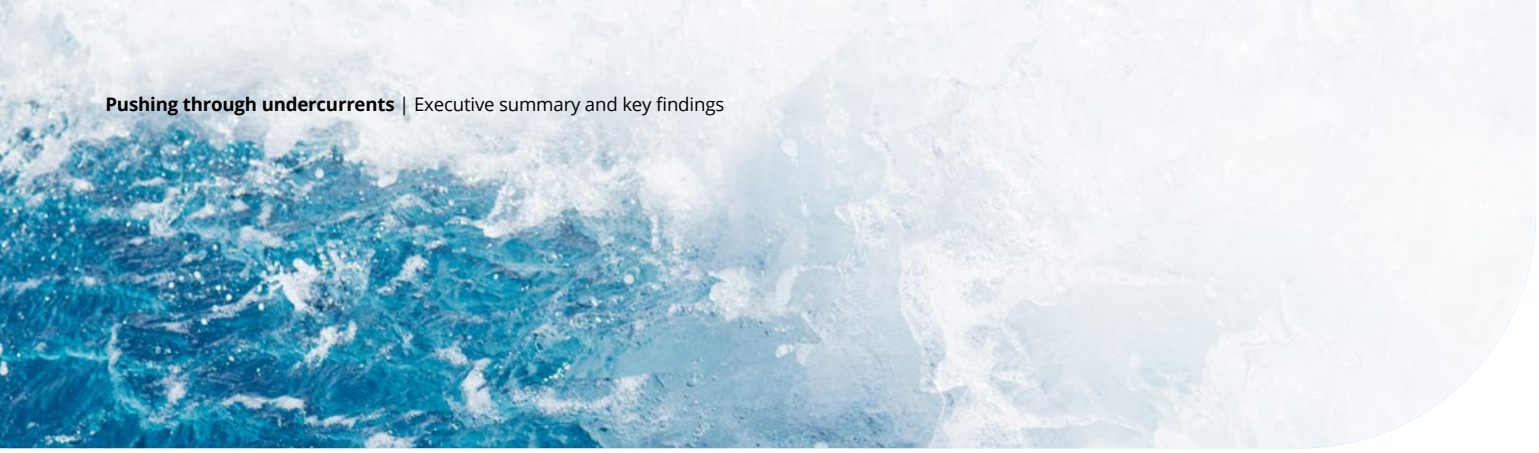
Deloitte.

Pushing through undercurrents

Sectoral and regional forces that influence technology-driven systemic risk in financial services

MAKING AN IMPACT THAT MATTERS since 1845

Table of contents



Executive summary and key findings

Six takeaways about the forces behind technology-driven systemic risk in financial services

Recently, the World Economic Forum (the Forum) and Deloitte set out to explain how technology can both increase and mitigate systemic risk in the financial system. In the first installment of our two-part series, we identified different types of technology-driven systemic risk.

Since then, technology's role in financial instability has become even more relevant. Social media and digital banking may have contributed to recent banking crises, boosting uncertainty about financial services' resilience to systemic shocks. Advances in generative AI have raised questions about the financial system's vulnerability to misinformation. And the threat of cyberwar from ongoing geopolitical conflict is now putting financial institutions in the line of attack.[1]

These themes led us to consider how financial institutions could be affected by the sectoral and regional forces that drive technology-driven systemic risk. To find out what those risks are and how they can be mitigated, we consulted over 100 financial services and technology experts globally to inform the second installment of our series. This paper is an executive summary of that report.[2]

Here are six takeaways from our conversations.

1 In financial services, technology-driven risks can proliferate across sectors and regions, becoming systemic when product development and distribution are fragmented.

Fragmentation is growing most significantly through the extension of financial infrastructure, the provisioning of credit, and the sourcing of market intelligence.

Financial infrastructure is fragmenting through as-a-service models that regulated financial services entities offer. The risk of incomplete oversight will grow as those responsible for risk oversight split from those that make and sell financial products. For example, banks are extending their existing infrastructure to non-financial players via banking-as-a-service products and depending on partnerships with platform and application programming interface (API) providers to participate in embedded financial offerings.

