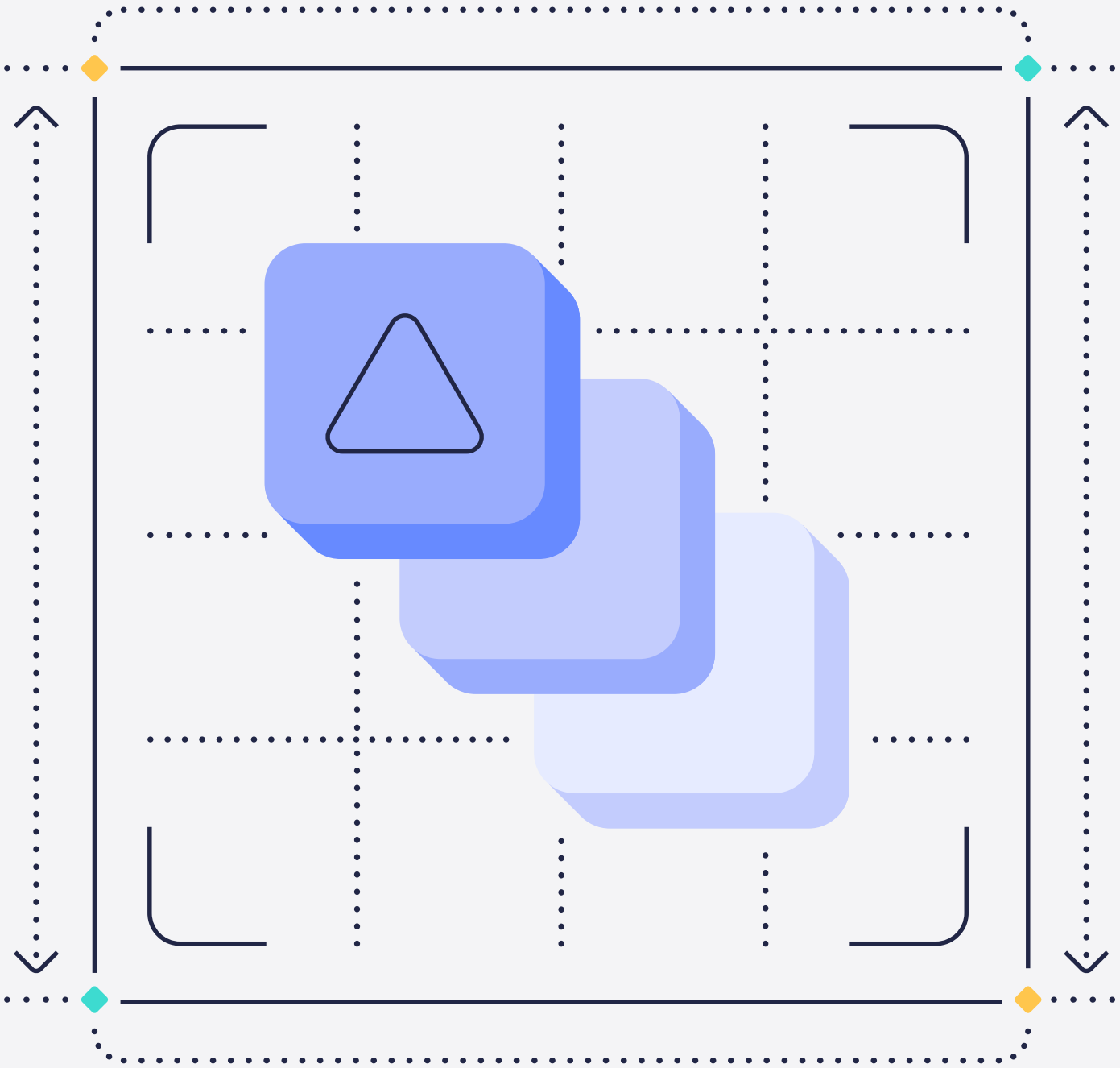
Fireblocks

# **Compliance and Risk Architecture for Banks:** A Blueprint for Building Digital Asset Operations



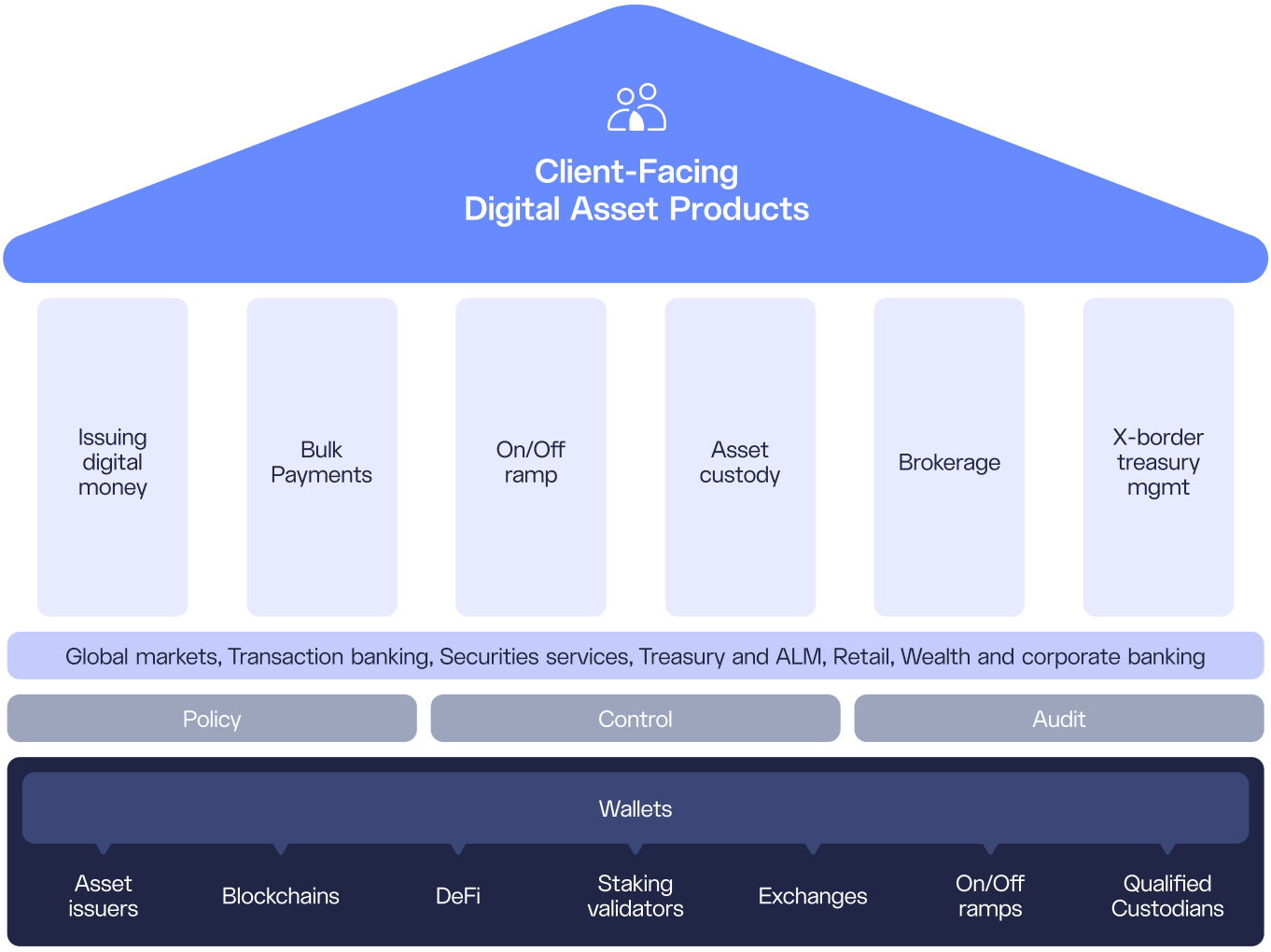
Fireblocks

# Table of contents:

Wallet Infrastructure for Banks: A Blueprint for Building Digital Asset Operations established the seven requirements for wallet infrastructure. Compliance integration is the third requirement: sanctions screening, Travel Rule, blockchain address screening, and suspicious activity monitoring.

This Blueprint covers the regulatory frameworks that need to be applied, the control domains that have to be operational before go-live, and how the architecture sits across the bank's governance structure.

While wallet infrastructure is use-case agnostic, the compliance and risk architecture that sits on top of it is not uniform. It has a common foundation: the configuration varies by use case, asset class, and jurisdiction. The architecture does not.



