NTT DATA

Resilience as strategy: Future-ready banking in an unstable market

From AI and digital money to quantum risk, we explore what banks must do today to be competitive tomorrow

Sections

The banking landscape in 2025: Automate or become obsolete

The name of the game in banking is optimization and advancement through technology. Industry leaders are forging ahead with technological development at a faster pace than ever before.

A willingness to assume greater risks is necessary to sustain a competitive edge, and we're already seeing this play out in the industry. More and more banking CIOs are members of the board as well as of the Group Executive Committee and giving them a "seat at the table" with significant strategic influence.

Right now, the banking landscape is being defined by four shifts in how banks operate and how customers interact with their finances. We explore these shifts and how they are forcing banks to adapt their products, services, and operations to remain competitive and relevant. Where possible, we also provide clear recommendations for banks to adopt.

> "Banks that separate their product functions from core operations, implement AI within well-defined governance frameworks, and demonstrate resilience through service level objectives (SLOs) are likely to achieve superior cost-to-income ratios and enhanced risk management.
>
> The rest might not make it."

4 shifts in banking

1. Digital currency replaces physical currency

Because of the ease and proficiency of card and online transactions, cash usage and physical bank branches have been in decline for years now. In 2023, cash accounted for 12% of UK payments (down from 14% in 2022).[1] Since 2019, the UK has lost around a third of its bank branches.[2]

As customers, our preference is to tap rather than bother with the hassle of cash and coins, even when traveling abroad. Fintechs and some banks now offer low- or zero-fee foreign exchange (FX) options.

This only strengthens the case for fully digitized money, especially given the benefits of central bank digital currencies (CBDCs) such as programmability and settlement resiliency. While some central banks in the EU and India are advancing further than the rest into design and testing, key challenges, including privacy protection, sustainable bank funding and offline functionality, are still unresolved. Wholesale adoption will likely precede retail, but momentum is undeniable, with 137 countries and currency unions now exploring CBDCs, up from just 35 in 2020.[3]

2. AI as an accelerator of innovation

What used to take years of work can now be completed in a matter of weeks with the right conditions and AI algorithms. Banks can be more responsive than ever to customer demands, regulatory requirements and cybersecurity threats by using AI to support the development of new products, services and programs.

3. Ambient banking makes financial services ubiquitous

Apps have become central to how banks do business and how customers manage their money. However, in the future of digital banking, expect ambient banking experiences across wallets, operating systems and other surfaces to front more customer journeys. Transferring money, paying for goods, and other transactions will be integrated into everyday digital experiences, not requiring a separate login or app.

4. Quantum computing introduces new risks

Gartner notes that "Asymmetric encryption is in almost all software, billions of devices worldwide and most of the communications over the internet. Yet by 2029, advances in quantum computing will make asymmetric cryptography unsafe and by 2034 fully breakable. 'Harvest-now, decrypt-later' attacks may already exist."[4] A combination of Shor's and Grover's algorithms will certainly make the majority of encryption used to protect financial data breakable. Hackers are already engaging in a process called store now, decrypt later (SNDL) — collecting and storing encrypted data with the intention of decrypting as soon as advancements in decryption technology, particularly quantum computing, make it feasible to do so.

With such significant shifts shaping both the present and future of banking, banks need to engage in technological innovation to keep pace. Financial institutions must act now, starting with securing network and data layers, piloting post-quantum cryptography (PQC), and building crypto-agile interfaces to prepare for what's next.

Recommendations

The age of the super app is over

- **Shift toward a wallet-first or ambient-banking approach, where financial services meet customers on operating systems, voice assistants and retail surfaces.**
- **Keep your app lean and focused on high-trust moments, like onboarding or dispute resolution.**
- **Redirect heavy front-end investments to platform contracts, clean exits and ongoing de-integration drills, shifting at least 15% of channel spend to these priorities.**
- **Run an annual "deintegration" test with each wallet partner.**

[1]UK Finance. UK Payment Markets Summary 2023. September 2023.

[2]The Financial Times. UK banks have closed more than one in three branches over past five years. August 2025.

[3]Atlantic Council. Central Bank Digital Currency Tracker. July 2025.

[4]Gartner. Begin Transitioning to Post-Quantum Cryptography Now. September 30, 2024.