Technology platform providers are working with non-financial companies to displace traditional financial credit offerings and harvest more first-party data. This has increased blind spots to credit default risk and fragmented the development and distribution of credit products across multiple non-financial entities. For example, short-term point-of-sale products like Buy Now Pay Later are helping retailers access customer spending data and giving customers access to credit without direct risk and compliance oversight offered by traditional banks.

Market intelligence has fragmented into partially regulated entities. This intelligence is feeding directly into AI models that make real-time financial decisions and can amplify the impact of data deception tools on financial markets and customer trust (e.g., deepfakes). For example, investment firms are using unregulated data brokers to access market intelligence from retailers and other companies.

2 Some new entrants across financial services sectors are unintentionally emphasizing near-term competitive advantages over long-term resilience and transparency.

Many new players in financial services specialize in offering instant and affordable access to financial products for customers. With a focus on instant access, managing and anticipating long-term risks like chronic overborrowing and personal data protection is beginning to go by the wayside.

Customers' financial activities are now more distributed across multiple non-traditional players, instead of a few traditional financial institutions. Examples include investments in an online trading platform, loans with technology platforms, and budgeting activities with apps. As this trend grows mainstream, fewer private entities will have the obligation or the visibility to protect customers from financial losses or cybersecurity incidents.

3 Highly dynamic geopolitical and regional forces are outpacing a financial institution's resilience measures against cybersecurity, workforce shortages, and environmental threats.

Cyberattacks against financial institutions and their critical service providers are becoming more geopolitically motivated, sophisticated, and frequent. Given limitations in the risk assessments of a financial institution's client base and supplier network, the evolving nature of cyberattacks may be putting financial institutions at risk.

Regional competition for technology talent, along with growing competition from adjacent industries, may leave some financial institutions vulnerable to shortages in the talent required to maintain critical operations (e.g., disaster recovery solutions), protect customer data, and ensure consistent availability of financial services to customers.

Financial institutions also face limitations in accessing the data required to accurately price the effects of climate change on their clients. This may lead to inaccurate predictions of a business' ability to repay loans and make insurance premium payments. This may also lead to downstream inaccuracies in the risk profile of assets that investors buy.

4 Sectoral and regional nuances reveal targeted opportunities for traditional financial institutions and fintechs to promote trust-enhancing products and services that help reinforce financial system stability.

Incumbents and fintechs can address a market gap by offering customers personal financial management services across their financial dealings while maintaining a convenient, affordable shopping experience. Examples include wallet connector products and financial data aggregator services. Traditional financial institutions in particular are uniquely positioned to extend their role as trusted partners for customers who have multiple financial dealings with niche and adjacent players.

Liability insurance products can protect customers from data breaches or unauthorized activities, such as compromising a customer's bank account data on a merchant website hosted by a third-party provider.

Alongside existing financial and media literacy efforts, financial institutions and fintechs can embed authentication and digital credential services for financial services-related content to help protect customers from disinformation and data deception tools.

5 **Public and private sector players can collectively dismantle information siloes to help better identify technology-driven risk at the ecosystem level.**

As we explored in the first installment of our series, bigger network size is a relevant indicator of a financial ecosystem player's systematic importance. Regulators and institutions can get a handle on the risk these ecosystems present by breaking down information siloes. Open banking platforms and transactional data-sharing, for instance, might give regulators an idea of how regional credit risk is trending. Analysis of this data could also reveal how different regulatory approaches affect financial activity.

To identify technology-driven risk at the ecosystem level, firms and regulators can map relationships across cloud infrastructure, alternative data, and API stack providers. This in turn could make way for intelligent monitoring solutions that predict disruptions to a third-party vendor's financial health and security posture, enabling proactive action.

6 **Financial services players' predictive analytics capabilities should reflect future geopolitical and regional uncertainty and be applied towards resilience efforts.**

Operational resiliency takes on new meaning amid geopolitical and regional uncertainty. In their scenario modeling and resilience strategies, financial institutions should weigh conditions that can compromise important customers and service providers. They should also update risk profiles and price financial products with exposure to regional risk vectors in mind.

