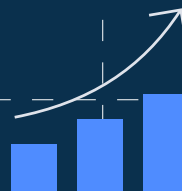


Banking on Stablecoins

A risk mitigation blueprint for
financial institutions



With the recent passage of the [GENIUS Act](#), the regulatory landscape for [stablecoins](#) is rapidly evolving, bringing greater clarity and driving more traditional financial institutions to engage with digital assets. In a swiftly changing financial ecosystem, banks are becoming more active in the development, issuance, and integration of stablecoins – a [cryptocurrency](#) designed to maintain a stable value by pegging its price to a reserve asset, such as fiat currency or commodities.

Historically cautious about digital assets, traditional financial institutions now recognize the utility of stablecoins to modernize payments, retain customers, and compete with fintech challengers in the blockchain space. This shift is being further accelerated by growing regulatory clarity, exemplified by the US Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act.

As banks begin facilitating [fiat-backed](#) stablecoin payments – both for retail customers and B2B transactions – they face a broad spectrum of risks. Stablecoins offer the promise of faster, programmable payments. But regulators warn they come with new risks in areas like credit, liquidity, operations, and reputation that go beyond the traditional banking space.

In this paper, we take a closer look at four key risk categories related to stablecoins and provide a mitigation framework for each – covering **people** (roles/skills), **processes** (controls/governance), and **technology** (tools/vendors) needed to ensure secure and compliant stablecoin operations.

RISK CATEGORY 1

Mitigating regulatory and compliance risk

Stablecoin payments raise complex regulatory and compliance challenges. Chief among these are [anti-money laundering \(AML\)](#) and [sanctions](#) risks, since stablecoins can move outside traditional banking networks and potentially be exploited by illicit actors.

Banks must also navigate evolving regulatory frameworks and expectations, and ensure consumer protection obligations are met when offering stablecoin services. Regulators explicitly expect banks to uphold stringent AML/CFT (combating the financing of terrorism) controls and consumer protection requirements in any crypto or stablecoin activities, underscoring the need for robust compliance risk management.

To counter regulatory compliance risks associated with stablecoins, financial institutions should ensure the following people, processes, and technologies are in place.

People to have in seat

- Dedicated **compliance officers** (with crypto compliance expertise and training) and to oversee AML/KYC ([Know Your Customer](#)) programs
- **Legal counsel** versed in financial regulations and digital assets to interpret new stablecoin laws
- **Regulatory affairs specialists** to monitor guidance from central banks and agencies
- **Internal auditors** to periodically review crypto-related compliance controls

Processes to put in place

- Implement comprehensive **KYC and customer due diligence** for all stablecoin users (verifying identities and wallet ownership)
- Conduct ongoing **transaction monitoring** and **suspicious activity reporting** for stablecoin flows
- Screen all transactions and wallet addresses against **sanctions lists** and high-risk indicators
- Ensure compliance with the **FATF Travel Rule** by collecting and transmitting required originator/beneficiary information for stablecoin transfers
- Establish **clear policies** on which stablecoins are supported (favoring fully reserved, regulated stablecoins) and require thorough due diligence on stablecoin issuers
- Maintain consumer protection measures such as **clear disclosures** to retail customers about stablecoin risks (e.g. not FDIC-insured, potential loss of value) and procedures for error resolution

Regular compliance audits and staff training on crypto-specific risks should continually reinforce these processes.

Technology to invest in

- **Blockchain intelligence tools** to trace and flag illicit or suspicious on-chain activity in real time
- **Automated screening systems** that integrate with core banking and wallet platforms to check for sanctions or blacklisted addresses before processing stablecoin payments
- Robust **identity verification platforms** – particularly during onboarding – and solutions for Travel Rule compliance to securely share required sender/receiver data with other institutions
- Integrated **case management systems** that can connect fiat and digital asset activity into a single, holistic customer profile view

RISK CATEGORY 2

Mitigating cybersecurity risk

Supporting stablecoins introduces new considerations for banks, particularly in the areas of cybersecurity and blockchain infrastructure. As institutions engage with digital wallets, private keys, and APIs connected to blockchain networks, it's essential to ensure strong safeguards are in place. While these components represent valuable access points, banks are well-positioned to secure them through tested IT protocols and emerging best practices in blockchain security.

Protecting against threats like phishing, unauthorized transactions, or vulnerabilities in smart contracts requires a thoughtful approach – combining traditional cybersecurity expertise with new tools tailored to the blockchain environment. With the right investment in technology, controls, and talent, banks can not only manage these risks but lead in building a secure, trusted digital asset ecosystem.