Integrating AI in everything from CX, HR to enhancing cybersecurity

AI isn't just a new tool; it's a new way of working. For the best results, it won't be deployed as an add-on but used to rewrite systems and processes to make them more effective and better leverage human talent in the organization. We are already seeing this in the areas of customer experience, human resources and cybersecurity.

CX: The need for connection will always be there

With the decline of physical branches, the customer experience when dealing with a bank is starting a new chapter. AI can manage customer interactions, meeting the need for immediate, around-the-clock responses, with the nuance that has previously been lacking.

Agentic AI and the customer service desk

Agentic AI has driven the effectiveness of chatbots that customers can quickly and conveniently reach out to for answers. Now, it's becoming an active participant in the customer service desk.

"By 2029, agentic AI will autonomously resolve 80% of common customer service issues without human intervention, leading to a 30% reduction in operational costs, according to Gartner, Inc." With its ability to interpret a request, gather relevant data, and take appropriate action, including initiating multistep processes, it can handle many of the tasks managed by the service desk. Requests that require complex problem-solving or a sensitive approach can be managed by customer service agents.

With AI shouldering much of the workload, the service desk can speed up timelines, maintain responsiveness during busy periods, and improve cost-effectiveness.

Empathetic AI in contact centers

Beyond that is the development of empathetic AI, which will revolutionize contact centers.

"A Gartner poll of 163 customer service and support leaders conducted in March 2025 found 95% of customer service leaders plan to retain human agents to strategically define AI's role. This approach ensures a "digital first, but not digital only" strategy, avoiding the pitfalls of a hasty transition to an agentless model."

In this digital-first but not digital-only model of customer care, AI handles the triage through sentiment and prosody analysis — analyzing what customers say and how they say it to detect tone and urgency. Humans take over to handle issues like credit queries and complaints, and also step in to manage potentially vulnerable accounts. For clarity, banks should also publish a clear handoff policy.

HR

The quick evolution of AI will inevitably have an impact on what the workforce looks like and how it operates in the world of banking.

The goal by no means is to remove human talent from financial institutions altogether. As NTT DATA CEO Abhijit Dubey says, "This isn't about replacing people. It's about reshaping the role of humans, from operators to orchestrators." The idea is to deploy AI to speed up, scale and refine the accuracy of processes, and this isn't possible without human input.

Agentic AI is creating a new path for workflows, as it can make decisions, follow multistep processes and adapt to changing circumstances with minimal human intervention. It's much more autonomous, so it can be trusted with more of the workload, streamlining systems even further.

However, you still need people to create and maintain AI systems and carry out the high-value tasks that can't be automated and codified.

Cybersecurity: Faster processing, less disruption and lower costs

AI can be used to quickly process large amounts of data and find patterns and solutions. This makes it a very useful tool for hackers who are looking for new ways to bypass security defenses, decrypt sensitive data and hide the malware they are using to pose attacks.

On the other hand, AI can also be applied to identifying weak spots, predicting potential attacker methodology and accelerating threat detection, even at high volumes.

Cybersecurity threats are only getting more advanced with AI-powered attack obfuscation. AI-powered security measures are needed to counteract them, improving mean time to detect (MTTD) and mean time to repair (MTTR), phishing pass rates and model risk management (MRM).

These are three central areas of banking that can be enhanced with AI to effectively meet customer needs: speed up processing, avoid disruption and delays and save costs.

Recommendations

Cap AI deflection by quality, and do it publicly

- **Set a deflection cap tied to customer satisfaction (CSAT) and quality assurance (QA) scores, with automatic failback to humans when thresholds aren't met.**
- **Commit to it in quarterly reliability reports.**
- **Block promotion of any model whose features aren't governed by auditable data contracts with lineage and retention policies.**
- **Most importantly, put risk in the driver's seat: The CRO should have complete control over AI models, with quarterly stop-and-review drills embedded in the lifecycle.**

Check out our Chief Technology Officer (CTO) scorecard table at the end of the document

[5]Gartner. Gartner Predicts Agentic AI Will Autonomously Resolve 80% of Common Customer Service Issues Without Human Intervention by 2029. March 5, 2025.