What should firms test for? Scenarios include sector resilience, resilience of shared global infrastructure, response patterns, and regional exposures to geopolitically motivated cyberattacks. International experiments and outcomes should also be analyzed at a regional level to determine the public funding backstops and buffers required to contain the systemic effects of attacks.

Building a mitigation agenda

Ultimately, mitigation of technology-driven systemic risk comes down to each firm's ability to understand its unique exposure to sectoral and regional forces. Explore sector-specific risks in our summaries for capital markets, investment management, payments, banking, and insurance. Gain an understanding of regional risks in our summaries for cybersecurity, tech talent, and climate risk. If you have any questions, or would simply like to continue the conversation, please contact us.

Sector perspectives

Certain risks originate uniquely within a sector of financial services and have the potential to become systemic. In the pages that follow, we unpack two examples of sector-specific risks for each sector, along with targeted mitigation opportunities.

Capital markets

Risk 1: Market manipulation from the distribution of synthetic media

What could go wrong?

Synthetic media (like deepfake voice phishing and social botnets) may spread disinformation that maliciously influences capital markets. The risk is growing because:

- Ease of access to deepfake tools, open-source libraries, and generative AI is lowering the cost of producing synthetic media
- The growing volume of images and videos of central bank governors, bank CEOs, and other high-profile individuals increases the precision and effectiveness of malicious synthetic media
- Important institutions that use social media to communicate with the public can increase the degree of trust placed in these platforms

This risk could become systemic if, for example, someone used AI to generate a video of a trusted public official announcing a dramatic drop in interest rates, then posted the video to social media.

What sectoral and regional forces could amplify the risk?

- Communities highly dependent on alternative media
- Technology companies lowering the financial barriers to generate synthetic media
- High-frequency trading algorithms connected to real-time, high-speed data feeds

How can the industry mitigate it?

Goal	Mitigation opportunities
Stronger synthetic media moderation	• Limit opportunities to monetize synthetic media • Crowdsource social media fact-checking
Stronger content authentication and media literacy	• Embed digital content credentials in social media uploads • Use plug-in AI fact-checking tools

Risk 2: Contagion from cryptocurrency exchanges

What could go wrong?

The collapse of a crypto-asset ecosystem may spread contagion into traditional capital markets. The risk is growing because:

- Democratized access to highly leveraged trades can threaten the liquidity of exchange operations
- Limited transparency of leveraged trading volume and capital reserve data can make investor deposits vulnerable to loss
- Pseudonymous design of the underlying blockchain technology can make it challenging to assess creditworthiness
- Custody, lending, and borrowing offerings can create conflicting incentives for an exchange when facilitating trades

This risk could become systemic if, for example, a large cryptocurrency exchange becomes unable to meet customer withdrawal requests and puts a freeze on future requests, prompting other investors to withdraw funds from other cryptocurrency exchanges in a panic.

What sectoral and regional forces could amplify the risk?

- Fragmented and inconsistent crypto-asset regulation
- Growing adoption of decentralized cryptocurrency exchanges
- Interconnected decentralized finance applications

How can the industry mitigate it?

Goal	Mitigation opportunities
Protection of investor deposits	• Impose restrictions on using customer deposits to fund risky activity • Set up shared reserves to help financially healthy exchanges facing liquidity challenges
Controlled access to leveraged trading for investors	• Use publicly available blockchain transaction data to assess creditworthiness
Transparency on indicators of exchange solvency	• Mandate proof-of-reserve certificates from third-party auditors

To learn more about technology's impact on systemic risk in capital markets, including examples, please see pages 24-35 of the full report.

Investment management

Risk 1: Market volatility from speculation fueled by social media

What could go wrong?