# Section 1: How Digital Asset Compliance Differs From Traditional Banking Controls

Only 15% of banks describe their governance infrastructure as fully production-ready, according to our 2026 Financial Grid survey. That gap is structural: banks are encountering three characteristics that their existing control frameworks weren't built for.

- **Settlement is irreversible at the protocol level.** Once a transaction reaches finality onchain, it cannot be reversed. Certain token standards and issuer-level mechanisms support recovery within defined windows, but a bank cannot rely on that systematically.
- **Control is cryptographic and direct.** Private keys govern asset movement, and the party initiating a transaction is also the party executing it. Most bank compliance frameworks assume a review step between those two moments. Here, that review has to be built into the same system that holds the keys.
- **Infrastructure runs continuously.** There's no batch window and no market close to catch an error before it compounds.

The result: controls have to be enforced automatically, at the point of transaction, before finality. After that point, recovery isn't something the bank's compliance architecture can depend on. Whether you're designing from scratch or moving from pilot to production, the compliance architecture is a design decision. Resolve it at go-live and it becomes a blocker instead.

Your bank has mature governance frameworks, established risk disciplines, and proven compliance infrastructure. The table below maps how the same control objectives are operationalized in a digital asset environment.

## Table 1: Traditional banking controls vs. digital asset controls, by domain

| Control domain | Traditional banking infrastructure | Digital asset infrastructure for banks |
|---|---|---|
| Compliance-related controls | AML, sanctions screening, and transaction monitoring operate on known counterparties through established correspondent and clearing relationships. Post-onboarding vetting controls are applied through periodic review cycles and batch monitoring. | The same obligations apply. Counterparty wallet addresses are not descriptive and not bound by correspondent relationships. Controls must operate at the point of transaction, before execution, on every operation. Blockchain address screening is an additive requirement specific to this environment. Travel Rule compliance is more challenging than traditional transaction processes because there's no correspondent relationship carrying originator and beneficiary information automatically. That data has to be transmitted separately, and counterparty VASPs don't all support the same protocol. |
| Technical and operational safeguards | Key management and access controls are enforced through established IT security frameworks, including HSMs for sensitive operations. Segregation of duties is procedural and system-enforced. | Cryptographic key management using MPC or threshold signatures distributes signing authority across multiple independent parties. HSM infrastructure may be retained and integrated. No single person, device, or system can sign a transaction unilaterally. Role-based access and quorum requirements are enforced. |
| Transaction processing | Transaction authorization is enforced through system limits, approval workflows, and manual exception handling. | Authorization must be enforced programmatically before transaction submission. User authorization policies need to evaluate every transaction against defined parameters before it reaches the network. Manual controls are unworkable at digital asset transaction speeds. Settlement is continuous and 24/7. |
| Monitoring and resilience | Security monitoring is integrated into existing SIEM environments. Operational resilience obligations are met through documented BCP/DR procedures and periodic testing. | Digital asset activities must be integrated into the bank's existing SIEM environment. Anomaly detection operates continuously. Wallet freeze capability must be available in real time. BCP/DR documentation must meet DORA or other equivalent prudential standards for critical ICT systems. |

Every domain in the table requires compliance embedded at the point of transaction. That's what lets your bank operate at digital asset speed without losing the supervisory integrity regulators expect.

# Section 2: The Regulatory Baseline Banks Need To Satisfy

Most banks with cross-border digital asset operations are subject to multiple regulatory frameworks at once. For example, a European bank with US custody operations is navigating DORA, MiCA, OCC guidance, and Basel requirements in parallel. One architecture, designed to the highest common standard across the four supervisory areas that these frameworks share, satisfies all of them together. The frameworks differ by jurisdiction. The control domains they map onto don't.

## The Converging Supervisory Standard

Across the jurisdictions where banks are building digital asset operations, regulators are applying consistent expectations in four supervisory areas:

- **Governance and Oversight.**
- **Operational Resilience**
- **Third-party Risk Management; and**
- **Financial Crime Controls.**

The specific frameworks differ by jurisdiction, but the requirements map onto the same control domains.

