

Beneath the Surface

Technology-driven Systemic Risks and the Continued Need for Innovation

Part of the Future of Financial Services series

Prepared in collaboration with Deloitte

Foreword

For feedback or questions, please contact:

Drew Propson, Lead Author
drew.propson@weforum.org
+1 (917) 224-6239

The World Economic Forum applies a multistakeholder approach to address issues of global importance. Consistent with this mission, the creation of this report involved extensive outreach to, and dialogue with, numerous organizations and individuals. These included the Forum's financial services, innovation and technology communities, as well as leaders from academia and the public sector.

The outreach comprised over one hundred interviews, a survey and seven global workshops, conducted virtually over the past twelve months to capture insights around the role of technology in both increasing and mitigating systemic risk in the financial system.

The holistic and global content of this report would not be as complete without contributions from the subject matter experts who helped to shape our thoughts on the emergence of technology-driven systemic risks and possible risk mitigation approaches. We particularly thank this project's Steering Committee and Working Group. Their expertise and generosity with their time have been invaluable. Also critical has been the ongoing institutional support for this initiative from the World Economic Forum and the leadership of our Chairman, whose vision for a more inclusive, resilient and sustainable post-pandemic world has been integral to this work. Finally, we are grateful to Deloitte for their commitment to, and support of, this project.

Editor’s note

Recent years have seen an impressive acceleration of technology adoption in financial services. It is no surprise, then, that the potential for digital transformation to improve and strengthen the global financial system has been a primary topic of discussion at many World Economic Forum gatherings. As these discussions continue, they are increasingly accompanied by conversations around new - sometimes hidden - risks that must be considered if we are to unlock the promise of technology and innovation.

Many studies have explored risks to the financial system. However, few have specifically examined technology-driven systemic risk and considered the role technology can play in the risk mitigation process. In this comprehensive study, we bring together a global community of stakeholders across industries and disciplines to better understand these areas and to provide strategic insights to both the public and private sectors.

This study, the first in the Forum’s two-part ‘Technology, Innovation and Systemic Risk’ initiative, builds on previous work focused on the future of artificial intelligence (AI) and emerging technologies in financial services.

Outcomes from our research reinforce that is it not only essential for leaders within the financial services ecosystem to have a solid understanding of the risks forming as a result of the increased use of technology in financial services; of equal importance is collaboration between ecosystem players as solutions are devised.

We hope this document will allow you to dive beneath the surface for a complete view of technology-driven systemic risks and will guide you in decisions around mitigation.

With regards,

Drew Propson

Head, Technology and Innovation in Financial Services
World Economic Forum

Rob Galaski

Vice-Chairman and Deputy Global Leader, Financial Services
Deloitte

Other recent reports from the Future of Financial Services series



2018



2019



2019



2020

Members of the steering committee



Kfir Godrich
Managing Director, Global Head of Technology and Enterprise Services
BlackRock



Chris Mendes
Head, Data and Analytics Strategy and Planning
BMO Financial Group (from July 2021)



Ren Zhang
Chief Data Scientist
BMO Financial Group (through June 2021)



Alan Kaplan
Global Head of Model Risk Management
Citi



Robert Contri
Global Financial Services Leader
Deloitte



Shivaji Dasgupta
Global Head of Data Products and Artificial Intelligence
Deutsche Bank



Kate Platonova
Group Chief Data Officer
HSBC



Max Neukirchen
Chief Executive Officer, Merchant Services
JP Morgan Chase



Nicolas de Skowronski
Head Wealth Management Solutions, Member of the Executive Board
Julius Baer



Moises Nascimento
Chief Data Officer
Itaú



David Craig
Senior Adviser (Former CEO, *Refinitiv*)
London Stock Exchange Group



Abby Fiorella
Chief Technology Risk Officer
Mastercard



Lena Mass-Cresnik
Chief Data Officer
Moelis & Company



Sami Ahmed
SVP, Data and Advanced Analytics
OMERS



Michael Zerbs
Group Head, Technology and Operations
Scotiabank (through June 2021)



Thomas Zschach
Chief Innovation Officer
SWIFT



Michael Dargan
Head of Group Technology
UBS

Members of the working group



Vinod Baya
Head of Emerging Technology
Citi Ventures



Dean Soteropoulos
Managing Director, Innovation Lead (CFO Office)
Credit Suisse



Sophie-Luise Baratta
Strategic Data Lead
Deutsche Bank



Michael Leibrock
Managing Director of Credit and Systemic Risk
DTCC



James Harborne
Head of Group Digital Public Policy
HSBC



Anand Autar
Global Head of Analytics Business Development
ING Group (from March 2021)



Ayse Duran
Global Head of Analytics Strategy and Special Projects
ING Group (through March 2021)



Jonathan Hayes
Head Digital Assets Development
Julius Baer



Laura Sartenaer
Strategy Manager
London Stock Exchange Group



Philip Garner
Head of Innovation
Lloyds Banking Group



Carl Jansson
SVP Enterprise Architecture and Technology
Mastercard



Nabeel Vilcassim
Managing Director
Moelis & Company



Vincent Loy
Assistant Managing Director (Technology)
Monetary Authority of Singapore (MAS)



Roland Fejfar
Head, Technology Business Development and Innovation EMEA/APAC
Morgan Stanley



Kevin Hanley
Head of Innovation
NatWest



Steven Asprey
Managing Director, Global Diversified Program
OMERS



Eva Gustavsson
Director, Government Relations EMEA
PayPal



Shawn Rose
Chief Digital Officer and EVP
Scotiabank (through June 2021)



Christian Mittelberg
Global Risk Officer
S&P Global



Shane De Zilwa
Vice President of Analytics
Verisk Analytics



Michael Jabbara
Vice President, Global Risk
Visa



Gero Gunkel
Chief Operating Officer, ZCAM
Zurich Insurance

Members of the project team

Project leadership

The Technology, Innovation and Systemic Risk project leadership team includes the following individuals:

World Economic Forum

Drew Propson, Lead Author, Head of Technology and Innovation in Financial Services

Matthew Blake, Head of Financial and Monetary System Initiatives

Professional services leadership from Deloitte

Rob Galaski, Co-Author, Project Adviser, Vice-Chairman and Deputy Global Leader, Financial Services

Hwan Kim, Project Adviser, Director

Taryn Mason, Project Adviser, Chief of Staff

Project authors

The World Economic Forum expresses its gratitude to the following individuals on the project team:

Deloitte

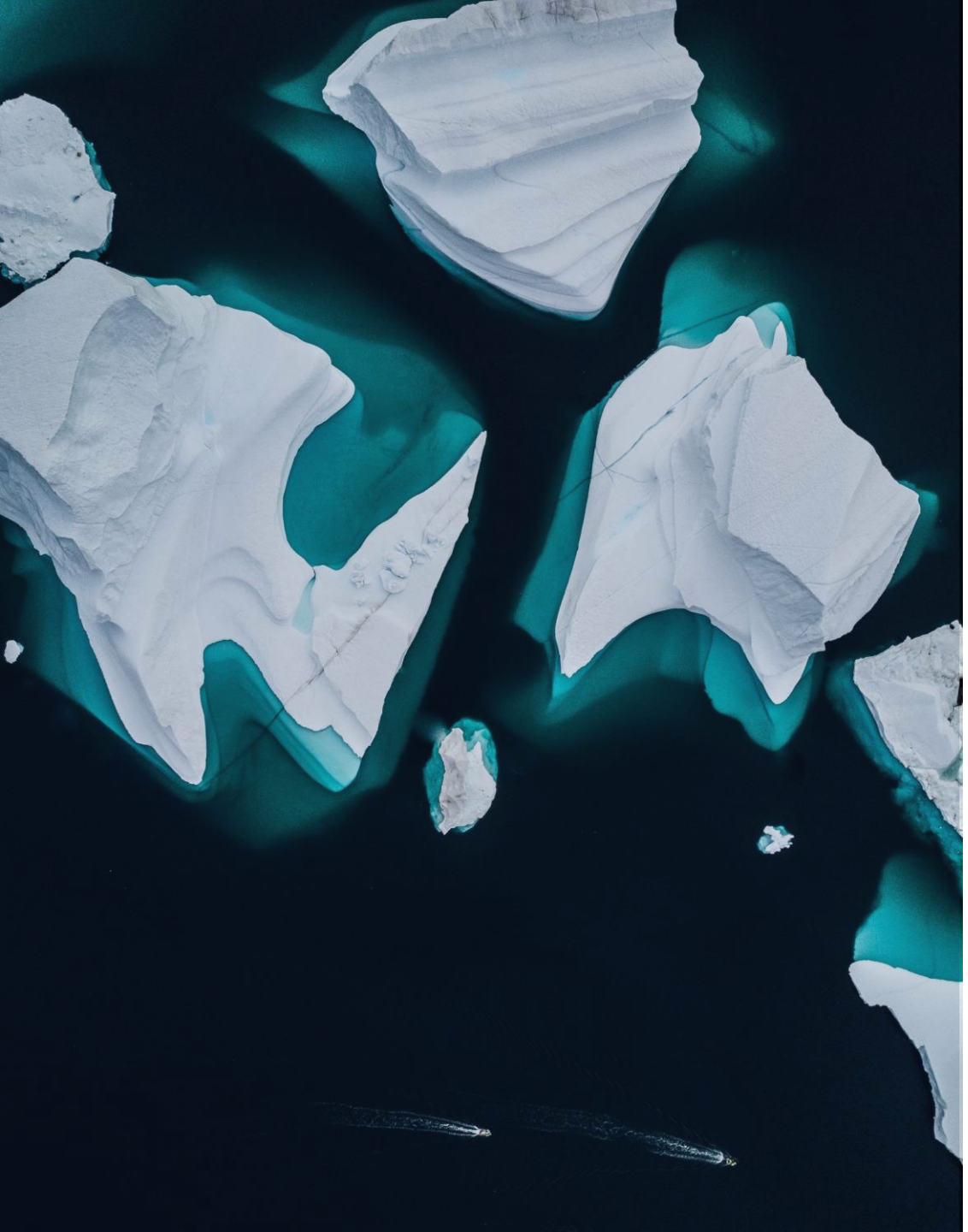
Anthony Korshunov, Manager (Secondee to the Forum)

Megan Long, Senior Consultant (Secondee to the Forum)

Additional thanks

The project team expresses gratitude to the following individuals for their contributions and support:

Emina Ajvazoska
Anne Ardon
Derek Baraldi
Itan Barmes
Filipe Beato
Andre Belelieu
Allen Chen
Luca De Blasis
Seán Doyle
Noah Faulkner
Chris Knackstedt
Isaac Kohn
Haleh Nazeri
Colin Soutar
Denizhan Uykur
Ben Weisman



Cover and inside art: Unsplash/Annie Spratt[1] and Deloitte Image Library

Table of contents

Context and approach	8
Executive summary	13
Key findings	19
Defining systemic risk	26
Deconstructing current sources of risk	32
Exploring and mitigating technology-led systemic risks	44
Conclusion	122
Acronyms and abbreviations	126
Acknowledgements	128
Endnotes	132

Context and approach

An emerging field of inquiry is the role of technology in both increasing and mitigating systemic risk in the financial system and, by extension, the economy.

- The most recent report of the Future of AI in Financial Services project began to uncover how emerging technologies are giving rise to entirely new and highly complex risks, while also unlocking new approaches to mitigating certain risks.
- To this end, the Technology, Innovation and Systemic Risk initiative has been launched to further explore the relationship between the adoption of technologies in financial services and systemic risk.

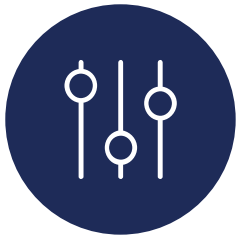
Research objectives:



Identify potential and evolving short- and long-term risks stemming from the increased utilization of technologies in financial services.



Deconstruct the identified risks and explore the potential scenarios and associated implications that could emerge as these technologies become more prevalent.



Explore plausible mitigation strategies and ways that innovation and the technologies themselves can be leveraged in the risk mitigation process.

Over the past year, around 200 financial services and technology experts have been engaged in a series of global workshops and expert interviews.*

Research approach

Global workshops

Seven workshops were conducted during 2021 – all virtually. These sessions brought together leaders from financial system 'players': financial institutions (e.g. banks, asset managers, exchanges, infrastructure providers); financial and non-financial technology firms; regulators and policy-makers. Non-governmental organizations and academic institutions were also engaged in a series of interactive discussions with these entities. Four workshops were hosted to derive insights across unique risk themes and two were focused on risk mitigation. An additional workshop was hosted in collaboration with the Forum's 'Quantum Security' initiative to explore emerging risks related to quantum technology in financial services.

Expert interviews

Interviews were conducted with over 100 public and private sector leaders from prominent entities, as well as with experts adjacent to the industry.

Survey

Over 50 representatives participated in an anonymized survey focused on the sources of risk (SoR) and their perceived impact on players, the ecosystem and the related likelihood of occurrence. While not a scientific mapping, this survey offered indications of the level of concern associated with the sources of risk.



The inclusion of company case studies or references within this report does not reflect an explicit endorsement of the company or its products and services by the World Economic Forum.

*Note: Please see Acknowledgements (p. 126) for a list of individuals who participated in the workshops, interviews and survey.

This report will provide leaders, regulators and policy-makers with a perspective on the most significant technology-led systemic risks in financial services and how they can be mitigated.



This report **WILL…**

- **Explore the most significant, technology-led systemic risks** that financial services ecosystem players should be concerned about and detail the potential impacts of these risks.
- **Illustrate the current gaps in mitigation strategies**, alongside the potential uncertainties and unintended consequences players should consider.
- **Highlight examples of players deploying specific mitigation strategies**, enabled by technology and innovation.
- **Share insights on potential innovative mitigation applications** that can be explored by ecosystem players moving forward.



This report **WILL NOT…**

- **Focus on systemic risks that are not either created or amplified by technology** in the financial services ecosystem.
- **Provide a detailed sectoral or geographical perspective** as it relates to both the exploration and mitigation of identified systemic risks.
- **Provide in-depth technical explanations of financial, operational or technological dimensions of use cases** or mitigation applications.
- **Evaluate use cases or make specific recommendations** on which mitigation applications individual players should pursue.

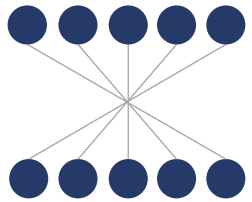
This report **seeks to help…**

- **Leaders focused on strategy, innovation and/or risk at financial and non-financial organizations to:**
  1. Understand the most pressing systemic risks created or exacerbated by technology in financial services
  2. Evaluate the actions that can be undertaken to mitigate these risks
  3. Assess potential, innovative mitigation applications that can be explored in the future.
- **Regulators and policy-makers** to understand the potential impact of technology-led systemic risks on the financial services ecosystem. It aims to help craft mitigation responses that foster an innovative ecosystem while ensuring adequate safeguards are built for consumers, markets, players, and society.

Research efforts have focused on uncovering heavily interconnected and deeply ingrained risks that can create exogenous shocks to the system.

Numerous risks that create varying degrees of impact exist within the ecosystem.

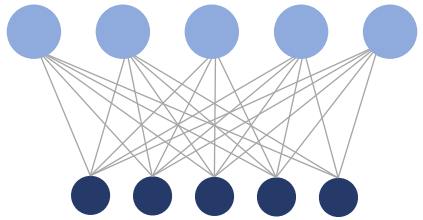
Idiosyncratic risk



Truly isolated risks that are organization-specific and resolvable. Otherwise known as unsystematic risks *(e.g. operational risks within a single entity)*.[2]

Out of scope/adjacent area of input

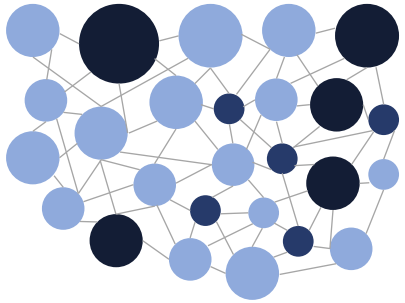
Systematic risk



Broader market risks that cannot be resolved by diversification of organizational operations but can be managed - to a certain extent - through coordination *(e.g. exchange rate risk)*.[3]

Out of scope/adjacent area of input

Systemic risk

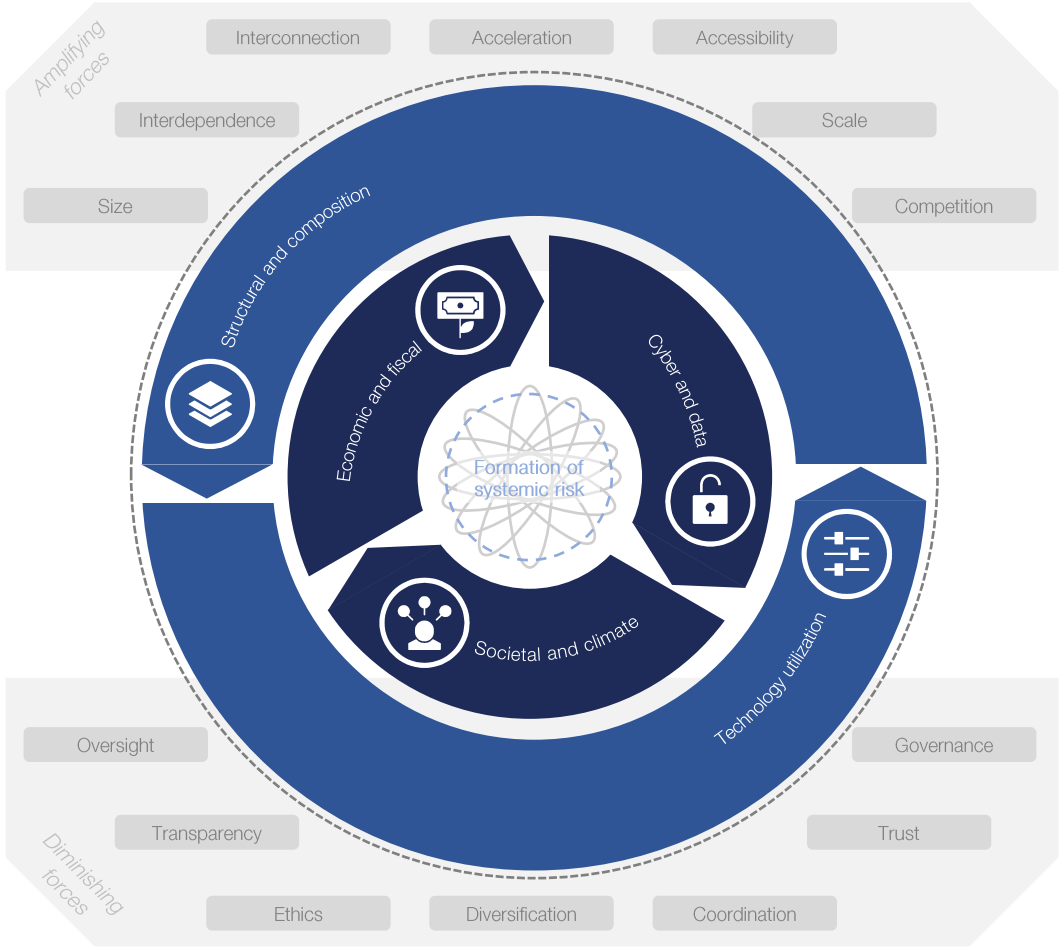


Seemingly isolated risks that grow and spread across heavily interconnected and deeply ingrained products, services, and systems *(e.g. "Too big to fail" risks, leading to the 2008 Global Financial Crisis (GFC))*.[4]

Key focus area

Executive summary

The growing adoption of technology is giving rise to new sources of risk (SoR), which can accumulate across the ecosystem to form systemic risks.



Deconstructing sources of systemic risk

Systemic risk is often difficult to interpret and anticipate, and mitigation approaches are predicated on learnings derived from past incidents. Looking into the future, potential systemic risk scenarios can be broken down into their underlying components.

Sources of risk

SoR are the short- and long-term situations that create loss or drive uncertainty in the financial services ecosystem. Risk-focused leaders often look at these as independent variables that are unlikely to be systemic on their own. However, when these sources come together and materialize as ecosystem events, they can contribute to the development of systemic risk. For this reason, it becomes crucial for ecosystem players to assess their exposure across these sources to better anticipate and measure outcomes of systemic risk.

SoR can be organized across five key topic areas, two of which are cross-cutting.* Select examples of sources include:

Structural and composition

- Consolidation of a few vendors that offer critical capabilities
- Growing ecosystem interconnectivity and modularity
- Undefined regulatory oversight for new entities/business models

Technology utilization

- Algorithmic and model deficiencies
- Inexplicable machine- and model-led outputs
- Operational consequences of technology implementation

Foundational and cross-cutting

Economic and fiscal

- Obscurity in increasingly complex supply chains
- Increasing displacement of deposits
- Asset price volatility

Cyber and data

- Lagging cybersecurity mechanisms
- Identity misrepresentation and authentication vulnerabilities
- Stagnant and inconsistent data privacy controls

Societal and climate

- Dissemination of media and false information
- Damage caused by natural disasters/catastrophic events
- Rising geopolitical tensions

***Note:** The sources of risk outlined in this report are not intended to be exhaustive, however a comprehensive list of the identified SoR and the resulting risks can be found on pp. 35-39.

Individual sources of risk can be combined into six distinct themes that highlight the role of technology in creating and amplifying systemic risk.



Digital interdependencies

New interconnections and collective dependencies on certain critical service providers significantly contribute to the number of vulnerable nodes that could threaten and exploit the financial system's essential functions.



Shared model vulnerabilities

The lack of common taxonomy across external policies and the absence of forward-looking information being embedded into modelling applications present extensive uncertainties for how players anticipate stochastic risk events.



Gaps in entity-based regulation

Certain emerging financial activities remain unaccounted for by the current regulatory regime due to unapplicable customary approaches, presenting risks to financial stability, consumer protection and market integrity.



Conflicting national priorities

Incompatible nation-state approaches, coupled with a lack of sound global conduct and coordinated efforts, are allowing cyberattacks, financial crime and cross-border data issues to create harm to the global financial system.



Emerging sources of influence

Emerging sources of influence are creating new opportunities for market manipulation and a paradigm shift to participation in financial markets that extends beyond the scope of current protection mechanisms.



New drivers of financial exclusion

While technology has been instrumental in promoting financial inclusion, several unintended consequences are emerging, such as inaccessibility and algorithmic biases, which are hindering global financial prosperity.

The increased frequency of systemic events signals a pressing need for industry players to act and address seemingly isolated risks before they grow and spread across the ecosystem.

Lessons learned from past mitigation efforts in financial services



Systemic risk is hard to measure and difficult to prevent without solving information asymmetry

As players continue their digital transformations, there is an impetus to introduce **novel, forward-looking methodologies for monitoring and anticipating risk** that can be supported by enhanced data and analytical capabilities. Keeping regulatory functions informed in real time will also kick-start resiliency plans and recourse measures to prevent the scaled impact of a potential crisis.



