISO/IEC 27001:2022

Certification of the information security management system, covering the confidentiality, integrity, and availability of information assets.

3. ISO/IEC 27701:2019

Certification of the privacy information management system, supporting compliance with data protection and privacy governance requirements.

4. ISO 9001:2015

Certification of the quality management system, demonstrating standardized operational processes and continuous improvement mechanisms.

Taken together, these independent assessments provide an externally verifiable foundation for BIT's security and custody trust framework, supporting institutional confidence in the platform's security governance and operational controls.

V. Security Training and Security Culture

Technology and controls alone are insufficient without informed and accountable personnel. Human behaviour remains a critical factor in preventing security incidents, particularly in high-value asset environments.

BIT promotes a security-first culture through structured training programmes, continuous awareness initiatives, and clearly defined responsibilities. Security principles are embedded into daily operations and enforced at the individual level.

"Security First" is one of BIT's core cultural principles and is reflected throughout the employee lifecycle:

- Background screening during recruitment
- Mandatory security training and assessments for new hires
- Regular phishing simulations Annual organization-wide cybersecurity examinations
- Role-specific security requirements
- Clear disciplinary mechanisms for security violations
- Continuous strengthening of employees' ability to identify security risks and incidents

Through the integration of policy, training, and practice, security awareness is transformed from procedural requirements into organizational habit.

VI. Security as the Foundation of Trust

BIT's security framework is not a collection of isolated technical controls, but a system that integrates ***governance, processes, engineering practices, and infrastructure***. Through continuous improvement, embedded risk controls, and independently verifiable external assessments, security capabilities are systematically integrated into both daily operations and long-term platform development.

Together with compliance and audit arrangements, this security framework forms a core pillar of ***BIT's Trust Framework***, enabling it to address evolving security and risk challenges while maintaining asset protection and client trust amid changing business scale, technological environments, and regulatory expectations.

BIT

Audit and Assurance Framework

BIT's institutional audit and assurance framework integrates multiple, independent audit and assurance mechanisms. It provides verifiable evidence relating to the security of custody services, the reliability of financial information, and the effectiveness of internal control environments. The framework is designed to support the due diligence requirements of institutional clients, regulators, and ecosystem partners, rather than relying on any single audit or assurance as the sole basis of trust.

The overall audit and assurance framework is composed of the following four complementary layers:

- International standards–based management system audits (ISO)
- Independent third-party assurance (SOC)
- Annual financial audit
- Internal audit mechanisms

Note
All ISO and SOC audits apply to Cactus Custody only, and do not constitute group-wide coverage across other BIT legal entities or business lines.

I. ISO International Standards-Based Audit Framework

Within the currently publicly disclosable information, the custody service operating framework of Cactus Custody is subject to multiple third-party audits and certifications against internationally recognized ISO management system standards. Audit scope, control objectives, and applicability are defined in the approved ***Statement of Applicability (SoA)***.

ISO management system audits are conducted to verify that, across the design, development, delivery, and operation of digital asset custody services, ***Cactus Custody*** has established and operates management and control mechanisms aligned with applicable international standards. These audits form a core component of the externally verifiable security and management assurance framework.

Key standards audited and maintained publicly include:

1. ISO 9001 – Quality Management System (QMS)

Covering the design, development, delivery, and operational processes of digital asset custody services.

2. ISO 27001 – Information Security Management System (ISMS)

Covering the information security management framework supporting digital asset custody services, with an audit scope defined by the approved Statement of Applicability.

3. ISO 27701 – Privacy Information Management System (PIMS)

Extending privacy management requirements based on ISO/IEC 27001, covering data controller roles and customer information processing compliance within internal operations.

ISO audits are conducted on an annual basis. Detailed audit reports, control mappings, and conclusions are made available within applicable compliance and confidentiality frameworks and are not published as general public disclosures.

II. SOC Third-Party Independent Assurance (AICPA Attestation Reports)

In addition to ISO audits, ***Cactus Custody*** undergoes independent SOC assurance to provide a third-party evaluation of its custody-related control environment.

Cactus Custody has obtained the following SOC reports:

1. SOC 1 Type II Report

Providing independent assurance over the design and operating effectiveness of internal controls relevant to user-entity financial reporting over a defined assessment period.

