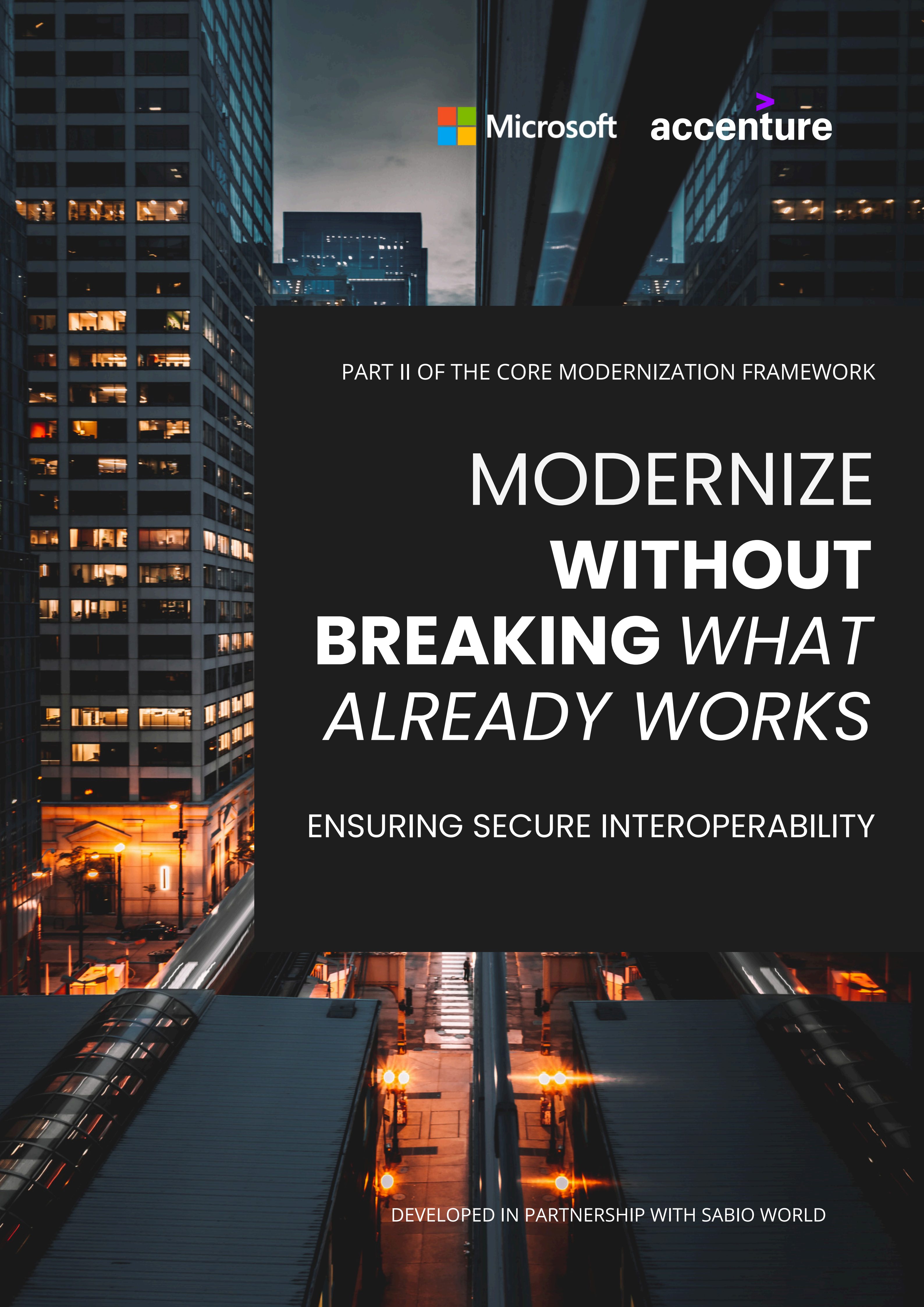


PART II OF THE CORE MODERNIZATION FRAMEWORK

MODERNIZE **WITHOUT BREAKING** *WHAT ALREADY WORKS*

ENSURING SECURE INTEROPERABILITY

DEVELOPED IN PARTNERSHIP WITH SABIO WORLD

WHY COEXISTENCE, NOT REPLACEMENT, DEFINES

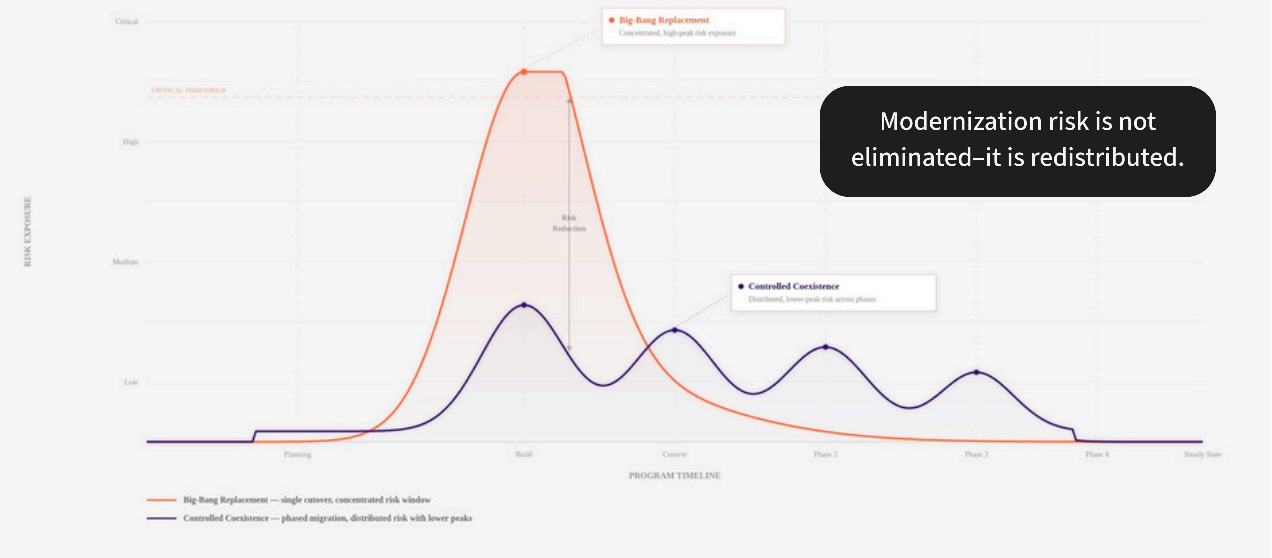
PLATFORM MODERNIZATION

Banks are transitioning toward modern, componentised banking platforms—not simply swapping one core system for another. This shift reflects a fundamental change in how modernization is conceived: from monolithic replacement to the progressive construction of a modular, service-based platform capable of continuous evolution.

Yet modernization does not occur in greenfield environments. It occurs alongside legacy platforms that already process billions of transactions, support critical products, and satisfy regulatory obligations every day.

These systems may be constrained and expensive, but they work.

For regulated financial institutions, destabilizing live operations is not an acceptable trade-off for innovation. Modernization must therefore proceed in a way that reduces risk at every step, rather than introducing new sources of systemic exposure.



Modernization risk is not eliminated–it is redistributed.

At the same time, advances in automation, Generative AI, and emerging agentic technologies are materially changing what is feasible. AI-assisted engineering, intelligent testing, and automated configuration reduce delivery risk and accelerate timelines. Platform modernization is now faster, cheaper, and more achievable than in previous generations.

None of this, however, removes the central constraint: Live operations must not be destabilized.

For this reason, the defining challenge of modernization is not adopting new technology. It is ensuring secure, auditable, and reversible interoperability between legacy systems and the emerging modern platform.

This is why secure interoperability—not architectural elegance—is the defining success factor of platform-based core modernization.

BANKS BUY

INTEROPERABILITY

Not technology

Modern core platforms promise flexibility, speed, and configurability. Cloud-native architectures offer elasticity and continuous innovation. APIs enable modularity. AI and analytics unlock new possibilities for decisioning, personalization, and automation.

Yet when modernization moves from concept to execution, CIOs, COOs, CROs, and regulators ask a more fundamental question: How does the new platform coexist safely with what we already have?