## Table 2: Regulatory frameworks governing bank digital asset operations by jurisdiction

| Framework | Applies to | Relevant requirements |
|---|---|---|
| OCC (United States) | National banks and federal savings associations | • OCC Interpretive Letter 1183 reestablished permissibility for custody, stablecoin activities, and participation in blockchain networks.<br>• Interpretive Letter 1184, issued in May 2025, confirmed that banks may buy and sell custodied crypto assets at a customer's direction and may outsource bank-permissible crypto activities to third parties, subject to third-party risk management.<br><br>Together, the letters confirm banks may engage in these activities without prior supervisory approval.<br>Safety and soundness expectations, operational risk, and third-party risk management requirements apply in full. |
| DORA (European Union) | EU-regulated financial entities including banks | • Article 30 establishes mandatory contractual and oversight requirements for critical ICT third-party providers.<br>• ICT risk management framework requirements, operational resilience testing, and incident reporting obligations apply. |
| MiCA (European Union) | Banks seeking CASP authorisation for crypto-asset services | • Authorisation requirements for crypto-asset service provision. |

| Framework | Applies to | Relevant requirements |
|---|---|---|
| MAS (Singapore) | Qualifying full banks and merchant banks | • MAS Notice on Technology Risk Management.<br>• Digital payment token service licensing under the Payment Services Act for banks operating relevant functions. |
| FCA/PRA (United Kingdom) | UK banks and firms offering cryptoasset services | • FSMA 2000 (Cryptoassets) Regulations 2026: FCA authorisation requirements for cryptoasset activities including custody and stablecoin issuance. Full commencement scheduled for October 2027. Authorisation application window opens September 2026.<br><br>Banks building now should design to the emerging standard: custody safeguarding, operational resilience, and financial crime controls. |
| Basel Operational Risk Framework | Internationally-active banks | Cross-cutting requirement.<br><br>Digital asset operations are subject to Basel operational risk capital requirements.<br><br>The severity of digital asset losses and the limited recovery options once a transaction reaches finality elevates operational risk exposure relative to traditional activities. |

Whatever the jurisdiction, meeting these frameworks comes down to the same question: can the bank prove, at any point, that its controls operate as designed? That's what examiners are actually testing for.

## What Supervisors Are Looking For

Regardless of jurisdiction, supervisory examinations of bank digital asset operations are focusing on the same questions:

- Can the bank demonstrate that controls are embedded in the infrastructure and enforced at the point of transaction, not applied retrospectively?
- Is there an audit trail that supports supervisory examination without manual assembly?
- Is the governance framework documented, tested, and operating as described?
- Is the bank's exposure to its digital asset infrastructure provider managed as a critical third-party risk?

These are the same supervisory concerns bank examinations have always applied, now extended to a new operating environment. The banks that pass examinations build compliance architecture as infrastructure, embedded before go-live.

# Section 3: The Four Control Domains

The table in Section 1 maps these four domains against your existing controls. Together they form the control layer that sits between the wallet infrastructure below and the governance framework above. What follows is what each one requires in practice, and what it looks like when a bank gets it wrong.

# Domain 1: Compliance-Related Controls

Digital asset operations extend the bank's existing financial crime compliance program into a new operating environment. Your obligations remain the same, but your enforcement mechanisms do not.

Onchain transactions introduce risks that traditional financial crime controls were not designed for: pseudonymous counterparties, settlement finality, and the ability to transact directly with wallets across jurisdictions without a correspondent bank intermediary. Effective compliance-related controls extend the bank's existing AML and sanctions frameworks. They operate at the point of transaction, before execution, on every digital asset operation.

## What This Domain Requires For Banks

- **AML and transaction monitoring:** Automated monitoring of onchain transaction flows integrated with the bank's existing suspicious activity reporting framework. Monitoring that operates at digital asset transaction speeds, not in batch cycles.
- **Sanctions screening:** Real-time screening of counterparty wallet addresses directly against OFAC, EU, UN, and relevant domestic sanctions lists before transaction execution.
- **Travel Rule compliance:** For banks operating as virtual asset service providers or facilitating transfers above relevant thresholds, originator and beneficiary information transmission to comply with FATF Recommendation 16 as implemented across jurisdictions. Integration with Travel Rule protocol providers such as Notabene.
- **Blockchain address screening:** Sanctions screening catches a wallet directly on a designated list. Blockchain address screening catches what that check can't: blockchain intelligence tools such as Chainalysis or Elliptic trace a wallet's transaction history for indirect exposure, funds connected to sanctioned entities, darknet markets, or high-risk exchanges, even when the counterparty address itself isn't listed.
- **KYC and counterparty due diligence:** Extension of existing customer due diligence standards to digital asset counterparties and wallet addresses used in institutional transactions.
- **Tamper-evident audit trails:** Complete, immutable records of all compliance checks performed, decisions made, and transactions executed. Required for supervisory examination and internal audit.