With retail investor activity and speculation on social media platforms on the rise, the market volatility from strategies like meme-stock investing may have systemic implications. The risk is growing because:

- The democratization of trading complex investment products through online trading platforms can multiply the effects of speculative trading by unsophisticated investor
- Social media platforms, recognized by retail investors as a trusted source of market data, can create echo chambers that reinforce speculation and bias
- The unpredictability of meme-stock episodes can make it difficult for investment firms to update their risk models and for retail investors to make informed investment decisions

This risk could become systemic if, for example, unfounded rumors about undervalued stocks circulate on social media and spark multiple activist online campaigns on alternative media, prompting herd buying among retail investors.

What sectoral and regional forces could amplify the risk?

- Online trading platforms that encourage risky trading behavior
- Social media penetration rates across communities
- Investors who use social media to boost a company's stock price

How can the industry mitigate it?

Goal	Mitigation opportunities
Deterrence from participating in speculative trades	• Embed financial literacy programs in online trading platforms • Increase retail shareholder engagement through social media
Greater transparency for institutional investors on leading meme-stock indicators	• Set up exchange-traded funds and indexes to help investors track meme stocks • Use machine learning algorithms to help institutional investors spot warning signs of a meme-stock surge

Risk 2: Investor manipulation from compromised sensor-generated data

What could go wrong?

More investment firms are using sensor-generated data to inform their decisions, expanding the attack surface for malicious actors to compromise and manipulate market data. The risk is growing because:

- Open-source channels help cyber criminals share malware source code quickly and accelerate the rate of new types of attacks on internet-connected devices
- High-speed 5G networks help investment managers gain instant access to real-time sensor data feeds
- The Internet of Things, with its multiple end points, has a wide attack surface that makes comprehensive security oversight challenging
- Sensors that are interconnected make all devices vulnerable if one is attacked with malware

This risk could become systemic if, for example, a shared set of sensor devices is compromised for a global commodity (either through manipulated or falsified data), causing investment firms and hedge funds to make the wrong trading decisions

What sectoral and regional forces could amplify the risk?

- Service providers using non-proprietary components to connect devices to 5G networks
- Consolidation of sensor device makers
- An unregulated data broker industry

How can the industry mitigate it?

Goal	Mitigation opportunities
Increasing data quality sourced from sensors	• Establish global certification and labeling for connected devices • Mandate due diligence for alternative data vendors
Containing malware contagion across a sensor network	• Protect sensor data through entropy service providers • Employ extended threat response techniques that integrate data across devices

To learn more about technology's impact on systemic risk in investment management, including examples, please see pages 36-47 of the full report.

Payments

Risk 1: Accumulation and securitization of "buy now, pay later" debt

What could go wrong?

Easy access to point-of-sale financing, paired with weak underwriting rules, may lead to overborrowing and spill over to the financial system through debt securitization. The risk is growing because:

- Weak credit controls create opportunities for impulse buying and easy accumulation of debt
- Limited reporting requirements for buy now, pay later (BNPL) debt limit the visibility of customers' total debts
- Securitization of BNPL debts could create contagion in the wider financial system
- The conflicting incentives of protecting customers and increasing sales may accelerate debt accumulation

This risk could become systemic if, for example, a recession hits—affecting customers' ability to repay their loans—when the volume of BNPL debt is at significant levels and a large percentage is securitized as subprime borrower debt.

What sectoral and regional forces could amplify the risk?

- Big Tech companies offering BNPL loans
- An absence of regulations in jurisdictions where BNPL financing is offered
- Low rates of financial literacy

How can the industry mitigate it?

Goal	Mitigation opportunities
Customer protection from overborrowing	• Establish safeguards to protect against overborrowing and misleading advertising • Develop codes of conduct for BNPL providers
Transparency on customers' ability to pay	• Improve data sharing among BNPL providers • Include BNPL data with credit bureau reporting

Risk 2: Security vulnerabilities of decentralized central bank digital currencies architecture

What could go wrong?