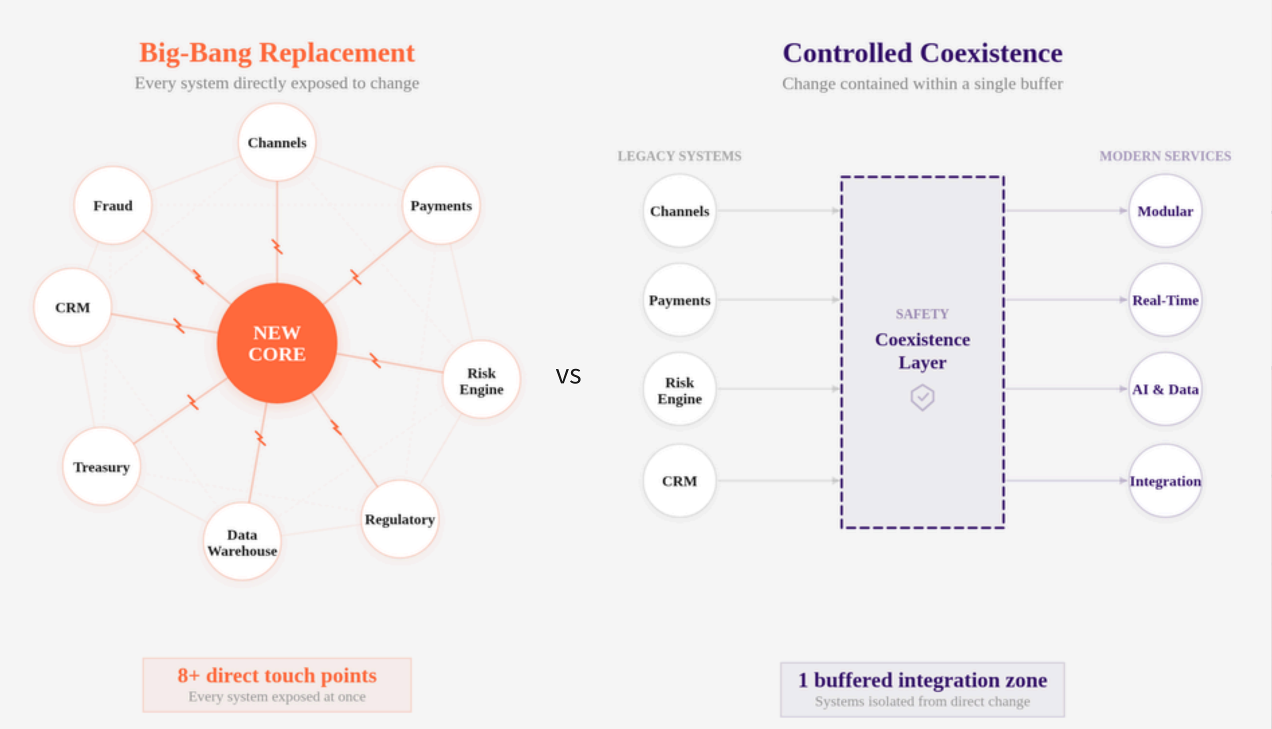
This question reflects a hard-earned lesson across Asia-Pacific: Modernization programs fail not because target architectures are flawed, but because interoperability is treated as an integration problem rather than a governance problem.

Interoperability must be:

- Secure by design
- Auditable at all times
- Reversible during transition
- Resilient under stress

Without these properties, modernization introduces new operational and regulatory risks rather than mitigating existing ones.

Banks therefore do not buy technology for its own sake. They buy confidence that new and legacy systems can operate together safely, predictably, and transparently over an extended transition period.



Big-Bang Replacement

Every system directly exposed to change

Controlled Coexistence

Change contained within a single buffer

8+ direct touch points

Every system exposed at once

1 buffered integration zone

Systems isolated from direct change

Coexistence does not reduce complexity–it reduces exposure.

INTEROPERABILITY IN A

COMPONENTIZED

PLATFORM WORLD

In a modern banking platform, capabilities are decomposed into modular, loosely coupled components:

- Product engines
- Pricing and fees services
- Customer and party services
- Ledger components
- Risk and decisioning services
- Channel orchestration layers

During transition, some of these components will be modern, while others remain on legacy platforms.

Interoperability, therefore, is not a temporary bridge. It becomes the fabric that allows mixed-generation components to function as a single logical platform.