## What Failure Looks Like

A bank that screens counterparties at onboarding but not at the point of digital asset transaction execution has a gap that will surface in examination. The onchain environment changes faster than onboarding cycles. A counterparty that was clean at onboarding may be sanctioned or flagged by the time of a transaction six months later. Real-time screening at execution is the minimum standard.

# Domain 2: Technical and Operational Safeguards

The security architecture of the digital asset infrastructure is the CISO's primary concern and the foundation of the bank's operational risk management for digital assets. Once a transaction reaches finality onchain, a security failure isn't a recoverable incident the way a traditional IT breach might be. The control architecture must prevent loss, not just detect and respond to it.

## What This Domain Requires For Banks

- **Cryptographic key management:** MPC or threshold signature schemes that distribute key material across multiple independent parties, eliminating single points of failure. No single person, device, or system should be able to sign a transaction unilaterally. For banks with existing HSM infrastructure, integration that preserves existing hardware investments while meeting digital asset security requirements.
- **Hardware security modules (HSMs):** Hardware-based protection for key material at rest. TEE-based transaction signing that isolates the signing operation from the broader IT environment.
- **Secure Software Development Lifecycle (SSDLC):** Formal security review processes for any code that interacts with wallet infrastructure or transaction signing. Smart contract audit requirements where applicable.
- **Cryptographic audits and secure enclave operations:** Regular third-party assessment of key management architecture, cryptographic implementations, and signing operations.
- **Role-based access with quorum requirements:** No single individual should be able to initiate and approve a transaction. Access controls enforced at the infrastructure layer, not just at the application layer. Role definitions that map to the bank's existing segregation of duties framework.
- **Real-time access revocation:** The ability to immediately revoke a user's access to wallet operations in the event of a security incident, role change, or departure. Revocation that operates at the infrastructure layer, not dependent on application-level controls.

## What Failure Looks Like

Single-operator signing authority, application-layer-only access controls, and key material that can be reconstructed by a single party are the failure modes that have produced the largest digital asset losses at financial institutions. For a bank, the reputational and regulatory consequences of a custody or operational loss of this type are disproportionate. The investment in getting this domain right is the investment that prevents an existential operational event.

# Domain 3: Transaction Processing

Banks operate within risk frameworks that define what transactions are permissible, who can authorize them, and under what conditions. In traditional banking, these controls are enforced through a combination of system limits, approval workflows, and manual exception handling. Digital asset transaction speeds make manual controls unworkable at production scale. Authorization has to be enforced programmatically instead, automatically, at the point of transaction, before execution.

## What This Domain Requires For Banks

- **Programmatic authorization enforcement:** Transaction approval logic that evaluates every transaction against the bank's defined parameters before it is submitted to the network. Parameters include transaction origin and destination, asset class, counterparty risk tier, transaction volume, jurisdiction, and time of day.
- **Blockchain address screening, embedded in transaction flow:** The screening described in Domain 1 runs inline as part of transaction processing here, checked before every transaction executes, not as a separate step before or after.
- **Transaction simulation:** The ability to simulate a transaction and predict its outcome before submission. Particularly important for smart contract interactions where execution results are not always predictable from the transaction parameters alone.
- **Approval workflows:** Multi-party approval requirements enforced for transactions above defined risk thresholds. Workflow logic that maps to the bank's existing transaction authorisation framework.
- **Exception handling, connected to authorization enforcement:** When a transaction falls outside the parameters set above, it needs a defined process, not ad hoc review. Exception logging creates a complete audit trail for supervisory examination.

## What Failure Looks Like

A bank that relies on human review to enforce transaction limits at production volume is still running at pilot scale. Programmatic authorization enforcement is what converts pilot-scale manual oversight into production-scale automated control. Banks that haven't built this before go-live aren't ready for production, regardless of the quality of their wallet infrastructure.