People to have in seat

- A strong **information security** team led by a **chief information security officer (CISO)**, with staff experienced in cybersecurity and blockchain systems (e.g. crypto security engineers, wallet specialists)
- **Security architects** to design hardened wallet and key management systems, **DevSecOps engineers** to secure any smart contract or API integrations, and **incident response experts** to handle breaches
- Blockchain-savvy IT **auditors and risk managers** to continually assess vulnerabilities

Additionally, regular training should be provided to all staff (including customer-facing teams) on phishing awareness and the safe handling of cryptographic keys.

Processes to put in place

- Establish rigorous security protocols for all stablecoin-related operations. This includes **multi-factor authentication** for system access and transaction initiation, and **multi-person approval** workflows for transfers above set thresholds to prevent a single point of failure
- Conduct regular penetration tests and **vulnerability assessments** on wallet platforms, blockchain nodes, and related applications to identify weaknesses
- Maintain an up-to-date **incident response plan** tailored to crypto incidents (e.g. procedures for managing a compromised private key or responding to a blockchain network attack), and drill this plan periodically
- Enforce the **principle of least privilege** and segregation of duties – for example, require that one employee initiates a stablecoin transaction and another independently reviews/approves it, so no individual can unilaterally control funds
- Ensure there are **backup and key-recovery** procedures to prevent loss of access

TRM IN ACTION

In the event of an exploit or loss of funds, TRM supports financial institutions in mitigating and recovering the loss of assets through multiple tools and recovery paths, including:

Automated alerting

TRM's Detect module enables institutions to continuously monitor wallet activity, including both hot and cold storage, delivering real-time alerts when funds move in or out of any selected wallet. This ensures compliance teams can be alerted and respond to potential security incidents or hacks the instant funds move unexpectedly.

Collaboration with issuers

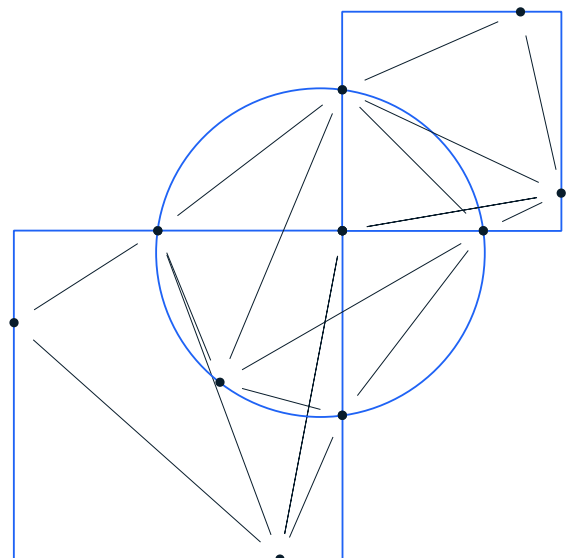
The [T3 Financial Crime Unit](#) is a groundbreaking partnership between TRON, Tether, and TRM, designed to assist asset issuers in identifying, freezing, and seizing illicit assets – irrespective of where those funds are in the digital asset ecosystem. T3 works closely with law enforcement, and since its inception has frozen over USD 200 million in illicit assets.

Collaboration with VASPs

TRM works closely with the largest VASPs, in conjunction with law enforcement authorities around the world, to facilitate real-time network communication to freeze stolen assets before funds are cashed out. TRM recently assisted one the largest financial institutions in the world in recovering over USD 25 million dollars that were stolen from a bank customer.

Technology to invest in

- Deploy strong cryptographic key management solutions; for example, **Hardware Security Modules (HSMs)** or multi-party computation (MPC) wallets to secure private keys. Many banks opt for institutional-grade digital asset custody platforms like **Fireblocks**, which provide MPC key protection and policy-based access controls.
- **Whitelisting of withdrawal addresses**, tiered approval requirements, and tamper-resistant audit trails
- Ensure that all integrations with blockchain networks (nodes, RPC endpoints) are secured via **encryption and access controls** (VPNs, allow-listed IP addresses)
- **Transaction risk scoring** tools that can identify suspicious patterns (e.g. sudden large stablecoin transfers) and halt them for review



RISK CATEGORY 3

Mitigating operational risk

Operational risk arises from the internal processes, systems, and third parties on which stablecoin transactions rely. Unlike traditional payment systems, stablecoin operations depend on blockchain networks and external issuers, introducing new points of failure and complexity.

