DXC TECHNOLOGY

What's in store for banking in 2025?

Foreword by Jeremy Donaldson

We (continue to) live in interesting times. In 2025, banks will need to deal with issues related to security, the rapid adoption of new technologies (i.e., GenAI-based processes), the ongoing maturity of digitization initiatives (e.g., the UK government's digital Driver's License/Digital ID program), and (potentially the most disruptive) the rapidly evolving geo-political risks that are emerging. Wars (e.g., Ukraine, Gaza), dramatic climate events (e.g., L.A. fires, Spanish floods), inflation, recession, and numerous other challenges will continue to contribute to the uncertainty of the banking environment. If the Executive Orders signed by President Trump on his first day teach us anything, it is that we can no longer take for granted any consistency of policies from one administration to the next. Taken together, all of these factors shine a stark light on a standard board agenda item: Operational Resilience. Never has it been more important for banks to be operationally agile, secure and resilient. This reality has already been recognized through DORA, the UK Critical Third-Party risk regulations, and NIS2 regulations.

In this age of social media weaponization, the withdrawal of "fact checking" services, and emboldened "crusaders," banks simply cannot afford to make significant operational blunders. The reputational risk has shifted to the extreme end of the social spectrum. Reputational damage now carries significantly more risk to earnings, liquidity and capital. Cybersecurity breaches, data loss, ransomware attacks, service outages, lost payments, fraudulent transactions are but a short list of issues that can, when amplified through social media platforms, severely disrupt and potentially bring down a bank.

There will also be debates at the Board level regarding climate change. At COP26, the most pressing issue facing society was transitioning to a more sustainable global environment. Apart from managing their own Scope 1-3 emissions, banks carved out a critical role for themselves in helping to creatively fund the transition to a Net Zero world. The Trump administration's decision to withdraw from the climate accords will force boards

to demonstrate their own commitments to the pledges they made at COP26 and since. Will they choose to back away from those commitments to satisfy the short-term objectives of shareholders, or will they continue to play a pivotal role in moving global society toward the Net Zero goals, as supported by the broader stakeholder community? We believe that navigating the politics of this will be a theme in 2025.

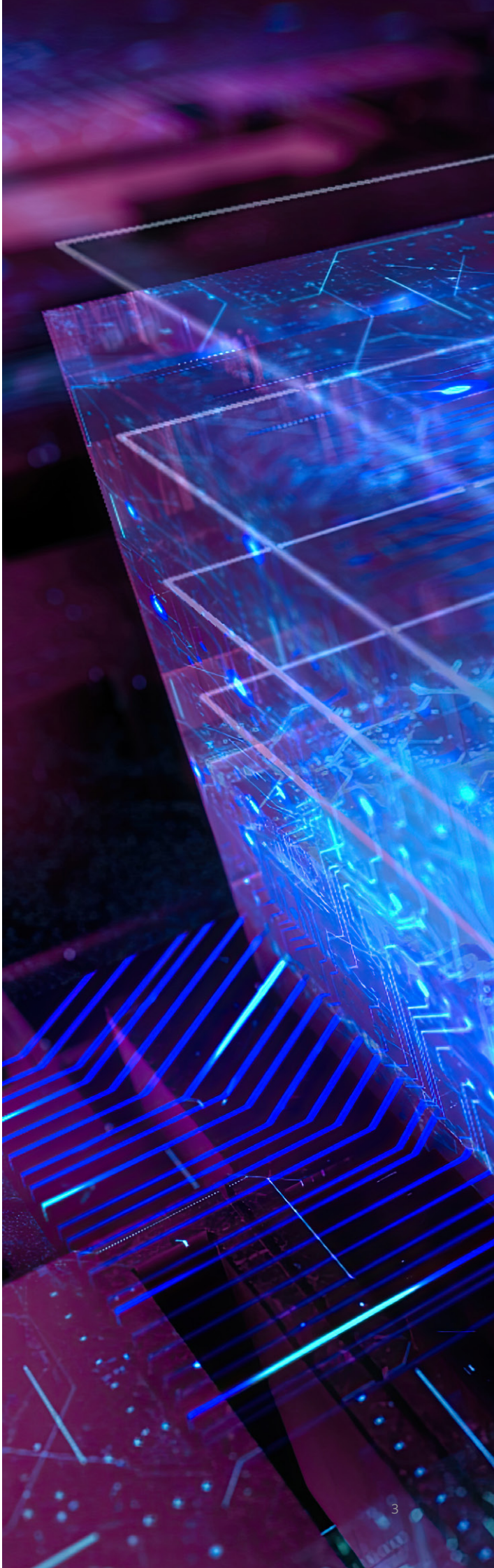
This paper discusses some of the many forces that are in play with our clients as we begin 2025, and what can be done to mitigate (or capitalize on) their impact. The extraordinary pace of change in technologies (like Artificial General Intelligence — AGI) will not slow down. It will only accelerate. The challenge to adopt and safely integrate these new technologies into banking operations will not disappear and will force a reckoning with firms' existing technical debts.