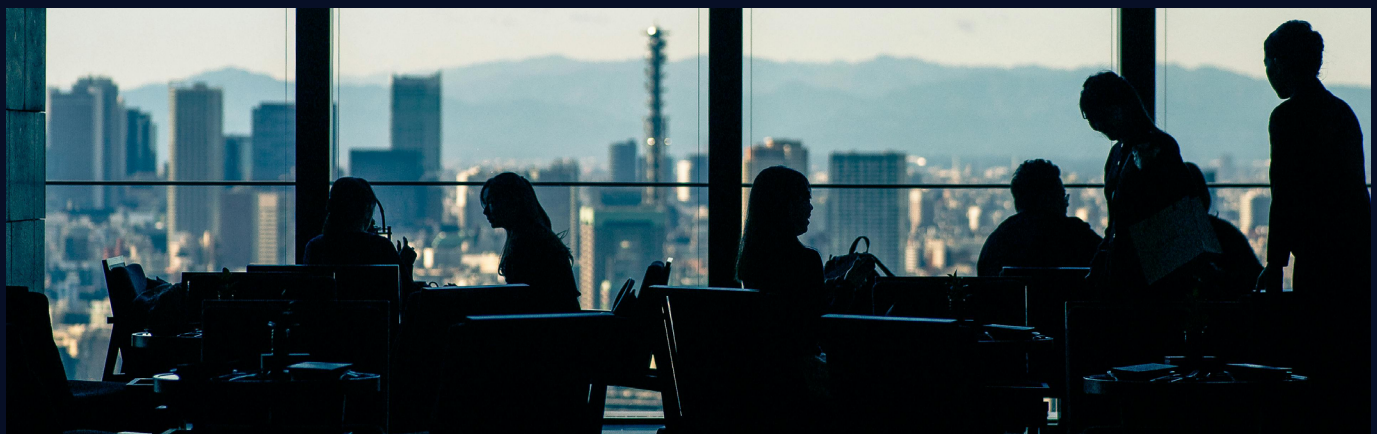
[6]Gartner. Human agents reemerge as essential components in customer service strategies amid AI integration challenges. June 10, 2025.

[7]Abhijit Dubey. The AI copilot era is already over. September 2025.

The open banking upgrade

The best way to describe today's digital advancements is that they're making banking more intuitive. The flow and convenience of banking systems and processes are greatly improved, and customers are also finding it easier to interact with banks and manage their money.

No development represents this better than the potential of open banking.



Ambient banking, the open apps of tomorrow

There's very little that customers can't do through mobile banking apps. The next barrier to convenience that's being brought down is the use of multiple contained financial apps.

All limitations considered, open banking in the UK now has more than 11.7 million active users, and over 22.1 million payments are made monthly — boosted in 2024 by voluntary funding from 20 leading firms.[8]

Although its success has been debated, what it represents is what's important: the foundation of ambient banking. In this future, financial services are omnipresent yet unobtrusive. There's one interface across accounts and flows. The interface is consented to by users, and they can revoke permissions at any time.

Variable recurring payments (VRP) and wallet integrations are the next step in the near term. While it may seem counterintuitive to open the gates to competitors, housing all banking services under one roof opens up other opportunities, such as seamless transfers between bank accounts. The technology already exists to take care of the entire switching process hands-off.

The role of mobile manufacturers

Imagine a world where you could transfer money with a tap on your smartphone. There's no need to open an app, input details and so on. That world is not far away. In this future, major mobile providers will become a UX layer, while banks stay regulated balance-sheet providers, forming partnerships with exit plans.

The best way to leverage the benefits of open banking is to help forge the path, solidifying a strong reputation in this new era.

