2026 BANKING ARCHITECTURE: A FRAMEWORK FOR OPERATIONAL RESILIENCE

Sebastien Rousseau
contact@sebastienrousseau.com
London, United Kingdom

ABSTRACT

The 2026 banking landscape is defined by three forces moving in parallel: the Digital Operational Resilience Act (DORA) has elevated legacy cryptographic debt from a hygiene concern into a board-accountable regulatory liability; the November 2026 SWIFT MT/MX cut-over renders MT103-based translation strategies obsolete, with 44% of banks off-track on the most recent industry survey; and the rise of multi-rail liquidity — SWIFT CBPR+, PSD3 / A2A, and tokenised deposits — has shifted the competitive question from which bank to which rail, under what policy.

This whitepaper presents an architectural roadmap for Corporate and Investment Banking (CIB) and corporate treasury teams to transition from legacy technical debt to an autonomous, rail-agnostic orchestration model. It proposes a three-pillar framework — the Resilience Trinity — composed of cryptographic stewardship, an ISO 20022 canonical data substrate, and multi-rail orchestration, and sets out a sequential three-phase implementation roadmap aligned with the 2026 DORA reporting cycle and the November 2026 SWIFT cut-over.

1 Executive Summary

The Digital Operational Resilience Act [1] has elevated legacy cryptographic debt — specifically stagnant, un-rotated password hashes and supply-chain-exposed C dependencies — from a hygiene concern into a board-accountable regulatory liability. Article 5 of DORA assigns explicit board accountability for ICT risk management. Stagnant Argon2id parameters, un-peppered hashes, and unvetted C foreign-function-interface dependencies are no longer technical-debt line items; they are findings waiting to be written.

The November 2026 SWIFT MT/MX cut-over renders MT103-based translation strategies obsolete. Banks still emitting unstructured remittance and address data will be surcharged on every message and cut off from MX-only correspondents. The BIS Committee on Payments and Market Infrastructures (CPMI) ISO 20022 harmonisation requirements [2] make the architectural posture clear: harmonisation is no longer a recommendation, it is a precondition for the G20 cross-border payments programme [3] targets on cost, speed, transparency, and access. By the most recent industry survey, 44% of banks are off-track for the cut-over.

The rise of multi-rail liquidity — SWIFT CBPR+, PSD3 / A2A (FedNow [4], SEPA Instant [5], RTP, and the major instant payment systems in Asia and Latin America), and tokenised deposits — has shifted the competitive question from which bank do we use to which rail does this payment go down, and under what policy. The orchestration layer, not the rail, is where margin lives.

This whitepaper sets out a three-pillar architectural framework — the Resilience Trinity — to address these three forces with a single, coherent operating model.

2 The Resilience Trinity

We propose a three-pillar framework for modernising the core banking stack: **hardened security**, **canonical data**, and **multi-rail orchestration**. Each pillar addresses one of the three converging pressures introduced above, and each is independently valuable; together they compose an end-to-end posture that survives the 2026/2027 regulatory cycle.

- **Pillar I — Cryptographic Stewardship.** The foundation. Move beyond C-based foreign-function-interface to pure-Rust cryptographic frameworks with multi-algorithm dispatch, hardware-security-module (HSM)-interlocked peppering, and `verify_and_upgrade`

semantics that re-hash on every login without user-visible downtime.

- **Pillar II — The ISO 20022 Data Substrate.** The language. Adopt an ISO-first canonical schema across every API contract, validation gate, and downstream consumer. Translate MT up to MX once at ingress and discard the MT; never carry MT downstream.
- **Pillar III — Rail-Agnostic Orchestration.** The execution. Move orchestration out of the model and into a policy-as-code engine that routes payments based on corridor, ticket size, settlement risk, and counterparty relationship — with the agent acting only within the bounds the policy defines.

The framework is deliberately modular. A bank constrained by a 2026 DORA reporting deadline can sequence the pillars to match its compliance pressure points; a bank competing for treasury mandate share can sequence them to match its commercial road-map. The dependencies run one way: Pillar II is harder without Pillar I (you cannot enforce schema integrity on a control plane whose authentication primitives you do not trust), and Pillar III is harder without Pillar II (you cannot route on machine-readable purpose codes you do not have).

3 Pillar I — Cryptographic Stewardship

The Foundation

In the era of DORA and GPU-accelerated threats, "deploy-and-forget" password hashing is a systemic liability. Cryptographic rot — stagnant Argon2id parameters, un-peppered hashes, supply-chain-exposed C foreign-function-interface (FFI) — is no longer a technical debt line; it is a regulatory finding waiting to be written.

