Technology Trends

The technology shifts shaping a more intelligent, resilient bank

temenos

Technology built for continuous change

Technology is becoming inseparable from banks' ability to compete. AI is accelerating this shift, but the opportunity is bigger than deploying new tools. Banks need technology foundations that allow them to innovate faster, use data more effectively, adapt to regulatory change and strengthen resilience.

Technology leaders in banking innovate at nearly twice the pace of the average bank. They spend 17.5% of revenue on IT and 59.1% on growth and innovation vs 10.1% and 33.9% respectively at the average bank.[1] AI is speeding up innovation even further, with banks now wanting transformations that pay back in two to three years instead of five to ten.

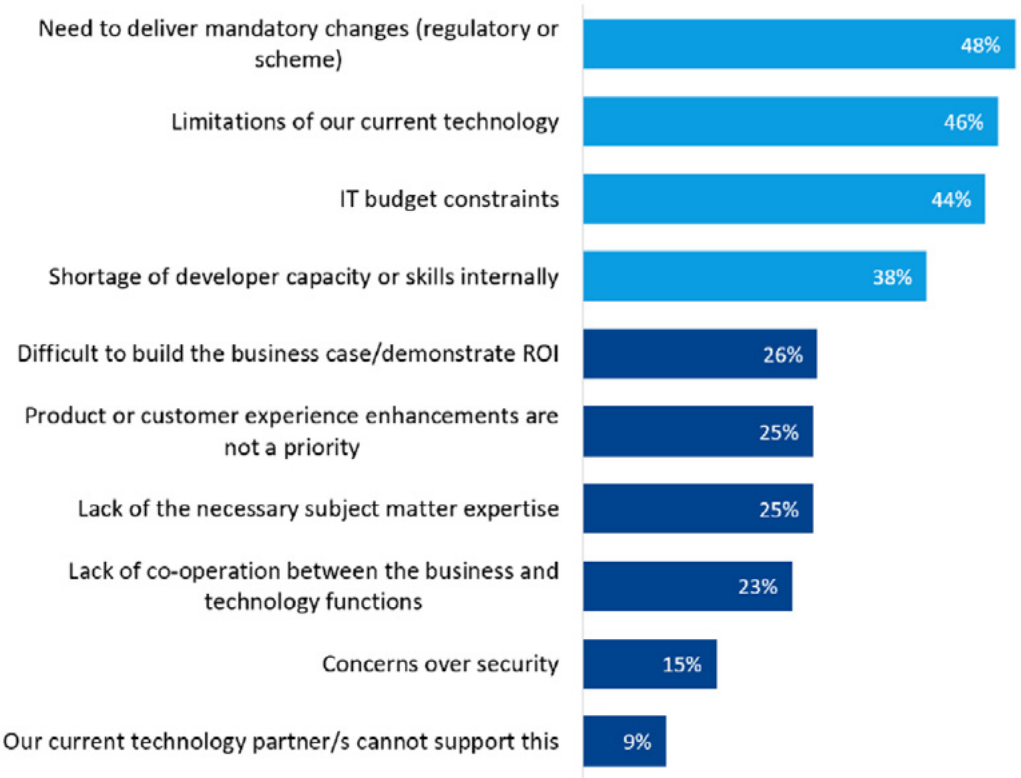
For many institutions, legacy technology remains the constraint. Complex architectures, fragmented data and batch-based processes make change slower and more expensive, whilst also limiting the real-time capabilities increasingly needed for AI and intelligent banking. Regulation is adding more pressure. Celent found that 48% of banks identify mandatory regulatory or scheme changes as a barrier to innovation.

Banks are therefore moving towards technology that is more composable, connected and intelligent. Generative AI is changing how people interact with banking systems. Agentic AI is beginning to automate more complex workflows. Cloud, APIs and modern data architectures provide the foundations for both, while progressive modernization gives banks a way to move forward without the risk associated with big-bang transformations.

The opportunity for banks is not simply to modernize technology. It is to build an architecture that can continue to evolve, allowing them to innovate faster without compromising resilience, security or control.