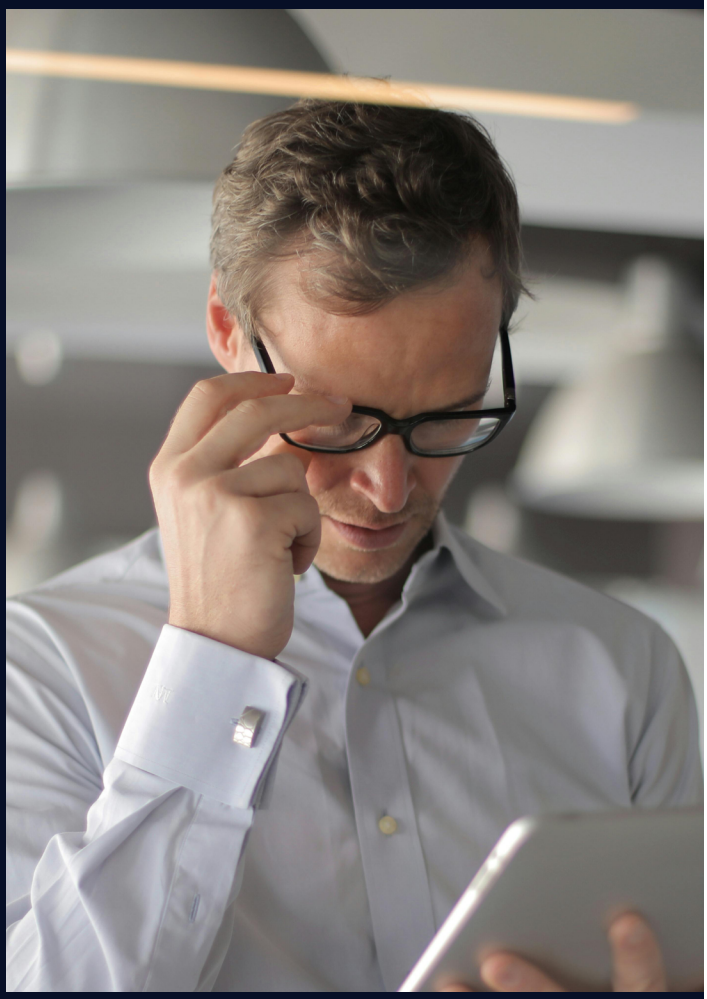
Recommendations

Choose partnerships over parity

- **Deep wallet or merchant integrations with revenue-sharing contracts will deliver more value than simply copying every competitor feature.**
- **Build in portability.**
- **Demand exit clauses, data egress rights and deintegration tests from the start.**

[8] Payment Systems Regulator. PSR and FCA set out next steps for open banking. January 23, 2025.

Digital money



Recommendations

An interbank view of financial risk is better than single-bank surveillance

- **It's not just about seeing more; it's about putting it all together.**
- **Invest in privacy-preserving, consent-based data-sharing to reduce false positives and improve intelligence.**
- **Track impact through case-handling time and suspicious activity report (SAR) conversion rates.**

In many ways, money is already digitized. We see this in the decline in physical branches, a disengagement from cash currency and the move toward intuitive fintech. Taking money from the physical world to the digital world opens up opportunities for development, both to improve the way banks serve customers and to strengthen the frameworks of financial transactions.

Making the switch to CBDCs

Digital currencies have made headlines many times. Behind the hype is a genuine opportunity when digital currencies are managed correctly. It's an option 91% of central banks surveyed by Bank of International Settlements (BIS) are exploring because of the greater security and stability it would provide, even in times of global uncertainty.[9]

Interestingly, the biggest barrier to the development of CBDCs isn't the technology; it's the psychological impact.

Most businesses and many individuals already do the majority of their banking digitally. Taking away the cash option wouldn't be a practical issue. But there are those who value having a cash option and resist every transaction being trackable. Because of behavioral economics, the adoption path for wholesale CBDC will therefore be much smoother than for retail CBDC. This is reflected in BIS' findings that exploration into wholesale CBDC is more advanced than retail.

Whether wholesale or retail, there are still risks to CBDCs. Questions of privacy, disintermediation caps and creating a resilient offline mode mean it's not quite ready for widespread adoption yet.

Streamlining compliance with KYC

Know your customer (KYC) remains one of the heaviest responsibilities for financial institutions. Digital currencies make transactions inherently trackable, and with blockchain ensuring sensitive data is used only as intended, banks can monitor risks more effectively. This creates opportunities for continuous KYC triggers, automated ownership verification and faster detection of adverse media.

Distributed ledger technology (DLT) presents a compelling option for a secure system where financial institutions can more closely track transactions and share data between banks to build a full picture of a customer's behavior. Through partners like Tradle, which already offers a DLT-based KYC solution we take to market together, this potential is already being realized.

That said, there are issues of interoperability and, as always with sensitive data, privacy. Customers must consent to data sharing, and opt-outs will inevitably create blind spots. But initiatives like the EU Digital Identity Framework, which provides citizens with a cross-border digital wallet they control, demonstrate how progress can be made without sacrificing transparency or trust.

[9] Bank for International Settlements. BIS Papers No 159: Advancing in tandem – results of the 2024 BIS survey on central bank digital currencies and crypto. August 2025.

The new infrastructure

With so many changes available now and on the horizon, we have to look inward at the infrastructure we use to house these tools, upgrades, products and services. Banks need infrastructure that can handle more and adapt more often while maintaining resilience. Two areas of development offer strong potential for future-proof financial infrastructure: quantum computing and observability tools.