2. ISO 27001 – Information Security Management System (ISMS)

Providing independent assurance over controls within the custody-related IT environment, assessed against applicable Trust Services Criteria, including security, availability, and confidentiality.

All SOC engagements are performed by internationally recognized independent accounting firms and provide institutional clients and partners with objective assurance regarding maturity and operational sustainability.

III. Annual Financial Audit

BIT and its relevant affiliated entities conduct independent external financial audits on an annual basis, in accordance with applicable regulatory and statutory requirements in their respective jurisdictions.

The scope of annual financial audits typically includes:

- Assessment of the accuracy and completeness of financial statements.
- Evaluation of the effectiveness of key financial controls.
- Review of the consistency between accounting policies and applicable accounting standards.

All audit opinions are issued independently by external audit firms based on professional judgement and in accordance with applicable auditing standards.

IV. Internal Audit Framework

At the internal governance level, BIT has established internal audit arrangements that include:

- Risk identification and assessment
- Control testing
- Audit reporting and internal communication
- Remediation tracking and continuous improvement

Internal audit functions serve as a complementary layer to external audit and assurance mechanisms, supporting continuous improvement and alignment with the international standards framework.

V. Business-Line Level Audit and Transparency Assurance

1. Cactus Custody

Audits and assurance arrangements relating to custody service are incorporated within the ISO management system and SOC assurance frameworks described above and are not reiterated in this section.

Cactus Custody

Trust Whitepaper

2. Matrixdock

In *real-world asset (RWA)* scenarios, particularly those involving tokenized physical assets such as precious metals, trust requirements extend beyond on-chain controls and smart contracts. They rely on structured operational governance, disclosure mechanisms, and verification arrangements spanning issuance, custody, and ongoing operations.

Within RWA-related business activities, BIT's RWA platform *Matrixdock* does not rely on a single entity or technical component as the sole basis of trust. Instead, it applies a multi-layered assurance model combining governance arrangements, technical controls, and third-party participation to support *transparency and verifiability*. Key elements include:

2.1 Physical asset custody and disclosure arrangements

Physical assets are typically held by qualified third-party custodians. Matrixdock applies defined custody and disclosure frameworks to support verification of custody status, quantities, and asset attributes within agreed parameters, based on reports and validation provided by custodians and auditors.

2.2 On-Chain Transparency & Verifiability

Matrixdock leverages the transparency and auditability of blockchain infrastructure to enable independent verification of issuance, circulation, and token-to-asset correspondence, supporting visibility for users and counterparties.

2.3 Third-Party Participation & Support

Trust in RWA scenarios is supported by the participation of multiple independent parties, including custodians, auditors, and verification service providers, helping to establish clear responsibility boundaries across on-chain and off-chain components.

These asset-level transparency and verification arrangements operate in conjunction with system-level controls, audit, and compliance mechanisms to address the specific assurance requirements arising at the intersection of on-chain and off-chain trust.

Matrixdock

Trust Whitepaper BIT

VI. Multi-Layer Audit and Assurance Model

BIT's disclosed audit and assurance arrangements reflect a multi-layer assurance framework structured in accordance with the Three Lines of Assurance model:

1. First layer: Operational and Management Systems (ISO)

Supporting standardized operations, data governance, and security management aligned with international standards.

2. Second layer: Independent Control Assurance (SOC/ External Audit)

Providing third-party verification of control design and operating effectiveness.

3. Third layer: Asset-Level Transparency and Verifiability (RWA/Matrixdock)

Combining custody arrangements and on-chain verification to support real-world asset tokenization scenarios.

By integrating international standards-based audits, independent third-party assurance, annual financial audits, and internal audit mechanisms, BIT establishes a structured and verifiable trust foundation across different business lines and risk layers.

This framework emphasises the ***independence and complementary function of different assurance mechanisms***, avoids reliance on any single audit or certification, and supports informed due diligence by institutional clients, regulators, and ecosystem partners.