This has two important implications:

1. Interoperability must be designed as a permanent enterprise capability, not a short-term migration artifact.
2. Governance of interoperability becomes as important as governance of credit, liquidity, or capital.

> Interoperability serves as the permanent backbone for integrating diverse banking components, necessitating robust governance on par with credit and capital management

THE

SAFETY BUFFER

Modernising without Live Exposure

A core element of the Modernization Safety Architecture is the **Safety Buffer**: a controlled environment that allows modernization to proceed without exposing live operations to unvalidated change.

The Safety Buffer includes several mutually reinforcing mechanisms:

- Digital twins that replicate production environments, data flows, and transaction patterns without touching live systems
- Parallel run capabilities that allow new services or platform components to operate alongside legacy platforms, validating performance, accuracy, and resilience
- Controlled integration layers with full observability, enabling precise monitoring of latency, failure points, and data consistency
- Explicit rollback and stop-loss mechanisms, ensuring that any migration step can be reversed without cascading impact

Together, these mechanisms allow banks to learn and adapt at speed, while preserving operational stability.

In many core banking programs, digital twin capabilities are implemented through an emulation or abstraction layer that mirrors legacy behaviors while allowing individual modules to be replaced transparently behind the interface.

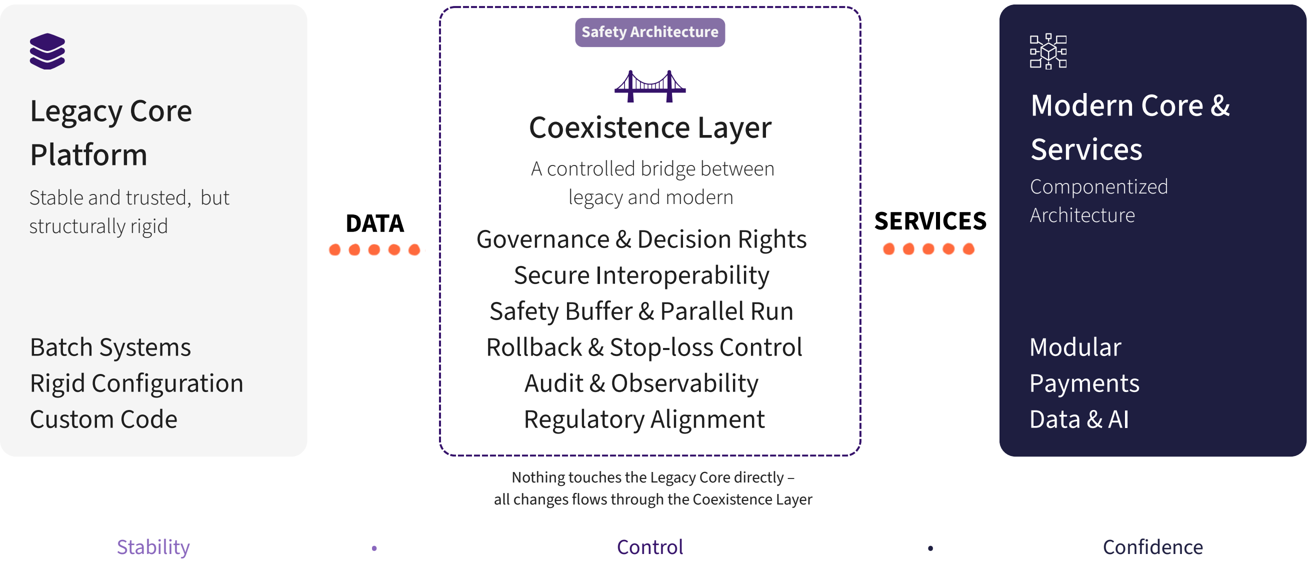
Importantly, the Safety Buffer is not a one-time construct. It becomes a permanent institutional capability that supports future change, regulatory testing, and innovation initiatives long after initial migration phases are complete.