Central bank digital currencies (CBDCs), that run on decentralized ledger technology (DLT) widens the attack surface for malicious actors. The risk is growing because:

- DLT networks have many participants that hackers could exploit
- A bug or malfunction in a supporting DLT platform could cripple the system
- Side-channel attacks could be used to break into user wallets and steal customer funds

This risk could become systemic if, for example, a rogue nation-state launches a distributed denial-of-service cyberattack on the CBDC payment network of another country, causing outages of critical services.

What sectoral and regional forces could amplify the risk?

- A complex CBDC network architecture
- Interoperability with other networks
- A large number of participating institutions

How can the industry mitigate it?

Goal	Mitigation opportunities
User protection and data privacy	• Incorporate protection to end-user digital wallets challenges
Strong access control and network security	• Set up a tiered ledger system for CBDCs • Use quantum-resistant algorithms to protect CBDC systems
Cross-border security standardization	• Standardize CBDC security protocols

To learn more about technology's impact on systemic risk in payments, including examples, please see pages 48-59 of the full report.

Banking

Risk 1: Risk exposure from Banking as a Service offerings

What could go wrong?

Banking as a service (BaaS) increasingly relies on application programming interfaces, introducing vulnerabilities that can pose risks for banks. The risk is growing because:

- Customers' sensitive data and funds may be at risk from phishing and social engineering attacks
- Flawed APIs might provide a back door for hackers to penetrate banks' systems
- Noncompliance with data privacy rules by BaaS providers might expose partner banks to reputational risks

This risk could become systemic if, for example, a malicious actor launches a distributed denial-of-service attack on a BaaS provider, keeping customers from accessing their accounts or making transactions.

What sectoral and regional forces could amplify the risk?

- A complex BaaS technology stack
- Limited redundancy measures
- A lack of input validation, enabling attackers to upload malicious code into a bank's systems through its APIs

How can the industry mitigate it?

Goal	Mitigation opportunities
Strong security for BaaS platforms and API connectivity	• Use input validation protocols • Apply network segmentation and access control measures
Properly vetted BaaS partners	• Improve due diligence on BaaS providers
Institutional knowledge transfer from banks to BaaS partners	• Help BaaS and other fintech providers get better at risk management and compliance

Risk 2: Inadequate stability mechanisms for stablecoin arrangements

What could go wrong?

Stablecoins mimic fiat currencies but without the backing of a central bank, heightening the probability of a run. The risk is growing because:

- Governance and regulatory gaps could perpetuate illicit activities that might threaten the integrity of the broader financial system
- The novel technologies used for minting and managing stablecoins are exposed to security risks
- The absence of a stability mechanism like deposit insurance increases the risk of a run

This risk could become systemic if, for example, a significant stablecoin issuer fails to promptly honor large customer withdrawal requests, touching off a run and eventually collapsing the stablecoin arrangement.

What sectoral and regional forces could amplify the risk?

- A less mature regulatory environment
- Stringent capital controls, which may encourage individuals in those jurisdictions to park their assets in global stablecoins
- Unsecure systems and poorly managed internal processes

How can the industry mitigate it?

Goal	Mitigation opportunities
Standardization and oversight of stablecoin arrangements	• Requirement for anti-money laundering and "know your customer" processes for stablecoin issuers
Investor and customer protection	• Offer insurance coverage for stablecoin tokens • Enforce responsible marketing rules and customer education
Transparency of capital reserves	• Periodically audit and stress-test stablecoin issuers' reserve assets

To learn more about technology's impact on systemic risk in banking, including examples, please see pages 60-70 of the full report.

Insurance

Risk 1: Vulnerabilities in parametric insurance smart contracts

What could go wrong?

Because smart contracts are designed to automatically execute, any programming flaws or security vulnerabilities could result in substantial insurance losses. The risk is growing because:

- Smart contracts could be undermined by coding errors in their blockchain networks
- The immutability feature of smart contracts makes it harder to resolve errors in a timely manner
- Reliance on external data sources that could be manipulated exposes smart contracts to risks
- The evolving regulatory and legal landscape creates uncertainty around the enforcement of smart contract agreements

This risk could become systemic if, for example, a breach in third-party data causes multiple insurers to make wrongful payouts on their smart contracts.