Trust Whitepaper
BIT

Conclusion

This *Trust Whitepaper* provides a structured presentation of the trust-related systems, governance arrangements, control environments, and third-party verification mechanisms that BIT has established and continues to operate across the dimensions of security, compliance, transparency, and verifiability. Through structured articulation of key areas including risk governance, compliance and regulatory foundations, security architecture and asset protection mechanisms, and audit and assurance frameworks, the paper is intended to serve as an understandable, comparable, and verifiable due diligence reference for institutional clients, regulators, and ecosystem partners.

In digital asset and technology-driven financial services environments, ***trust is not the result of any single measure or isolated mechanism***. Rather, it emerges from the sustained and coordinated operation of ***multiple institutional arrangements*** over time. BIT's practices demonstrate that a stable trust foundation requires clear allocation of responsibilities and boundaries at the governance level, embedded risk identification and control mechanisms at the process level, executable security and monitoring capabilities at the technical level, and independent audit and assurance to provide external verification. These elements are interdependent and mutually reinforcing, together forming an institutional foundation capable of operating sustainably as business scale, technological environments, and regulatory requirements evolve.

From a ***risk governance*** perspective, BIT treats risk management as an institutional capability rather than a post-event control tool. Through defined risk classification, articulated risk appetite, and structured organizational governance, risk identification, quantification, monitoring, and response are embedded across the full business lifecycle. This approach supports a long-term balance between business innovation, capital efficiency, and client protection. It provides an overarching framework within which specific controls and technical measures can operate consistently within defined risk boundaries.

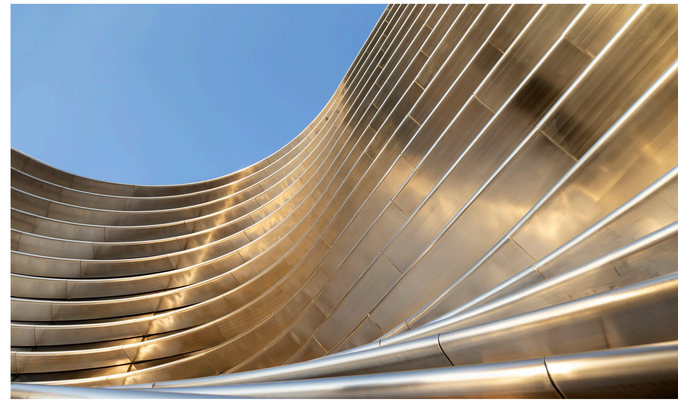
At the ***compliance and regulatory*** level, BIT establishes the legal and supervisory boundaries applicable to its business activities through multi-jurisdictional regulatory arrangements, established AML/KYC policies and procedures, and ongoing compliance governance. A risk-based approach is applied across key areas, including client onboarding, transaction monitoring, and ongoing due diligence. These arrangements serve not only to meet regulatory obligations but also to provide a foundation of regulatory verifiability for institutional clients and partners.

At the ***security and asset protection*** level, BIT embeds security capabilities systematically across governance, processes, and engineering practices. Through architectural principles such as Zero Trust and Defense-in-Depth, combined with key management, custody controls, monitoring mechanisms, user security protections, and security culture initiatives, BIT has established a multi-layered protection structure. This security framework is not static, but is continuously evolved through institutional and engineering processes to address changing threat landscapes and technological risks.

At the ***audit and assurance*** level, BIT applies a multi-layered and complementary verification structure. By combining ISO management system audits, independent SOC assurance, annual financial audits, and internal audit mechanisms, BIT avoids reliance on any single audit or certification as the sole basis of trust. Clearly defined disclosure scopes and applicability boundaries support fact-based due diligence. In business scenarios involving coordination between on-chain and off-chain components, such as RWA, asset custody and disclosure arrangements, on-chain query mechanisms, and third-party participation provide supplementary transparency and verifiability at the asset level, enabling system-level controls and asset-level verification to operate in coordination.

As outlined above, BIT's approach to building trust is grounded in the alignment of governance structures, risk management, security engineering, and independent assurance. Together, these elements form a resilient, institutional-grade framework designed to safeguard client assets and support stable operation under adverse market or operational conditions.

As market environments, regulatory frameworks, and technological conditions continue to evolve, the relevant systems, controls, and verification mechanisms will likewise be refined. What this *Trust Whitepaper* presents is ***not a final or static state***, but a trust foundation that is designed to operate continuously, to be examined, and to evolve over time. Within applicable legal and compliance frameworks, BIT will continue to maintain and update this foundation through ***governance, control, and independent verification mechanisms***.