Players should be deliberate about which ecosystems they participate in

Private and public sector players should remain **conscious of their external relationships**. Broader vendor networks (e.g. fourth-party exposures) can be monitored using new forms of technology while reducing overreliance on a single vendor's shared capabilities. For example, while new monitoring capabilities can be enabled by 'as a service' providers, leaders must be aware of the trade-off when adding to ecosystem dependencies, which inadvertently create additional sources of operational risk.



New incentives can be sought for multilateralism

While many emerging use cases of systemic risk mitigation are being developed collaboratively, there is no industry-wide vision of the future across most jurisdictions; competing priorities and misaligned data-sharing mechanisms continue to limit the ability to effectively scale up functions. Although support from global policy bodies can make it easier for players to reach agreements, certain **burden-sharing and demand-driven incentives may be more effective in accelerating collective solutions.**



More alignment is required on the regulatory boundary of financial services

Certain non-financial players' business models and activities are not currently under the purview of financial services supervision and regulation. Public sector players **need to deconstruct the range of emerging activities to ensure a consistent taxonomy and adequate regulatory coverage** that appropriately defines the scope of oversight across new offerings. Suitable applicability may range from the optimization of existing processes to the creation of entirely new business models.



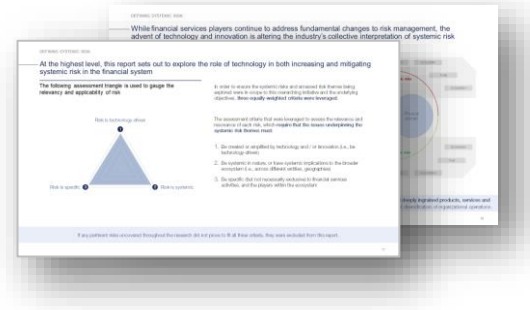
Sources of systemic risk are driven by context

'One size fits all' approaches do not exist to address the varying contexts that drive SoR. For example, societal issues such as digital or financial exclusion and literacy can be **recognized and addressed as separate but connected issues**. The nomenclature and understanding of these issues should be standardized across jurisdictions, however, their approaches must remain tailored.

This report is comprised of three core sections that explore the role of technology and innovation in creating, amplifying and mitigating systemic risk in global financial services.

Jointly presented across six systemic risk themes

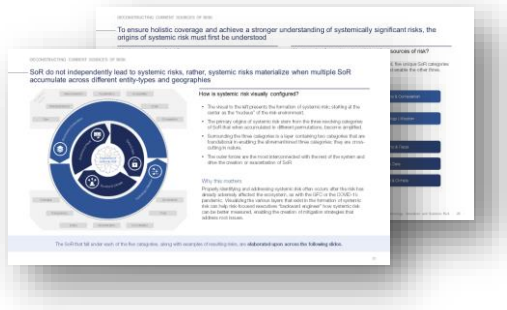
1 Defining systemic risk



Description

A brief precursor on systemic risk, including current ecosystem responses and the criteria employed to discover technology-driven systemic risk

2 Deconstructing current sources of systemic risk



An introduction to the most common sources of systemic risk and how they are creating vulnerabilities to global financial services players

3 Exploring and mitigating technology-led systemic risks

Risk exploration



An exploration of the most significant technology-driven systemic risks that are being observed today and the role that technology plays in creating or exacerbating these risks

Risk mitigation



An exploration of what can be done to address these systemic risks through individual and multilateral efforts, including potential technology-driven mitigation applications

Six key findings summarize how ecosystem actors need to respond to the role that technology plays in creating and amplifying systemic risks within financial services.

Technology-driven systemic risk is…



Introducing protection mechanism vulnerabilities

1. Unregulated and partially regulated financial players are contributing to a disproportionate share of systemic risk.
2. The traditional determinant of an entity's systemic importance (i.e. the size of its book) is becoming less relevant than the size of its network.



Increasing the importance of external risk management

3. Ecosystem interconnections are no longer bilateral; as the number of interlinkages between service providers continues to grow, players will need to comprehensively understand their entire ecosystem exposure.
4. As stochastic events grow in intensity (e.g. cyberattacks, climate change), industry players must deploy forward-looking risk prevention and detection mechanisms.



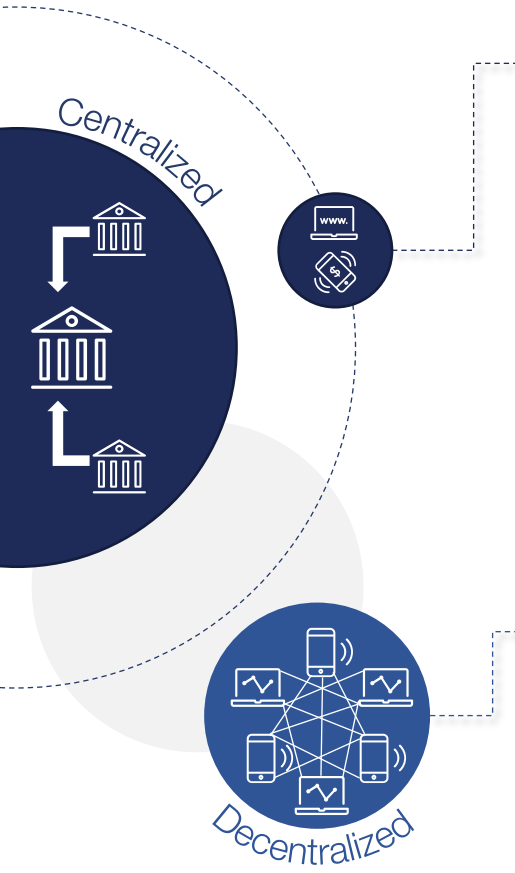
In need of collective, foundational solutions

5. To successfully combat financial crime and cybercrime, global players must undertake joint efforts that account for inconsistent national approaches and promote multilateral information sharing.
6. While the potential for technology to enhance risk mitigation is undeniable, addressing systemic risk must start with the basics (e.g. shared taxonomy, coherent frameworks).

Key findings

Unregulated and partially regulated financial players are contributing to a disproportionate share of systemic risk.

Examples include novel business models operating in, and at the periphery of, financial services.



Lightly regulated Big Tech* models

Big Techs are in the early stages of pursuing expansion in financial services; however, data-driven network effects could quickly turn these entities into large financial gatekeepers. Although subject to similar requirements as FinTechs (i.e. licenses), limited regulatory treatment exists to account for the full breadth of Big Tech business models.[5]

Unregulated decentralized finance (DeFi) models

Based on a blockchain foundation, DeFi is growing in the absence of intermediaries and central accountability. These offerings can seamlessly operate outside of regulatory structures. While the system offers a low-cost, transparent alternative to traditional financial services, its open-source protocols are predisposed to malicious hackers and financial crime.[6]

What should be considered?

As industry lines blur, so can regulatory functions

Coordinated action across regulatory functions (e.g. central banks, competition authorities, conduct regulators) will be needed to disaggregate existing rulesets and review individual business lines. Recalibrating the mix of entity-based and activity-based oversight may also be effective in expanding regulatory perimeters to cover new business models.

Novel business models can be unpacked

Understanding the nuances of new business models can be a crucial first step to tailored regulation. For example, the business objectives of Big Techs are not always based on interest income like those of incumbents; rather, they are often based on data and flow-of-business. The structural composition of these players should also be considered as they may differ by region and jurisdiction (e.g. China's integrated digital ecosystems).

***Note:** For the purposes of this report, 'Big Tech' refers to dominant global technology players, which also operate as Cloud, CaaS and SaaS providers in the ecosystem.

The traditional determinant of an entity's systemic importance is based on the size of its book, which is becoming less relevant than the size of its network.



A systemically important financial institution (SIFI) is defined by its 'size of book' (e.g. total assets) and other financial indicators*; this designation results in stricter capital requirements and increased supervisory scrutiny to prevent disruption to the financial system.[7]



While the financial definition of size and significance is an accurate indicator of systemic financial risk, it lacks direct attribution to non-financial players that are heavily digitally interconnected (e.g. cloud providers).



Ways of tackling systemic risks outside of financial networks remain in the formative stages (e.g. Digital Markets Act) and concerns around non-financial systemic importance grow as operational failures or cascading cyberattacks on vendors become harder to trace.[8]



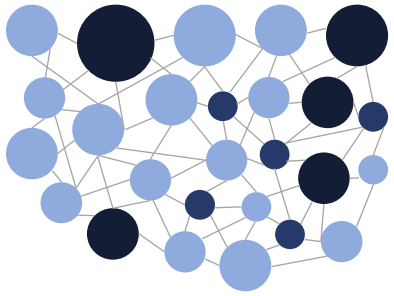
The players that pose systemic risks are more complex than the regulatory focus on financial entities indicates; although financial institutions are still some of the most interconnected in the economy, many of the most connected players today exist in other sectors (e.g. Big Tech, retail, telecommunications).[9]

Concerns around concentration risk can be addressed by creating an industry-agnostic systemic designation to account for the systemic nature of players outside of financial services. For example, nation states can explore standing up a dedicated entity-based regulatory body that accounts for data-driven business lines.

*Global systemically important banks (G-SIB) are classified based on financial indicators of size, complexity, intra-financial system transactions, cross-jurisdictional activity and substitutability. Non-banks undergo a three-stage process that covers size, plus at least one other indicator.

Ecosystem interconnections are no longer bilateral; as the number of interlinkages between service providers grows, players will need to comprehensively understand their entire ecosystem exposure.

Technology has changed how entity-to-entity relationships are made:



- Risk must be accounted for across every indirect node in the network; studies have shown that 'ripple events' have increased 20% annually since 2008 (where multiparty digital incidents or attacks impact an average of 10 downstream entities, e.g. third-, fourth- and fifth- parties).[10]
- The modularization of technology (e.g. the transition from integrated to modular technology stacks) further drives this complexity, as players become more exposed to inter-reliance risks
- This shifting dynamic necessitates players to employ technology-based solutions that enable them to map, monitor and oversee their networks more comprehensively, and to work with connected N^{th} parties to strengthen their overall network resilience.

Potential considerations for ecosystem players

Public sector — Multilateral — Private sector

Blockchain-enabled digital regulatory reporting (DRR)

By establishing a blockchain-based DRR platform, regulatory functions can be equipped with complete entity-level information in real time, to identify network abuses or vulnerabilities.[11]

Dynamic risk assessment (DRA) for interconnectivity

DRA platforms established on an open application programming interface (API) can help to factor interconnectivity and velocity into risk measurement, creating a better understanding of risk groupings that are likely to materialize across network nodes.

Monitoring of a comprehensive vendor inventory

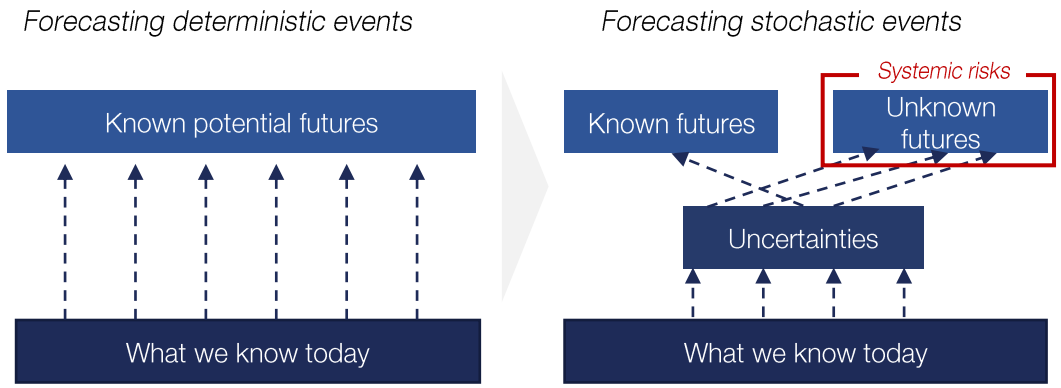
Digital vendor attestation programs will enable third-parties to automatically identify their fourth-parties within a central system. Players can then embed digital incident management into risk reporting functions.[12]

As stochastic events such as cyberattacks and climate-driven incidents grow in intensity, industry players must deploy forward-looking risk prevention and detection mechanisms.

The growing frequency of exogenous shocks is placing strain on the traditional models leveraged by financial players.

- If not properly anticipated and accounted for, the potential compounding effects of exogenous shocks could significantly compromise the resiliency of players, nations and the global financial system.

- As players move into a future where 'edge' cases grow in frequency and little data exists to predict an unknown or unknowable future (e.g. through historical or time series data), emerging technology and techniques must be leveraged to better detect these events before they occur.



What are some novel data sets that can be used to better anticipate stochastic events?

Synthetic data can enrich early warning indicators

Financial institutions can enhance their repository of early warning indicators by sourcing anonymized, synthetic data sets to uncover important interactions that exist in typical 'out-of-sample' predictions. Coupled with machine learning (ML) techniques, such analysis can capture the evolution of sources of risk before they form stochastic events.[13]

Spatiotemporal data can estimate the impacts of stochastic events

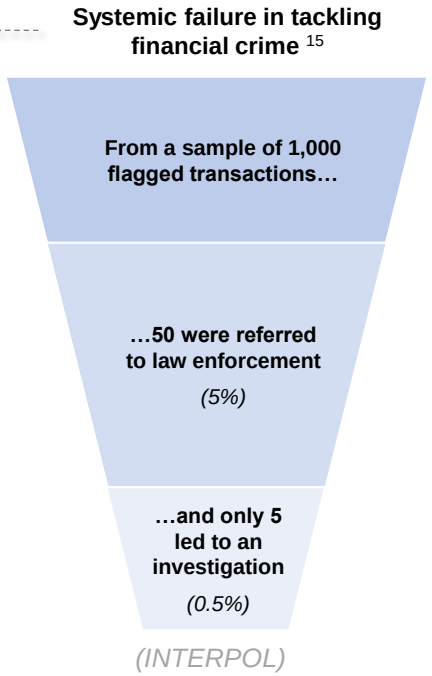
Spatiotemporal comparison data can also be used with ML techniques to formulate matches across space and time to uncover new events (e.g. climate-related weather patterns). This data can be mapped using correlation networks across shorter time horizons and will enable financial institutions to estimate stochastic events and their potential impacts more quantitatively.[14]

To successfully combat financial crime and cybercrime, global players must undertake joint efforts that account for inconsistent national approaches and promote multilateral information sharing.

While difficult to track, the global economic and social costs of financial crime and cybercrime are estimated to be upwards of $1.5 trillion.

Building multilateral alliances

- Despite a broad industry consensus for more legal clarity in cross-border information sharing, there is limited bandwidth and legal consistency across public-private alliances for sharing personal identifiable information (PII) data for the prevention of financial crime and cybercrime.
- In the absence of formal legal gateways, multilateral arrangements between nation states can be incentivized based on resolving common issues and tackling shared burdens.
- These arrangements could involve or augment existing efforts and build on the experience collected in other jurisdictions (e.g. on anti-money laundering (AML), combating the financing of terrorism (CFT) and cybersecurity).



What role can technology play in this?

1. While the role of privacy is debated globally, privacy enhancing technology (PET) presents a unique technical ‘answer’ to this problem. Homomorphic techniques are finding ways to safely cultivate personal data portability but require the backing of legal frameworks.
2. Steps towards secure data portability could lead to the formation of a shared database for illicit transactions, enabled and scaled through distributed ledger technology (DLT). This would allow for the easy traceability of bad actors across all participating players.
3. Another option could be to explore the design of a multi-state utility with full-scale monitoring and alert-handling capabilities that supplement transaction monitoring (TM) for global banks.
4. At the entity level, monitoring solutions such as natural language processing (NLP), network analytics, and knowledge graphs can more readily identify relationships between entities to support due diligence and monitoring of potentially suspicious actors.

While the potential for technology to enhance risk mitigation is undeniable, addressing systemic risk must start with the basics.

Making a case: “If you can’t resolve the issue on the back of a napkin, then you likely can’t resolve it with a sophisticated digital tool”.

In parallel to testing and deploying mitigation applications, players need to ensure that these solutions are resilient for the future.

A common understanding of risk is an essential first step. Without a common understanding in the form of frameworks, principles and standards, fragmented efforts and siloed information will make global prevention of systemic risk difficult. It also makes it more challenging for non-risk focused executives to integrate, improve and apply mitigation techniques.

What is a proof point for this?



It is difficult to produce decision-useful information with global climate risk assessment methodologies and tools (e.g. scenario analysis). Despite some actions by stakeholder groups (e.g. reinsurers, financial institutions, regulatory and standard-setting bodies), initiatives remain fragmented and considerable work lies ahead because of the quickly evolving nature of climate science, alongside factors that will influence transition efforts.[16]

‘Speaking the same language’ on risk will enable meaningful consultations both within and across sectors, industries and nation states.

Key steps to consider:

- Middle power nations can create an objective-driven framework for calibrating on emerging risks (e.g. responsible AI) across businesses, governments and policy-/standards-makers.
- Global policy bodies can create specific risk indexes (e.g. quantum ‘readiness’) to benchmark efforts and raise awareness of clear action points among decision-makers.
- National public and private sector players can establish a platform to foster partnerships across industries and align on innovative models (e.g. innovation networks, sandboxes), specifically between the financial industry and broader economy (e.g. Big Tech, telecommunications providers).
- Financial institutions can enhance how they evaluate their ecosystem beyond what is required for consumer-focused compliance (i.e. the shift from ’know your customer’ (KYC) to ‘know your product, partners and people’).

Defining systemic risk

Six recent developments have led to fundamental shifts in the dynamics of the global financial services ecosystem.

1



Accelerated digital transformation

There is an increasing need for agile, scalable, secure and resilient technology infrastructures, with large incumbents revamping their ‘core’ to address the volume and pace of digital change. While doubling down on advanced technologies such as AI, incumbents recognize true digital success is contingent on sound back-end foundations such as system architecture, APIs, DLTs, and robotic process automation (RPA) to enable all-digital processes.

2



Increased value chain disruption

FinTech players are rapidly developing innovative solutions while technology (i.e. Big Tech), telecommunications and retail players are entering the ecosystem with financial products of their own to reduce the dependency on intermediaries. Intensifying competition along the value chain is leading to more agile decision-making and the development of new, adaptive products.

3



Augmented regulatory pressure on financial activity

The regulatory landscape is highly jurisdictional whereas the digital world is inherently global. Although the magnitude and speed of regulatory change continues to lack uniformity across jurisdictions, greater regulatory attention is being placed on preventing financial failures and enhancing consumer protection, especially around new technology-enabled financial products. The emergence of new business models also raises the question of whether the coverage provided by current entity-based regulatory frameworks is sufficient.

Six recent developments have led to fundamental shifts in the dynamics of the global financial services ecosystem.

4



Enhanced focus on ESG priorities

As environmental disasters and societal incidents rise in frequency and severity, sustainability is of increasing importance globally for governments, businesses and citizens, cementing environmental, social and governance (ESG) as a key pillar of decision-making. While sustainable investing continues to shape the bottom line of organizations and regulators demand stringent reporting, incumbents are prioritizing ESG initiatives and related mitigation efforts (e.g. climate-related disclosures, green finance, sustainable investments, resilience planning).

5



Growing democratization of data

As data-sharing partnerships between incumbents and third-parties continue to rise, with new integrations to data and service offerings, markets are shifting towards more open and economically distributed models of data access (e.g. open banking). Greater levels of standardization and data security are improving data-driven innovation and risk management efforts.

6



Rising malicious activity

Cybersecurity and financial crime prevention have been top strategic priorities for most financial players, but the COVID-19 pandemic exposed severe vulnerabilities and unpreparedness. Given the maintained pace of digital interconnectedness, malicious activity is poised to increase in velocity and magnitude, requiring greater coordination of resources from both the private and public sectors.

These fundamental technology-related changes to the ecosystem are altering the industry's collective interpretation of systemic risk management.

What is technology-driven systemic risk as it is known today?

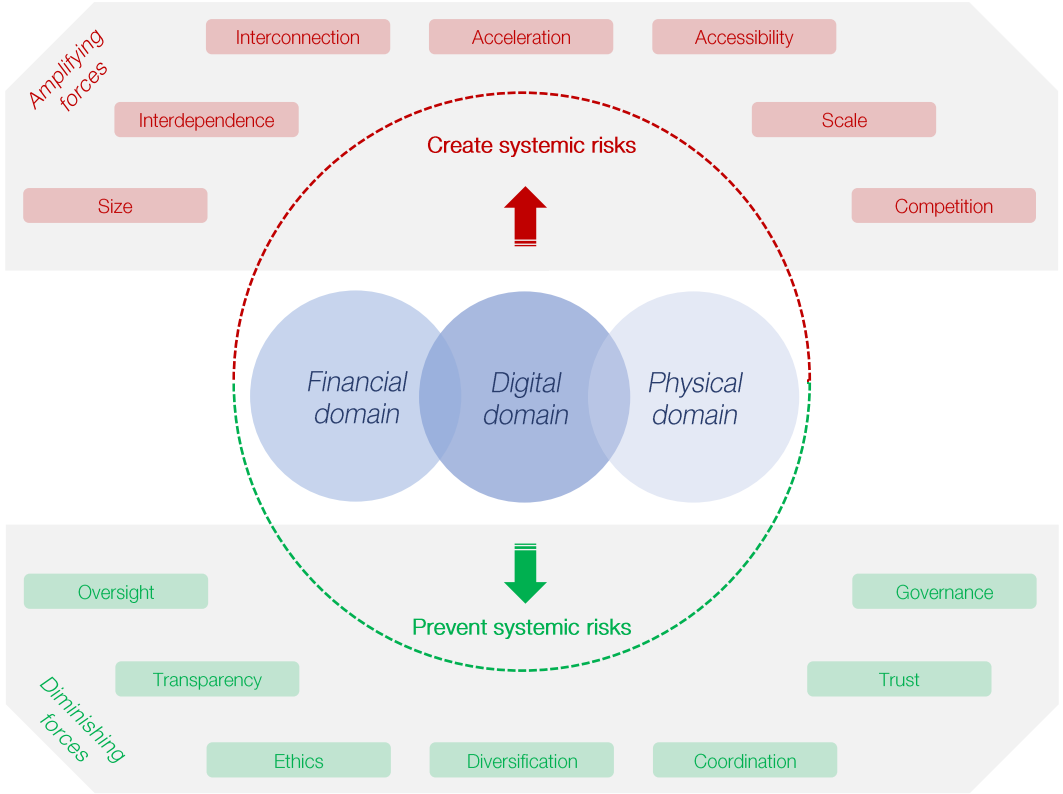
Demonstrated by the 2008 GFC and again during the macroeconomic shock from the COVID-19 pandemic, financial linkages remain an important aspect of analyzing systemic risk, however, inconsequential attention is being paid towards digital interlinkages across the financial services ecosystem and the broader economy.