What sectoral and regional forces could amplify the risk?

- Unclear legal and regulatory standards governing digital contracts
- Underdeveloped technological infrastructure
- Limited knowledge of how smart contracts operate

How can the industry mitigate it?

Goal	Mitigation opportunities
Cyber and operational resilience	• Audit smart contract source codes • Adopt best practices and use safe programming languages
Robust governance	• Reinforce governance mechanisms in smart contracts
Regulatory and legal coverage	• Include smart contracts in existing regulatory and legal frameworks

Risk 2: Growing protection gap for catastrophic cyberattacks

What could go wrong?

Financial institutions' ability to recover from large-scale cyberattacks may be diminishing as insurers begin to limit their exposure. The risk is growing because:

- Cyberwarfare tactics are increasingly being used to accelerate geopolitical tensions between nation states
- Generative AI is lowering barriers to entry for cyber criminals (e.g., using ChatGPT to create malware)
- Funding from nation states enables sophisticated, high-impact attacks
- Limited ability to predict and defend against large-scale cyberattacks is helping to make cyber insurance less affordable

This risk could become systemic if, for example, a cyberattack cripples multiple banks or critical third-party providers that are covered by the same insurer.

What sectoral and regional forces could amplify the risk?

- A large network of third-party service vendors
- Limited availability of cybersecurity diagnostic data
- Lack of cross-border coordination between governments

How can the industry mitigate it?

Goal	Mitigation opportunities
Alternative sources of capital to cover growing cyber risks	• Raise funds in private markets through insurance-linked securities
Public-Private support to prevent or absorb cyberattack damage	• Stress-test cyber underwriting risk and financial resilience • Create resource centers that offer access to cybersecurity tools and services
Intelligence on cyberattack damage	• Quantify cyber risk damage to measure portfolio exposure to cyber threats

To learn more about technology's impact on systemic risk in banking, including examples, please see pages 71-81 of the full report.

Regional conditions

Some systemic risks cut across the financial system, and have either regional dependencies or varied exposure across regions. Here, we look at three examples of regional risks, including some of the ongoing mitigation approaches that the public and private sectors have explored.

Cybersecurity

What is the risk?

Geopolitical tensions, a widening attack surface, and the advancement of hacking tools are causing cybersecurity threats to spike in some regions.

What are the regional factors influencing the risk?

- The availability of technology skills and resources
- The regulatory and legal environment's maturity
- The level of regional cooperation and alliances
- The degree of dependency on external market infrastructure

How are regions mitigating the risk?

Mitigation effort	Example
Harmonization of cybersecurity initiatives and laws	The European Union's Digital Operational Resilience Act aims to improve management of all components of operational resilience, including cybersecurity and incident reporting
Greater availability of cybersecurity tools and techniques	Open-source software such as Snort and OpenVPN, as well as platforms like AWS Security Hub and Google Cloud Security Command Center, offer cost-effective access to basic cybersecurity services
Public-private joint incident response and partnerships	Under the Canadian Financial Sector Resiliency Group, the Bank of Canada is collaborating with the private sector on a sector-wide response to systemic-level operational incidents
Improved cybersecurity capabilities across borders	The Australian Cyber Security Centre provides training to countries in the Indo-Pacific region

To learn more about regional impacts on technology-driven systemic risk relative to cybersecurity, including examples, please see pages 84-86 of the full report.

Tech talent

What is the risk?

Amid labor shortages and a growing reliance on technology, industry players across regions are struggling to find the talent they need to drive innovation or even maintain core operations.

What are the regional factors influencing the risk?

- Economic and social factors
- Immigration policies
- The presence of innovation and technology hubs
- The availability of educational and training programs

How are regions mitigating the risk?