Quantum computing

AI has been a game changer in many ways, including risk assessments, personalized customer interactions and the way banks handle the data they need to support their operations. But it's safe to say that when it comes to the impact quantum computing will have, AI will seem like a software upgrade. A significant one, but an upgrade nonetheless. These machines will be able to handle a level of complexity we can hardly imagine today.

> "When it comes to the impact quantum computing will have, AI will seem like a software upgrade."

Quantum computing could create $622 billion in value by 2035.[10] This is because of the way it will transform many processes in the financial sector. These include optimizing investment, because of its ability to solve multivariable problems at speed, and being able to make payments, with the introduction of quantum money. This would be even more secure than blockchain because it cannot be cloned or falsified.

Quantum computing is a major opportunity for banks, which is why some of the world's largest banking institutions already have quantum-computing teams, despite the timeline for this technological development being uncertain.

With the benefits come risks. Quantum computing could undermine the security procedures we've relied on for years. This is such a concern that the National Institute of Standards and Technology (NIST) has already published principles to protect against quantum-computing cyberattacks, and the G7 Cyber Expert Group followed with its own recommendations.

The call is to adapt now.

Observability tools for resilience building

Knowledge is power, so the key to unlocking the resilience required to adapt to changes and challenges is advanced observability.

NTT DATA approaches observability through a site reliability engineering (SRE) lens. Business objectives are translated into service level objectives (SLOs), measured via service level indicators (SLIs) and governed by error budgets. This framework doesn't just monitor systems; it operationalizes reliability.

Banks that decouple products from core systems and implement AI with auditable controls supported by these levels of observability can target a 5-to-7-point improvement in cost-to-income ratio over the next 24 months, provided there is disciplined execution and consistent performance tracking.

The goal is not just visibility but actionable control.

[10] QNu Labs. The quantum revolution in finance: How leading banks are preparing for a $622 billion opportunity. August 7, 2025.

Institutions should be able to report the following metrics

MTTR	P95 latency	Availability
< 2 hours	< 400ms	≥ 99.95%

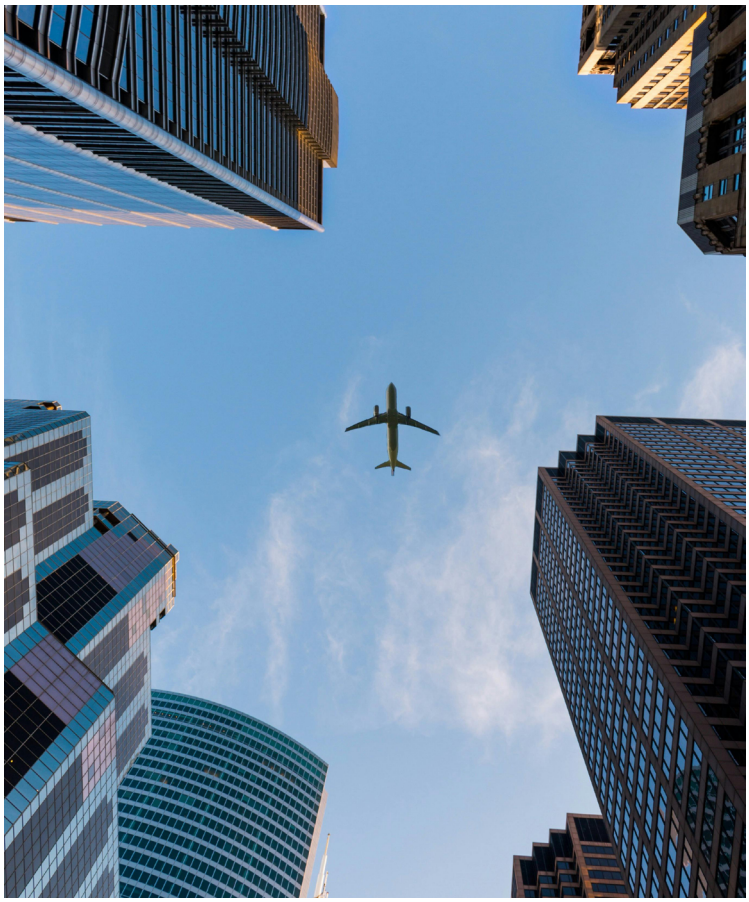
They should also be able to operate under a defined error-budget policy that triggers engineering prioritization. This approach supports internal performance management and provides a strong evidence base for regulators. This way, resilience becomes not just achievable but measurable.