Critical systemic interlinkages exist across three spheres of impact: the financial domain (e.g. transactions, credit, markets), the digital domain (e.g. technology-based networks), and the physical domain (e.g. critical infrastructure).

Systemic risk events can now seamlessly cascade between the digital domain and the two other spheres. Digital-physical risks (e.g. cloud outages due to extreme weather events) and digital-financial risks (e.g. cyberattacks halting central transaction clearing) can take on different forms and magnitudes of impact.

To effectively understand and mitigate systemic risk today, financial services players need to recognize the close relationships between the digital, financial and physical domains, alongside the associated cascading implications between each one.

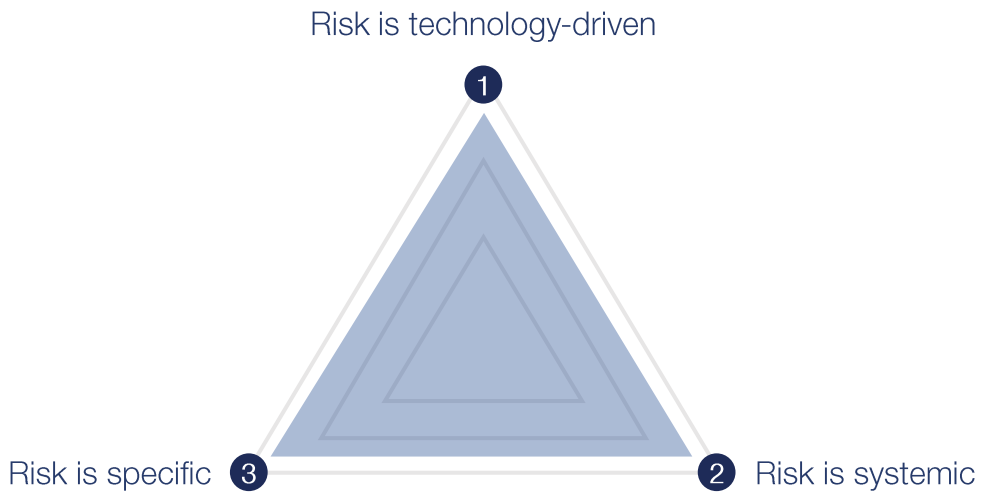
Particular attention must also be paid to the amplifying and diminishing forces alongside the origins/SoR to inform the necessary frameworks and mechanisms that can successfully prevent its evolution.



This report views systemic risk as a compilation of **seemingly isolated risks that grow and spread across heavily interconnected and deeply ingrained products, services and systems over a defined time horizon**. Upon inception, this type of risk cannot be resolved by a single entity or through the broader diversification of organizational operations.

Three equally-weighted criteria were applied to determine which risk themes were considered in-scope for this report.

The following assessment triangle is used to gauge the relevancy and applicability of risk.



The criteria used to assess the relevance and resonance of each risk **require that the issues underpinning the systemic risk themes must**:

1. Be created or amplified by technology and/or innovation (i.e. must be technology-driven).
2. Be systemic, or have systemic implications to the broader ecosystem (i.e. across different entities and geographies).
3. Be specific (but not necessarily exclusive) to financial services activities and the players within the ecosystem.

If any significant risks uncovered throughout the research did not fit all three criteria (e.g. environmental impact of emerging technologies, extreme natural events hindering contingency plans, replacement of reserve currencies), they were **excluded from this report.**

One example of a significant risk theme that was excluded is the energy consumption and unintended environmental consequences of emerging technologies in the financial sector.

Defining the risk



- While the accelerated adoption of emerging technologies is generally perceived to be beneficial to reducing the carbon footprint of financial services, the energy consumption of these technologies presents new environmental concerns; while these concerns may have systemic implications, the ability to directionally measure the magnitude of carbon-linked impacts - and how those could disrupt the financial ecosystem - is limited.

- High-performance computing technologies (e.g. crypto asset mining, training AI systems, reliance on cloud data centres, quantum computing) can be notoriously power-hungry. With the inevitable transition towards increased digitalization, the associated liabilities are not yet well understood.[17]

- Not only do players have an imperative to understand and manage climate risk, but they are also expected to report on their climate impact; this obligation has not yet extended to cover the measurement, reporting and verification of their deployments of, and investments in, emerging technologies.[18]

Mitigating the risk

The question of how best to mitigate the potential impact of emerging technologies contributing to the global climate crisis has turned to the technologies themselves. The 'switch to green' is already happening in various technology domains (e.g. crypto assets, cloud technology), however, more can be done in striving for sustainable energy practices across the entire ecosystem.



DLT-fueled disclosures: Climate-related disclosures are a prerequisite to improving issues related to transparency and can be strengthened by using DLT applications that are immutable and automated (e.g. self-executing contracts to automate disclosure incentive systems) to better track, capture and deploy information.[19]



Climate-friendly innovations: Starting with the transition to proof of stake blockchain systems, coupled with the pursuit of other sustainable improvements (e.g. minimizing hardware requirements for blockchain nodes, integrating with eco-friendly hardware), blockchain and crypto-assets continue to lessen their net carbon impact.



Offsetting carbon emissions: As financial and technology players face increasing pressure to decarbonize, players can not only estimate the carbon footprint of their digital asset holdings but must also look to offset their carbon emissions by using carbon credits or transitioning to green resources (e.g. solar power-fueled crypto mining, data centres).[20]

While this risk theme, alongside other significant issues, did not prove to fit all three of the assessment criteria, they remain resonant systemic risks that **financial services players should actively monitor and prevent**, especially given the role that **technology may have to play in their mitigation**.

Deconstructing current sources of risk

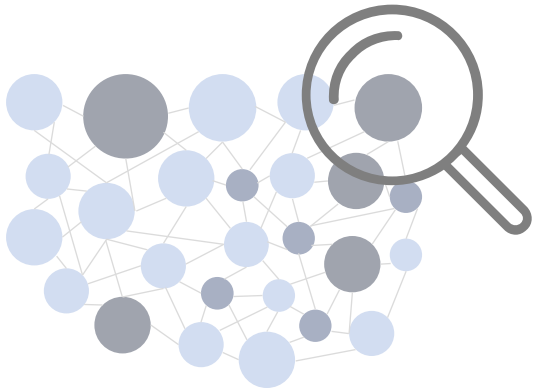
To ensure holistic coverage and achieve a stronger understanding of systemically significant risks, the origins of systemic risk must first be understood.

What are sources of risk (SoR)?

Systemic risk is often difficult to interpret and anticipate, and mitigation approaches are often predicated on learnings derived from past incidents. Looking into the future, potential systemic risk scenarios can be broken down by their underlying components (i.e. SoR).

SoR are the short- and long-term situations that create loss or drive uncertainty in the financial services ecosystem.

SoR are unlikely to be systemic on their own. However, in accumulation, they can contribute to the development of systemic risk. They can also help to identify resulting risks and have served as research 'guideposts' when investigating the role that technology plays in both amplifying and mitigating risk.



What five categories of sources of risk have been identified?

Given the number of SoR that may exist, five unique SoR categories were identified, two of which enable the other three:

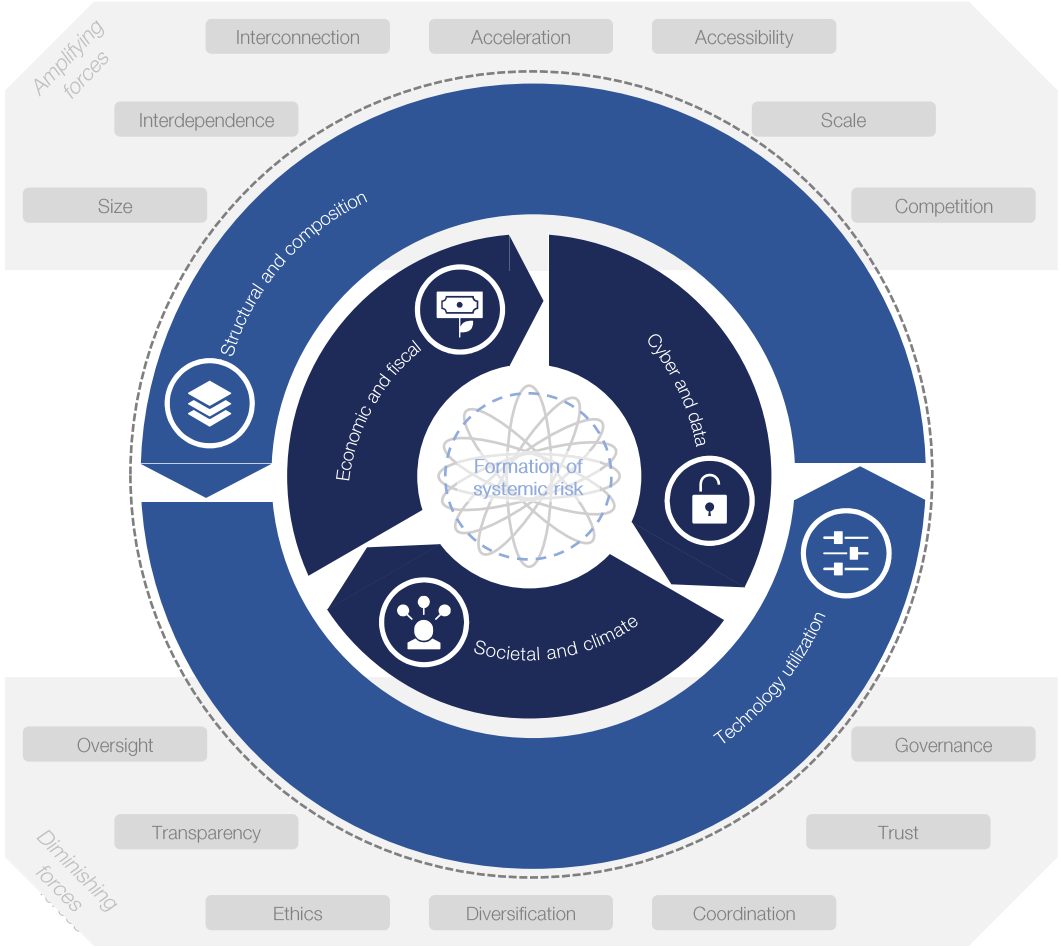
These two SoR categories are viewed as foundational and enable…

- Structural and composition
- Technology utilization

…three other SoR categories that directly contribute to the formation of systemic risk.

- Economic and fiscal
- Cyber and data
- Societal and climate

SoR are not independently systemic; rather, systemic risks materialize when multiple SoR accumulate across different entity types and geographies.



How is systemic risk visually configured?

- The visual to the left presents the formation of systemic risk; starting at the centre as the ‘nucleus’ of the risk environment.
- The primary origins of systemic risk stem from the three revolving categories of SoR that become amplified when they accumulate in different permutations.
- Two wider categories surround the three revolving categories; these serve as foundational drivers of risk and are cross-cutting in nature.
- The outer amplifying and diminishing forces are interconnected with the rest of the system and drive the creation or exacerbation of risk.

Why does this matter?

Identifying and addressing systemic risk often occurs after an event has already adversely affected the ecosystem, as with the GFC or the COVID-19 pandemic. Visualizing the layers that exist in the formation of systemic risk can help risk-focused leaders ‘backward engineer’ how future systemic risk can be better measured, enabling the creation of mitigation strategies that address root issues.

The SoR that fall under each of the five categories, along with examples of resulting risks, are **elaborated upon across the following slides.**

Structural and composition: SoR can stem from the structural state of the financial services ecosystem and dynamics between players.



Consolidation of few vendors that offer critical capabilities

The outsourcing of key organizational activities to a handful of services is creating significant dependencies on a small number of providers and systems to successfully enable critical functions.



Concentrated financial services market structure

The structural composition of the financial services landscape is concentrated on a few data-rich players with differentiated technology-based capabilities, raising the bar to compete effectively.



Diluted financial services market structure

The structural composition of the financial services landscape is amplified from a few dominant players to multiple players due to digital adoption and lower barriers to entry (i.e. excessive competition).



Undefined regulatory oversight for new entities/business models

Regulatory oversight, being unilateral and unable to address rapid innovation efforts at pace, is creating a patchwork of requirements and blurred lines between new players, business models, technologies and traditional institutions.



Growing ecosystem interconnectivity and modularity

The digital landscape is becoming increasingly intertwined and interconnected across modules and platforms, leading to direct and indirect risks/impacts to linked players within the ecosystem.

Resulting risk examples

- Potential outsized losses from failures of heavily ‘networked entities’ (e.g. cloud providers)
- Software as a service (SaaS) vendor/proprietary lock-ins

- Oligopolies lead to reduced consumer choice
- Capability investment barriers for smaller entities
- Ineffective antitrust measures

- Commoditization and margin pressure for banking products
- Ineffective oversight on non-financial players

- Blurred definition of a ‘financial institution’
- Unsound financial disintermediation activities
- Inappropriate market conduct
- Time-to-market impediment

- Third-, fourth- and fifth-party misconduct and liability concerns
- Risk assessment constraints (e.g. silos, time-intensity)
- Reduced interoperability with legacy systems

Technology utilization: SoR can stem from the side effects of new technologies being used in the financial services ecosystem.

Algorithmic and model deficiencies	Inexplicable machine- and model-led outputs	Digital consumption weakening human efficacy	Technology skillset shifts and talent scarcity	Operational consequences of technology implementation
The widespread application of technology is driving decision-making biases or redundant feedback loops because of the input data, technologies themselves, or the personnel that operate the technologies.	The outcomes derived from technology (e.g. deep learning models, AI techniques) do not provide sufficient context or interpretable explanations behind decision-making.	Humans are inhibited to effectively capture, retain and conceive information as a result of machine-assisted learning and self-serve digital interactions with financial services providers.	The pace of innovation and the resulting requirements for technology development (e.g. statistical modelling) are creating a lack of availability in relevant skillsets and lack of digital leadership to enable and manage offerings.	The operational shortcomings associated with the transition from legacy systems to new technologies and processes are impacting unprepared incumbents and their consumer base.
Resulting risk examples				
• Algorithm design flaws (e.g. biased logic, assumptions) • Quantum misclassification • Monetary losses from misguided high-frequency trading algorithms	• Trade-off of complexity vs. explainability (in credit/liquidity risk, insurance pricing) • Inability for risk teams to interpret complex models • Forceful regulatory pressure for explainable model results	• Budgeting apps encouraging users to overspend • Overreliance on automated investing experiences • Loss of judgement as a result of enhanced automation	• Global cyber expert demand outpacing supply • Lagging digital literacy among leadership • Lack of allure for top technology talent to work in financial services	• Platform and/or service migration data exposure • Interruptions to and/or inactivity in business-as-usual operations • Organizational risk mismanagement across horizontal (platform-based) business models

Economic and fiscal: SoR can stem from macroeconomic conditions and related influences on the safety and soundness of the global financial system.



Credit risk management constraints

Technology constraints make it difficult for central and commercial incumbents to accurately assess creditworthiness and effectively manage economic resilience through known and unknown events (e.g. unprecedented government-led fiscal intervention).



Increasing displacement of deposits

Funds held within traditional financial institutions are being increasingly displaced due to innovations such as digital wallets, payment alternatives, digital currencies and robo-advisory solutions.



Increasing velocity of deposits

The optimization of the rate at which deposits are siphoned across accounts and financial products is accelerating due to automated money movement and new value propositions in the market.



Obscurity in increasingly complex supply chains

Supply chains that are growing in complexity and modularity are becoming less transparent due to stagnant risk resilience/readiness checks and limited solution adoption (e.g. smart contracts).



Asset price volatility

The significant deviations in the market price of assets and digitization of certain trading activities/asset classes are driving market volatility and the potential for rapid sell-offs.



New and emerging drivers of market movement

The growing prevalence of external systems and platforms that organize themselves to directly impact financial markets is leading to previously unseen market responses and stoppages.

Resulting risk examples

- Inaccuracy of existing credit forecasting models
- Cash flow and working capital instability
- Distortion of credit metrics in various asset classes

- Distorted ability to accurately predict liquidity and/or respond to financial crises
- Stability concerns associated with working capital

- Unauthorized/fraudulent payment transactions
- Limited visibility over money movement/'sweeps'

- Poor due diligence on operations and vendors
- Compliance violations
- Product/service flow interruptions

- Asset bubbles formed by passively managed funds
- 'Flash crashes' from high-frequency trading
- Illiquid fixed income assets (e.g. corporate bonds)

- Rapid stock price manipulation enticed by coordinated actors (e.g. retail traders who leverage online platforms)
- Inability for markets to find equilibrium

Cyber and data: SoR can also stem from the use of data and practices for either exploiting or safeguarding information technology.



Lagging cybersecurity mechanisms

Vulnerabilities associated with compromised technical infrastructure or emerging cyberattack tactics are growing and leading to the lack of timely mechanisms to properly address rapidly evolving security concerns.



ID misrepresentation and authentication vulnerabilities

Ineffective digital authorization and/or authentication mechanisms to validate an intended user (e.g. KYC, digital ID) are being exploited by malicious actors that utilize tactics to commit fraud (e.g. deep fakes).



Stagnant and inconsistent consumer data privacy controls

The lack of control and trust in the appropriate and transparent usage of consumer data is amplifying the need for effective governance and market mechanisms to protect sensitive data.



Ineffective portability-related data protection

Vulnerabilities associated with the rise of data portability (e.g. data breaches) and consumer connectivity are amplifying the need for effective tools to prevent data-focused cyberattacks.

Resulting risk examples

- Malware attacks, hacks and ransomware
- Bypassed encryption due to quantum
- Missing shadow IT or third-party system governance

- Unauthorized account openings and takeovers
- Synthetic identity fraud and PII modifications
- Harmful exploitation of biometrics (e.g. voice, video)

- Unnecessary data collection/usage/retention
- Unclear open banking and open data frameworks
- Absence of controls for non-regulated entities

- Flawed implementation of PETs and cryptography
- Data monitoring and tracking gaps
- Insufficient localized data security requirements

Societal and climate: Lastly, SoR can stem from the ways humans coexist through social constructs and interact with the natural world.



Dissemination of verbose and false information

The concentration of information sources and the growing prevalence of excessive, misleading and false information is driving 'analysis paralysis' or faulty decision-making for consumers, players and markets.



Growing social inequities and fragmentation

Interdependence between growing social inequities and digital/financial exclusion is both creating and exacerbating a lack of mainstream access to technology services and worsening the ability to sufficiently adopt financial products.



Blurring jurisdictional boundaries

Instances of innovation and globalization are further blurring jurisdictional boundaries, with the heavily regulated financial services industry and its players being challenged to keep pace.



Climate change transition imperative

The necessary transition towards a low-carbon economy, derived from policy, technology and business model innovations, can create risks to the financial services ecosystem and global economy.



Rising geopolitical tensions

Emerging conflicts surrounding international relations between state actors are leading to the prevalence of cybersecurity events, financial crime and intellectual property protectionism.



Damage caused by natural disasters/ catastrophic events

Technological infrastructure and operational vulnerabilities caused by extreme weather-related/ catastrophic events are growing as financial services become more digitally dependent.

Resulting risk examples

- Misguided investment decisions/asset price volatility
- Over-gamification of digital financial activities
- Big Tech moderation of information sharing

- Cyberattacks on vulnerable populations
- Financial exclusion increasing the wealth gap
- Underbanked/unbanked inaccessibility and digital exclusion

- Incomplete or inconsistent compliance for institutions
- Restrictions to cross-border data flows (e.g. localization)
- Insufficient offerings for international consumers

- Carbon footprint of cloud migration and AI
- Lack of asset-level data on climate-related valuations
- Inadequate climate-related financial disclosure

- Global battle for AI dominance/quantum supremacy
- State-led cyberattacks or warfare
- Ethical data privacy and tech policy discrepancies

- Inability to transact, trade, or access necessary financial data/systems as a result of major technology service outages
- Interruptions to usual operations and financial losses

Public and private sector players can apply a three-pronged framework to assess their exposure to SoR; when surveyed for this report, players shared their level of concern associated with each source.

Overview of evaluative dimensions



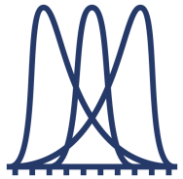
Degree of ecosystem impact

What is the degree to which the SoR will impact the broader ecosystem and contribute to the formation of a systemic threat?



Degree of organizational impact

What is the degree to which the SoR will negatively impact the respective organization?



Relative probability

What is the likelihood of the SoR increasing in prevalence or materializing into a real-world issue within the next 24 months?

How dimensions were used

Survey

Over 50 industry players were surveyed about SoR and their contributions to systemic risk. These regional and global players consisted of regulators, policy-makers, banks, asset managers, insurers, financial technology players, and technology providers, among others.

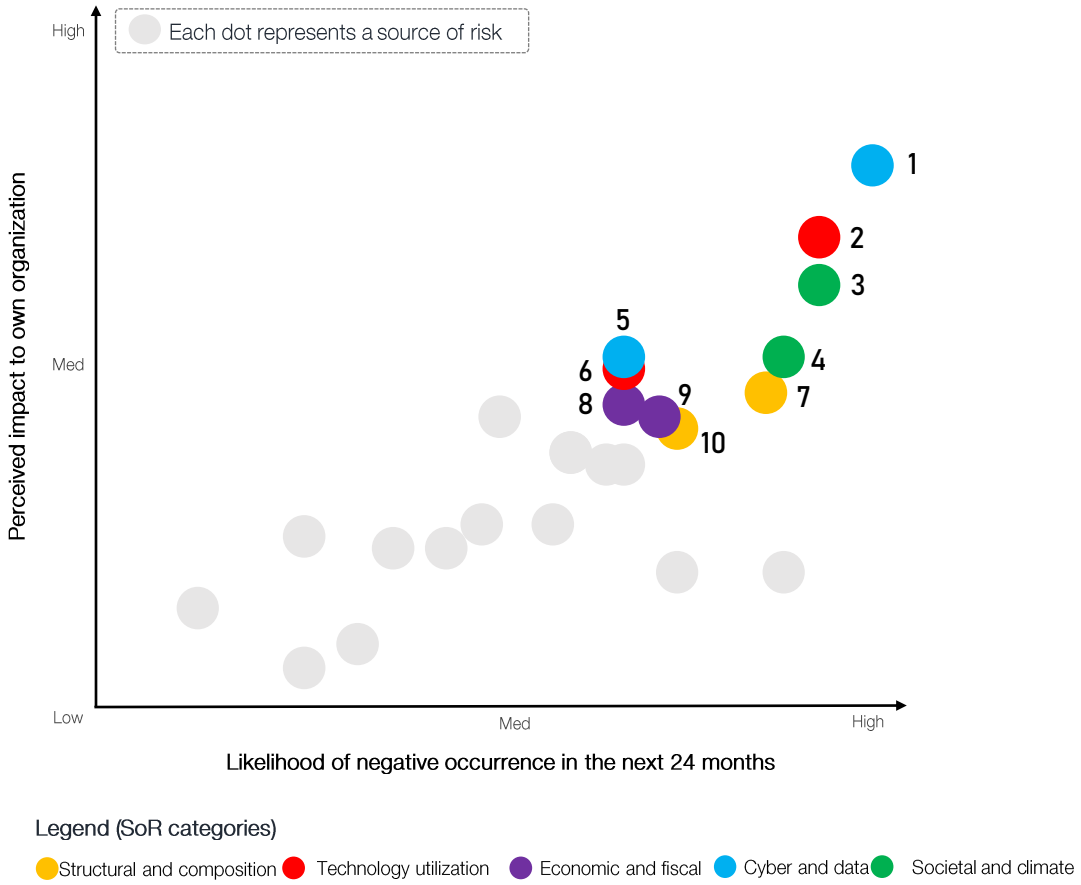
When evaluating the dimensions (left), players were diverse in their responses due to entity-type, sector and geographical representation.