Figure 14: Top Barriers to innovation

Q: Which are the biggest barriers to delivering enhancements to your products and customer experiences?



Base: Retail banking respondents (sample: 216)
Source: Celent 2026 Global Consumer Survey 2026

[1]Temenos Value Benchmark

Ask, don’t navigate: generative AI transforms productivity

Like in many other sectors, natural language interfaces are revolutionizing productivity in banking. Generative AI is changing how business users interact with systems, replacing complex workflows and the need for multiple screens with conversational interfaces that turn data into real-time, actionable insights.

Instead of navigating endless menus or writing SQL queries, business users can ask for reports or actions in natural language and get immediate results. For example, asking the interface to “Identify customers aged 34–50 who opened a personal account and a mortgage before 2021” instantly surfaces relevant demographics for proactive engagement aimed at supporting financial wellbeing, strengthening customer relationships and potentially creating revenue opportunities. Crucially, the underlying logic or SQL is always visible, so outputs can be explained and audited. Standards such as Model Context Protocol (MCP) are also emerging to connect AI applications with context, data and tooling held across systems, without duplicating that data or embedding underlying banking logic into the AI model.

In a legacy technology environment, answering this type of query would not be feasible, and could take weeks or even months of manual effort. By spending less time searching for information, financial institutions can act on insights faster, innovate more quickly, and respond to customer needs with greater impact.

As AI adoption accelerates, regulation will increasingly shape where and how banks deploy it. The EU AI Act takes a risk-based approach, with greater requirements for designated high-risk applications. This reinforces a practical path already emerging across banking: proving value through employee productivity and operational workflows, while taking a more controlled approach to higher-risk customer-facing applications. Celent research shows banks currently favor internal and middle-office AI use cases, although more than 20% expect to expand AI into direct customer-facing applications.



But this shift goes beyond employee productivity. As customers become increasingly familiar with Claude, ChatGPT, Gemini and other AI assistants, expectations for digital banking could move from navigation towards conversation. Celent found that 68%[2] of banking consumers currently use or would use a conversational interface for open-ended banking questions and advice. Revolut’s AI initiatives offer an emerging example of this shift, showing how conversational experiences could bring support and financial insights into a natural-language interface.

The bigger question is what happens when the customer experience is no longer delivered through the bank's own channels. With banking data increasingly accessible through open banking, the bank's app may become less important than the intelligence, products and data behind it. Banks that win, will be those that extend trusted and secure experiences into the agentic channels of tomorrow, while continuing to strengthen their own digital channels. By combining differentiated products, accessible data and the best experiences across all channels, they can remain central to the customer relationship.

[2] The Banking Expectation Gap - Global Edition - Temenos and Celent

Agentic AI drives operational autonomy

While generative AI creates content based on learned patterns, agentic AI combines these capabilities with goal-driven actions to perform tasks. This is fundamentally transforming banking workflows, with AI agents able to autonomously install, run, operate and upgrade systems coupled with the necessary human oversight.

As deployments accelerate, financial institutions are expected to see clearer, more measurable ROI from large scale agentic AI implementations.

In payments, AI agents can detect and repair broken transactions in real time, identifying causes such as formatting errors. With such issues much less reliant on manual intervention, more transactions can be processed using fewer resources.

In watchlist screening, AI agents can action and resolve alerts as they arise, reducing false positives and easing workloads. Low-risk alerts are automatically assessed and cleared, allowing teams to focus on higher-risk investigations.

According to industry research, banks are most open to using agentic AI for reducing labor costs in operations (86%), followed by support (75%), and maintenance (71%). On average, labor accounts for almost half (49%) of core banking total cost of ownership (TCO), making it the largest cost category, and, currently, the greatest opportunity for agentic AI to reduce TCO.[3]

These efficiencies free human staff to focus on tasks such as handling complex customer or operational cases, investing in R&D, evaluating growth strategies and delivering empathy and judgement that automation cannot entirely replace. When combined with appropriate human oversight, agentic AI minimizes downtime, strengthens operational resilience, and supports scalability.