For accountability and impact, banks should publish three SLIs per top 10 customer journeys, such as retail payments, transaction history, and customer logon, covering:

- **Availability**
- **Payment success**
- **P95 latency**

P95 is the point in time where 95% of user requests are completed, meaning the other 5% of requests are slower than this threshold. It is a way to measure performance that goes beyond the average, providing a better understanding of user experience by highlighting the slowest requests that might be frustrating for some users.

These metrics should inform a clear error-budget policy and SLO burn-rate thresholds that drive engineering priorities in real time. Quarterly failover drills must be run and documented, with outputs forming part of a regulator-ready evidence pack that includes a service map, dependency list, incident history and classification of third-party criticality.



Recommendations

Stop focusing on achieving multicloud symmetry

- **Designate a primary cloud and prove portability.**
- **Pass a 90-day exit drill every year covering data egress, contract-level tests and traffic flip. No symmetry, just proof.**
- **In parallel, treat crypto agility as an immediate priority, not a distant goal. Complete a full cryptographic inventory, classify secure network and data layer (SNDL) assets and initiate PQC dual-stack pilots within the year.**

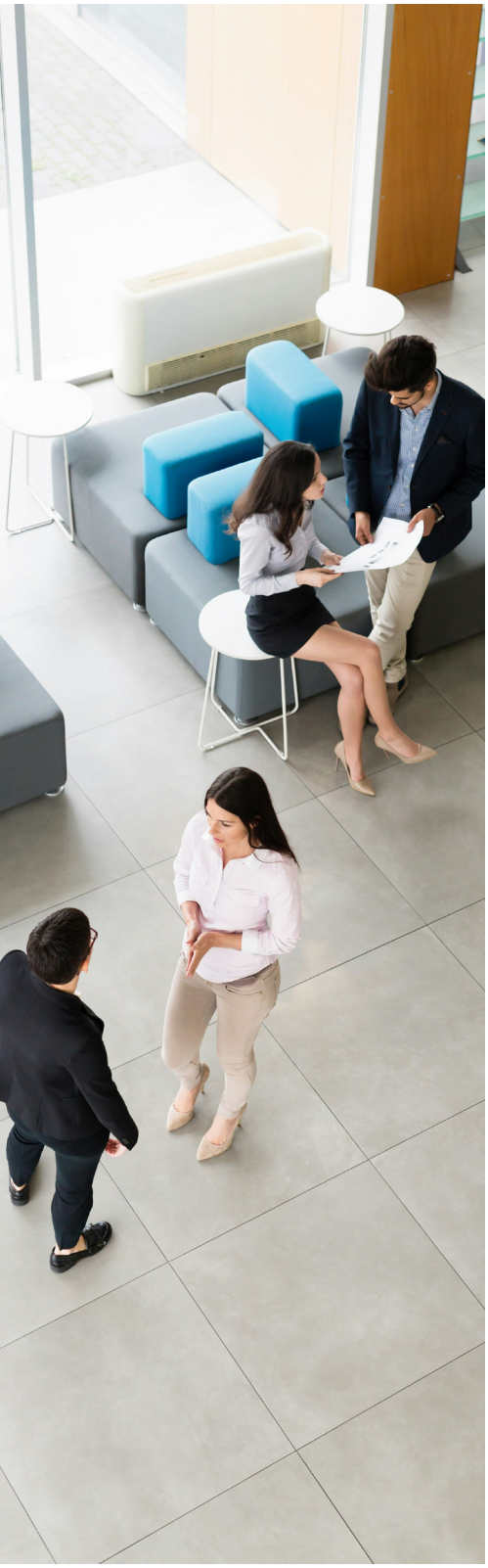
These actions are essential to resilience ahead of quantum-era threats.

Some of the elements that should be tracked are provided as a scorecard at the end of this document

The challenges of change

When starting a large-scale transformation project, you can't ignore the potential for resistance that could create a barrier to uptake, integration and, ultimately, return on investment. An innovative solution shouldn't just include the technical requirements; it must be a holistic pathway to adoption designed to maximize outcomes.

There are a few areas that could present a challenge for financial institutions engaging with technical advancements in the industry.



A workforce in flux

With the advent of new technologies, the workforce is inevitably changing as some roles become obsolete and others emerge. The most outdated roles in the finance sector will be those that rely on manual processing and repetitive tasks, as AI can do so much already, and will be doing even more in five years. The jobs most in demand will be those focused on implementing and managing AI, including training and data management.