Analysis

Over the following pages, survey responses have been plotted against the three evaluative dimensions to indicate the level of concern associated with the SoR and to highlight diverging areas that warrant further exploration. These insights and the questions which arise from them are intended to support the refinement of mitigation strategies based on the areas of concern.

Preliminary survey findings reveal the most significant SoR for global and regional financial services players to keep on their radar.

SoR were evaluated based on their perceived impact to the organization and the anticipated probability of their occurrence.



Respondents viewed ten SoR as having the *most* material impact on their organization in the near future:

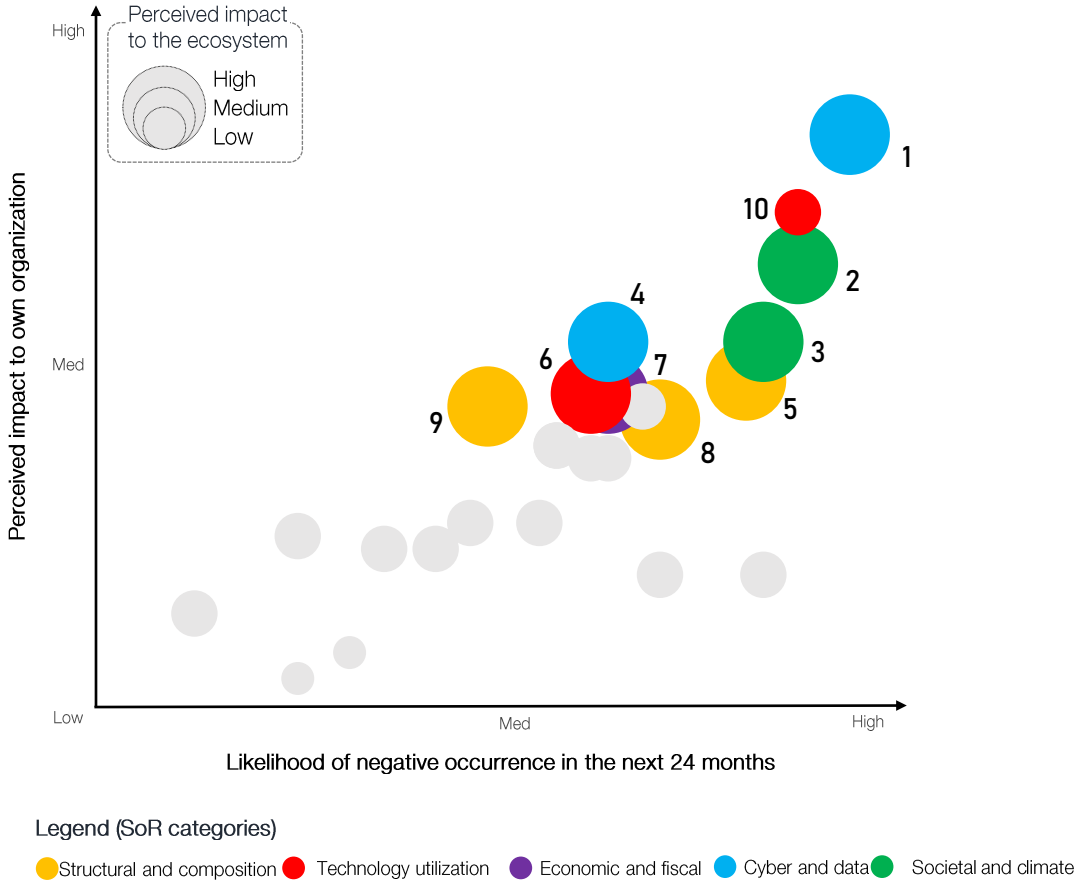
1. Lagging cybersecurity mechanisms
2. Technology skillset shifts and talent scarcity
3. Climate change transition imperative
4. Rising geopolitical tensions
5. Identity misrepresentation and authentication vulnerabilities
6. Operational consequences of technology implementation
7. Growing ecosystem interconnectivity
8. Obscurity in increasingly complex supply chains
9. Asset price volatility
10. Undefined regulatory oversight for new entities and business models

Despite this ranking, those surveyed view all SoR to have *some* probability of occurrence in the next 24 months. Regardless of the degree of perceived impact, all SoR should be on the radar of ecosystem players.

Note: Given the limited sample size and non-random selection process, survey results are not intended to be a full representation of global industry views, but rather are intended to offer indications.

Survey findings also reveal that many of the top SoR remain highly ranked when perceived impact to the ecosystem is considered alongside perceived organizational impact and likelihood of occurrence.

When a third dimension (perceived impact to the ecosystem) is introduced, new priorities emerge.



Respondents viewed ten SoR as having the *most* material impact on the ecosystem in the near future:

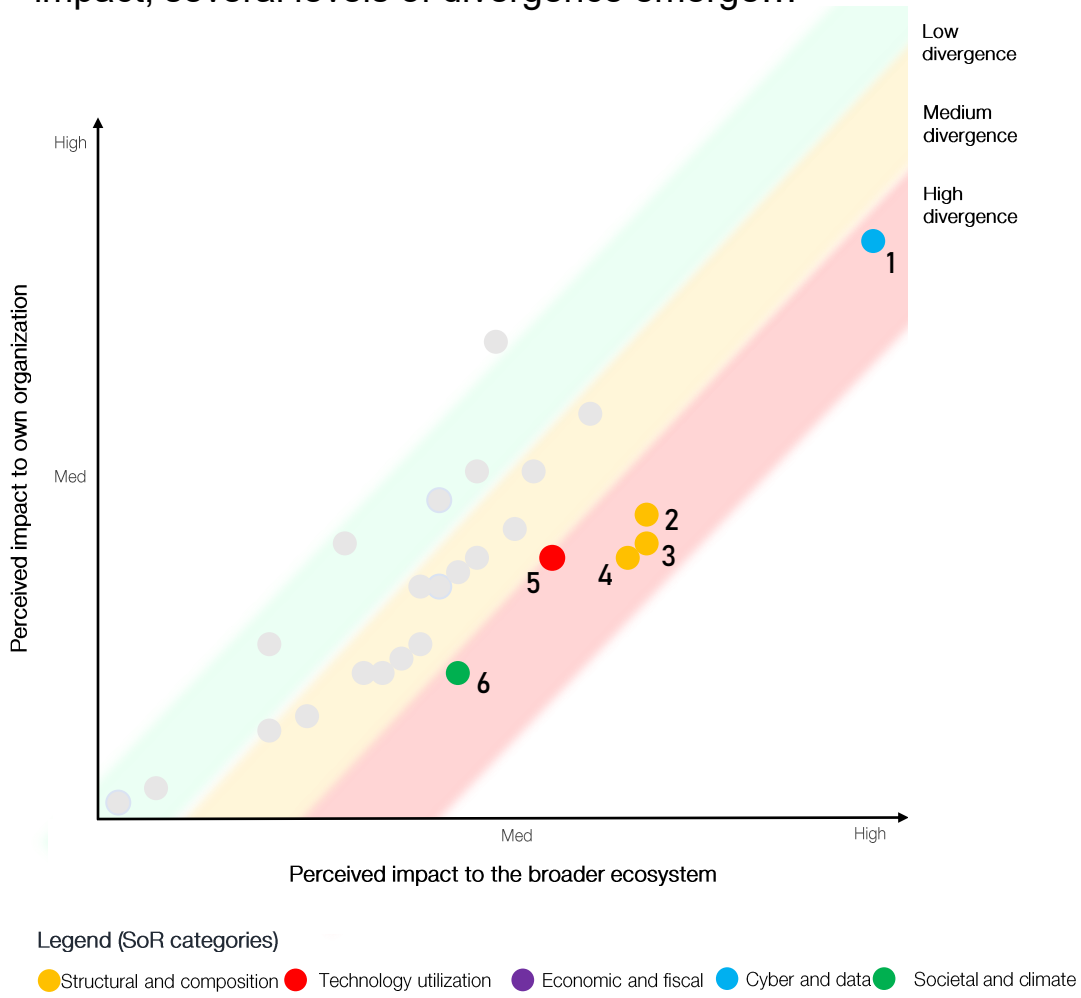
1. Lagging cybersecurity mechanisms
2. Climate change transition imperative
3. Rising geopolitical tensions
4. Identity misrepresentation and authentication vulnerabilities
5. Growing ecosystem interconnectivity
6. Technology skillset shifts and talent scarcity
7. Obscurity in increasingly complex supply chains
8. Undefined regulatory oversight for new entities and business models
9. Consolidation of few vendors that offer critical capabilities
10. Algorithmic and model deficiencies

Cybersecurity, climate change, identity misrepresentation and geopolitical tensions remain the most significant SoR to survey respondents across all three dimensions.

Note: Given the limited sample size and non-random selection process, survey results are not intended to be a full representation of global industry views, but rather are intended to offer indications.

While leaders had differing responses to SoR, the greatest divergence exists between the perceived impact that SoR will have on the ecosystem versus the organization.

When comparing responses relating to the two dimensions of impact, several levels of divergence emerge…



…indicating that SoR may have a greater impact on the broader ecosystem than the individual organization.

The collective responses revealed various levels of divergence on the perceived impact of SoR.

Although not definitive (given the sample size), most SoR are perceived to have a greater impact on the broader ecosystem than on the respondent's organization. The following SoR were found to have the highest degree of divergence between organizational and ecosystem impact:

1. Lagging cybersecurity mechanisms
2. Growing ecosystem interconnectivity
3. Undefined regulatory oversight for new entities and business models
4. Consolidation of few vendors that offer critical capabilities
5. Algorithmic and model deficiencies
6. Growing social inequities and fragmentation

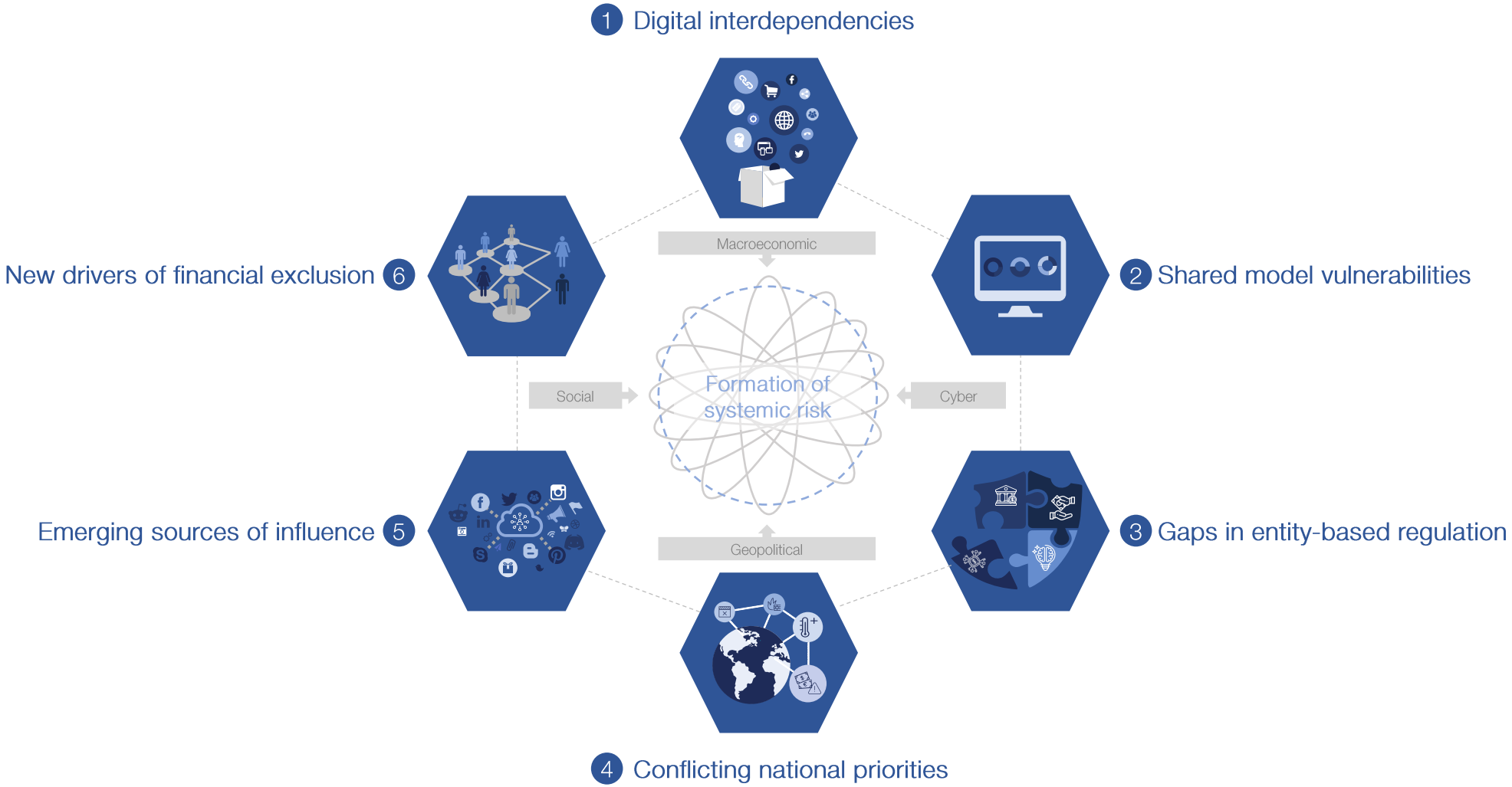
While findings on divergences warrant additional exploration, leaders can attain a better understanding of their presence in the ecosystem by considering the following:

- Is my organization operating with a false sense of 'insulation' against the rest of the ecosystem?
- Is my organization equipped with the right mechanisms to feel protected against the rest of the ecosystem?
- Are certain SoR predisposed to have a greater impact on the ecosystem rather than a single organization?

Note: Given the limited sample size and non-random selection process, survey results are not intended to be a full representation of global industry views, but rather are intended to offer indications.

Exploring and mitigating technology-led systemic risks

Six cross-cutting themes highlight the role that technology plays in creating and amplifying systemic risk in global financial services:



The following section dedicates space to each systemic risk theme, covering an exploration of the risks alongside potential mitigation approaches. It can be read as follows:

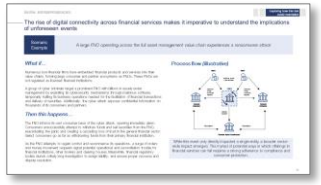
Risk exploration

(3 - 4 pages)



1. Defining the systemic risk:
Background and context on the risk theme, including its importance to the industry.

2. Identifying the key ecosystem players *(where applicable)*:
Profiles on public and private sector players that are central to risk themes.



3. Exploring how this risk could materialize:
Scenario narrative with a schematic that showcases an example of the systemic risk(s).



4. Determining implications to the ecosystem:
Key insights on how the systemic risk(s) can significantly impact the financial services ecosystem, with impetus for industry response.

Risk mitigation

(7 pages)



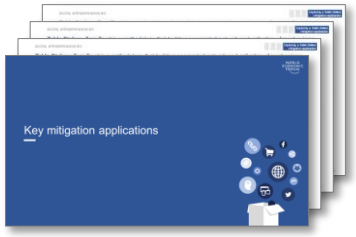
1. Reviewing current mitigation efforts:
Summary of mitigation approaches being employed by players, including relevant case studies.

2. Identifying gaps in current mitigation efforts:
Summary of current gaps and uncertainties across mitigation approaches.



3 - 4. Understanding what more can be done:
Overview of tactics to improve current leaders' mitigation efforts, both individually and multilaterally. *Tactics, along with unintended consequences, are organized by the key stages of risk mitigation:*

Risk prevention; Risk intervention; Risk resolution.



5 - 7. Key mitigation applications:
Deep-dive on promising mitigation applications across projected timelines of commercial availability.

- *Table stakes:* Currently existing
- *Emerging:* 3 - 5 years
- *Novel:* 5+ years

Each of the outlined elements correspond to the associated bar in a tracker on the upper right-hand side of the page

1 2 3 4 5 6

Digital interdependencies



Any entity, large or small, that is highly interconnected and/or plays a critical role in enabling digital financial services could cause ecosystem disruptions with cascading implications.

Overview

Preceding spillover

The collapse of the US housing bubble and subsequent GFC in 2008 proved that the **failure of a large financially interconnected entity** (e.g. Bear Stearns, Lehman Brothers) can ripple through the entire financial system and spill over into the real economy.[21]

Following this event, entities classified as SIFIs were heavily scrutinized.[22]

Insufficient attention

The ongoing analysis of SIFIs' financial interconnections remains a crucial aspect of evaluating systemic risk. However, this focus lacks **direct attribution to the growing centrality of digitally interconnected players.**

Insufficient attention is being paid to the **extent of digital interconnections** across players in the broader ecosystem, especially as wide-scale operational failures or cascading cyberattacks become more prominent.

Non-financial dominance

Unsurprisingly, market offerings from technology vendors will **continue to enable key services and operations across the ecosystem.** The power dynamics between financial and non-financial players will continue to shift as a result.

As technology providers' roles in financial services continue to expand, the **degree of digital dependence for all financial players will increase,** whether solely or partially technology-enabled.[23]

Inward perception

While one of the benefits of outsourcing capabilities is to improve the entity-level risk balance sheet, outsourcing to few vendors is leading to **structural changes and the pooling of risk.**

The modularization of technology presents even greater threats given the pace at which third-, fourth- and fifth-party providers are **expanding their geographical footprint and leveraging new digital tools** to scale globally.[24]

Why is it important?

Vulnerable nodes

Endogenous and exogenous threats can **compromise a single, shared digital vendor that can immediately or gradually cascade vulnerabilities** across its vast direct/indirect user and supplier base (e.g. through threats to data integrity or losses of data availability).

The more concentrated, complex and interconnected the digital ecosystem becomes, the **greater the number of vulnerable nodes** that could threaten and exploit its essential functions.

PRIMARY SOURCES OF THIS RISK

- Consolidation of few vendors that offer critical capabilities
- Growing ecosystem interconnectivity and modularity
- Obscurity in increasingly complex supply chains

With the proliferation of financial and non-financial entrants, several technology-based entity types are emerging as protagonists in forming heavily interconnected networks within the ecosystem.



Infrastructure and platform service (cloud) providers*

Players rely on a small handful of cloud service providers for turnkey solutions (e.g. system back up, replacement) and advanced applications (e.g. big data and analytics). Financial players often use more than one provider but tend to pick their second from the same small pool of providers.[25]



Financial network orchestrators (FNO)

Often perceived as central ecosystem platforms or 'super apps', orchestrators operate across the full financial services value chain through embedded partner models. They typically have a robust technology stack and amass a large financial user base through network effects.[27]



Capabilities as a service (CaaS) providers*

Non-financial entities have entered the arena to provide embedded finance offerings and essential managed service applications. Similar to cloud providers, their capabilities integrate with core systems, enabling use cases such as onboarding, automation, compliance and cybersecurity.[26]



Financial technology players (FinTechs)

As the disruptors of incumbent-led financial services, FinTechs (including neobanks) often leverage Big Tech players and other 'as a service' capabilities to scale up their operations globally at a low cost. To compete, many incumbents have launched their own digital-first offerings.



Software as a service (SaaS) providers*

Shared enterprise services support the management of day-to-day business activities and are a leading interface for players, with notable offerings across enterprise resource planning, customer relationship management, portfolio management, human resources and payroll.[26]



Financial market infrastructure (FMI)

Designated public infrastructure is responsible for the facilitation of value (e.g. to record, clear or settle transactions) and can adopt or enable emerging frameworks (e.g. digital identity, decentralized technology). Given their roles as central conduits, they are typically directly overseen by a regulator/central bank.[27]

***Note:** For the purposes of this report, 'Big Tech' refers to dominant global technology players, which also operate as Cloud, CaaS and SaaS providers in the ecosystem.

It is essential to understand the implications of unforeseen events created by the rise of digital connectivity across financial services.

Scenario example

A large FNO operating across the full asset management value chain experiences a ransomware attack.

What if…?

Numerous non-financial entities have embedded financial offerings into their value chains, forming large consumer and partner ecosystems as FNOs. These FNOs are not regulated as licensed financial institutions.

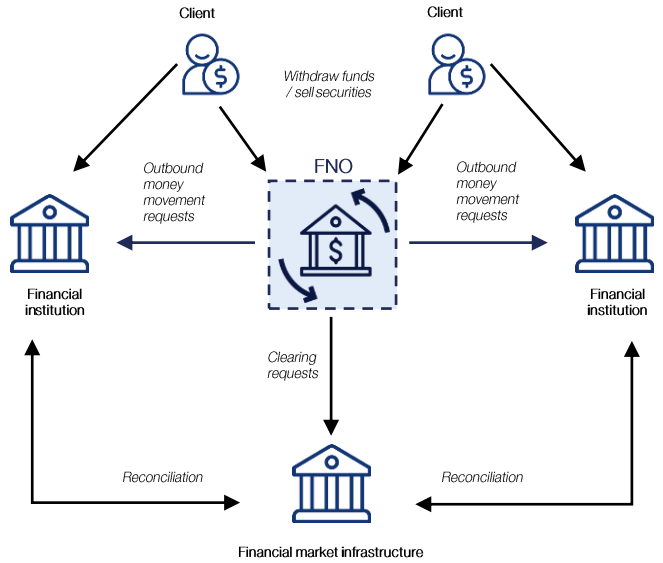
A group of cybercriminals target a prominent FNO with billions in assets under management by exploiting its cybersecurity mechanisms through malicious software, temporarily halting the operations needed for the facilitation of its financial transactions. Additionally, the cyberattack exposes confidential information about thousands of its consumers and partners.