Modernizing the technical and operational environments will allow for rapid strategic decisions and agile execution. As we have seen with some of our clients, achieving this is not an insurmountable problem — but it requires trade-offs. With all of the other growth and regulatory pressures on today's boards, huge investments in "risk mitigation" modernization programs are tough to sell. Keeping an institution's environment secure, agile, and reliable is not.

We hope you enjoy our views and perspectives in this report. Our DXC Technology UK&I FSI team, and indeed our global organization, are at your disposal should you wish to discuss the views or perspectives that are of interest to you, and to assist you along your journeys.

We will further expand on our views in our next report, "Addressing the challenges in 2025 and beyond." Look out for it in the near future.

Jeremy Donaldson
Managing Director, Financial Services — UK&I



Banking on survival

by Dr. Alex Kokkonen

Evolving risk

From threats related to credit risk or market fluctuations, the concerns have now shifted to the very core of banking operations and the business models of banks. Cybersecurity breaches, which were once a rare occurrence, have now become an everyday occurrence that could bring down even the mightiest banking giants. Where fintech and decentralized finance (de-fi) increasingly threaten banks, economic shocks if anything, amplified by global interconnectedness can wipe out even the sturdiest of balance sheets in the blink of an eye. For Tier 1 banks, the stakes have never been higher. Given their systemic importance, a single failure might trigger a cascading effect throughout the global economy. Tier 2 banks are smaller, yet not immune. A regional focus belies a vulnerability to economic downturns or shifts in consumer behavior at the local level.

Technological disruption

The rapid pace of technological change is fundamentally changing banking. Fintech and big tech have forced banks to embrace digital technologies. These market players are forcing banking institutions to continually and dramatically improve, expand, and innovate their services, processes and customer-oriented strategies.

These disruptors deploy technology in an endeavor to execute solutions at lower cost, with higher speed and far more convenience, appealing to the significant share of the market which could lead to a loss of both market relevance and market share for banks. The rise of cryptocurrencies and, more so, de-fi threatens to upend the very fabric of the traditional banking model. These disruptors could impact the role of traditional banks in the financial ecosystem as these trends continue to gain traction. 2025 will see these changes accelerate at unprecedented rates.

Artificial Intelligence (AI)

by **Tim Meng Ching** and **Lars Klinghammer**

The banking industry stands at the threshold of an AI-driven transformation that promises to radically reshape the way institutions operate and serve their customers. The integration of AI presents both an opportunity and a challenge. Those banks able to execute complete AI strategies in line with regulatory, ethical, and workforce considerations will acquire a competitive advantage. With the fast-paced continuous development of this industry, a delicate balance between innovation and responsibility is the only viable way to ensure sustainable competitiveness in the AI-driven future of banking.