[3] Hanover Research for Temenos, September 2025

BAIN & COMPANY

Progressive modernization: A lower-risk path to core banking transformation



Joseph Edwin
Partner

Core banking technology modernization is a high-stakes transformation. Banks are increasingly avoiding “big bang” implementations where entire core systems are replaced simultaneously. This style of modernization is expensive, risky, and often fails. Instead, many are adopting progressive modernization, an approach where individual core components are upgraded gradually. With the evolution of integration frameworks, this approach has become more feasible as modern methods such as event-driven architecture, microservices, and domain-based decomposition are widely adopted.

Legacy core banking systems typically have a monolithic architecture. Components such as customer data, deposits, lending, and payments are tightly intertwined. As a result, there is a high risk of system-wide disruption when updating one component. A progressive modernization approach allows banks to gradually break apart the monolith by carving components into independent systems connected by application programming interfaces and events.

This approach greatly reduces the risk of system-wide disruption during transformation. Rather than taking a multi-year, all-or-nothing gamble, banks can prioritize modernizing higher-priority components such as lending while leaving other core components unchanged until needed. As decomposition progresses, the approach delivers business value earlier and more frequently. Investment is also spread over time, accelerating ROI as components go live sooner than in a traditional core replacement.

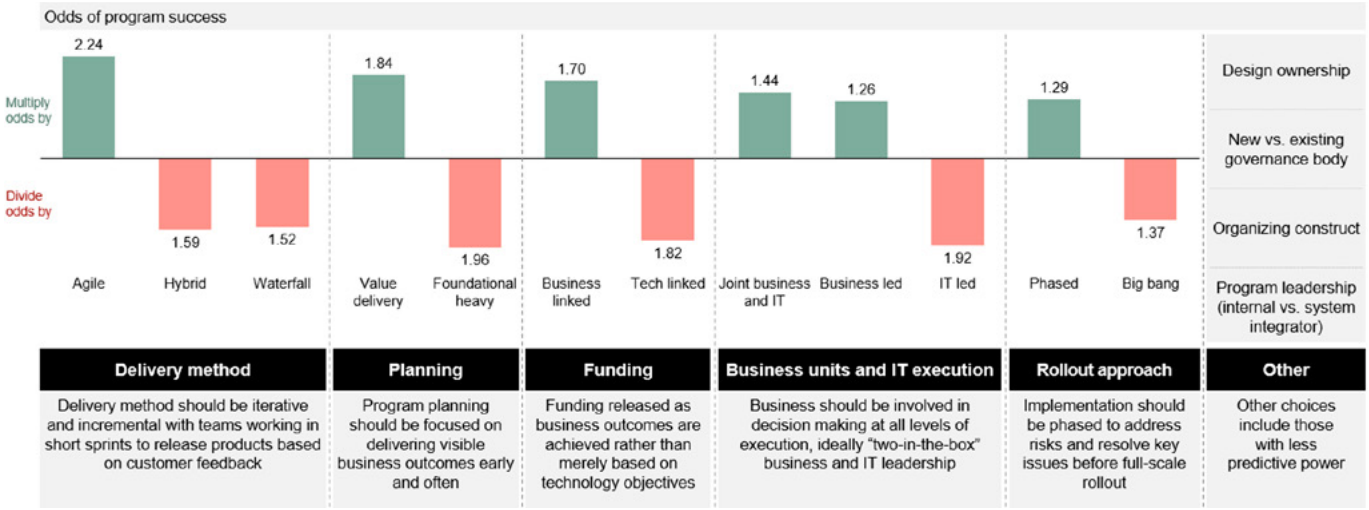


However, this approach can introduce challenges, including:

- Extended transition: Old and new systems coexist for a longer period, increasing complexity in the interim.
- Leadership fatigue: Multi-year transformations test management patience, and stopping midstream can leave technology in an even more complex state.
- Operational shift: IT teams must run more standalone systems and increase investment in systems integration.

Bain & Company's analysis of over 45 core programs found that progressive modernization is one of the top five predictors of replacement success, balancing transformation with business continuity. For banks that plan for coexistence and integration, progressive modernization offers a lower-risk path to a modern core.