The PHC password-hashing competition recommendations [6] and the OWASP password-storage guidance [7] both treat algorithm and parameter currency as a live operational obligation, not a one-time choice. Argon2id parameters set in 2020 are below modern GPU-resistant thresholds; a hash store last re-keyed pre-2022 should be assumed below current floor.

The supply-chain dimension matters as much as the parameter dimension. Cryptographic primitives reached through C FFI inherit memory-safety properties of their host language — which is to say, none. NIST SP 800-218 (Secure Software Development Framework) [8] treats supply-chain provenance as a first-class control. ENISA's threat-landscape reporting [9] repeatedly highlights cryptographic-library compromise as a recurring vector.

The Thesis

Move beyond C-based FFI to pure-Rust cryptographic frameworks with multi-algorithm dispatch, HSM-interlocked peppering, and `verify_and_upgrade` semantics that re-hash on every login without user-visible downtime.

Three engineering properties make this pillar work:

1. **Multi-algorithm dispatch.** The verifier inspects the PHC string at parse time, routes to the correct algorithm (PBKDF2, scrypt, Argon2id), validates the password, and — if the stored algorithm or parameter set is below the current floor — re-hashes silently with the current standard. The user-visible behaviour is unchanged. The bank's authentication estate strengthens by one record on every successful login.
2. **HSM-interlocked peppering.** The pepper is sourced from an HSM or KMS at request scope, consumed via the cryptographic library's secret parameter (*not* via string concatenation), and dropped from memory after use. A database breach alone yields nothing crackable; a key-store breach alone yields a secret with no usable target. The system loses confidentiality only if both stores fail together.
3. **Pure-Rust supply chain.** No C FFI; no unvetted transitive dependencies. The cryptographic primitives are memory-safe at the language level, audit-able at the source level, and reproducible at the build level.

DORA mapping

Article 5 of DORA [1] assigns board accountability for ICT risk management. Article 7 requires identification and protection of ICT assets supporting critical functions; Article 9 requires cryptographic-key management. A cryptographic-stewardship posture built on the three properties above gives the board a defensible answer to each: every password store is audited; every algorithm and parameter is current; every pepper is HSM-resident; every credential read is logged with cryptographic provenance.

Key reference

Sebastien Rousseau, "Securing Password Management in Enterprise Banking: Multi-Algorithm Hashing and Upgrades with hsh," 2026 [10].

4 Pillar II — The ISO 20022 Data Substrate

The Language

With the November 2026 SWIFT MT/MX cut-over, ISO 20022 [11] is the non-negotiable data substrate. It is not a migration project; it is the wiring for agentic treasury.

The structural problem with the predecessor format is data. MT103 carries 35 characters of unstructured remittance in field 70 and a free-text address in field 50K. pacs.008 carries `<RmtInf>` with structured creditor reference, `<PstlAdr>` with street, post code, town, and country code as discrete elements, and `<RgltryRptg>` for jurisdiction-specific obligations. The 2024 CBPR+ uplift [12] turned what were once "may" fields into "must" fields. Banks that translate down to MT103 lose the data they need to satisfy FATF Recommendation 16 on originator and beneficiary information [13].

Without structured `<Purp>` codes, structured `<PstlAdr>` fields, and structured `<RmtInf>` remittance, a treasury agent has nothing to reason over. It has prose.

The Thesis

Adopt an ISO-first canonical schema across every API contract, validation gate, and downstream consumer. Reject on parse, not on settlement. Stop translating MX down to MT at the edge — translate MT *up* to MX once and discard the MT.

In practical terms, an agentic treasury automatically optimises intraday liquidity positioning by reconciling structured `<Purp>` codes and remittance data against real-time funding needs — moving cash, drawing on credit lines, or holding back execution without a human in the loop. The MX message is the nerve impulse. The treasury control plane is the spinal cord. SR 11-7 model-risk governance [14] and DORA Article 5 board accountability sit on top as the central nervous system. Strip the MX away and the agents go blind.