Artificial General Intelligence (AGI)

Artificial General Intelligence will likely become mainstream, as a greater number of banks incorporate AGI into their business processes. For banks who have incorporated machine learning, through pattern analysis on usage behavior, fraud detection and risk management, the incorporation of AGI will further enhance them.

Generative AI transformation

Generative AI is changing core banking in several big ways. Advanced language models make customer service interactions more natural and context-specific, enabling the virtual assistant to handle complex queries and give in-depth financial advice. AI-driven systems smooth document processing by automating document analysis, generating reports with insights, and extracting data, considerably reducing the time spent on manual processing. AI-driven solutions create less dependence on compliance management, by simplifying regulatory reporting, enhancing anti-money laundering through automated risk identification, and producing compliance documentation.

Agentic AI

Customer-oriented interactions require an increase in two-way digital conversations with banks, not today's one-way push notifications. The time is right for enterprises to build on this trend with the growth of Agentic AI platforms and appropriate use cases.

Security

by **Tim Meng Ching** and **Lars Klinghammer**

Data-centric security

In 2025, banks will increasingly leverage AI to drive efficiency and innovation, and the concept of data-centric security has become paramount. Traditional perimeter-based security models will continue to be foundational for AI security, but they are, on their own, no longer sufficient. As AI-enabled cyberattacks become more common, the need for enhanced data security measures will become more evident. This will continue to force renewed emphasis on data governance, compliance with data protection regulations, and new standards for data residency will demand it.

The cost of protection, like Zero Trust and data security controls, will be small compared to the costs associated with potential data breaches, unauthorized access and AI-driven adversarial attacks.

AGI security

Banks are utilizing AGI to transform their customer digital experience; threat actors will be using that very same technology to perform deep fake and other scams to fool bank customers. AI costs have decreased substantially, so an increasing use of AI to attack banks is expected.

Ransomware as-a-Service (RaaS)

Ransomware, like other threats, has evolved over the years. From the encryption-only approach, ransomware has morphed to a dual threat malware (exfiltrate data and encryption) to ransomware as-a-Service (RaaS) with threat actors offering ransomware and other tools and services to affiliates for a share of the profits.

Industrialization of cybercrime tools

The industrialization of attack tools increases the significant cyber risks that organizations face, including credential theft, data breaches, operational disruptions and reputational damage.

With deep fake and social engineering scams flourishing across the banking industry, criminal organizations have developed realistic audio, video, and image manipulations to exploit trust, identity theft, executive impersonation and market manipulation.

Supply chain

As in previous years, banks that depend on IT, cloud and telecommunication service providers in 2025 may discover certain vendors with whom they are working may suffer attacks and be compromised by state-sponsored adversaries or others.

The traditional response to mitigating supply chain attacks has been the evaluation of third-party risk management and assessment, as well as developing contractual agreements that impose financial penalties on these providers. Unfortunately, reliance on these activities is reactive and cannot prevent attacks from occurring.

In 2025, we see more information sharing and collaboration among industry players to learn from each other and build better defenses against infiltration from third-party providers. This is a main tenet of Digital Operational Resilience Act (DORA), UK regime for Critical Third Parties (CTP), and Network and Information Security 2 (NIS2). Strategic IT partners, such as DXC, can offer a great deal of value in helping to defend against infiltration, and in contributions to industry collaboration.

Resilience

by **Dr. Marc L. Brogle**
and **Dhritiman Mukherjee**

Reducing disruption

Throughout 2025, industries and sectors including banks will witness a significant change in the wake of regulatory requirements like DORA, CTP, and NIS2 for sound digital operational resilience.

The convergence of these regulations represents an evolutionary leap in how banks approach both operational resilience and cybersecurity. While adopting these new regulatory frameworks it will introduce a strategic differentiator by establishing improved operational efficiencies, customer trust, and a competitive positioning environment.

Banks are obliged to adopt sophisticated information and communications technology (ICT) risk management frameworks, including an effective incident reporting system, resilience testing, and third-party risk management. Banks need to implement sophisticated cybersecurity measures, conduct periodic security audits, and report significant cyber incidents in good time. This, together with the focus of the directive on collaborative defense mechanisms, will encourage banks to engage in information sharing with regulators and industry peers, further building the resilience of the overall financial sector.