# Domain 4: Monitoring And Resilience

Operational resilience for digital asset operations requires real-time visibility into the state of the infrastructure, the ability to detect anomalous behaviour before it results in loss, and the capacity to respond to and recover from incidents without interrupting the bank's digital asset obligations to clients and counterparties.

## What This Domain Requires For Banks

- **SIEM integration:** Integration of digital asset infrastructure events into the bank's existing Security Information and Event Management environment. Digital asset operations should not run as a parallel monitoring environment. They should be visible within the bank's existing security operations function.
- **Anomaly detection and threat intelligence:** Automated detection of transaction patterns, access patterns, and system behaviour that deviate from established baselines. Integration with threat intelligence feeds relevant to blockchain-based threats.
- **Wallet freeze capability:** The ability to immediately halt wallet operations in response to a security incident or supervisory direction. Freeze capability that operates at the infrastructure layer and does not depend on application-level controls.
- **Audit logs:** Immutable records of all system events, access operations, and transactions. Log integrity that can be demonstrated to an external auditor or supervisor without reliance on the bank's own attestation.
- **Business continuity and disaster recovery:** Key backup protocols, geographic distribution of key material, and recovery procedures that meet the bank's RTO and RPO requirements for critical systems. BCP/DR documentation that satisfies operational resilience requirements under DORA and equivalent prudential standards.
- **SLA enforcement and incident response:** Defined service level agreements with digital asset infrastructure providers that include incident response obligations, notification timelines, and escalation procedures. Incident response plans that cover onchain theft scenarios specifically, not just IT system outages.

## What Failure Looks Like

A digital asset operations environment that is not integrated into the bank's existing security monitoring is an environment the bank's security function cannot see. In a supervisory examination, the inability to demonstrate real-time monitoring of digital asset operations is a finding. In a security incident, the inability to detect anomalous behaviour before transaction finality is the difference between an incident and a loss.

# Section 4: Internal Governance Across The Control Functions

Getting the four control domains right is a technical architecture question. Getting the bank's control functions to sign off on go-live is an organizational one. The two are not the same problem, and the banks that move fastest from pilot to production are the ones that have resolved both.

At large banks, the digital asset build touches every control function, CISO, CRO, CCO, COO, and Chief Auditor. Each has sign-off authority. Each operates within its own governance structure. None of them is designed to reach collective decisions quickly.

The governance question for the digital asset build is how the bank structures the process by which all five functions reach alignment. Before the infrastructure can do that job, it has to satisfy five different sign-offs at once. The table below shows what each function needs from it.

### Table 3: One architecture, five sign-offs

| Function | What the infrastructure has to demonstrate |
|---|---|
| **CISO** | Security architecture documentation demonstrating no single points of failure in key management. SIEM integration plan. Incident response procedures covering onchain theft. Third-party security assessment of the digital asset infrastructure provider. |
| **CRO** | Operational risk assessment covering the new risk exposures introduced by digital asset operations. Risk appetite statement alignment. Capital treatment under Basel operational risk framework. Escalation procedures for risk limit breaches. |
| **CCO** | Financial crime controls documentation covering AML, sanctions, Travel Rule, and address screening. Regulatory engagement plan for relevant supervisors. Audit trail architecture demonstrating examination readiness. Regulatory change monitoring for jurisdictions of operation. |
| **COO** | Operational framework covering transaction processing workflows, exception handling, and escalation procedures. SLA framework with digital asset infrastructure providers. Operational resilience documentation meeting applicable standards. |
| **Chief Auditor** | Audit trail completeness and integrity. Third-party audit rights over digital asset infrastructure. Internal audit plan for digital asset operations. Examination readiness documentation. |

## The Governance Mechanism: Role-Based Access And Quorum As Shared Infrastructure

The single most effective mechanism for aligning the requirements of multiple control functions is building their governance requirements into the infrastructure itself. Role-based access controls, quorum requirements, and audit trails are the operational expression of each control function's governance requirements, enforced automatically.

When the CISO's requirement for no single-operator signing authority is enforced by the infrastructure's quorum logic, the CISO does not need to rely on procedural controls that may or may not be followed. When the CCO's requirement for a complete audit trail is met by the infrastructure's logging, the audit trail does not depend on manual documentation processes. When the Chief Auditor's requirement for examination-ready records is met by the infrastructure's reporting capability, audit preparation does not require a manual assembly exercise at period end.