Then this happens…

The FNO informs its vast consumer base of the cyberattack, spurring immediate alarm. Consumers unsuccessfully attempt to withdraw funds and sell securities from the FNO, exacerbating the panic and creating a cascading loss of trust in the general financial sector. Select consumers go as far as withdrawing funds from their primary financial institution.

As the FNO attempts to regain control and recommence its operations, a surge of orders and money movement requests signal potential operational and reconciliation trouble for financial institutions, other brokers and clearing houses. Meanwhile, financial regulatory bodies launch a resource-intensive investigation to assign liability and ensure proper recourse and dispute resolution.

Process flow *(illustrative)*



While this event only directly impacted a single entity, a sector-wide impact emerged. The myriad of potential ways in which offerings in financial services can fail requires a strong adherence to compliance and consumer protection.

Players operating in the financial ecosystem can only be as safe as their ability to monitor and respond to vulnerable nodes in their network.

Why does this risk significantly impact the financial services ecosystem?

Limited digital interconnectedness protections: The regulatory risk focus has been on the traditional definition of 'financially-oriented size'[28] and attention has not yet been broadened to cover systemic *digital* interconnectedness (measured by a relevant entity's 'size of network') and the threats posed by these vulnerable network nodes.

Maintenance of traditional oversight: The focus on traditional SIFIs should not be lessened, as the regulations implemented post-2008 will remain critical to ensuring the financial stability of markets.[29] Non-financial adverse events to all players in the ecosystem (e.g. operational failures, cyberattacks) continue to pose a risk of cascading losses due to scale in terms of both the 'size of book' and the 'size of network', and must be uniquely accounted for.

Shared responsibility for network protection: If players are not standing up the necessary safeguarding mechanisms across each node in their extended network, they are putting their security under the 'control' of their vendors and may unintentionally and unknowingly be participating in the contagion of risk. Existing individual tactics (e.g. network mapping capabilities), while helpful, may be limited (e.g. no real-time end-to-end visibility) given the degree of ecosystem linkages at the N^{th} degree.

Magnitude of impact from interconnected entities: With this shift in dynamics, the influence of smaller or adjacent players can be outsized (e.g. through shared APIs, cloud-based solutions) as even small threats to one seemingly negligible part of a chain can ignite chaos and engulf the entire ecosystem.

CASE STUDY

The wide-reaching damage caused by the SolarWinds breach in late 2020 was an important lesson for the financial sector. The digital supply chain attack saw adversaries compromise the SolarWinds monitoring software used by upwards of 18,000 companies and government agencies, including major financial institutions and IT vendors. The backdoor breach had gone unnoticed for months as a contagion effect ensued with adversaries hiding in interlinked systems and, in some cases, stealing valuable business intellectual property.[30]

While this breach had systemic implications, imagine if a similar event had occurred with a greater magnitude of impact…

What if a larger SaaS vendor experiences an undetected data breach that cascades across various business and government services within its supply chain?

Given their potential to amplify other systemic risks across the ecosystem, proactive measures are starting to anticipate for, and control, digital interdependencies.

What are some key efforts that ecosystem players have undertaken to mitigate this risk?

Public sector players*

- Looking to expand the scope of oversight across non-financial entities contributing to interdependence vulnerabilities, particularly those that account for concentration risks (e.g. cloud providers).[31]
- Implementing clear third-party guidelines and outsourcing risk management guidelines for financial entities, and actively exploring diversification mandates, such as multi-cloud strategy guidance.[32]
- Fostering safe and vetted partnerships between FinTechs and incumbents through controlled environments (e.g. accelerator initiatives, sandboxes).[33]

Multilateral efforts

- Prominent FinTechs and SaaS providers are actively working with regulators to prove the suitability of non-financial entities through sandboxes and testing hubs, particularly where requirements are absent.[33]
- Regulators are beginning to collaborate on the development of guidelines that will enable incumbents to better and more consistently manage their Nth-party risks, beyond simple due diligence requirements.[34]
- AI/ML capabilities are increasingly being leveraged to improve network mapping and real-time interconnection monitoring across supply chains and the broader ecosystem.[35]

Private sector players

- Proactively assembling due diligence teams to examine risks posed by third-parties, especially those related to data sharing. [36]
- Expanding assessments of how third parties are performing due diligence on *their* third-parties, given the propensity of vendors to use another party's services.[36]
- Employing diversification strategies to avoid operational downtime (e.g. multi-cloud) and automating workflows to ensure a holistic view of compliance.[37]
- Increasingly adopting risk transfer solutions that are typically excluded from traditional commercial liability (e.g. cyber insurance, parametric downtime insurance).[38]

RELEVANT CASE STUDIES



In China, regulators have instructed Ant Group (a large FNO and FinTech) to form a financial holding company under their supervision, as well as to shrink its money market fund, Yu'e Bao. Given the scale of Ant Group, regulators believe it poses a systemic risk and have asked the entity to tighten its lending offering.[39]

Microsoft GDPR

To comply with or exceed GDPR guidelines, Microsoft recently launched its 'EU Data Boundary for the Microsoft Cloud' initiative. This leading approach will offer information control across more services and types of data, including developments like virtual lockboxes, to provide real-time logs that generate a trail of all data-based ecosystem interactions.[40]

TruSight™

TruSight Solutions is an industry consortium designed to help all financial institutions mitigate vendor risks and was founded by leading financial incumbents in the US. TruSight elevates standards and simplifies the process of managing third-party relationships and associated risks, developing best practices that benefit financial institutions and their third-parties.[41]

*Note: 'Gaps in the current entity-based regulatory regime' are closely connected to the issue of digital interdependencies and are explored in a distinct risk theme on pp. 72-84.

While many entities have begun to explore technology-driven risk prevention and monitoring initiatives, more needs to be done by players to expand upon existing efforts.

What gaps exist in current mitigation efforts?

Public sector players

- Non-financial entities that are mission-critical capability providers are not designated as systemic institutions, nor do they have the appropriate resiliency mandates.[42]
- Given the legal barriers and lack of global data standards, data sharing among regulators is limited (often due to data localization) and cross-jurisdictional collaboration remains challenging.[43]
- Regulatory reporting for financial institutions and supervisors remains manual, highly aggregated, template-based and inflexible, preventing meaningful real-time usage.[44]

Multilateral efforts

- Collaboration to enhance the oversight and security of the network while increasing visibility across all nodes remains limited, particularly with non-financial entities.
- Platforms for mapping and monitoring vendors present comparability challenges, leading to fragmented ecosystem transparency, especially beyond third-party providers (e.g. fourth- and fifth-parties).[45]
- Potential vendor diversification guidance set by regulators (e.g. multi-cloud mandates) must account for the increased enterprise costs and added complexity of new interconnections.[46]

Private sector players

- Valuable data remains buried across market players and between disconnected business processes, making it difficult for financial entities to collaborate and apply enterprise-level mitigation applications.
- Data privacy, security and intellectual property concerns among players and third parties prevent the development of a comprehensive view of network interdependencies and potential points of vulnerability.

KEY MITIGATION UNCERTAINTIES

1 *While individual regulators can work to implement policies that mitigate this risk, will there be limitations if a cross-sectoral/cross-border regulatory framework is not developed?*

2 *If the necessary cooperation mechanisms and incentives to ensure all ecosystem players participate in ecosystem-wide mitigation efforts are not implemented, are multilateral risk monitoring and prevention efforts going to remain hindered?*

3 *Will an ecosystem-level view of digital networks, alongside the ability to monitor these networks in real time, be possible without commercial access to applications that enable secure, encrypted data sharing?*

Given the challenging nature of comprehensive interdependence monitoring and control in the ecosystem, new policies and tools should be sought to improve risk mitigation for individual entities.

How can current mitigation efforts be improved? What more can be done by individual entities to address this risk?

Risk prevention

- Homomorphic data encryption: To enable ecosystem transparency and address data availability concerns, financial entities could look to partner with technology players to deploy case-specific homomorphic encryption applications. This would enable the secure sharing of highly sensitive data for ecosystem-level analysis without the information itself ever being readable by unintended parties.[47] To further 'future proof' encryption, quantum key distribution (QKD) can be explored.
- Enhanced entity-level stress testing: Private sector entities can look to bolster existing stress testing initiatives across operational resilience scenarios (e.g. edge, corner, boundary and base cases) and enhance assessments of potential risks from service provider disruptions/failures. This would better account for, and address, extreme outcomes when developing robust resiliency plans.
- AI-driven insights: Entities could leverage AI and NLP capabilities to improve insight gathering from network maps and understand the degree of organizational reliance on N^{th} parties. Regulators and central banks could also explore opportunities for developing integrated platforms to enable early warning indicators of ecosystem-level risks.
- Big Tech visibility: Technology players (e.g. Big Techs, FinTechs) can be incentivized by the public sector to develop more robust external APIs and provide greater transparency on their network connections, given their roles as primary interconnectors in the ecosystem.

Risk intervention

- Zero trust architecture: To contain the spread of a harmful cyber event, a segmented zero trust model can be deployed with intelligent 'circuit breakers' that prevent full intra-system access.[48]
- Geospatial network mapping: To better detect and manage vulnerabilities as they arise, players can leverage geospatial data with network maps to monitor and visualize both their physical and digital footprint. This can help players to centrally identify any service disruptions, outages or cyberattacks that may interfere with operations as they happen, creating opportunities for real-time intervention.[49]

POTENTIAL UNINTENDED CONSEQUENCES



While homomorphic encryption has secure data-sharing potential, it is yet to reach fulsome commercialization and lacks widely accepted standards. Early adoption may present new security concerns that are not widely understood and may be exacerbated by the 'black box' nature of this encryption method, especially when combined with AI subsets (e.g. deep neural networks, ML).[50]



Future real-time network monitoring will likely be enabled by multiple 'as a service' providers (e.g. for underlying digital capabilities and cloud infrastructure). New partnerships and instances of outsourcing will add to ecosystem dependencies and create other points of operational risk.

Given the challenging nature of comprehensive interdependence monitoring and control in the ecosystem, new policies and tools should be sought to improve collaborative risk mitigation.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Multilateral scenario planning: Public and private sector players of all sizes can jointly create scenario planning exercises and develop extensive stress tests with a broader ecosystem orientation. This cooperation could be accelerated by cutting-edge innovation from Big Tech players (e.g. artificial neural networks, quantum-based Monte Carlo simulations).

Risk intervention

- Regulatory coverage for 'size of network': Regulators can look to solve fragmented oversight (between prudential, competition and consumer protection bodies) by conducting a review of relevant policies and consolidating administration into a single, public sub-entity. Further regulatory expansion can be explored to ensure that the full range of activities of interconnected entities is accommodated for in financial services (e.g. provisioning tiered licenses to non-financial entities based on role and scope of services).

Risk resolution

- Public-private transparency: As an interim solution to cross-jurisdictional data governance issues, incident transparency can be strengthened through standardized reporting requirements and open APIs between private and public sector entities. This would enable seamless access to more data, which can be used to quickly understand the ramifications of an event and its potential to evolve into a systemic risk.
- Joint resiliency: Multi-party consultations can educate leading organizations and regulators on how to effectively manage risks and relationships between technology service providers (e.g. understand the risk controls that IaaS providers have in place). Such consultations can be further elevated to create stronger recovery and resilience plans, alongside an industry-wide understanding of dependencies.
- Dispute resolution service: A private sector-led dispute resolution mechanism that operates on clearly defined grounds (co-developed with regulators) could be established to objectively assess concerns for third-party vulnerability and misconduct. Such a mechanism could be utilized as the initial step to launching liability claims.

POTENTIAL UNINTENDED CONSEQUENCES

By investing heavily in multilateral scenario planning and stress testing exercises, ecosystem players could become distracted by the scale and scope of potential outcomes. This could result in decision-making 'paralysis' when contingency and resilience plans must be developed for prioritized potential risk events.

With increased regulatory oversight and scrutiny towards cloud service providers, these players are likely to express opposition to invasive or overly ambitious regulatory steps or mechanisms. This could leave certain initiatives ineffective, administrative-only, or could increase costs for the end-users.

If regulators were to enhance transparency and provide visibility into all network interdependencies within a digital platform, the housing of this sensitive data could become a potential target for bad actors, inadvertently creating yet another critical network node.

Key mitigation applications



Note: The mitigation applications highlighted in the following slides are intended to be considerations and have not been assessed for viability or feasibility.

Table stakes: The 'zero trust' methodology builds a segmented system and a collection of mechanisms, allowing organizations to enforce consistent security policies across their vast networks.

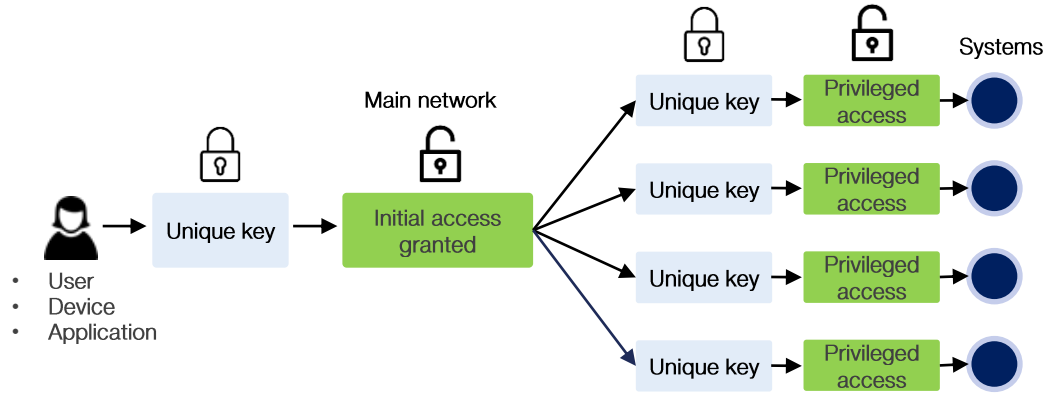
Overview

The distributed configuration of today's business-critical applications requires an unorthodox approach to provisioning access, prompting players to rethink how they view trust across their network and security models.

The degree of visibility and control across applications can be vastly improved if systems are segmented in such a way that access to one does not mean access to all (i.e. if there are intelligent 'circuit breakers' that prevent the flow of data from one system to another).[51]

Zero trust architecture prevents broad access and makes it difficult for vulnerabilities to spread laterally and exfiltrate any data or business processes. This means that users or applications trying to access an organization's network must be continuously verified by mechanisms such as multi-party authentication. This works best when each destination across a network has a unique encryption key that can stop threats and enforce granular access across on-premises data centres or multi-cloud environments.[52]

How it works



Once provisioned access through the initial firewall, entities must pass **additional security measures** to access each system, application and database

Use in financial services



- Ensuring a robust security posture is a critical objective for most financial services players due to the complexity imposed by IT environments, new business models and the recent shift to a remote workforce.
- As players harmonize their technology stack across legacy and cloud systems, simultaneously implementing a zero trust model will aid in the containment and rapid identification of consequential breaches. [52]
- For example, a scaled zero trust approach with the right 'guard rails' could have prevented the magnitude of the SolarWinds cyberattack that implicated hundreds of players, some of which were prominent financial services institutions.[53]

Emerging: Geographic information systems (GIS) allow real-time network insights to be plotted alongside location data to attribute information and create a clearer picture of network activity.

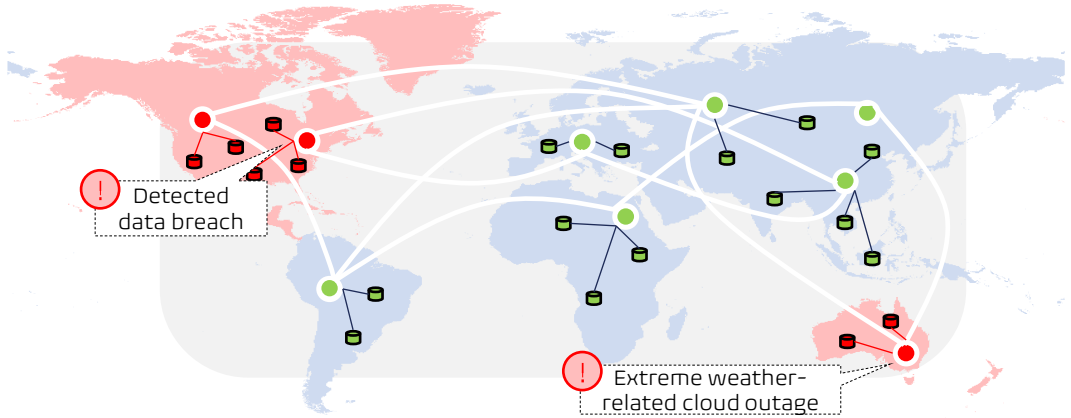
Overview

Players can achieve optimum visibility across their ecosystem and connected footprint by further augmenting foundational capabilities, such as network maps and vendor risk management platforms that use GIS to integrate geospatial analysis.

GIS can help to detect meaningful trends by mapping physical and digital connections across assets and Nth-party applications; these can then be leveraged to form actionable intelligence outputs regarding operational disruptions, outages or cyberattacks.[54]

Spatial data can tie an incident to a specific location and promote faster recoveries from detected threats or wide-scale issues (e.g. a cloud provider outage due to a climate event, reported data breaches, or instances of jurisdictional expropriation) across an enterprise's entire network.[55]

How it works



GIS connects data layers to a map, integrating location data with descriptive information to provide insights that aid with **decision-making and transparency.**

Use in financial services

Monitor — Avoid — Assume — Control

- Armed with supplementary data from geolocated endpoints, organizations' security teams can more reliably determine whether activity is malicious or benign, conduct forensic investigations to understand the full scope of impact, and inform scenario models which influence business continuity plans.[56]
- GIS allows financial institutions and regulators to dynamically visualize the location of digitally-critical assets beyond the means of network maps (e.g. locations of connected third-parties), allowing them to be better prepared in the case of an emergency.
- Additionally, GIS insights can be coupled with automated reporting capabilities to simplify regulatory disclosure requirements, providing governments with a holistic picture of the potential risk exposure of systemically significant institutions.[57]

Novel: In an emerging ecosystem where communications could be intercepted by malicious or compromised parties, quantum key distribution (QKD) may offer a safe exchange of encryption keys.

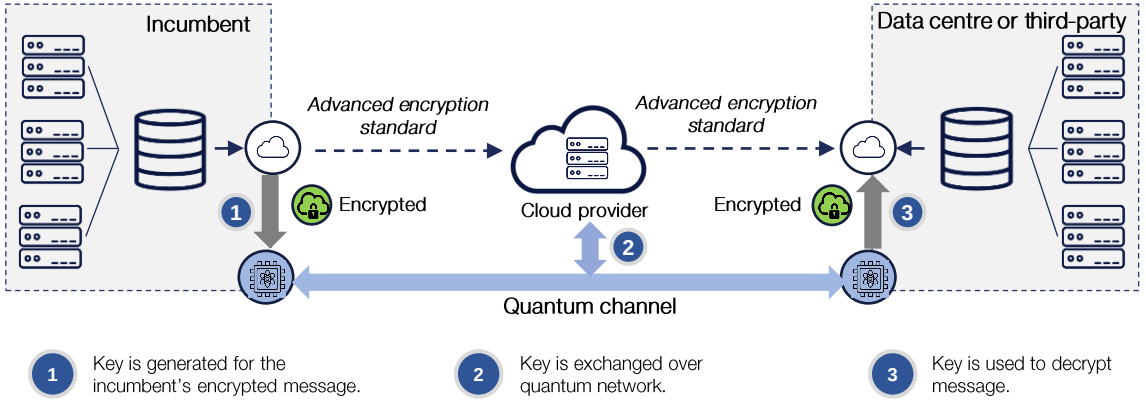
Overview

The multitude of software- and API-enabled connections will be subject to greater security concerns over the coming years as new technologies such as quantum computing become commercially available and pose an exogenous threat to common encryption methods.

Although not currently commercially viable, players should be aware of the applications of QKD; it can be leveraged for the encryption and decryption of sensitive external communications between parties if public-key cryptosystems can no longer appropriately secure data that requires long-term confidentiality. QKD may offer an additional layer of security to an existing system by providing a quantum-protected channel for key exchange to take place.[58]

To support quantum resiliency, prominent cloud and telecommunications providers can lead the charge on developing QKD networks to 'future-proof' cybersecurity.[58]

How it works



QKD leverages quantum physics to enable any two parties to **securely distribute symmetric encryption keys** in a provably secure channel.

Use in financial services

Monitor — **Avoid** — Assume — Control

- Although quantum computing remains relatively inaccessible, opportunistic cybercriminals are starting to scrape and store encrypted financial data, along with the corresponding communications, to help them decipher data in the future once quantum capabilities are within reach.
- As such, private and public sector players can begin to identify use cases and forecast investments to eventually leverage QKD for their most sensitive data across digital assets (e.g. for bank-to-bank, bank-to-party, or bank-to-regulator communications), until post-quantum cryptography is fully available.[59]
- While this solution is not yet ready for scaled deployment, regulators can act now to better understand quantum vulnerabilities and set standards for post-quantum cryptography.



1 2 3 4 5 6

Shared model vulnerabilities

SHARED MODEL VULNERABILITIES

Modelling techniques are critical for interpreting risk; however, traditional models that leverage historical or time-series data can be inconsistent when predicting forward-looking outcomes.

Overview



Model dependence

A rapidly changing global environment has led organizations to become **increasingly reliant on models to anticipate and mitigate risks** across areas such as liquidity, market, credit, capital and conduct.

While models drive faster and better decision-making, they also raise significant issues with incomplete risk capture or overly optimistic outputs sometimes **misleading financial players into believing they are better off than they are.**



Model risk management (MRM)

As a result of increased model usage, attention to MRM has become a necessity for entities to **achieve data visibility, enhance decision-making** and comply with financial reporting and regulatory requirements.[60]

Despite these efforts, numerous **negative consequences with potentially systemic outcomes** (e.g. liquidity shortages, incalculable losses) can arise even if a consistent MRM framework is in place.



Vulnerable techniques

The importance of model trust and governance is not overlooked by financial institutions and there is an **increasing level of investment dedicated towards enhanced models** across the industry (e.g. outsourced model validation assurance).

Modelling techniques that rely on time series data are likely to continue to be **less effective when unprecedented, exogenous shocks occur,** however, and may leave players unable to manage the fallout.



Recent setback

Many models that financial institutions operationally depended on did not properly account for the COVID-19 crisis due to built-in assumptions of a relatively stable future and limited acknowledgement of extreme potential outcomes.[61]

The resulting economic disruption **rendered these risk models ineffective in supporting decision-making**, exposing an overreliance on historical modelling outcomes and a broad lack of resilience across many entities.[61]

Why is it important?



New path forward

While scrutiny is being applied to model inputs, usage and transparency by the public sector, there remains a **critical lack of common taxonomy across policies**. There is also an **absence of forward-looking data and information** being embedded into modelling applications.[62]

Together, these dynamics present **extensive uncertainties around how players can appropriately detect emerging threats** and they point to a need for more intelligent models.