Operational consequences

The CIB that wins on cross-border in 2026 enforces a stricter message profile than the standard requires — and rejects on parse, not on settlement. Three consequences follow:

- **Routing is data-driven.** The treasury workstation reads a pain.001 once and decides the rail per payment based on corridor, ticket size, cut-off, and counterparty relationship — without remapping the message.
- **Remittance data survives the hop.** Structured remittance fields (`<RmtInf><Strd>`) carry through correspondent legs without truncation. Auto-reconciliation rates climb because the data is no longer lost at the rail boundary.
- **Sanctions screening becomes auditable.** Structured `<Dbtr>` / `<Cdtr>` / `<DbtrAgt>` / `<CdtrAgt>` fields with Legal Entity Identifier (LEI) references [15] replace free-text name screening. Hit rates fall. Investigation queues shrink.

Key reference

Sebastien Rousseau, "From Pain.001 to Programmable Liquidity: ISO 20022 as the Autonomic Nervous System of Treasury in 2026," 2026 [16].

5 Pillar III — Rail-Agnostic Orchestration

The Execution

Treasury in 2026 is no longer about picking a bank — it is about picking a rail. SWIFT CBPR+, PSD3 / A2A, and tokenised deposits are commodity execution venues. Success lies in the orchestration layer that binds them — and in keeping that layer *outside* the agent so model risk, audit, and DORA accountability remain enforceable.

The wholesale settlement leg now splits into two structurally different token models [17]. **Bank-issued tokenised deposits** are a direct claim on the issuing bank, with settlement near T+0 inside the network. Compliance is the issuing bank's responsibility; the rail is fully regulated, fully traceable, and constrained to participants the issuer has on-boarded. **Integrated regulated stablecoin rails** are a claim on the reserve, audited under MiCA [18] or the equivalent regional regime, and settle corridors where bank-issued tokenised deposits do not yet reach. Compliance is shared between issuer, on-ramp, and off-ramp.

The two models are not competing. They are stacked. A CIB cross-border product in 2026 typically uses bank-issued tokenised deposits for the in-network leg and a regulated stablecoin for the corridor where the in-network rail terminates. The corporate sees one ISO 20022 payment. The settlement story underneath is multi-token.

The Thesis

Move orchestration out of the model and into a policy-as-code engine that routes payments based on corridor, ticket size, settlement risk, and counterparty relationship — with the agent acting only within the bounds the policy defines.

The architecture is one ingress, one canonical message, three rails, one settlement reconciliation:

1. Corporate Enterprise Resource Planning (ERP) emits a pain.001 ISO 20022 message.
2. Bank ingress schema-validates against the bank's stricter-than-CBPR+ profile; rejects on parse.

3. The policy-as-code orchestrator routes per corridor, ticket size, and counterparty relationship:
    - High-value cross-border → SWIFT CBPR+ (pacs.008).
    - Domestic instant within cut-off → A2A / Open Finance (PSD3 / FedNow / SEPA Instant / RTP).
    - In-network tokenised corridor → Tokenised deposit on permissioned ledger.
4. Settlement status returns as pacs.002, regardless of rail.
5. Auto-reconciliation consumes structured `<RmtInf>` end-to-end.

Operational discipline

The board-level question is the same one operational-risk committees have been asking since the first programmable-liquidity pilots: *who carries the credit exposure on the token, and for how long*? Tokenised deposits give a clean answer — the issuing bank, until burn. Regulated stablecoin rails give a more nuanced one — the reserve, subject to the audit cycle and redemption guarantee. A treasury team that does not document the answer per rail per corridor is carrying unmeasured credit risk on its balance sheet.

Key reference

Sebastien Rousseau, "Cross-Border 2026: ISO 20022, Open Finance and Tokenised Deposits in Corporate Treasury," 2026 [19].

6 Architectural Implementation Roadmap

Three sequential phases. Each is independently valuable; together they compose the Resilience Trinity end-to-end. The roadmap maps directly to the 2026 DORA reporting cycle, the November 2026 SWIFT MT/MX cut-over, and the 2027 deepening of programmable-liquidity adoption signalled by the BIS Project Agorá workstream [20].

Phase 1 — Audit and Secure

Remediate cryptographic rot using memory-safe primitives to meet DORA resilience mandates.

- Inventory every password store, key-derivation-function parameter set, and cryptographic library — including indirect C dependencies behind FFI layers.
- Migrate to a pure-Rust cryptographic framework with `verify_and_upgrade` dispatch, HSM-interlocked peppering, and audit-grade key-rotation telemetry.
- Document the migration as a DORA Article 5 board-accountable change and as a NIST SP 800-218 supply-chain control [8].

Exit criterion: no password store on legacy parameters; no cryptographic primitive reached through unaudited FFI; every login executes a `verify_and_upgrade` path; every pepper is HSM-resident.