Our analysis showed five choices are the strongest predictors of successful progressive modernization



Notes: Out of 46 bank programs, 36 have a clear milestone to measure success; multiplier effect to the odds of being a successful program vs. being an unsuccessful program
Source: Bain analysis

Regulation is becoming a modernization catalyst

Regulatory change is no longer simply a compliance challenge. It is increasingly testing how quickly banks' technology can adapt. Almost half (48%) of banks identify mandatory regulatory or scheme changes as a barrier to innovation. Europe's PSD3 and Payment Services Regulation illustrate the growing technology implications, with requirements spanning open banking, APIs, fraud protection and customer control over data access. Banks with real-time, API-enabled architectures will be better placed to absorb continual regulatory change without allowing compliance demands to crowd out innovation.



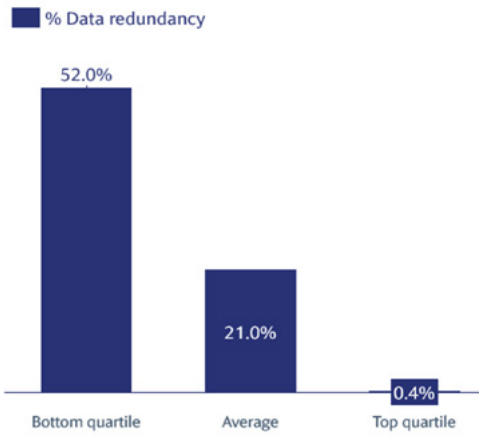
BAIN & COMPANY

Cloud and data mesh underpin the “intelligent bank”

Banks across segments are leveraging cloud platforms and SaaS to renovate fragmented back-office systems and scale for the huge volumes of data required for real-time insights and AI-driven services.

Cloud native architectures provide the elasticity, resilience, and processing power needed to handle high frequency data flows, while SaaS solutions remove reliance on legacy infrastructure and enable financial institutions to deploy new capabilities faster.

While “data is the new gold” remains true, the reality for many is much more complex. Data is often fragmented and difficult to access, making it challenging to leverage in meaningful ways. Temenos Value Benchmark data indicate that over a fifth of bank data is duplicated[4], increasing costs, reducing accuracy, and potentially limiting analytics and AI. For banks in the bottom quartile over half of their data is duplicated - potentially a huge drain on bank resources and limiting their ability to implement intelligent services in the future.



In response, financial institutions are increasingly adopting data mesh architectures to organize and extract value. Data mesh architectures are decentralized but well-governed frameworks that ensure data is organized, compliant, and accessible across all business lines, not housed in one function.

Supporting tasks like sharing real-time transaction data for regulatory reporting, data mesh architectures and cloud platforms help to establish the foundations needed to thrive in increasingly automated and AI-driven banking operations.



[4]Temenos Value Benchmark 2025

BAIN & COMPANY

Banks' cybersecurity reset: From perimeter to zero trust



Frank Fordl
Partner & Global Head of Cybersecurity



Andrew Cousins
Associate Partner & Chief Security Architect

The cybersecurity landscape is shifting rapidly, driven by the adoption of AI and advances in quantum computing. Banks' transition to modern digital banking platforms demands a transition from legacy perimeter controls to a comprehensive zero-trust approach.

Zero trust moves security from the perimeter into access decisions and continuous verification. In practice, it spans device integrity, tighter privileged workforce access, and modernized cryptography to stay ahead of AI-powered and quantum-era risks while meeting evidence-based regulatory expectations.

Mobile device access to banking services is a prime example of a zero-trust security model. Banks increasingly use app and device attestation to cryptographically confirm that banking apps are genuine and running on uncompromised devices. When paired with hardware-backed biometrics and passkeys, these controls secure account data and reduce the risk of fraud compared to legacy credential-based systems.

As banks deploy AI tools internally, they need guardrails to prevent chatbots from manipulation or sharing sensitive data. Key risks include hallucinations that produce incorrect outputs and prompt-injection attacks, where inputs are used to bypass safeguards and can result in leaked sensitive information.