PRIMARY SOURCES OF THIS RISK



Algorithmic and model deficiencies



Inexplicable machine- and model-led outputs



Credit risk management constraints



Ineffective portability-related data protection

Events once deemed improbable are now expanding the boundaries of conventional risk and have the potential to expose multiple players and critical financial services functions to cascading losses.

Scenario example

A series of natural disasters create a massive service outage for a leading critical infrastructure provider, triggering losses in the billions for insurers.

What if…?

Cloud service providers continue to be integral enablers of new capabilities and digital infrastructure throughout financial services. To address emerging client needs, prominent providers have started to deliver embedded insurance, a distribution model where insurance products are integrated into the cloud provider's services.

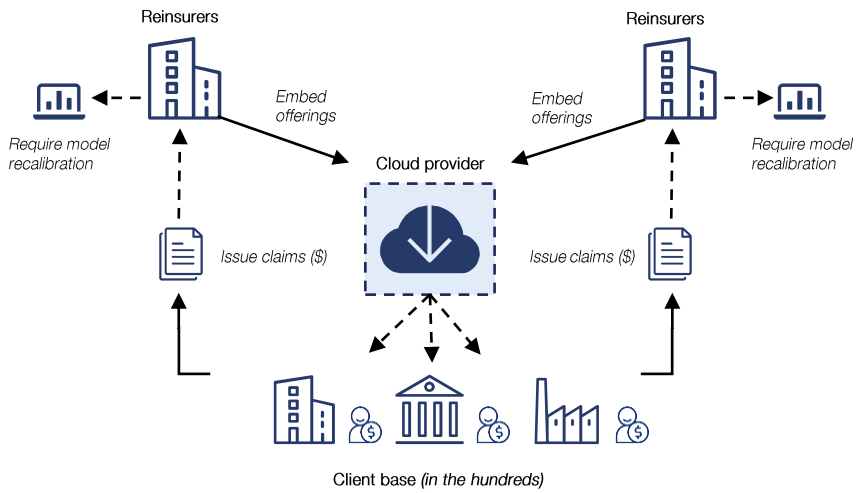
A series of natural disasters (e.g. persistent forest fires in one region, flash floods in another) severely devastate a cloud provider's data centres. Given the sporadic nature of climate-related disasters, the events were undetectable. With personnel being unable to access the site location, it takes numerous days for the cloud provider to troubleshoot operations and restore services for its clients.

Then this happens…

The system-wide shutdown leads to losses from business interruption and cascading operational disruptions. Furthermore, the provider's vast client base issues claims against this interruption, triggering total disbursements in the billions for the underlying insurers.

While the claims are administered, select insurers take note of this event and scale back their catastrophe insurance offerings due to uncertainties associated with high (potentially incalculable) losses. The 'randomness' of the event coupled with the lack of historic data available to properly assess the probability of this risk leads the insurers that continue to provide these offerings to significantly hike their premiums.

Process flow *(illustrative)*



Through improvements in forward-looking data and enhanced analytics, reinsurers can gain a much more granular understanding of these scenarios, enabling them to allocate capital appropriately and develop more nuanced underwriting strategies.

Traditional risk assessment struggles to capture the accelerated complexity of systemic risk, presenting an industry-wide opportunity for better interpretation of stochastic events.

What does this mean for the financial services ecosystem?



Deterministic shortcomings: Although effective through a linear and deterministic lens of the future (i.e. understanding how a system has behaved in the past by looking for correlations, which can help to indicate causation), the configuration of conventional models often misinterpret stochastic processes that can become systemic events.



Imminence of systemic repercussions: Another exogenous shock, whether humanitarian-, climate-, or macroeconomic-driven, may exhaust the limited support available by governments, central banks and incumbents across many jurisdictions. Without enhanced, enterprise risk assessment in the prudential and private domain, the 'safety nets' of nations and financial sectors risk further disruption and contagion.[62]



Challenges in timely resolution: While financial and technology players attempt to address general data availability issues and invest in multi-disciplinary analytics and cloud-based technology, the standard approach to modelling risk (by extrapolating historical values) is no longer valid and will not keep pace in a world that is fundamentally reshaped by non-deterministic events.[63]



Call for 'future-proof' solutions: As market players continue to digitally transform their technology stacks, there is an impetus to introduce novel, forward-looking risk assessment methodologies that can be supported by enhanced data and analytical capabilities across a variety of scenarios.

CASE STUDY

In April 2021, the European Central Bank (ECB) claimed that the biggest eurozone banks have repeatedly been too optimistic in their risk modelling. The central bank, which supervises the largest 115 eurozone banks, discovered more than 5,800 deficiencies in how 65 of the biggest lenders used internal models to calculate their capital requirements.[64]

While large lenders can look to reconcile their models against existing MRM frameworks and regulatory requirements as a first step, data availability issues must be addressed to accurately determine the asset risk level.

While this event did not create systemic implications, imagine if a similar event with a greater magnitude of impact occurred…

What if a highly leveraged hedge fund severely miscalculates its risk position across its derivatives (e.g. swaps), triggering margin loan calls that force big banks to mass-liquidate stocks?

Players are investing resources into new frameworks and approaches for model development, validation and ongoing monitoring activities.

What are some key efforts that ecosystem players have undertaken to mitigate this risk?

Public sector players

- Routinely assessing internal models used by banks for reliability and comparability (e.g. ECB's *Targeted Review of Internal Models* report determines the exposure of total risk-weighted assets).[65]
- Deploying MRM guidance into emerging regulatory initiatives (e.g. Basel, MiFID II, Solvency II), where supervisors are trying to constrain model risk through standardized modelling practices.[66]
- Actively establishing industry-wide approaches to evaluate emerging risks, such as setting up industry-led forums and processes, public consultations, conducting surveys and calling for voluntary disclosure.

Multilateral efforts

- Agreeing on stress testing approaches - alongside related disclosure and transparency - to reduce information gaps; incumbents and supervisory authorities are attempting to agree on timelines.[67]
- Industry bodies and reinsurers are collectively defining metrics for insurability and affordability across select digital domains (e.g. ransomware risks) and geographic locations (e.g. physical risks), particularly in the absence of active mitigation and adaptation measures by governments.[68]

Private sector players

- Monitoring emerging risks through both a qualitative and quantitative lens and leveraging new metrics to measure risk exposure based on their business mix and the complexity of operations.
- Exploring new ways to federate data from disparate databases and alternative sources (e.g. social media, mobility), and visualize data and insights (e.g. dynamic dashboards, control centres).[69]
- Applying an enterprise-wide validation process to address shifting regulatory requirements and cost efficiency; with a focus on upskilling resources or outsourcing select activities where expertise is required.[70]

RELEVANT CASE STUDIES

TCFD · TNFD · NGFS

To make climate risks more transparent, central banks and regulators are stress testing the financial system. The most notable initiatives are by the Task Force on Climate-related Financial Disclosures (TCFD), the Task Force for Nature-Related Disclosures (TNFD) and the Network for the Greening of the Financial Systems (NGFS).[71]

THE GENEVA ASSOCIATION

In 2020, the insurance industry took steps to strengthen industry-level collaboration globally, through the Geneva Association Task Force on Climate Risk Assessment, which aims to innovate and advance climate risk assessment and scenario analysis to produce meaningful and decision-useful information.[72]

FitchRatings · CyberCube

Fitch Ratings collaborated with CyberCube, a leading cybersecurity quantification company, to model the impact of systemic cyber events on the US banking sector under cyber risk scenarios. CyberCube's model focuses on single points of failure for cyber incidents that could impact parts of the US banking system.[73]

While select players are leveraging tools and scenarios to assess potential losses, further action is required to ensure that overly optimistic models do not mislead organizations.

What gaps exist in current mitigation efforts?

Public sector players

- Reactive auditing practices often mean that supervisory bodies have thousands of models to review and announced timelines are pushed back, delaying time-to-action for stakeholders.[74]
- Regulators may be exposed to overconsumption and over-analysis of data as they attempt to understand unquantifiable and non-linear risks, thereby delaying the formation of resiliency plans.[75]

Multilateral efforts

- While climate change discussions between supervisory bodies and the private sector are ongoing (including modelling scenarios on global warming), such findings have yet to materialize into formal recourse actions for the financial sector.[76]
- Ongoing guidance and principles-based approaches are, at times, hindered by disagreement and resistance to organizational change; leaders in both the public and private sectors may fail to realise that 'unlikely' risks could happen, and fail to create the necessary resiliency plans to handle them.[77]

Private sector players

- Scenario analysis and stress testing usually rely on a comparison of a limited set of scenarios (e.g. one business-as-usual scenario vs. an adverse one) over short periods, however, even realistic scenarios have difficulty dealing with unprecedented events.[78]
- Access to alternative data is possible, however, models would need to integrate new information in an agile manner because the systems and infrastructure on which they are built lack the necessary functionality and architecture.
- Uses of AI and ML across unstructured data can lead to players operating in a 'black box', where a lack of human monitoring and explainability may challenge existing risks or create new reputational risks.

KEY MITIGATION UNCERTAINTIES

1 *As no one-size-fits-all methodology exists for interpreting risk, will a lack of clarity regarding regulatory objectives and time horizons hamper progress towards developing the right solutions for risk interpretation?*

2 *Current mitigation tactics for stochastic processes often rely on quantified potential losses that are rendered arbitrary when faced with an extreme scenario. How can sound investment decisions for mitigation then be made without relying on a business case with an expected financial return?*

3 *Given the current configuration of models, changes may present pain points around gaining senior management buy-in and sourcing the appropriate, specialized resources. What incentive structures can account for the growing number of models in use that must be regularly reviewed and monitored?*

Mitigation approaches by individual players should focus on risk prevention, with consideration for scenario design and computational innovation.

How can current mitigation efforts be improved? What more can be done by individual players to address this risk?

Risk prevention

- Qualitative scenario design: Where a lack of relevant data exists to conduct stress tests with appropriate quantitative assessments, narrative-driven scenario analysis can provide insights into the operations and channels of risk transmission, and qualitative findings from such assessments can be reflected in business strategies and risk management practices.
- Prescriptive policies: Beyond creating a strong risk culture, both small and large entities can instil prescriptive model policies across areas such as vetting, testing, controls, systems integration and production. Ongoing areas such as training and feedback requirements for users, error quantification, monitoring, and usage reporting will be equally important.
- Open-source catastrophe modelling: Incumbents can leverage open marketplaces for modelling platforms that accommodate for 'closed box' approaches and provide turnkey components for deploying and testing catastrophe models through secure APIs.[79]
- Quantum-based simulations: Once commercially viable, quantum-based simulations (e.g. Monte Carlo) promise to provide a greater range of computational options for probability distributions that are currently hampered by classical computers, allowing players to better understand financial risk and prepare for unforeseen events.[80]
- 'Regulatory ready' models: Players can explore low code models to streamline auditability and trace the precise origins of data for regulatory reviews. These models can be further enhanced with independent, cross-disciplinary teams to challenge model thinking through structured expert judgement (e.g. deploying learnings from data scientists in the investment industry with experience of building models for predicting future scenarios).

CONSIDERATIONS FOR SCENARIO DESIGN



To begin developing an understanding of the material risks that an organization is exposed to, complex uncertainties can be segmented between **predictable and stochastic** outcomes.



By accounting for these uncertainties, **forward-looking scenarios** can be developed as narratives that span possible futures (including best and worst cases).



Scenarios can be quantitively assessed across **short- and long-term horizons** through forward-looking data (e.g. synthetic and alternative data) and expert judgement. For stochastic scenarios, long-term assessments will likely remain qualitative.



Organizations should then decide on which scenarios to **prescribe mitigation actions** to and reflect these decisions into their overarching business strategy or resiliency plan.

While multilateral mitigation approaches should also focus on risk prevention, particular consideration should be given to data alliances and forming insights for policy development.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Federated data analysis: To circumvent data sharing limitations, federated techniques can combine information from decentralized datasets without aggregating them into a single location. This allows for private collaborations where model-learning leverages data without exposing it between players.[81]
- Enriched early warning indicators: Players can enhance their repository of early warning indicators from comparable data sets and ML techniques, which can help to uncover important non-linearities and interactions that typically only exist in out-of-sample predictions and forecasting. To enable this, players can look to establish new relationships with external providers that offer multi-structured data in real time.
- Private sector-led standard-setting: As an interim solution to pending regulatory guidance, incumbents can develop a mutually agreed set of risk standards that facilitate the access, sharing and use of associated data inputs. This can reduce costly redundancies and provide a greater choice of models for all industry players.
- Central MRM platforms: Purpose-built vendor solutions developed for MRM applications can enable faster compliance, streamlined workflow management and automation of critical processes. Technology players can work with supervisory bodies to establish a centralized dashboard and repository for model information while providing governance, reporting and analytics capabilities to help all stakeholders better understand and manage model risk.
- Public insight gathering: Before mandating industry response or exploring industry-wide change incentives, regulators could undertake a public consultation route, seeking feedback from stakeholders on proposed opinions, approaches, methodologies and tools. This could be further enhanced with a call for voluntary data from the industry around operational footprints, security mechanisms, and quantitative information on certain scenarios. To prevent further fragmentation across efforts, policy-makers and supervisory functions can band together to establish a commonly understood taxonomy for emerging, covert risks (e.g. integrated risk glossary).

POTENTIAL UNINTENDED CONSEQUENCES

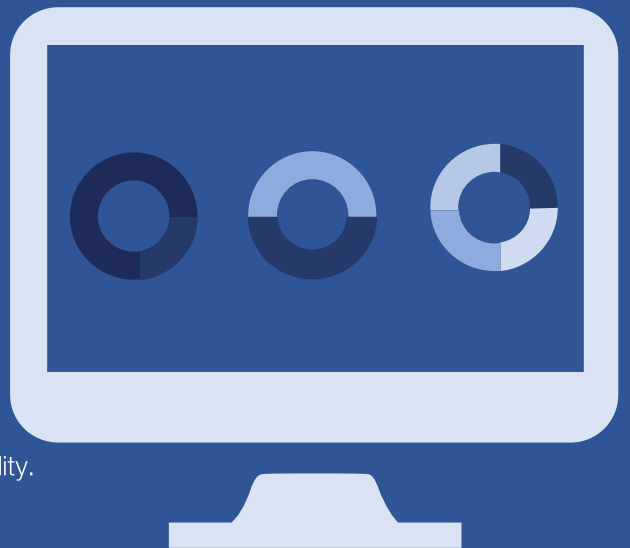


The value in stress tests depends on the quality of the underlying scenario(s). If a scenario exercise (e.g. design or analysis) cannot capture the full range of likely and unlikely effects deriving from a shock - or anticipate the source of shocks - then the stress test may lose viability.



Modelling enhancements may lead organizations astray due to built-in optimism biases. As organizations look to integrate sophisticated tools and become forward-thinking with their approach to models, they should remain cognizant of the drawbacks associated with quantifying rare events with unknown time horizons. Model overreliance may influence reckless risk-taking positions.

Key mitigation applications



Note: The mitigation applications highlighted in the following slides are intended to be considerations and have not been assessed for viability or feasibility.

Table stakes: To enable the confidential sharing of valuable inputs, entities can use federated analysis techniques to address information gaps while adhering to data privacy and localization needs.

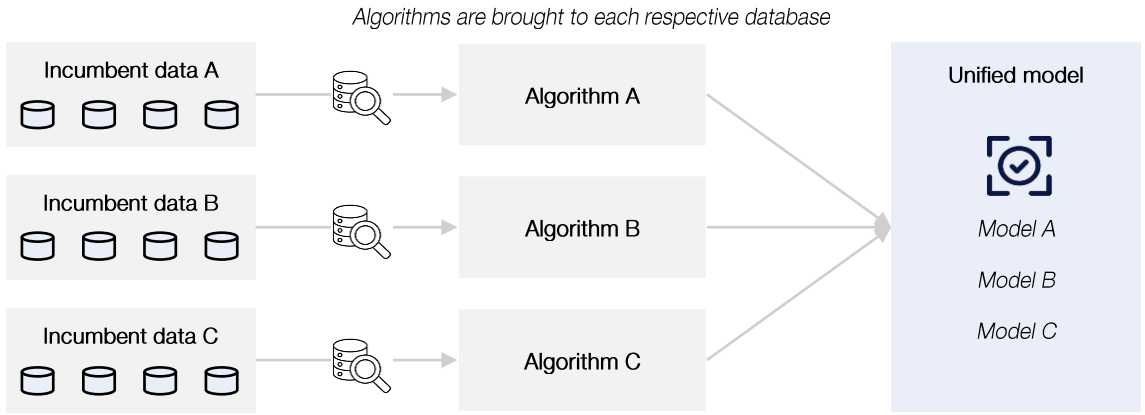
Overview

When a financial institution seeks to analyze multiple data sets across databases, the common practice is to combine them into a single setting and conduct analysis across the entire set at once. This practice introduces three issues for players: a lack of permission to transfer local data, confidentiality concerns, and an increased threat of data breaches.

Where traditional data science brings information into one central data lake, federated analysis (e.g. private federated knowledge graphs) leverages information from disparate and decentralized datasets without gathering it into a single location. Rather than sharing the underlying data, players can apply bespoke models and algorithms to respective data sets and outputs can then be aggregated to create a unified model.[81]

This approach can result in a robust data analysis engine, allowing players to benefit from a large pool of data without the need to share their confidential data and seek permission for bilateral data transfers. While this approach is mature from a technical standpoint, its application across financial services is very limited.

How it works



Federated analysis creates an aggregated system that **results in robust modelling to address data gaps** or where data does not exist in a single domain.

Use in financial services



- As financial institutions continue to enhance the data embedded within their models, federated analysis would combine insights from a variety of industry and broader economy players, allowing incumbents to benefit from an aggregated system of risk analysis.
- A federated method (e.g. knowledge graphs) enables players to collaboratively learn from a shared prediction model while keeping all respective data within their own ‘walls’.
- This will also decouple the ability to run AI and ML applications from the need to store data in the cloud, thus eliminating centralization concerns.

Emerging: Open-source catastrophe modelling encourages collaboration, transparency and consistency, allowing organizations to predict risk exposure more confidently.

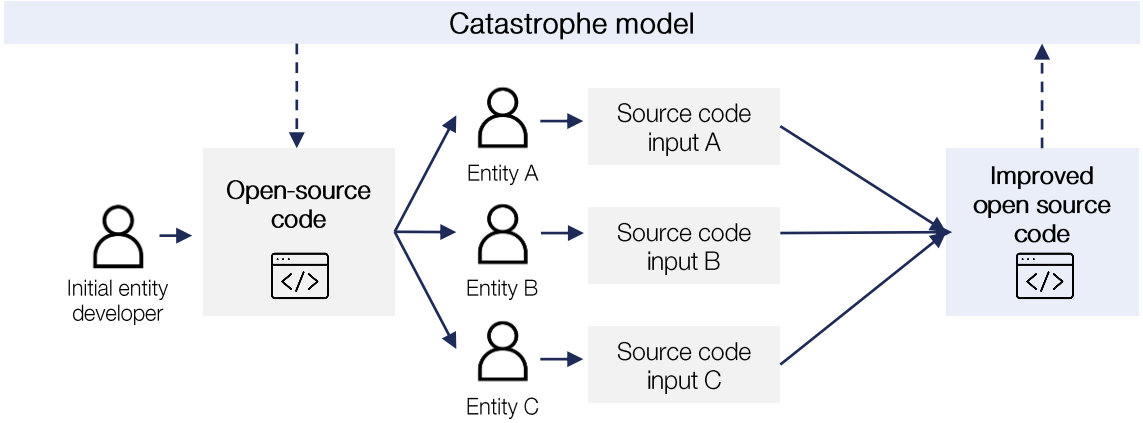
Overview

Current catastrophe models typically fail to account for events that lack historical data. Commercial use of these models may also focus on risks in which some incumbent players may have a predetermined bias towards or a stake in (e.g. an interest in premium profitability).

In contrast, new risk models leveraging publicly accessible, open-source data could not only leverage a transparent methodology but could also consider the best structured expertise (e.g. input from a climate scientist) to incorporate the relevant parameters needed to better understand risk exposure.

Open-source constructs allow for data collectors to present alternative types and sources of data to support the issue of information gaps, ensuring that client models are fed unbiased data sets. Investments into more comprehensive and open-sourced modelling capabilities (e.g. with advanced big data models or hyper-localized ML models) can be broadened to interpret internal, external and interdependent risks that focus on extreme outliers rather than expected outcomes.[82]

How it works



Open-source modelling offers a **transparent methodology** while incorporating industry-wide knowledge to better understand and interpret risk exposure.

Use in financial services



- Open-source modelling can provide insurers with a marketplace platform for developing, deploying and executing climate catastrophe models.
- The open-source model leverages a simulation engine (with no restrictions on the modelling approach) to help solve pricing inconsistencies that exist in the insurance market.
- The Oasis Loss Modelling Framework, for example, provides financial services players with a platform to leverage open-source modelling and design catastrophe models based on constant iterations from third-party climate experts.[82]

Novel: The introduction of quantum algorithms embedded in Monte Carlo analyses will enable players to forecast the likelihood of evident and covert risks more accurately.

Overview

The Monte Carlo method is a forecast modelling technique used to assess the likelihood of certain outcomes by accounting for uncertainty and randomness in complex systems. Instead of estimating for a single outcome, Monte Carlo simulations construct probability distributions over many possible outcomes.[83]

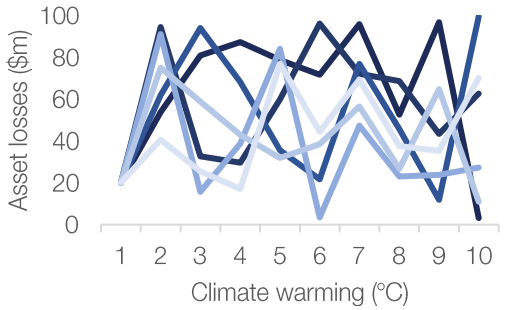
Although Monte Carlo is a primary methodology for analyzing risk, computational outcomes can become hampered by the limitations of classical computers.