MODERNIZATION IS NOT REPLACEMENT

IT IS A **SAFE TRANSITION**

How banks modernize the core safely, without disruption – ensuring stability while enabling continuous change

Figure 1: The Modernization Journey – from legacy stability to modern services, without disruption



Legacy Core Platform

Stable and trusted, but structurally rigid

Batch Systems
Rigid Configuration
Custom Code

DATA

Safety Architecture

Coexistence Layer

A controlled bridge between legacy and modern

Governance & Decision Rights
Secure Interoperability
Safety Buffer & Parallel Run
Rollback & Stop-loss Control
Audit & Observability
Regulatory Alignment

Nothing touches the Legacy Core directly – all changes flows through the Coexistence Layer

SERVICES

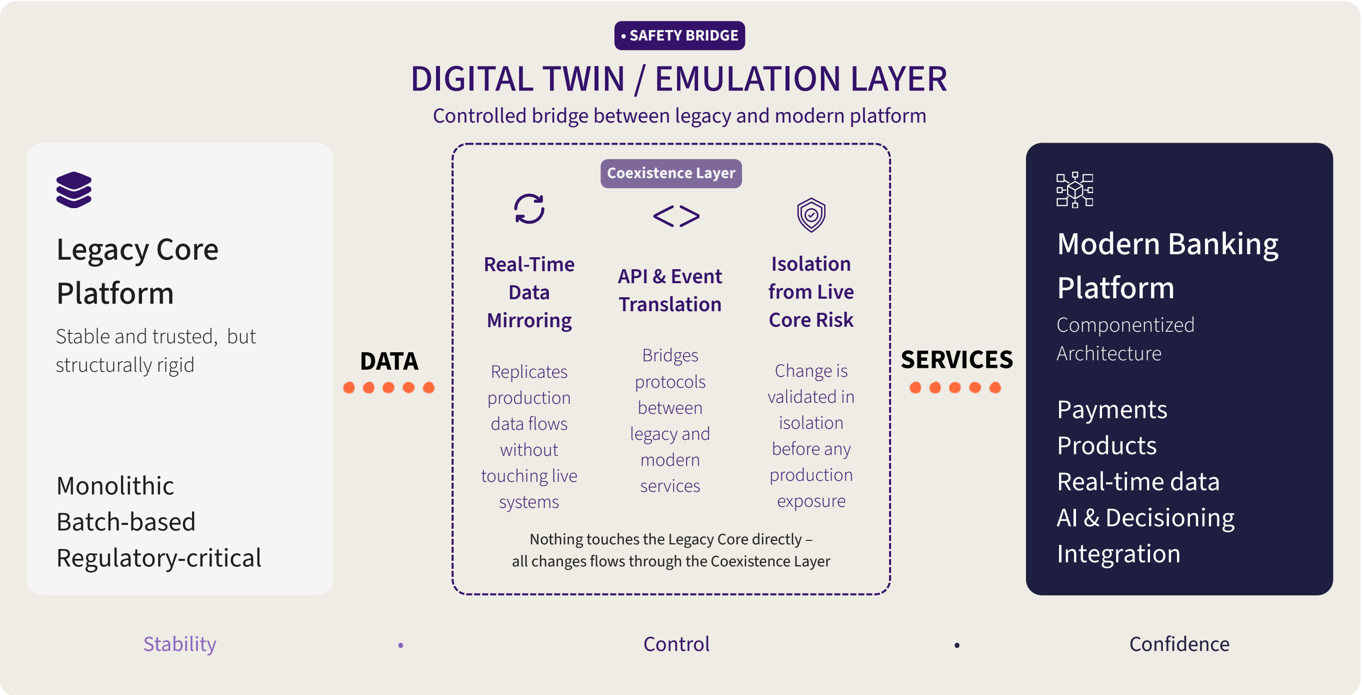
Modern Core & Services

Componentized Architecture

Modular
Payments
Data & AI

Stability • Control • Confidence

The coexistence layer is what makes safe modernisation In practice, this is implemented through a **Digital Twin / Emulation Layer**



• SAFETY BRIDGE

DIGITAL TWIN / EMULATION LAYER

Controlled bridge between legacy and modern platform

Legacy Core Platform

Stable and trusted, but structurally rigid

Monolithic
Batch-based
Regulatory-critical

DATA

Coexistence Layer

Real-Time Data Mirroring

Replicates production data flows without touching live systems

API & Event Translation

Bridges protocols between legacy and modern services

Isolation from Live Core Risk

Change is validated in isolation before any production exposure

Nothing touches the Legacy Core directly – all changes flows through the Coexistence Layer

SERVICES

Modern Banking Platform

Componentized Architecture

Payments
Products
Real-time data
AI & Decisioning
Integration

Stability • Control • Confidence

Figure 2: The Digital Twin / Emulation Layer – the safety bridge that enables coexistence

New capabilities connect to the safety buffer while the live core continues operating uninterrupted

INTEROPERABILITY AS A

RISK MANAGEMENT DISCIPLINE

Interoperability is often discussed in technical terms—APIs, middleware, event buses. In practice, however, its most critical dimensions are organizational and procedural.