Bridging ideas and outcomes

How do financial institutions avoid potential pitfalls and produce positive business outcomes from their investment in innovation? One of the biggest concerns in realizing the potential of AI is sourcing the right data, because even the best AI algorithm won't perform unless it's trained on enough quality data. This can be resolved through data contracts, stewardship, lineage and a governed feature store.

The question of regulation

The pace of change, especially in the area of AI, is so fast that regulation can't keep up. Adopting technology when there is yet to be a consensus on how it will be regulated, particularly across international borders, means you have to get ahead of future requirements. That's why we provide flexible system infrastructure that can be adapted to evolving criteria, as well as the security and observability to prove compliance.

A new cultural wave

Financial institutions have been perceived as slightly behind the curve in adopting new technology as they seek to avoid the risks of early adoption. That culture is evolving as the need to stay ahead has become so apparent. Now, we are seeing more banks investing in digital transformation in the first wave of adoption, before there are long-term case studies for new technologies. This cultural change must continue to maximize savings and opportunities from today's technology.

Any decision has pros and cons, risks and opportunities. With so much to gain from embracing the latest technology and so much to lose if banks find themselves too far behind the times, the need to take action is clear — but it must be taken in a way that strategically manages the challenges of change.

Recommendations

Tie executive compensation directly to SLOs and model risk

- **Incentivize reliability, compliant AI operations and time to-ship.**
- **No model goes to production without green data-quality SLOs on freshness and completeness, backed by signed data contracts.**
- **Red or amber gates must block deployment.**

The value of a strategic partnership

The end goal is always to improve operational resilience to avoid issues and instill trust. Technology provides banks with opportunities to turn the dial on measures of operational resilience, including risk reduction, cost optimization, regulatory compliance and enhanced UX.

From saving time and costs and preventing disruptive delays to driving efficiency, intuitive innovation and next-level security, AI has a bright future in the financial industry. It's not just about implementing innovation; it's about achieving results.

This is where NTT DATA can make a real difference. As experts in digital transformation with deep experience in the financial industry, we provide strategic solutions that are technically advanced, commercially viable and designed with change management in mind.

As your strategic partners, we use our unique perspective and expertise to identify gaps, close missing connections, and streamline infrastructure and integration. We measure our success by maximizing the value our clients gain from the technological opportunities available today.

Take the next step toward the future of banking and financial services with NTT DATA as your strategic partner in operational resilience and supporting innovation.

Recommendations

Better outcomes require better accountability

- **Strategic partnership isn't about implementation alone; it's about measurable transformation.**
- **Demand:**
  - **Quarterly impact scorecards**
  - **Milestone-based delivery**
  - **Clear thresholds for iteration or termination from your partners**

CTO scorecard

Abbrev.	Full form	Notes / where used
KPI	Key Performance Indicator	Column header / metric language
CIR	Cost-to-Income Ratio	Economics domain
PP	Percentage points	Target deltas (e.g., —2.0 pp)
CFO	Chief Financial Officer	Owner
CTO	Chief Technology Officer	Owner
DW	Data Warehouse	Source (Finance DW)
M	Monthly	Review cadence
Q	Quarterly	Review cadence
A	Annual	Review cadence
SDLC	Software Development Life Cycle	Source / engineering workflow
ADR	Architecture Decision Record	Source / platform modernisation
SRE	Site Reliability Engineering	Owner / reliability metrics
APM	Application Performance Monitoring (a.k.a. Management)	Source for latency/availability
MTTR	Mean Time To Recovery (a.k.a. Restore/Repair)	Incident metric
MTTD	Mean Time To Detect	Incident metric
SecOps	Security Operations	Owner with SRE
IM (tool)	Incident Management (tool)	Source alongside SIEM
SIEM	Security Information and Event Management	Security monitoring
CISO	Chief Information Security Officer	Owner
IAM	Identity and Access Management	Security capability
PAM	Privileged Access Management	Security capability / logs
CX	Customer Experience	Owner for AI containment
ML Ops / MLOps	Machine Learning Operations	Owner / runtime ops
QA	Quality Assurance	Quality gate for automation
CSAT	Customer Satisfaction (score)	Quality gate / experience
CDO	Chief Data Officer	Owner (data & AI / DQ)
ML Eng	Machine Learning Engineering	Owner with CDO
PMO	Program (or Project) Management Office	Owner (ML PMO)
MRM	Model Risk Management	Owner / governance SLA
DQ	Data Quality	Data platform SLOs