This is the shift that moves compliance architecture from an overhead to a governance asset. The control functions' requirements, embedded in the infrastructure, become self-enforcing.

That embedding compounds across business lines. The authorization enforcement, access control framework, and audit trail architecture stay consistent whether the bank is running stablecoin payments or tokenized securities, what varies is configuration: transaction limits, approval thresholds, counterparty risk tiers, and asset-specific parameters. The governance work done for the first use case doesn't need to be repeated for the second. It only needs to be extended.

## Board-level Reporting

Digital asset operations introduce material operational risk that requires board-level visibility. The board risk committee needs a reporting framework that covers the bank's digital asset risk exposure, the operational performance of the control framework, and any material incidents or near-misses. This reporting does not need to be separate from the bank's existing operational risk reporting. It needs to be integrated into it.

Transaction volume and uptime are the metrics boards default to. The one that actually matters: whether the control framework is operating as designed, and whether the bank could demonstrate that to its regulator today.

# Section 5: Third-Party ICT Risk And Vendor Audit Obligations

Banks that rely on external providers for digital asset infrastructure are required to audit those providers directly. Certifications and periodic reporting satisfy part of the obligation, not all of it. The infrastructure that controls key management, transaction signing, and onchain connectivity is critical ICT infrastructure. This expectation isn't confined to the EU or US: DORA, OCC guidance, MAS, and the emerging FCA regime all point banks toward the same standard, a documented, ongoing audit programme that goes beyond the provider's own attestations.

## DORA Article 30: The EU Standard

DORA Article 30 makes the obligation explicit for EU-regulated banks: any provider supporting a critical or important function must be audited directly and on an ongoing basis, with minimum contractual requirements covering audit rights, service levels, security standards, incident notification, and subcontracting restrictions. Where a provider is designated a Critical Third-Party Provider under DORA's oversight framework, the bank must also cooperate with the relevant supervisory authority directly.

For banks using digital asset infrastructure providers that are subject to DORA oversight, the practical implication is a structured vendor audit programme that goes beyond standard IT security assessments. The audit scope should cover cryptographic architecture, key management practices, operational resilience, incident response capability, and subcontracting arrangements.

## The Pooled Audit Model

For most EU-regulated banks, building an independent annual audit programme for each critical ICT provider is operationally intensive: it requires internal audit resources, negotiated access to the provider's security team, and a documented evidence base that can withstand supervisory examination. The pooled audit model addresses this directly.

A shared audit conducted by an independent auditor on behalf of multiple institutions produces findings that each participating institution can rely on in its own regulatory reporting, without each institution bearing the full cost and resource burden of an independent assessment. The audit is conducted against a shared scope designed to satisfy DORA Article 30 obligations, with direct access to the provider's CISO and senior security personnel. Each participant leaves with the audit documentation and evidence base required for supervisory examination.

This model has been discussed with EU supervisors including BaFin.

## OCC And US Prudential Standards

OCC Interpretive Letter 1184 confirmed that banks may outsource bank-permissible crypto activities to third parties, subject to third-party risk management. That confirmation is the regulatory basis for treating a digital asset infrastructure provider as a third-party relationship subject to standard OCC oversight, rather than as a novel arrangement requiring separate authorization.

US-regulated banks are subject to OCC guidance on third-party risk management, which establishes expectations for due diligence, contract management, and ongoing monitoring of third-party relationships. For digital asset infrastructure providers, the OCC's expectations map closely to the DORA framework: documented due diligence on the provider's security architecture, contractual audit rights, defined incident notification obligations, and a monitoring program that is commensurate with the criticality of the service.

The OCC's focus on operational risk for digital asset activities means that the third-party risk management program for a digital asset infrastructure provider will be subject to examination. Banks should expect examiners to review the due diligence documentation, the contract terms, and the evidence of ongoing monitoring.

DORA and OCC converge on the same underlying expectation: continuous oversight of the provider, not a point-in-time certification.