Phase 2 — Standardise

Align internal API contracts with canonical ISO 20022 schemas to ensure data fidelity end-to-end.

- Define a stricter-than-CBPR+ message profile and reject on parse at every internal boundary.
- Translate MT up to MX once at ingress; never carry MT downstream.
- Verify `<Dbtr>` / `<Cdtr>` / `<DbtrAgt>` / `<CdtrAgt>` carry LEI references end-to-end [15] so sanctions screening becomes auditable rather than heuristic.
- Run dual-running CBPR+ validation against live correspondent traffic for at least one quarter before the November 2026 cut-over to surface field-usage drift.

Exit criterion: 95%+ auto-reconciliation rate on cross-border flows; zero MT-only outbound traffic; LEI coverage validated across the top-20 corridors.

Phase 3 — Orchestrate

Deploy a rail-agnostic control plane that treats SWIFT CBPR+, A2A / PSD3, and tokenised deposits as commodity execution venues governed by policy-as-code.

- Document credit-exposure profiles per rail per corridor.
- Bind the agent to the policy, not the rail.
- Wire SR 11-7 model-risk governance [14] and DORA Article 5 accountability into the orchestration layer, not the model.
- Treat tokenised deposits and regulated stablecoin rails as stacked, not competing — the corporate sees one ISO 20022 payment regardless of the settlement story underneath.

Exit criterion: every corridor is routable via at least two rails; every rail has a documented credit-exposure profile and a policy-as-code routing rule; every agent action is auditable as a function of policy state, not model state.

7 Internal Review Summary

The section below is the executive page of the briefing, written for stakeholders running architecture, risk, and treasury modernisation programmes.

Purpose

This document provides a cohesive architectural framework for addressing the systemic risks and infrastructure requirements facing Tier-1 banking and corporate treasury functions in 2026. It is intended for Architecture Review Boards (ARB), Risk Committees, and Digital Transformation steering groups.

Executive Challenge

The industry is navigating three converging pressures:

1. **Regulatory liability.** DORA [1] has elevated legacy cryptographic debt — specifically stagnant, un-rotated password hashes and supply-chain-exposed C dependencies — to a critical regulatory finding.
2. **Structural data shifts.** The November 2026 SWIFT MT/MX cut-over renders MT103-based translation strategies obsolete. Banks failing to implement an ISO-first data substrate face material margin erosion through correspondent surcharge schedules and message-rejection cost.
3. **Orchestration complexity.** The rise of multi-rail liquidity — SWIFT CBPR+, A2A / Open Finance (PSD3), and tokenised deposits — has shifted the competitive burden from "accessing a rail" to "orchestrating across rails".

Proposed Resilience Trinity

A modular modernisation strategy built on three pillars:

- **Pillar I — Cryptographic Stewardship.** Move from vulnerable legacy C libraries to memory-safe, pure-Rust implementations with HSM-integrated peppering. Satisfies DORA resilience mandates and eliminates a documented class of supply-chain attack vectors.
- **Pillar II — The ISO 20022 Data Substrate.** Transition from "translation-at-the-edge" to an ISO-first canonical data model. Enables the machine-readable purpose, remittance, and regulatory data required by agentic treasury engines.
- **Pillar III — Rail-Agnostic Orchestration.** Adopt a policy-as-code orchestration layer that separates execution rail from payment logic. Minimises credit-risk exposure and maximises capital efficiency across corridors.

Strategic Objectives for 2026 / 2027

- **Compliance.** Fully remediate cryptographic rot to align with 2026 DORA standards by Q4 2026.
- **Operational efficiency.** Achieve 95%+ auto-reconciliation rates by enforcing strict CBPR+ ISO 20022 schemas across all corporate Application Programming Interface (API) endpoints.
- **Risk management.** Document credit-exposure profiles for every settlement rail and corridor used by the treasury control plane.

Conclusion

This framework transitions banking infrastructure from a maintenance-heavy cost centre to a programmable, resilient, audit-ready treasury machine. The three referenced articles — cryptographic stewardship [10], ISO 20022 as autonomic substrate [16], and cross-border multi-rail orchestration [19] — detail the technical implementation for each pillar, including code-level patterns, sequence flows, and the multi-rail orchestration trace.

Distribution Note

This document is intended for internal use by technology and risk-architecture teams evaluating modernisation roadmaps. For live code implementations and repository access, see the digital appendix at `sebastienrousseau.com`.