Effective coexistence requires banks to treat interoperability as a risk management discipline, governed with the same rigor as credit, liquidity, or operational risk.

Key elements include:

- Clear ownership of integration points, with named accountability for data flows and failure modes
- Consistent security and resilience standards enforced across both legacy and modern environments
- Auditable data lineage, ensuring regulators and internal audit functions can trace decisions and transactions end-to-end
- Formal change management and release governance, preventing uncontrolled drift between systems

In Asia-Pacific, where regulators place increasing emphasis on operational resilience, outsourcing risk, and third-party governance, these controls are not optional. They are prerequisites for supervisory confidence.

By embedding interoperability governance into the modernization journey, banks shift from reactive risk mitigation to proactive assurance.

> Interoperability is more than a technical issue; it’s about managing risks through strict governance, clear responsibilities, and consistent standards to ensure proactive assurance and regulatory trust

COEXISTENCE OVER TIME

WHY PARALLEL OPERATIONS IS NOT A WEAKNESS

A common misconception is that prolonged coexistence between legacy and modern systems represents indecision or execution failure.

In reality, parallel operation is a deliberate risk control strategy.

Extended coexistence allows banks to:

- Validate new capabilities under real operating conditions
- Engage regulators transparently during transition
- Sequence migration according to business priorities rather than technical convenience

This approach is especially important for complex products, high-volume transaction environments, and systemically important institutions.

By designing for coexistence, banks preserve optionality. They retain the ability to pause, adjust, or redirect modernization efforts without destabilizing core operations.

WHY ONE ACCOUNTABILITY PARTNER MATTERS MORE THAN EVER

Interoperability failures are often amplified by fragmented vendor ecosystems. When multiple providers own different components—core platforms, integration layers, cloud infrastructure, and governance tooling—accountability becomes diffuse.

During incidents or regulatory inquiries, this fragmentation leads to:

- Delayed root-cause analysis
- Conflicting remediation plans
- Extended resolution timelines

A unified Accenture + Microsoft delivery model directly addresses this risk by providing:

- A shared interoperability and governance blueprint
- Clear accountability across legacy and cloud environments
- Integrated security, resilience, and monitoring capabilities
- Simplified supervisory engagement through consistent documentation and controls

For banks, this translates into reduced execution risk, faster decision-making, and greater confidence at both executive and regulatory levels.

INTEROPERABILITY AS A STRATEGIC ADVANTAGE

When governed correctly, interoperability becomes more than a defensive control.

It comes a strategic asset.

Banks that master secure coexistence can:

- Introduce new products without destabilizing operations
- Experiment safely with advanced analytics, AI, and GenAI
- Respond more quickly to regulatory change
- Evolve continuously without repeating large-scale transformation cycles

This capability distinguishes institutions that merely survive modernization from those that institutionalize change.

Closing Perspective

Modernization succeeds not when the old core is switched off, but when new and legacy systems can operate together with confidence.

By treating interoperability as a first-class design objective—supported by governance, safety buffers, and accountable execution—banks can modernize without breaking what already works.

That is the foundation of secure, resilient, and regulator-aligned platform transformation.

Executing a business-led modernization program at enterprise scale requires more than technology. It requires disciplined execution, operating-model change, and accountability over time.

Together, Microsoft and Accenture bring complementary strengths:

- Accenture leads on governance, execution discipline, and enterprise operating-model transformation, drawing on deep experience with large-scale financial services change programs
- Microsoft Azure provides a secure, resilient public cloud platform with regional APAC presence, enabling interoperability, scalability, and continuous innovation

Crucially, the partnership offers one roadmap, one shared blueprint, and one accountable partner. This unified delivery model reduces integration risk, accelerates decision-making, and simplifies regulatory engagement—critical advantages in complex, multi-year transformations.

DEVELOPED IN PARTNERSHIP WITH SABIO WORLD