Glossary

A

AICPA Attestation Reports

Independent assurance reports issued under American Institute of CPAs (AICPA) attestation standards, including SOC reports.

Annual Financial Audit

An independent audit is conducted on an annual basis to assess financial statements in accordance with applicable regulatory requirements and auditing standards.

AML (Anti-Money Laundering)

A regulatory and compliance framework designed to prevent, detect, and report money laundering and related financial crime.

AR (Appointed Representative)

A regulatory status in the UK for a firm operating as an appointed representative under the Financial Conduct Authority (FCA).

B

Bid-Ask Spread

The difference between the price at which a buyer is willing to purchase an asset and the price at which a seller is willing to sell it.

Bug Bounty Programme

A formal vulnerability disclosure programme offering rewards for validated security findings.

C

C&ED (Customs and Excise Department)

The Hong Kong authority responsible for the registration and AML supervision of DPMS Category A entities.

Cactus Custody

An institutional digital asset custody platform operated by BIT that provides secure storage infrastructure for digital assets.

CDD (Customer Due Diligence)

Due diligence is performed on customers, authorised representatives, connected parties, and beneficial owners as part of the AML/CFT policy framework.

CFT (Countering the Financing of Terrorism)

Measures and controls designed to identify, prevent, and report the financing of terrorist activities.

Cold Wallet

An offline wallet is used for the secure storage of digital assets. Because it remains disconnected from the internet, it reduces exposure to cyber threats and is typically used for long-term asset storage.

Concentration Risk Monitoring

Monitoring of risk concentration as part of market risk measurement alongside VaR, stress testing, and liquidity indicators.

D

Defense-in-Depth

A layered security approach designed to provide multiple levels of protection rather than relying on a single control.

DPMS Category A (Dealer in Precious Metals and Stones)

A Hong Kong registration category for dealers in precious metals and stones.

DPT Service (Digital Payment Token Service)

A regulated activity under Singapore's Payment Services Act relating to services involving digital payment tokens.

E

EDD (Enhanced Due Diligence)

Additional due diligence procedures are applied to higher-risk customers or relationships, including factors such as PEP status, high-risk jurisdictions, adverse media, or elevated transaction risk.

F

FCA (Financial Conduct Authority)

The United Kingdom's financial regulatory authority is responsible for supervising financial services firms and markets.

FINMA

The Swiss financial supervisory authority is responsible for regulating financial institutions and asset managers.

FinCEN (Financial Crimes Enforcement Network)

The US Financial Crimes Enforcement Network is responsible for regulating and supervising Money Services Businesses (MSBs).

FIPS 140-3 Level 3

A security standard specifying requirements for cryptographic modules used to protect sensitive information.

Four-Eyes Principle

A control principle requiring at least two authorized persons to participate in critical operations to reduce single-point error and internal operational risk.

G

GMC (Gelephu Mindfulness City)

A special administrative and financial centre initiative in Bhutan associated with financial innovation and digital asset regulation.

H

HSM (Hardware Security Module)

A dedicated hardware device designed to securely generate, store, and manage cryptographic keys.

HTTPS

A secure communication protocol used to encrypt data transmitted between systems over the internet.

I

Independent Testing

Periodic independent reviews or audits are conducted to assess the effectiveness of an AML/CFT programme and related control mechanisms.

Internal Audit Framework

A structured internal governance system is used to evaluate risk management, internal controls, and operational processes through audit activities and continuous monitoring.

ISO 9001 (QMS)

Quality Management System standard covering the design, development, delivery, and operational processes of digital asset custody services.

ISO 27001 (ISMS)

Information Security Management System standard covering the information security management framework supporting custody services; scope defined by the approved Statement of Applicability (SoA).

ISO 27701 (PIMS)

Privacy Information Management System standard extending privacy management requirements based on ISO/IEC 27001, covering data controller roles and customer information processing compliance within internal operations.

K

KYC (Know Your Customer)

Customer due diligence procedures are used to verify the identity of customers and assess their risk profile in accordance with regulatory requirements.