Quantum-based algorithms will not be restricted by computational power due to the possibilities of quantum computers; these can run multiple scenarios simultaneously and reduce simulation errors. By emulating these quantum effects on classical computers, organizations can take advantage of quantum computing approaches to design faster Monte Carlo sampling strategies and be more confident in their simulation outputs.[83]

How it works

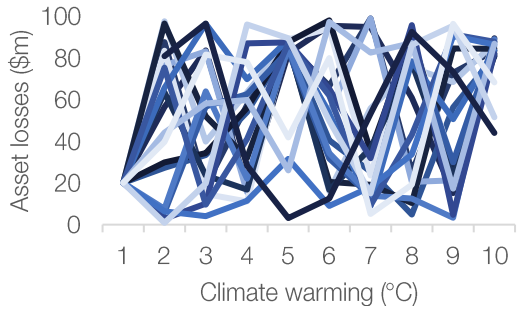
Traditional scenario output (illustrative)

Duration: ~5 hours
Accuracy: 91.3%



Quantum scenario output (illustrative)

Duration: ~1 hour
Accuracy: 98.8%



Quantum-based algorithms increase speed, accuracy and volume when risk modelling, enabling players to **improve forecasting techniques and risk anticipation.**

Use in financial services



- The use of quantum-based Monte Carlo simulations will allow for extremely complex situation modelling and could lead to groundbreaking discoveries in the field of financial risk assessment.
- Financial institutions have recently redesigned their existing risk models and are under pressure to confidently run a larger number of simulations; as time progresses, incumbents may want to consider investment into quantum Monte Carlo simulations.
- Beyond their applicability for modelling emerging risks, quantum algorithms enable a range of use cases (e.g. consumer targeting and prediction) that complement risk forecasting applications and could enable comprehensive risk profiling capabilities.



1 2 3 4 5 6

Gaps in entity-based regulation

Current regulatory approaches may lack the flexibility and scope to accommodate technology-based activities and players operating in, and around, the financial ecosystem.

Overview



Unregulated scale

Non-traditional financial players are rapidly evolving, hand in hand with global digital adoption. Lightly- or unregulated activities across nonbank financial offerings, decentralized finance and digital assets continue to see accelerated market growth.

While financial regulators are joining their supervisory counterparts to scrutinize the potential risks presented by these activities, **further exploration of the potential ecosystem implications** is needed.



Uncharted waters

As novel or peripheral financial activities remain relatively nascent, the **full range of risks has yet to be seen.** Players may be disproportionally exposed to exogenous threats and could unintentionally participate in propagating fraud, illicit financing and the misuse of financial data.[84]

This presents **unique regulatory challenges for financial stability, safe transactions and general consumer protection** in an uncharted arena.



Entity-based focus

Current regulatory approaches are **geared towards individual entities *or* specific activities**, with the primary focus being on the former. Incumbents performing a specific financial activity are subject to strict prudential regulations that may not apply to nonbanks performing a similar activity.[85]

Despite **policies and frameworks being gradually adjusted to cope with risks that new players and offerings may pose**, reform has yet to be fully applied.



Asymmetric pace

Although proactive approaches between regulators and innovators are proving to be successful (e.g. sandboxes, innovation offices), the **pace of innovation continues to surpass governance efforts and the scope of current mechanisms.**[86]

Trustless innovations are further exacerbating such gaps. For example, the lack of consumer protection and liability mechanisms led to the unaccounted loss of nearly $82 million in crypto scams from late 2020 to early 2021.[86]

Why is it important?



Exposed ecosystem

If emerging financial activities and players continue to grow in scale and bridge further into traditional financial markets while remaining unaccounted for, they may present risks to **financial stability, consumer protection and market integrity.**

The current regulatory regime may **not be fully equipped to protect the system from these issues or prevent the emergence of related systemic events.**[87]

PRIMARY SOURCES OF THIS RISK

- Undefined regulatory oversight for new entities/business models
- Stagnant and inconsistent customer data privacy controls
- Blurring jurisdictional boundaries
- Concentrated financial services market structure

Despite the complex nature of modern financial services, regulatory and supervisory bodies can be rooted in fragmented procedural frameworks designed to accommodate traditional domains.

What are the typical functions of regulatory, policy-making and supervisory bodies?



Prudential function

To promote the safe and sound functioning of entities. Also responsible for key policy instruments, including risk management, reporting requirements and limitations on risk concentration.[88]



Conduct function

To promote protection across consumers and markets by setting permissible activities and behaviours for market participants. Also responsible for the conduct of business, effective financial markets and consumer protection.[88]



Structural and competition function

To promote effective market competition (can sometimes fall under the purview of the conduct function). Also responsible for preventing possible abuse of monopoly power by dominant entities through antitrust measures, entry restrictions and merger controls.[88]



Organizational function

To promote the efficient functioning and integrity of financial markets and information exchanges. Also responsible for participation rules, including approving rulemakings made by self-regulated organizations and markets.[88]



Macroeconomic function *(i.e. central banks)*

To promote the monetary and financial stability of a nation. Also responsible for maintaining control over aggregate economic activity through reserve requirements, interest rate controls and the oversight of the interbank payments system.[89]

COMMON REGULATORY MODELS[90]

While the models below are most utilized globally, select jurisdictions employ a combination of the functions described.

1. Institutional model: The legal status of the financial entity determines which regulatory body has purview over its supervision and market conduct oversight. — *Hong Kong*
2. Functional model: The financial entity's activities or function within the sector determines which regulatory body oversees it. — *USA*
3. Unified model: Both prudential supervision and market conduct of all financial entities is regulated by a single, unified regulator. — *Singapore*
4. 'Twin peaks' model: One regulator is responsible for prudential issues and a second is responsible for the market conduct supervision of all financial entities. — *UK*

*Note: For the purposes of this report, the actors carrying out the listed functions of regulatory, policy-making and supervisory bodies will be referred to as 'regulators'.

Unclear and limited oversight of DeFi activities is raising financial stability concerns, as the attractive benefits are inadvertently enticing participants looking to exploit the space.

Scenario example

DeFi activities continue to accelerate and grow in scale, unintentionally creating a haven for illicit activity that bypasses integral global regulatory safeguards

What if…?

Consumer demand for DeFi offerings rapidly grows across economically developing nations. These offerings replicate the products of the traditional financial system while providing greater incentives and consumer benefits (e.g. high-yield savings accounts, cheaper peer-to-peer (P2P) lending, enhanced financial privacy and security).

Despite efforts made by regulatory and supervisory bodies to control unregulated exchanges, new decentralized and permissionless applications continue to emerge at an exponential rate. Consumers eventually phase out their participation in traditional finance (e.g. no longer have a primary bank) and begin to solely contribute to DeFi applications.

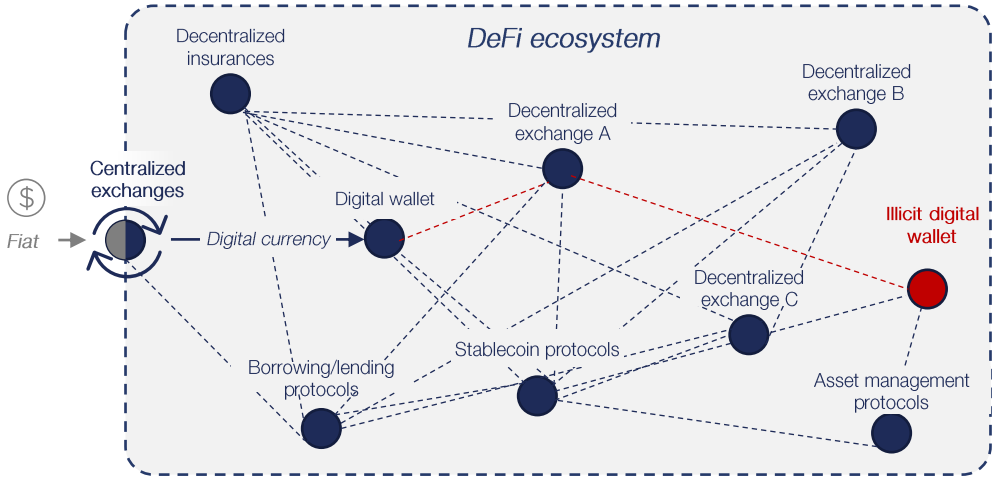
Then this happens…

Illicit transactions for money laundering and terrorist financing quickly proliferate. In this system, bad actors easily bypass the existing robust AML/CFT laws that are bound by fiat money in the traditional system.

Regulators attempt to remedy the situation within their respective jurisdictions, however, regulatory mechanisms do not appropriately translate to this new DeFi system. Beyond efforts to better monitor and track malicious activities, regulators try to implement a mechanism to punish these bad actors. Despite this attempt, fragmented policies and reactive recourse actions (e.g. penalties and blacklists) do little to prevent illicit financial activities and safeguard consumers' assets. Regulators are also unable to mandate risk disclosure or KYC requirements, leaving DeFi as an open 'black market' system.[91]

Process flow *(illustrative)*[92]

Traditional financial system (i.e. regulated entities and activities)



Without the ability to implement a balanced oversight approach that promotes the development of a DeFi ecosystem while limiting its misuse, negative impacts will likely carry over into the real economy and jeopardize societal wellbeing and financial security.[93]

While nonbank financial services must satisfy current requirements, discrepancies persist due to entity-based confines and direct oversight limitations.

What does this mean for the financial services ecosystem?

Regulatory applicability is in question: As trustless innovations (e.g. DeFi) raise concerns related to governance and conduct complexities, regulators are signalling the desire for greater consumer protection. If these activities grow in scale or further bridge into traditional financial markets (e.g. as seen with the launch of Bitcoin exchange traded funds), the lack of fully applicable and purpose-fit regulation will pose an increasing area of systemic concern.[94]

Differential entity-based treatment: Public authorities treat players differently because of entity-based rules (e.g. banks require prudential regulatory treatment, whereas credit providers that cannot accept deposits do not). These rules are required when risks emerge both from the provision of a specific service or activities in combination.[95]

Scope expansion of policy objectives: While certain regulatory asymmetries can be justified on policy grounds (e.g. financial stability, competition), there are areas where existing gaps cannot be justified based on primary policy objectives (e.g. consumer protection, AML). This dynamic has created unique complexities for oversight bodies that determine how to regulate and create appropriate policies.[96]

The call for adequate supervision: Improved regulatory configuration is required to ensure sound interaction with regulated financial services and national legal frameworks. As issues such as barriers to entry, anti-competitive practices and financial crime grow in prevalence, the configuration of regulatory frameworks, standards and associated tools can be improved to ensure adequate oversight and regulatory coverage.[97]

Regulatory amalgamation and coordination: An effective regulatory response to emerging players and financial activities in the ecosystem is likely to involve a combination of existing regulation, retrofitted regulation and new, bespoke regulation. While most jurisdictions have begun to undertake at least one of these three initiatives, more comprehensive regulatory shifts must be explored to address systemic gaps.[97]

CASE STUDY

In October 2020, an attacker stole $33.8 million from DeFi application Harvest Finance by exploiting an engineering mistake using flash loans (an uncollateralized instant lending offering). The developer team failed to track down the attacker and did not yield centralized control over the project.[98]

Flash loan attacks in DeFi are common and highlight the need for liability controls and further governance. While integrated regulatory models (e.g. unified, twin peaks) offer more flexibility in oversight mechanisms, the emergence of DeFi signals prevailing gaps.

While this event had systemic implications, imagine if a similar event occurred with a greater magnitude of impact…

What if a surge in the adoption of decentralized applications leaves millions of consumers stranded with uninsured deposits?

Ecosystem players are looking to improve the way they influence and react to digitally-focused changes, based on the current scope of the regulatory regime.

What are some key efforts that ecosystem players have undertaken to mitigate this risk?

Public sector players

- Exploring activities-based and principles-based regulatory approaches that strike a balance between promoting nonbank innovation and establishing 'guardrails' that minimize potential risks to the system.
- Taking direct action to constrain the development of financial services outside of the regulatory perimeter (e.g. increasing the regulation of nonbank players in China's financial sector).[99]
- Considering new regulations for the DeFi space (e.g. securities law oversight for digital assets, centralized exchange intermediary requirements) to prevent fraud and ensure investor protection.[100]
- Partnering with supervisory technology (SupTech) players to streamline administrative and operational compliance procedures and automate the supervision process.[101]

Multilateral efforts

- Regulators are co-developing third-party risk management frameworks with incumbents to indirectly manage vendor activities (e.g. due diligence requirements for entities employing vendor services).[102]
- Incumbents and FinTechs are working with regulators to establish principles and frameworks on consumer data access (e.g. open banking) and authentication (e.g. digital identity).[103]
- Financial institutions are collaborating with regulators, cloud providers and systems integrators to explore multi-cloud approaches and create resilient cloud offerings.[104]
- Certain countries are continuing to establish innovation hubs and regulatory sandboxes in response to FinTech developments to better understand new business models and regulatory gaps.[105]

Private sector players

- Engaging with other private sector players to develop a shared understanding of the evolving digital transformation landscape and participating in consultations to shape data sharing schemes.
- Vocalizing concerns for oversight over data aggregators and other non-financial entities to ensure strengthened consumer protection and a consistent playing field for all private sector players.[106]
- Lobbying for key policy recommendations, including standards for consumers to access and share their financial data safely and securely.[107]
- Partnering with regulatory technology (RegTech) players to reduce compliance costs and efficiently fulfil regulatory requirements.

RELEVANT CASE STUDIES

In the EU, the Digital Services Act contains entity-based provisions for Big Techs through a supervisory regime. The goal of the Act is to ensure adequate management of the different operational risks that Big Techs generate, including requirements for governance, risk management and audit.[108]

The Financial Conduct Authority's (FCA) TechSprints events bring regulatory and industry experts together to solve specific regulatory problems each year. In 2019, the FCA hosted over 40 organizations to tackle the issue of financial crime by developing PET-based solutions.[109]

Data aggregators like Plaid are asking the Consumer Financial Protection Bureau to clarify standards on sharing consumer financial data. They are requesting direct supervision from the agency, which would replace the current system in which US banks oversee aggregators as third-party vendors.[110]

With the influx of new, digitally-native providers and activities in financial services, public and private sector players are noting that loopholes exist in the current supervisory scope.

What gaps exist in current mitigation efforts?

Public sector players

- Regulating the cross-border activities of nonbank offerings would require multiple licenses from multiple regulators across many jurisdictions; such a patchwork would be unlikely to result in full oversight of all financial activities, especially as the digital-native world does not adhere to jurisdictional boundaries.
- Existing, centrally regulated financial systems and other national legal schemes (e.g. taxation, national identity systems) do not apply to DeFi applications and require the bespoke prevention of regulatory arbitrage.[111]
- Data regulation (e.g. custodial rights, portability, privacy and security) remains fragmented between jurisdictions and players, further disjointing oversight and creating geopolitical implications.[112]

Multilateral efforts

- Despite ongoing consultation processes, authorities struggle to understand and react to evolving business models; a lack of coordination remains across a multitude of supervisory bodies.[113]
- Much of the current global public-private regulatory system operates in analogue (e.g. with a lack of digital information flow), rendering assessments and recourse measures time consuming and reactive.[114]
- The supervision of DeFi activity will remain challenging due to the lack of central intermediaries and the prevailing reliance on infrastructure.[115]

Private sector players

- Complex and time-consuming reporting requirements persist; this challenge is exacerbated by an absence of information requirements (e.g. incumbents do not need to share their vendor network).[116]
- Indirect risks connected with Big Tech activities are not fully captured, as substantive interlinkages and their role as critical service providers for financial institutions are difficult to quantify.
- While players increasingly develop market offerings in digital assets and cryptocurrency, reactive approaches have been undertaken to educate and provide expertise to public sector players.

KEY MITIGATION UNCERTAINTIES

1 *While public sector actors can work to implement policies to mitigate these innovation-focused regulatory gaps, what new expertise (i.e. tech- and data-oriented personnel) will be required to complement policy experts and respond to industry changes effectively?*

2 *With a limited understanding of the operations of certain technology-based players (e.g. Big Techs, decentralized exchanges), how can public sector players determine the right balance between promoting innovation and protecting the system itself?*

3 *As many non-financial entities do not have to uphold any regulations beyond activity-based requirements, a source of competitive distortion exists in entity-based policy for financial institutions; in comparison, can there be adequate rules to address the risks posed by Big Techs?*

Regulation is unable to fully keep pace with new technology and innovation in the ecosystem; however, there are a variety of initiatives that individual entities can explore to alleviate this gap.

How can current mitigation efforts be improved? What more can be done by individual entities to address this risk?

Risk prevention

- Specialized units: To better understand the applications of new technology or financial activities, regulators can strengthen their in-house expertise and deploy targeted teams to share knowledge with intermediaries and global policy bodies; this can inform the creation of tailored regulation and oversight.[117]
- Machine-readable regulations: To enable the automated provisioning and tracking of requirements at the entity-level against specific regulations, regulators can codify (i.e. electronically tag) their taxonomy of rules to be interpreted by software. Additional benefits include being able to respond to instances of potential misconduct and dispute resolution.[118]
- Single-party digital regulatory reporting (DRR): To better equip regulators with complete entity-level information in real-time, DRR systems that are coupled with machine-readable regulations can convert financial information into a digital form that can be easily and inexpensively obtained by regulators on an 'as-needed' basis.[119]
- Proactive resilience: To address inconsistent regulatory risk measures and the current inability to aggregate data, private sector entities can look to strengthen operational resilience, refine performance metrics and develop a robust third-party risk management framework for outsourcing beyond what is prescribed.[119]

Risk resolution

- Harmonized cyber and data policies: Cyber and data policies can be coordinated to avoid friction and uncertainty between inconsistent taxonomies and ensure rules with potential impacts on financial stability do not become entrenched in the long run. This may prevent 'races to the bottom' that can intensify destabilizing behaviour.[120]
- Bespoke nonbank supervision: To achieve a common denominator across the activities of interconnected nonbank financial players and financial orchestrators, regulators may consider incorporating financial data gathering and analytics as regulated activities within their established capacities.[121]
- Deployment of central bank digital currency (CBDC): To hedge risks associated with new forms of private digital money creation (e.g. crypto assets, stablecoins), regulators should continue to explore the creation of wholesale and retail CBDCs to support competition, efficiency, innovation and resiliency in payments, with public interest at the forefront of its design.[122,123]

POTENTIAL UNINTENDED CONSEQUENCES



While regulators and policy-makers can look to independently build machine-readable regulations based on their unique environments, revisions to risk taxonomy without contributions and collaboration from other jurisdictions can further create regulatory inconsistencies, especially for market players with large global footprints.



If regulators do not approach the formulation of Big Tech oversight with a balanced perspective between the commercial benefits being provided to the ecosystem and the potential structural risks these entities pose, innovation brought to the financial services ecosystem could be inadvertently stifled.



While the emergence of CBDCs may optimize payments for a nation, these currencies have complex consequences. Financial stability, data privacy and cybersecurity concerns should be accounted for during their design.

In addition to individual entities' actions, multilateral efforts around the most pressing and prominent regulatory issues should be pursued, to drive a regulatory framework that suits all.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Private sector-led council: To proactively advocate for regulatory gaps and consult on risk-based criteria, both financial and non-financial players can routinely participate in the sharing of evidence-based concerns and best practices, and work to establish alliances when addressing policy changes set by regulatory functions.
- Cross-border innovation: To enhance information sharing and achieve a standardized risk taxonomy based on best practices and use cases, regulators should look to collaborate with global policy bodies that offer cross-industry and cross-border collaboration to support automation objectives, alleviate regulatory gaps and enable disparate jurisdictional strengths.[124]
- Multi-party regulatory 'clearing house' utility: To better explore technology for meeting regulatory reporting requirements and monitoring incidents, RegTechs and SupTechs can work with regulators to build platforms that capture and administer the data required to adhere to regulatory requirements across multiple regulators, reducing the burden of data collection and retrieval for the entire sector. This would also enable the ongoing monitoring of incidents with seamless data flows between regulators and entities.[124]
- DeFi regulatory sandboxes: To equip ecosystem players with the opportunity to safely explore how to best operate and regulate novel DeFi applications, policy-makers can establish tailored sandboxes that ensure both public- and private-sector participants gain first-hand experience across a range of use cases prior to launch and market entry.[125]

Risk resolution

- Perimeter assessment: To balance meeting the objectives of regulatory regimes with promoting innovation and market development, an objective task force should look to assess and validate the existing financial regulatory framework within a jurisdiction. The task force should also determine how to either effectively allocate oversight responsibilities within the current framework or stand-up a regulatory body tailored to decentralized financial activity.[125]
- Digital identity convergence: To address the KYC risks imposed by select nonbank offerings, industry players can form consortiums to accelerate the adoption of identity verification mechanisms by these players (e.g. establish identity in the onboarding journey or when identities need to be re-verified when transacting).[126]
- Incentive-driven resilience: To better incentivize operational resilience (despite existing concentration risks), regulators can develop incentive schemes for the voluntary disclosure of user and network data within a nonbank's domain.

POTENTIAL UNINTENDED CONSEQUENCES

In certain jurisdictions with overlapping authority, technology advancements and novel applications (e.g. DeFi) that are being tested in regulatory sandboxes may face additional barriers to entry. Solutions developed in sandboxes and designed by one regulator may not be permissible by another, preventing sound coordination and resulting in duplicated efforts.

Even if regulators can formalize the direct oversight of DeFi and/or Big Techs, a strong framework will not work without adequate ongoing supervision that effectively understands the technology and assesses the nuanced activities and risks within its scope. Without informed and active oversight, more regulatory gaps will emerge.

Key mitigation applications



Note: The mitigation applications highlighted in the following slides are intended to be considerations and have not been assessed for viability or feasibility.

Table stakes: Regulatory jurisdictions can consider recalibrating their mix of entity- and activity-based oversight to expand regulatory perimeters and cover new and emerging technology-linked activities.

Overview

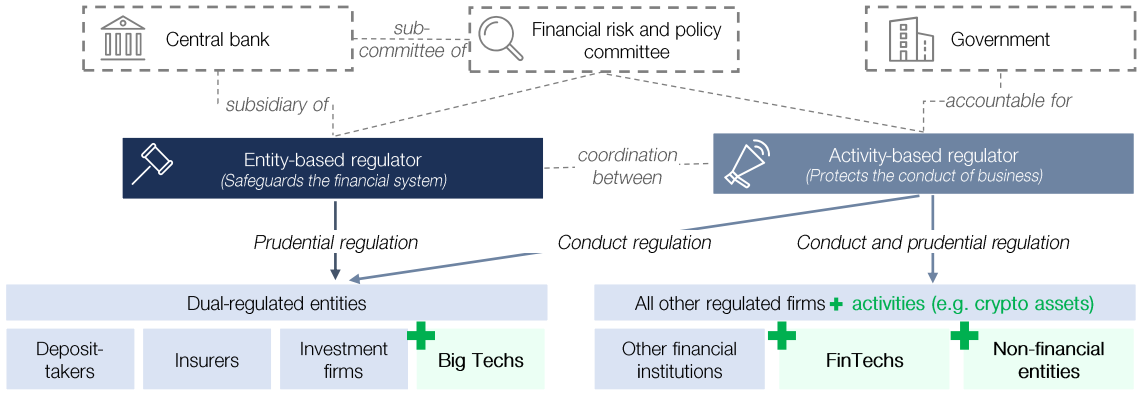
Certain jurisdictions have undertaken a unique, purpose-fit regulatory approach that combines activity-based and entity-based regulation (to varying degrees) across regulatory functions. While these jurisdictions are increasingly pivoting towards an 'integrated' model with designated oversight across prudential (i.e. entity-based) and protection (i.e. activity-based) rulesets, gaps in oversight remain as new players (e.g. Big Techs) and activities (e.g. decentralized peer-to-peer lending) enter the ecosystem.