Technical bugs, human error, or process gaps could lead to lost or misrouted funds, delays, or an inability to serve customers. For example, stablecoins may have technical vulnerabilities or dependencies on decentralized networks and [smart contracts](#), and banks rely on third-party platforms or stablecoin issuers to process and redeem tokens. High transaction volumes (especially in retail) and the 24/7 nature of crypto markets also stress operational capacity.

People to have in seat

- A dedicated **digital asset operations manager** to coordinate stablecoin-related workflows
- **Operations staff** trained in blockchain transaction handling (e.g. understanding block confirmations, address formats, potential error scenarios), so they can support customers and internal needs
- **Risk managers** involved in setting operational limits and monitoring compliance procedures
- **IT personnel (or vendors)** who manage the uptime and performance of blockchain nodes or APIs that the bank uses
- A **business continuity planner or resilience officer** to incorporate stablecoin scenarios into the bank's disaster recovery plans

Processes to put in place

- **Standard operating procedures (SOPs)** for all stablecoin payment activities. For example, have clear steps for accepting a stablecoin deposit from a customer (address generation, confirmation checks, crediting customer account after sufficient block confirmations), and for initiating a payout (address verification, required approvals, and post-transaction reconciliation).
- Dual control and verification for critical tasks (e.g. **whitelist approved recipient addresses** and require multi-person sign-off for large or high-risk transfers to avoid mistakes or fraud)
- End-to-end reconciliation of stablecoin transactions with **internal ledgers** – ensure that the amount of stablecoins held in custody matches customer balances and fiat reserve movements at all times
- Perform regular **stress tests and drills** (e.g. simulating a surge in stablecoin withdrawals or a failure of a key third-party system) to identify bottlenecks
- Appropriate **due diligence and oversight of any third-party service providers** (custody tech, blockchain node providers, etc.), ensuring they have strong uptime records and incident response commitments

Technology to invest in

- Utilize reliable **infrastructure and platforms** to support stablecoin operations. This might include running your own blockchain nodes or using reputable node-as-a-service providers to ensure consistent connectivity to the stablecoin's network.
- Integrate an **operations dashboard** that provides real-time visibility into pending transactions, confirmations, and system health
- Employ workflow management tools (potentially features within custody platforms like Fireblocks or others) that enforce **segregation of duties and approval policies** on transactions (e.g. the system will not execute a large stablecoin transfer until the required two authorized approvals are registered, as per the rules configured)
- **Alerting and exception management software** to quickly detect failures (such as a transaction that hasn't been confirmed within expected time or a deviation in balance reconciliations)
- Maintain **redundant systems** for critical components (e.g. a backup wallet solution or a secondary connectivity provider for the blockchain network) to seamlessly take over if the primary fails

RISK CATEGORY 4

Mitigating liquidity and counterparty risk

Fiat-backed stablecoins are meant to be redeemed 1:1 for fiat currency, but banks must consider liquidity and counterparty risks associated with this promise.

Liquidity risk refers to the ability to readily convert stablecoins to cash (or vice versa) without delay or loss of value. In normal conditions, a stablecoin may function as a cash equivalent. But under stress (e.g. a run on the stablecoin or a market panic), it's uncertain whether the token can be promptly redeemed for cash at par. This uncertainty was highlighted by the [temporary de-pegging](#) of major stablecoins during recent market turmoil.

Banks involved in stablecoin payments also face **counterparty and credit risk**: they rely on the stablecoin issuer to maintain adequate reserves and honor redemptions. If an issuer's reserves are incomplete, illiquid, or held with risky custodians, the stablecoin's value could falter, impacting the bank and its customers. In effect, users and banks must trust the issuer's integrity and stability.

People to have in seat

- **Treasury and liquidity management teams** to monitor stablecoin exposures and ensure convertibility. Treasury specialists and asset-liability management (ALM) officers should treat stablecoins similarly to other short-term assets, tracking inflows/outflows and potential liquidity gaps.
- **Risk managers** (credit risk and market risk analysts) to evaluate the financial health of stablecoin issuers and any reserve attestation reports
- A dedicated **relationship manager or due diligence officer** to liaise with the stablecoin issuer or its banking partners to understand their reserve management practices

Senior management and the board's risk committee should also be aware of and set **risk appetite limits** for stablecoin activities (e.g. how much stablecoin the bank or its clients can hold relative to capital).