KYT (Know Your Transaction)

A transaction monitoring process used to screen and analyse transaction activity in order to identify suspicious patterns and potential financial crime risks.

L

Least Privilege

A security principle that limits system access rights to the minimum necessary for users to perform their roles.

Liquidity Risk Indicators

Indicators used to monitor liquidity risk, including bid-ask spreads.

L

Loan-to-Value (LTV)

A financial ratio used to measure the proportion of a loan relative to the value of the collateral securing it.

M

MAS (Monetary Authority of Singapore)

The central bank and financial regulatory authority of Singapore responsible for supervising financial institutions and financial services activities.

MFA (Multi-Factor Authentication)

A framework requiring multiple authentication factors for account login and critical actions; supported methods include UKey, passkeys, and authenticator-based verification.

Matrixdock

BIT's real-world asset (RWA) platform supports the issuance and transparency of tokenized assets through governance, technical controls, and third-party verification.

ML (Money Laundering)

A financial crime involving the concealment of the origins of illegally obtained funds.

MLRO (Money Laundering Reporting Officer)

An appointed officer responsible for overseeing AML/CFT compliance and reporting suspicious activities to relevant authorities where required.

MSB (Money Services Business)

A US regulatory classification for entities engaged in money transmission or other financial services activities.

N

Net Exposure Limit

A risk management parameter used to limit the total exposure that may arise from lending or trading activities.

O

Operational Risk

The risk of loss resulting from inadequate or failed internal processes, systems, human factors, or external events.

P

Passkey

A passwordless authentication method that uses cryptographic keys to verify user identity.

PEP (Politically Exposed Person)

An individual who holds or has held a prominent public function may present a higher money laundering or corruption risk due to their position or influence.

Proliferation Financing

The provision of funds or financial services used to support the proliferation of weapons of mass destruction.

R

Risk Appetite

The level and type of risk that an organization is willing to accept in pursuit of its strategic objectives.

Risk Committee

A governance body appointed by the Board of Directors, providing oversight of business activities and capital/liquidity planning.

S

Sanctions Compliance

Screening and controls consistent with applicable sanctions regimes, including obligations related to proliferation financing, within the AML/CFT programme.

SoA (Statement of Applicability)

A document used in ISO 27001 information security management systems to define applicable security controls and their implementation status.

SOC 1 Type II Report

An independent assurance report providing assurance over the design and operating effectiveness of internal controls relevant to user-entity financial reporting over a defined assessment period.

SOC 2 Type II Report

An independent assurance report providing assurance over controls within the custody-related IT environment, assessed against applicable Trust Services Criteria (including security, availability, and confidentiality).

S

SOP (Standard Operating Procedure)

Documented procedures that define standard processes and actions to be followed in operational or risk management scenarios.

SRO (Self-Regulatory Organization)

A self-regulatory organization authorized to supervise certain financial service providers within its jurisdiction.

Stress Testing

A risk management technique used to evaluate the resilience of portfolios or financial systems under extreme but plausible adverse scenarios.

T

TCSP (Trust or Company Service Provider)

A licensing regime in Hong Kong for entities providing trust or company formation and management services.

TF (Terrorist Financing)

The provision or collection of funds with the intention that they be used to support terrorist acts or organisations.

TM (Transaction Monitoring)

A process used to analyse transaction activity over time in order to identify suspicious patterns or potential financial crime risks.

Travel Rule

A requirement (where applicable) for transmitting required originator/beneficiary information between VASPs/financial institutions.

Trust Services Criteria

A set of criteria used in SOC 2 assessments to evaluate controls related to security, availability, confidentiality, processing integrity, and privacy.

U

UKey

A hardware-based authentication device used as part of multi-factor authentication.

V

VaR (Value at Risk)

A quantitative risk measure estimating the potential loss of a portfolio over a specified time horizon at a given confidence level.

VQF (Financial Services Standards Association)

A Swiss self-regulatory organization (SRO) recognised by FINMA for the supervision of financial intermediaries under Swiss anti-money laundering regulations.

W

Whitelisting Mechanism

A security control that restricts system actions to pre-approved addresses, users, or processes.

Z

Zero Trust

A cybersecurity architecture model based on the principle that no user or system should be trusted by default.

BIT

WWW.BIT.COM