Abbrev.	Full form	Notes / where used
OB	Open Banking	OB gateway / payments
VRP	Variable Recurring Payments	Open banking payments
PSP	Payment Service Provider	Source (PSP logs)
SLO	Service Level Objective	E.g., journey availability (SLO)
GRC	Governance, Risk, and Compliance	Evidence-pack SLA owner/system
CMDB	Configuration Management Database	Crypto-inventory coverage
PQC	Post-Quantum Cryptography	Dual-stack pilots
KMS	Key Management Service (or System)	With PKI in crypto-agility
PKI	Public Key Infrastructure	Crypto-agility stack
JIT	Just-In-Time (access)	Mean privilege lifetime
P95	95th percentile (latency)	Performance target
Dev portal	Developer Portal	Platform adoption metric
LMS	Learning Management System	Training / enablement
CPO	Chief Procurement Officer (or Chief Product Officer*)*	Owner on third-party exit drill (context usually procurement)

Domain	KPI (definition)	target		Owner → Source	Review
		12-month	24-month		
Modernization	**Change blocked by legacy** (% of stories blocked by core deps)	<20%	<10%	Platform Eng → Jira/SDLC	Monthly
	Core dependency burndown (direct calls to core)	-30%	-60%	Platform engineering → ADR/ inventory	Quarterly
Reliability	**Journey availability** (top 10 journeys, SLO)	≥99.95%	≥99.97%	SRE → Observability	Monthly
	Payment success rate (authorised → settled)	≥99.90%	≥99.95%	SRE/Payments → PSP logs	Monthly
	P95 latency login pay transfer	 ≤400ms ≤1.5s ≤1.0s	 tighter by 15%	SRE → APM	Monthly
	Incident MTTR **Incident MTTD**	-40% -30%	-60% -50%	SRE/SecOps → IM tool/SIEM	Monthly
Security	**Critical vuln MTTR**	<7 days	<48 hours	CISO → Vuln mgmt	Monthly
	Phishing success rate	<0.5%	<0.3%	CISO → Red team metrics	Monthly
	Mean privilege lifetime (JIT access)	<24h	<8h	CISO/IAM → PAM logs	Monthly
Data and AI	**Use cases in prod (regulated)**	≥6	≥12	CDO/ML Engineering → Registry	Quarterly
	Time-to-ship AI use case (idea → production)	<8 weeks	<6 weeks	ML PMO → SDLC/Jira	Monthly
	AI containment (with QA gate)	30 to 50% @ CSAT ≥4.5/5	50 to 60% @ same gate	CX/ML Ops → QA/CSAT	Monthly
	Model governance SLA (drift alert → action)	≤24h	≤8h	MRM/ML Ops → Monitors	Monthly

Domain	KPI (definition)	target		Owner → Source	Review
		12-month	24-month		
Data quality	**Data contracts coverage** (priority domains)	≥80%	100%	CDO → Catalogue	Quarterly
	DQ SLO adherence (freshness/completeness)	≥99%	≥99.5%	CDO → DQ monitors	Monthly
Open banking and payments	**Pay-by-Bank share** (bill pay)	≥10%	≥25%	Payments → OB gateway	Quarterly
	VRP adoption (eligible merchants)	≥20%	≥50%	Payments/Partnerships	Quarterly
Compliance /Resilience	**Evidence pack SLA** (major incident → dossier)	≤48h	≤12h	Risk Ops → governance, risk and compliance (GRC) system	Monthly
	Third-party exit drill (primary cloud/vendor)	1 drill passed	Annual pass + gaps closed	CTO/CPO → Runbook	Annually
Crypto-agility	**Crypto inventory coverage**	100%	—	CISO/CTO → configuration management database (CMDB)	Quarterly
	PQC dual-stack pilots (non-customer flows)	≥2 services	≥6 services; rollout plan approved	CISO/CTO → KMS/PKI	Quarterly
Talent and ways of working	**Engineers on paved roads**	≥70%	≥85%	Platform engineering → Backstage	Quarterly
	Time to-proficiency (new stack)	≤90 days	≤60 days	Eng enablement → LMS	Quarterly

Visit nttdata.com to learn more.

NTT DATA is a $30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.


NTT DATA