Mitigation effort	Example
Partnerships with academia	JPMorgan Chase's "Tech for Social Good" initiative aims to bridge the tech skills gap by providing education, coding, and mentorship opportunities for young people
Reskilling existing employees	HSBC Malaysia created the Digital Black Belt Development Program, a virtual program to help its employees acquire digital skills in data analytics, machine learning, and automation
Use of no-code and low-code platforms	AXA used OutSystems, a low-code platform, to modernize its claims processing system in just three months, reducing the large volume of calls to the contact center
Establishment of technology hubs	Bank of Montreal (BMO) is setting up tech hubs across North America

To learn more about regional impacts on technology-driven systemic risk relative to cybersecurity, including examples, please see pages 87-89 of the full report.

Climate change

What is the risk?

Amid global pledges to meet net-zero commitments over the next three decades, financial institutions are facing limitations in accessing the data required to price the effects of climate change on their clients.

What are the regional factors influencing the risk?

- Reduced transparency from the share of capital flowing into private markets
- The affordability of remote sensing technology and access to talent pools
- Exposure to high carbon-emitting economies and transition risks
- Ambitious net zero commitments

How are regions mitigating the risk?

Mitigation effort	Example
Climate Hub initiatives for small and medium enterprises	The SME Climate Hub helps small businesses measure their full carbon footprint and tap into new funding opportunities
Publication of climate-related statistical indicators	The European Central Bank has published experimental and analytical indicators that illustrate the impact of climate-related risks on the financial sector
Establishment of global private-public data utilities	The Net-Zero Data Public Utility, which is under development, aims to become a trusted repository of verifiable transition data
Localized insights and regional predictions from complex climate models	The Climate Risk and Resilience Portal is a new, publicly available tool that reveals how future climate scenarios can impact cities and towns in the United States

To learn more about regional impacts on technology-driven systemic risk relative to climate change, including examples, please see pages 90-92 of the full report.

Concluding thoughts

As more financial institutions embrace digital innovation, risks emerge that could threaten the stability of the financial system. Some of these risks originate from a single sector. Others may be specific to a region. Either way, they could proliferate and become systemic without appropriate management.

What can the industry do to help mitigate technology-driven risk originating from outside the traditional financial system?

- Private sector organizations can reinforce their role as trusted partners in customers' financial decisions and engage diverse stakeholders to assess risk exposure
- Public sector organizations can use existing technologies to map common pools of risk and promote media as well as financial literacy among customers
- Private and public organizations can collaborate on stress-testing international response and resilience while strengthening buffers against systemic shocks

Keep in mind that technology-driven risks can be highly dynamic. That means mitigation may depend on a constant stream of knowledge exchange, along with experimentation across jurisdictions and sectors, to be effective and sustainable.

We welcome your questions and ideas and invite you to reach out to any of us by email. For more on this subject, please read the Forum report this summary is based on, Pushing through undercurrents: Sectoral and regional forces influencing technology-driven systemic risk, and resulting mitigation opportunities.

Contacts

Neal Baumann
Financial Services Industry leader
Deloitte Global
nealbaumann@deloitte.com

Rob Galaski
Vice-Chair and Managing Partner
Deloitte Canada
rgalaski@deloitte.ca

A special thank you to Ayesha Madan and John Okoronkwo (co-authors of the Forum report) Gayatri Suresh Kumar and Hwan Kim (project advisers) for their help in developing this report.

Endnotes

1. For more on the information in this paragraph, please see Beneath the surface: Technology-driven systemic risks and the continued need for innovation, World Economic Forum and Deloitte, 2021, https://www.weforum.org/reports/beneath-the-surface-technology-driven-systemic-risks-and-the-continued-need-for-innovation/

2. For more on the information in this summary report, please see Pushing through undercurrents: Sectoral and regional forces influencing technology-driven systemic risk, and resulting mitigation opportunities, World Economic Forum and Deloitte, 2023, https://www.weforum.org/reports/pushing-through-undercurrents-sectoral-and-regional-forces-influencing-technology-driven-systemic-risk-and-resulting-mitigation-opportunities/

3. 92. Fanti, Giulia et al., "Missing Key: The challenge of cybersecurity and central bank digital currency," Atlantic Council, 15 June 2022, https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/

Deloitte.