Processes to put in place

- Establish a robust **risk assessment framework** for any stablecoin supported; this includes performing due diligence on the issuer
- Set conservative **internal limits on stablecoin holdings or exposures** (for example, limit the total volume of a particular stablecoin the bank will hold on balance sheet or handle for clients unless certain conditions are met)
- Incorporate stablecoin scenarios into the bank's liquidity **stress testing** – for instance, model a situation where a stablecoin issuer temporarily suspends redemptions or a wave of customers convert stablecoins to cash, and ensure the bank could meet those outflows
- **Have contingency plans:** If a stablecoin loses its peg or faces a run, the bank should be ready to communicate with clients (to prevent panic), possibly facilitate conversions through alternate channels (like using exchanges or market makers to liquidate stablecoin holdings), or even temporarily pause support for that stablecoin if necessary
- Maintain **close communication with the stablecoin's issuer** or ecosystem partners, so the bank gets early warning of any issues (like reserve impairments or regulatory actions) that could affect liquidity
- Incorporate stablecoin liquidity and counterparty risk into the bank's **overall risk governance** (e.g. include it in regular risk reports and review at risk committee meetings) and ensure compliance with any emerging regulatory standards on stablecoin risk management (such as capital or liquidity buffers for stablecoin holdings)

TRM IN ACTION

The inherent transparency of public blockchain networks enables institutions to have increased visibility into the behavior and performance of digital assets – insight that is critical for managing liquidity and counterparty risk.

For fiat-backed stablecoins, this visibility translates into real-time access to indicators that are traditionally opaque in fiat finance. Banks and risk teams can use blockchain analytics tools like TRM to observe:

- **Circulating supply and rate of issuance or redemptions**, allowing institutions to assess if the supply is expanding rapidly (which may signal growing risk exposure) or if there are signs of an ongoing redemption wave (which may indicate stress or loss of confidence)
- **Transactional activity** – such as the number of active wallets, transaction volumes, and velocity of transfers – which offers clues into market demand, utility, and potential speculative behavior
- **Wallet-level holdings and flows**, making it possible to understand how stablecoins are distributed across users and entities – whether broadly dispersed or concentrated in a few wallets
- **Concentration risks** – by identifying if a significant portion of circulating supply is held by a small number of entities, which could pose systemic exposure if those wallets were to redeem simultaneously
- **Cross-exchange and cross-chain flows**, which provide early indicators of shifts in liquidity or attempts to exit a given ecosystem

These data points feed directly into treasury monitoring, stress testing, and counterparty due diligence processes. They help banks validate whether on-chain behavior aligns with the issuer's off-chain disclosures – especially reserve attestations – and whether reserve activity appears consistent with the stated 1:1 backing.

TRM empowers teams to convert this transparency into actionable insights – flagging abnormal behavior (e.g. sudden surges in redemptions), tracking institutional exposure, and helping financial institutions proactively manage risk.

Technology to invest in

- Use real-time **treasury monitoring systems** to track stablecoin positions and movements. Many banks will extend their existing liquidity management tools to include stablecoin balances, enabling triggers if, for example, stablecoin outflows exceed a certain threshold in a short time.
- Consider **integrating with the stablecoin issuer's platforms or APIs** (e.g. some issuers provide portals for institutions to mint/redeem directly) for faster conversion and visibility into the redemption process

- **Employ analytics** to watch market indicators of stablecoin health – for instance, on-chain data feeds or market price oracles that signal if a stablecoin is straying from its peg, or if large volumes are exiting (these can serve as early warning signals of stress)
- Use [blockchain intelligence](#) to help identify if a liquidity event might be driven by risk factors (such as a sudden influx of stablecoins from a risky exchange, indicating potential trouble)
- **Maintain** an updated database of information on each stablecoin the bank supports: reserve compositions, credit ratings of reserve assets, issuer’s financial reports, etc. – possibly aided by fintech data providers
- If the bank issues its own fiat-backed stablecoin or tokenized deposit, use **smart contract** technology that includes safeguards (pause functions, circuit breakers) to halt operations gracefully in extreme conditions
- Ensure the bank’s core banking or payment systems are **integrated with fiat on/off-ramp technology** (e.g. automatic minting and burning of stablecoins against fiat movements) so that liquidity can be managed smoothly, without manual delays

As banks enter the stablecoin arena to modernize payments and stay competitive, they must confront a range of emerging risks that transcend traditional financial operations. This blueprint provides financial institutions with a comprehensive framework to manage the regulatory, cybersecurity, operational, liquidity, and counterparty risks tied to fiat-backed stablecoin payments.

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM’s blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is [trusted by leading agencies and businesses worldwide](#) who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.

To learn more, visit www.trmlabs.com