## What A Bank-Grade Vendor Audit Program Looks Like

The vendor audit program for a critical digital asset infrastructure provider should cover five areas:

- **Security architecture review:** Independent assessment of the provider's cryptographic key management architecture, MPC or HSM implementation, and operational security controls. This should be conducted by a qualified third party, not solely reliant on the provider's own attestations.
- **Operational resilience:** Assessment of the provider's BCP/DR capability, geographic distribution, and recovery time objectives. Evidence that the provider has tested its recovery procedures and that the results are documented.
- **Compliance and regulatory standing:** Review of the provider's regulatory certifications, examination history, and any material supervisory findings. SOC 2 Type II certification as a minimum baseline for US-regulated banks. ISAE 3402 or equivalent for European requirements.
- **Subcontracting and concentration risk:** Documentation of the provider's subcontracting arrangements and the bank's resulting exposure to subcontractor risk. Concentration risk assessment where the provider relies on a small number of critical subcontractors.
- **Incident history and response capability:** Review of material incidents in the provider's operating history, the bank's notification of those incidents, and the provider's demonstrated response capability. Assessment of whether the provider's incident response obligations under the contract were met.

The output of this program is an ongoing evidence base the bank can present to its regulator at examination, demonstrating the third-party relationship is managed to the standard required for a critical ICT provider.

# Summary: Requirements For Bank Compliance And Risk Architecture

Your compliance and risk architecture is the control layer that determines whether your digital asset operations can go live and stay live under supervisory scrutiny. Get these seven requirements right and you have a framework that satisfies your regulators across jurisdictions, meets the sign-off requirements of every control function, and scales across every use case on your roadmap without a rebuild.

01 **Regulatory baseline mapping.** Identify the jurisdictional frameworks that apply to your operations: OCC guidance, DORA, MiCA, MAS, FCA, and Basel operational risk requirements. Map your architecture to the highest common standard across the four supervisory areas that all of these frameworks require. For banks with cross-border operations, this is not four separate compliance exercises. It is one architecture designed to satisfy all of them.

02 **Compliance-related controls.** AML and transaction monitoring operating at digital asset transaction speeds. Real-time sanctions screening and blockchain address screening at the point of transaction execution. Travel Rule compliance for cross-border transfers. KYC and counterparty due diligence extended to digital asset operations. Audit trails supporting supervisory examination.

03 **Technical and operational safeguards.** MPC-based key management eliminating single points of failure, or HSM-based key management where full control of key material is required. Multi-layered defense including hardware isolation, behavioral analytics, and proactive threat detection. Integration-compatible deployment for banks with existing HSM infrastructure.

04 **Transaction processing controls.** Programmatic authorization enforcement of the bank's risk framework at the point of transaction, before execution. Configurable parameters covering transaction origin, destination, asset class, counterparty risk tier, and volume. Transaction simulation capability. Multi-party approval workflows for transactions above risk thresholds. Complete exception logging.

05 **Monitoring and resilience.** Digital asset infrastructure events integrated into the bank's existing SIEM environment. Anomaly detection and threat intelligence. Wallet freeze capability. Immutable audit logs. BCP/DR documentation meeting applicable operational resilience standards. Incident response procedures covering onchain theft scenarios specifically.

06 **Internal governance framework.** Documented governance structure covering CISO, CRO, CCO, COO, and Chief Auditor requirements. Role-based access controls and quorum requirements that embed each function's governance requirements in the infrastructure. Single governance framework with configurable parameters across business lines. Board-level operational risk reporting integrated into existing frameworks.

07 **Third-party ICT risk management.** Vendor audit program covering security architecture, operational resilience, compliance standing, subcontracting risk, and incident history. Contractual audit rights and incident notification obligations meeting DORA Article 30 requirements and applicable US prudential standards. Ongoing monitoring program commensurate with the provider's criticality. Audit evidence base ready for supervisory examination.

## What Comes Next: The Blueprint Series Continues

Compliance and risk architecture is the control layer. Day-2 Operations, covered in the forthcoming third  Blueprint, can only be as resilient as the architecture they run on: reconciliation, regulatory reporting, and the operational disciplines that keep infrastructure performing to the standard your supervisors and clients expect.

More than 100 banks are already building their digital asset operations on Fireblocks, securing over $14 trillion in transactions across 150-plus blockchains, proven in production across every major jurisdiction.

**Reach out to one of our experts to discuss your compliance and risk architecture with our banking team.**