This shift will demand significant investment in ICT infrastructure and data analytics to support ongoing reviews of risk management to ensure compliance with new regulations and enhancements to operational resilience.

Necessary measures

The goal is to create a culture of proactive risk management and continuous improvement. A focus on operational resilience should reduce the impacts of ICT-related disruptions and their related costs (downtime events, data breaches, etc.), driving increased customer trust and satisfaction. It will spur innovation by providing solid security, a stable environment, and allow for the safe adoption of new technologies.

Omnichannel

by **Dave Wilson** and **Sachio Nishioka**

Getting everyone onboard

Today, most people use online banking; digital-only bank accounts are growing; utilization of mobile services is increasing with more people switching banks to obtain a better digital customer experience. Winning and retaining younger customers will be important to ensure long-term customer lifecycle growth for banks. Thus, we see even greater demand for investment in technologies that provide seamless, omnichannel, personalized experiences. Some examples include:

- Omnichannel technology advancements and capabilities are outpacing banks' abilities to respond promptly. Technology has created a society of customers who expect more and more from their digital online experience while demanding a more personalized customization, more protection and control of their data and privacy, and more two-way interactions through a one-stop shopping seamless omnichannel experience. The convergence of edge technologies, including AI, allows these frictionless interactions to happen and will continue to be a focus for banking services providers.

- As standard, embedded finance, powered by Open Banking and Application Programming Interface (API) ecosystems, will continue to be a focus area for investments by retail banks, ensuring that financial services are seamlessly integrated into the everyday lives of their customers.

- Advanced analytics will let banks provide hyper-personalized products and services. Digital wallets, real-time payments, and contactless transactions will facilitate the customer experience, bringing intuition and ease to customer interactions.

Payment technologies

The evolution in instant payment technologies and services is making it easier for customers to pay their peers (P2P), move money between accounts (A2A), and consume more products including quicker refunds. Will this evolution in technologies encourage the adoption of micro payments and transaction volumes in virtual worlds?

Identification and authentication

Decentralized digital identities, enabling secure and unique digital identification and authentication via digital channels, will grow in importance. They will support better control of personal data, protect user privacy, and facilitate standardization and interoperability across platforms (and borders). This may also support the ESG agendas of the banks by promoting inclusivity, reducing paper and securing identities.

Conclusion

2025 will be action-packed and unpredictable. DXC Technology builds and runs the world's mission-critical systems. We're entrusted with developing, building, securing, and innovating these systems to meet the critical and evolving needs of our clients and the communities we serve.

Resilience and security are embedded in our DNA thanks to our expert delivery teams, AI experts, and solution engineers. DXC Technology is well placed to work collaboratively with our clients as they navigate the challenges ahead in 2025.

We will further expand on this in our next report, "Addressing the challenges in 2025 and beyond." Look out for it in the near future.

For any immediate questions, please contact one of our relevant experts today.

About the authors

Jeremy Donaldson
Financial Services Sector UKI
jeremy.donaldson@dxc.com

Dr. Marc L. Brogle
CES Financial Services Industry
marc.brogle@dxc.com

Dr. Alex Kokkonen
Senior Principal Industry Strategist
alex.kokkonen@dxc.com

Dhritiman Mukherjee
CES Financial Services Industry
dhritiman.mukherjee@dxc.com

Tim Meng Ching
Security CTO
tching3@dxc.com

Dave Wilson
UKI Field Chief Technologist (GIS)
dave.wilson@dxc.com

Lars Klinghammer
Security Risk Management
lars.klinghammer@dxc.com

Sachio Nishioka
Analytics and Consulting — Asia
sachio.nishioka@dxc.com

Find out more

- Exogenic shocks: What could possibly go wrong?
- Zero Trust for maximum security.
- More insights.

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.