In the organization, zero trust prioritizes controlling privileged access across all users. Banks should use locked-down devices for sensitive tasks and issue permissions only when necessary and for limited periods. These controls, underpinned by role-based access and timely removal as roles change, ensure that only designated personnel can access critical security platforms.

Banks also need to prepare for post-quantum cryptography by adopting cryptographic agility-upgrading encryption for secure connections and access tokens as quantum-safe standards mature, and retiring weak ciphers that allow downgrade attacks. The regulatory landscape is also demanding rigorous technical evidence and tested validation of digital operational resilience. These measures strengthen security, support compliance, and mitigate risk in the evolving quantum and AI era.



AI raises the bar for continuous security

AI is changing cybersecurity on both sides. The same capabilities that can help identify vulnerabilities faster can also enable bad actors to probe systems and exploit weaknesses at greater speed and scale. For banks, this raises expectations of their technology partners. Security can no longer rely on a static set of controls; it requires continual testing, monitoring and response as threats evolve. Technology providers will increasingly need to use AI defensively too, continuously stress-testing their platforms, identifying vulnerabilities earlier and acting quickly when exposures are found.

What this means for banks

The technology choices banks make now will determine how quickly they can respond to what comes next. AI is accelerating this shift and creating new opportunities across banking. Realizing that potential, at scale, will depend on foundations that can support continuous innovation, regulatory change and resilience without continually adding complexity.

Modernize for continuous change

Banks should move beyond thinking about modernization as a one-off transformation. AI, regulation, new products and changing customer expectations will continue to evolve. Progressive modernization, composable architectures and APIs provide a way to respond continuously, introducing new capabilities and delivering value earlier while managing the cost and risk of change.

Build intelligence into the foundation

AI will create most value when it can access reliable, connected and real-time data, rather than operating as another layer on top of fragmented technology. Banks need foundations that allow generative and agentic AI to move from isolated use cases towards capabilities embedded across the business, from operations to customer engagement.

Build for innovation, resilience and control

Banks should not have to choose between moving faster and maintaining control. As technology becomes more connected and AI more embedded across banking, security needs to be built into the architecture, not added around it. Modern foundations should enable banks to innovate while strengthening cyber resilience, protecting data and maintaining the controls needed to respond to evolving threats and regulatory requirements. The goal is not simply a modern technology estate, but one that can keep evolving securely and resiliently as the market changes.

Talk to Temenos about these trends and what they mean for your bank.

Get in touch

Explore the Banking Technology Trends series



Meet the experts



Andrew Cousins
Associate Partner & Chief Security Architect, Bain

Connect with me



Arka Biswas
Strategy Director, Temenos

Connect with me



Frank Ford
Partner & Global Head of Cybersecurity, Bain

Connect with me



Joseph Edwin
Partner, Bain

Connect with me



Kaue Tozzi
Head of Product Strategy and Partners, Temenos

Connect with me



Mathieu Charles
VP Customer Strategy, Temenos

Connect with me



Nanda Badrappan
Deputy Chief Technology Officer, Temenos

Connect with me



Philipp Rindler
Expert Associate Partner, Data Science, Bain

Connect with me



Temenos Value Benchmark

The Temenos Value Benchmark is an industry-leading program that draws on insights from more than 200 banks and 100,000 data points to help financial institutions optimize their technology investments and improve profitability. As a customer value benchmarking and advisory service, it provides C-level banking executives with unique, data-driven insights into how technology can be leveraged more effectively to drive business value. In all graphs referenced in this report, quartiles are defined and sorted per metric.

Explore the program today

temenos

About Temenos

Temenos (SIX: TEMN) is a global leader in banking technology. Through our market-leading core banking suite and best-in-class composable solutions, we are modernizing the banking industry. Banks of all sizes utilize our adaptable technology – deployed on-premises, in the cloud, or as SaaS – to deliver next-generation services and AI-enhanced experiences that elevate banking for their customers. Our mission is to create a world where people can live their best financial lives.

For more information, please visit www.temenos.com