About the Author

Sebastien Rousseau is a senior banking technologist with 20+ years of experience across HSBC Commercial & Investment Bank, PayPal, Barclays, and Shazam. He specialises in applied AI, ISO 20022 migration, post-quantum cryptography for financial services, and the structural transformation of wholesale payments. He writes at `sebastienrousseau.com` and publishes the *Banking On Quantum* newsletter at `news.bankingonquantum.com`.

References

[1] European Parliament and Council. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). Official Journal of the European Union, 2022. URL `https://eur-lex.europa.eu/eli/reg/2022/2554/oj`. Application date 17 January 2025; cited Articles 5, 7, 9.

[2] Bank for International Settlements, Committee on Payments and Market Infrastructures. Harmonised ISO 20022 data requirements for enhancing cross-border payments. CPMI Papers No. 230,

2023. URL https://www.bis.org/cpmi/publ/d230.pdf.

[3] Bank for International Settlements, Committee on Payments and Market Infrastructures. Enhancing cross-border payments: building blocks of a global roadmap. CPMI Papers No. 193, 2020. URL https://www.bis.org/cpmi/publ/d193.htm.

[4] Federal Reserve. FedNow Service — ISO 20022 implementation guide, 2024. URL https://explore.fednow.org.

[5] European Payments Council. SEPA Instant Credit Transfer (SCT Inst) rulebook, 2024. URL https://www.europeanpaymentscouncil.eu/document-library/rulebooks/sepa-instant-credit-transfer-rulebook.

[6] Password Hashing Competition. Argon2 password hashing algorithm and parameter guidance, 2015. URL https://www.password-hashing.net. Selected as the PHC winner; parameter floors updated by RFC 9106.

[7] OWASP Foundation. Password Storage Cheat Sheet, 2024. URL https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html.

[8] National Institute of Standards and Technology. Secure Software Development Framework (SSDF) Version 1.1. Technical Report NIST SP 800-218, U.S. Department of Commerce, 2022. URL https://doi.org/10.6028/NIST.SP.800-218.

[9] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024 — supply-chain vector analysis, 2024. URL https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends.

[10] Sebastien Rousseau. Securing Password Management in Enterprise Banking: Multi-Algorithm Hashing and Upgrades with hsh. sebastienrousseau.com, 2026. URL https://sebastienrousseau.com/2026-06-22-hsh-zero-downtime-cryptographic-stewardship-rust-banking-2026.

[11] International Organization for Standardization. ISO 20022 Financial services — Universal financial industry message scheme. Technical report, ISO, 2022. URL https://www.iso20022.org. Multi-part standard; pacs.008 / pacs.009 / pain.001 message definitions.

[12] SWIFT. Cross-Border Payments and Reporting Plus (CBPR+) usage guidelines, 2024. URL https://www.swift.com/standards/iso-20022/iso-20022-programme. Mandatory November 2025; co-existence ends November 2026.

[13] Financial Action Task Force. International standards on combating money laundering and the financing of terrorism — Recommendation 16 on wire transfers, 2023. URL https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html.

[14] Board of Governors of the Federal Reserve System. SR 11-7 Guidance on Model Risk Management, 2011. URL https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm. Foundational guidance still in force as at 2026.

[15] International Organization for Standardization. ISO 17442 Financial services — Legal entity identifier (LEI). Technical report, ISO, 2020. URL https://www.gleif.org/en/about-lei/iso-17442-the-lei-code-structure.

[16] Sebastien Rousseau. From Pain.001 to Programmable Liquidity: ISO 20022 as the Autonomic Nervous System of Treasury in 2026. sebastienrousseau.com, 2026. URL https://sebastienrousseau.com/2026-06-23-iso-20022-pain001-programmable-liqu

[17] Trade Treasury Payments. Automation, contingency rails, ISO 20022 and stablecoins — the 2026 trends reshaping corporate finance and B2B payments, 2026. URL https://tradetreasurypayments.com/articles/automation-contingency-rails-iso-2002

[18] European Parliament and Council. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). Official Journal of the European Union, 2023. URL https://eur-lex.europa.eu/eli/reg/2023/1114/oj.

[19] Sebastien Rousseau. Cross-Border 2026: ISO 20022, Open Finance and Tokenised Deposits in Corporate Treasury. sebastienrousseau.com, 2026. URL https://sebastienrousseau.com/2026-06-24-cross-border-iso-20022-open-finance

[20] Bank for International Settlements. Project Agora: cross-border payments with tokenised commercial bank deposits and central bank money, 2024. URL https://www.bis.org/about/bisih/topics/fmis/agora.htm.