While many regulators are shifting their focus to activity-based regulation to address innovative applications, this should complement, rather than replace, entity-based regulation. Resulting policies can then be simultaneously configured and deployed to prevent systemically important risk gaps, as seen in mature 'twin peaks' models.[127]

Under specific design considerations, framework amendments and regulatory perimeter expansion will address the lack of accommodation for:
- The interconnected business models of Big Techs and large FinTechs, which receive different treatment from financial institutions performing the same activities.
- The lack of entity-linked accountability across the DeFi space, where smart contracts, digital assets and blockchain activities do not rely on financial infrastructure.[128]

How it works

Illustrative model based on a 'twin peaks' integrated regulatory model



By repositioning the regulatory scope, supervisors will be better equipped to uphold their critical objectives, while alleviating **unwarranted oversight asymmetries** and gaps.

Use in financial services



- While regulatory asymmetries between financial institutions and non-financial players can be justified where systemic issues are concerned, differences in requirements are only warranted when accounting for the *specific* risks posed by different entity types.
- The risks posed by financial institutions are adequately accounted for in prudential oversight; the digital risks posed by entities such as Big Techs and FinTechs are not holistically accounted for in entity-based financial services regulation.[129]
- A renewed entity-based focus can be complemented by distinct activity-based regulation in the DeFi and digital assets space, given that inherent decentralization is misaligned with traditional entity-based regulation.

Emerging: Regulators can leverage a digital regulatory reporting (DRR) platform to extract and analyze broad sets of data and gain context on emerging financial activities in real time.

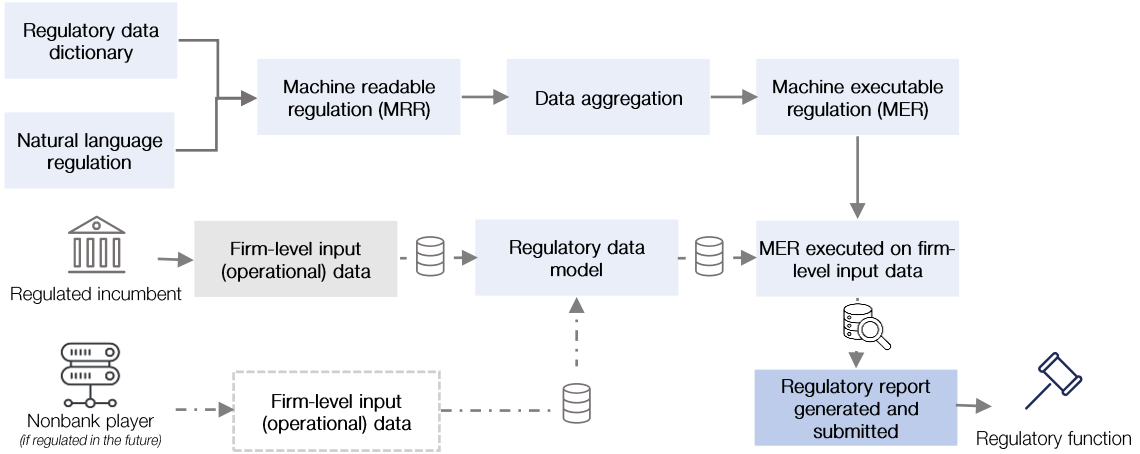
Overview

Regulators often struggle with heterogeneity across the data points they gather from financial entities (e.g. transaction volumes, credit risk). These are manually captured through the filing of written reports on a routine, but relatively infrequent, basis (e.g. quarterly or annually). Given the challenges of compiling and receiving this highly analogue data (i.e. relevant information must be extrapolated from the uploaded summary reports), these bodies are left with inconsistent and untimely data for decision-making.[130]

Manual processes can be digitally redesigned to collect and analyze data through the creation of an integrated DRR platform. The platform can help regulators convert historic and current financial (and eventually technical) information into a digital domain that can be easily accessed in real time, as needed. This foundational process overhaul can eventually enable expansion of coverage to non-financial ecosystem players.[131]

While DRR proof of concepts are being executed in select jurisdictions (e.g. in the UK, USA, Singapore), global adoption of DRR platforms would lead to a fundamental shift in the current regulatory reporting and compliance model, with the potential to eventually establish cross-border and industry interoperability.[131]

How it works



Enabled by machine-readable and -executable regulations, DRR equips regulators with complete information while **reducing the reporting burden** on entities.

Use in financial services



- Given that many regulatory reporting mechanisms in financial services remain manual, highly aggregated, and confined to only financial institutions that are in-scope, the data and resulting insights generated quickly become dated and static.[132]
- Real time and early warning indicators of ecosystem-level risks are not currently afforded by regulatory monitoring initiatives in most jurisdictions, due to the confines presented by analogue and entity-based reporting.
- An integrated DRR platform with a common data model and automated reporting rules would enable the shift away from template-based financial institution reporting and the potential for non-financial entities to be more seamlessly included in the formal oversight process (e.g. Big Techs).[133]

Novel: To fill the inherent oversight gaps that exist in a functional regulatory environment, collaborative regulators can build a designated utility that supports rules-based centralization.

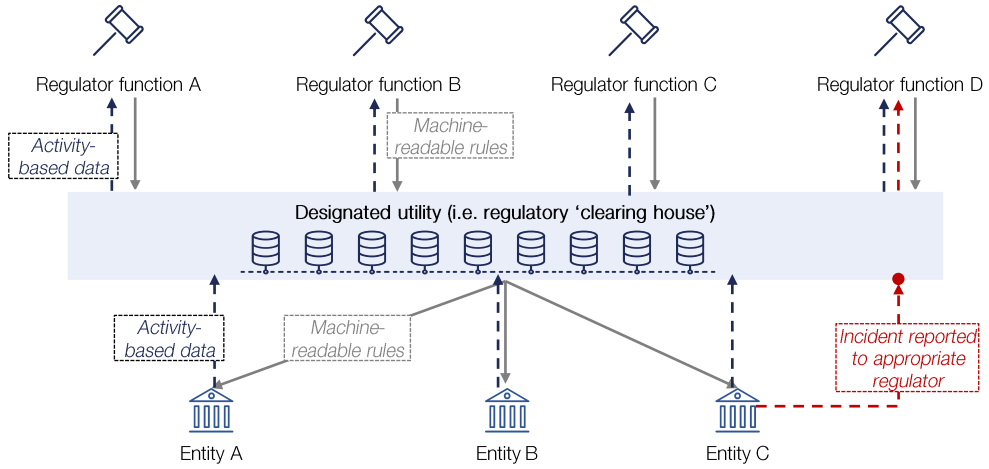
Overview

For a functional model to operate effectively, coordination among regulators is required to ensure the appropriate allocation of oversight so that no aspect of a given entity evades appropriate regulation.[134]

This becomes problematic when new products and activities do not neatly translate within the purview of regulators, given the overlap in oversight and disjointed taxonomies that may exist. In these fragmented regulatory environments, a designated utility could act as a 'clearing house' to coordinate and match regulations based on an entity's activities.[135]

Enabled by natural language processing (NLP) and rule-based techniques, regulatory rules could reside in a centralized platform that automatically disseminates the applicable ruleset for select entities in the ecosystem (i.e. the data 'outflow'). In return, regulators could be equipped with secure activity-based data that can trigger real time incident reporting and triage the findings to the designated regulatory function (i.e. the data 'inflow'). Such a solution, however, requires strong international cooperation.[136]

How it works

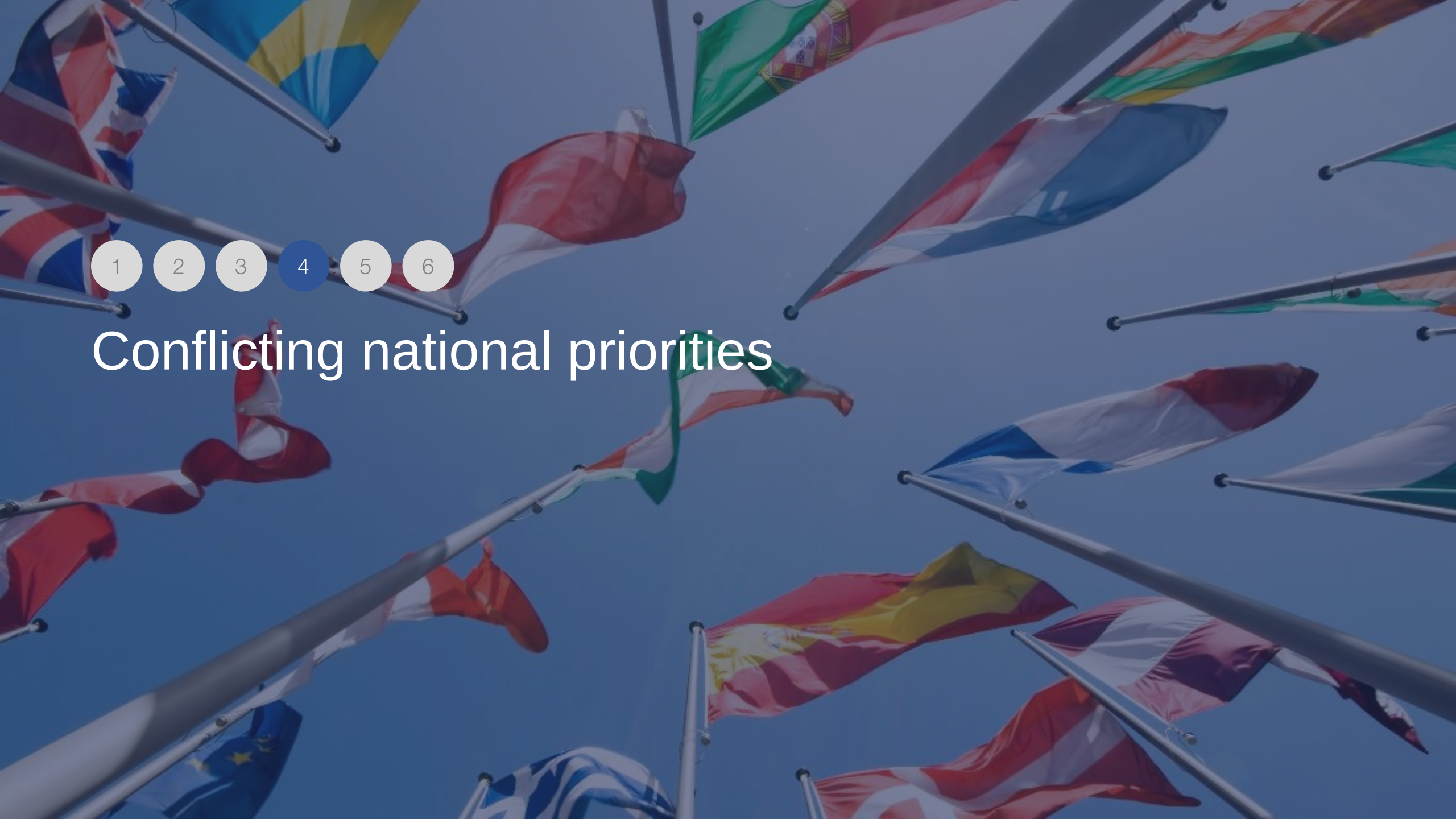


The utility facilitates the **digital coordination of rules provisioning, compliance and reporting** across all regulators and entities in a jurisdiction.

Use in financial services



- If all regulators in a given jurisdiction were to come together to create an objective and designated 'clearing house' utility, the landscape could benefit from the centralization and streamlining of all disparate rules and policies.
- Regulators would benefit from the inherent coordination afforded by the platform, as it would amalgamate the capture of reporting data and dissemination of real-time machine-readable rules. This is similar to the functioning of a DRR platform, however, it is designated for multi-party regulatory coordination and multilateral data flows.[136]
- Not only would this be beneficial to regulators, but it could also reduce compliance costs for private sector entities that would no longer need to submit data to multiple supervisors to adhere to requirements.



1 2 3 4 5 6

Conflicting national priorities

CONFLICTING NATIONAL PRIORITIES

Global issues such as nation-state sponsored cyberattacks, coordinated financial crime and fragmented cross-border data practices are increasingly harming global financial systems.

Overview



Globally significant events

International affairs are in a state of **disruptive transition and the global financial system remains exposed to systemically significant events.** Such events include, among others, protectionist economic policies, populism, cyber attacks, illicit finance and climate change.

Within this, the technology industry and financial system (which would benefit from greater cross-border collaboration) are often **challenged by conflicting national, political and economic interests.**



Technology-enabled risk

The transnational and borderless nature of digitally-enabled financial services means that nation states must work together to **safeguard critical infrastructure, businesses and people** despite financial and technology eminence rivalries.

Dangerous consequences of inaction are amplified by political rifts and conflicting investment priorities, as **state-sponsored cyberattacks grow in frequency, financial crime grows in severity and cross-border data flows are fragmented.**[137]



Fragmented efforts

Although such issues are widely recognized by most jurisdictions, recourse actions remain fragmented due to **multiple and conflicting national views.**

Variability is intensified where national interests, political agendas and perceived resource constraints are prioritized over broader goals to ensure the stability of the financial system. **While sometimes necessary given regional nuances, this dynamic poses significant risks to the system.**



Conflicting interests

Global incongruence is often due to the **dichotomy of rules that govern emerging risks and the lack of consensus on international norms** (e.g. cyber espionage for national security, prevention of illicit finance).

This challenge is further aggravated by determining which coordinated actions are **best for an individual nation's financial services and which that are best for the global economy.**[138]

Why is it important?



Prevention of global success

Incompatible national approaches to these complex global issues are **preventing the achievement of successful outcomes.**

Mutually beneficial coordination between nations should be sought. Without mechanisms to effectively regulate the dynamic between ecosystem actors with conflicting interests, **adverse consequences will continue to rise and threaten financial services.**[139]

PRIMARY SOURCES OF THIS RISK

- Rising geopolitical tensions
- Ineffective portability-related data protection
- Blurring jurisdictional boundaries
- Growing ecosystem interconnectivity and modularity

State-sponsored cyberattacks have the potential to discretely damage a nation's critical functions, resulting in cascading implications that include the erosion of consumer confidence.

Scenario example

A nation-state implements cyberattack tactics, introduces sanctions and promotes misinformation against another nation-state, causing unprecedented harm to the adversary's financial system.

What if…?

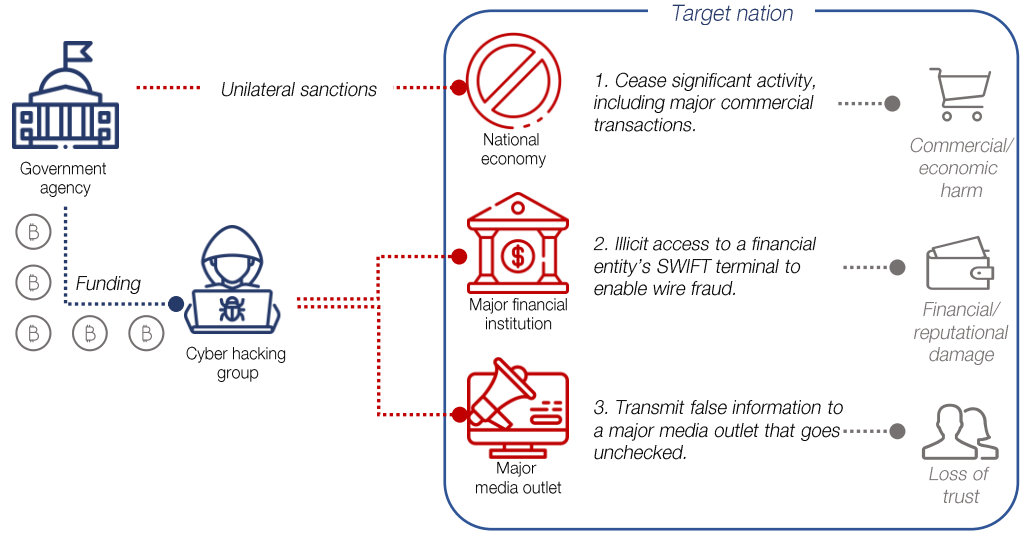
Poor relations between two economically robust nations manifest into severe geopolitical tensions. One nation state takes a brash and harmful approach against the other by issuing economic sanctions and discretely employing a cyber hacking group to wage digital warfare against its adversary's financial services system.[140]

Then this happens…

The relentless and coordinated attack on the target nation creates widespread implications. The group exploits vulnerabilities in bank systems, allowing them to gain control of credentials and initiate large-value outbound fund transfers. Furthermore, distributed denial of service (DDoS) techniques completely disrupt the functioning of critical market infrastructure. Financial transactions and financial market activity is halted; stock prices hosted on exchanges quickly plummet.

Scrutiny and cases of disinformation from major media outlets, fueled by the cyber hacking group, spurs controversy against the safety and soundness of the nation's financial institutions. Citizens view banks as untrustworthy, leading to a wave of deposit withdrawals. In combination, these factors cause a systemic financial crisis in the market with material impacts to the stability of the target jurisdiction's financial system moving forward.

Process flow *(illustrative)*[141]



A coordinated attack launched by a sophisticated nation with malicious intent would have implications that go well beyond monetary theft. An attack of this nature could create significant damage to the stability of, and trust within, the target nation's system.

Nation states are devoting significant time and resources to achieve technology-driven advancements, potentially at the expense of global coordination and coexistence.

What does this mean for the financial services ecosystem?



Competitive tendencies: Malicious activities to promote national competitive agendas such as offensive cyber techniques (e.g. espionage), sanction workarounds and cross-border payment barriers can be in pursuit of individual interests and at the expense of global progress. These competitive dynamics significantly hamper the financial system's ability to reap the benefits of globalization and technological innovation, which could ultimately help to mitigate globally systemic risks.[142]



Protectionist tendencies: The asymmetric exchange of insights and best practices can materialize across public sector policy mandates, defensive intellectual property measures or even the displacement of talent. For example, protectionist barriers and regulatory demand for data localization necessitated that most Big Techs create 'walled off' national subsidiaries.



Economics of change: Competition-linked incentives and interests (e.g. states rivalling for financial and technology eminence) of public and private sector entities to prevent or alleviate resulting risks are also creating uncertainties. Governments are, at times, in conflict with corporate decision-makers, who must choose between ambitious compliance commitments and their bottom lines.



Geopolitical stability and technology: Global financial stability can be a function of interdependence based on the economic and political relationships between nation states. If the fragmentation of global technological systems continues, new forms of confrontation between jurisdictions can hinder this stability. Developing functional mechanisms that allow national technological systems to talk to one another, despite technical, political or social differences, will be essential.[143]

CASE STUDY

AML policies differ by region, with over 40 regulators in Asia-Pacific alone. While $1.6 trillion is estimated to be laundered globally every year, less than 1% is intercepted due to varying data standards, lack of data sharing between institutions, and outdated global finance controls. Despite the Financial Action Task Force's guidance, there remains limited KYC/AML policy effectiveness, highlighting a need for a coordinated and centralized approach.[144]

Illicit finance activities pose a systemic risk to the ecosystem, agnostic of jurisdiction. The indicated AML policy fragmentation and magnitude of global money laundering highlights systemic implications. Imagine if policy fragmentation prevails as illicit financial activities rise, causing a systemic event…

What if the growth of foreign direct investment barriers, intellectual property protectionism and competitive imbalances between multiple nation states hinders multi-jurisdictional collaboration in tackling global financial crime?

Players are actively enhancing monitoring processes and legislative frameworks to both individually and collectively mitigate against the adverse effects of fragmented global action.

What are some key efforts that ecosystem players have undertaken to mitigate this risk?

Public sector players

- Monitoring geopolitical risks through active identification and horizon scanning processes to ensure they remain in line with designated risk tolerances.[145]
- Conducting a wave of investigations into suspected non-compliance with AML/CFT regulations and imposing sanctions requirements that result in financial penalties and license revocation.
- Establishing national financial intelligence units (FIU) that act as national centres of transaction analysis, which receive and analyze all reported suspicious transactions.
- Working diligently to prepare for, and curtail, state-sponsored cyberattacks by creating national standards and providing guidance to promote stronger cyber resilience.[146]

Multilateral efforts

- Standing up capacity-building think tanks to better understand and manage systemic implications to the industry caused by digital geopolitical risks.[147]
- Investigating and implementing new measures to improve financial crime detection and money laundering prevention through public-private sector cooperation (e.g. developing TM capabilities, launching joint-KYC utilities, creating public-private data-sharing initiatives).
- Introducing cooperative frameworks and legal measures to boost overall levels of cybersecurity by ensuring member states' preparedness, incident reporting and security measure implementation.[148]

Private sector players

- Monitoring the ongoing state of geopolitical tensions through risk dashboards that enable the analysis of geopolitical implications and market movement measures across significant risks.[149]
- Modernizing cross-border payments infrastructure to make use of rich data embedded in the ISO 20022 payment message format, unlock new insights on transactions, and automate KYC and AML activities.[150]
- Incumbents are mitigating against financial crime through robust customer due diligence (CDD) initiatives and TM processes, alongside crucial reporting mechanisms to national FIUs.

RELEVANT CASE STUDIES

enisa

The European Union's Network and Information Security Directive (NIS) is the first piece of EU-wide legislation on cybersecurity. The NIS is designed to protect an ever-growing list of critical infrastructure providers, online marketplaces and cloud services through preparedness and security measures.[151]

TMNL
Transactie Monitoring Nederland

Transaction Monitoring Nederland (TMNL) is a joint initiative of 5 Dutch banks. This collaboration led to the design of a central utility with multi-bank monitoring capabilities, increasing the effectiveness and efficiency of current TM and AML processes.[152]

BlackRock

The BlackRock Geopolitical Risk Dashboard is a private sector initiative that quantifies market attention and market movement related to risk events. The dashboard indicators are based on mentions in financial news stories and are enabled through NLP and ML capabilities alongside scenario assessment methodologies.[153]

Inconsistent and fragmented approaches will, however, continue to diminish global consensus and hamper financial stability.

What gaps exist in current mitigation efforts?

Public sector players

- In light of consumer and intellectual protectionism, data localization and data privacy rules in different markets make moving or sharing data across borders difficult and costly for all players.[154]
- AML procedures and controls implemented by regulators often emphasize technical compliance, leading to over-reporting, dilution of transaction insights and reactive measures against malicious activity.[155]
- Regulatory approaches to cybersecurity requirements in concentrated and highly integrated regions (e.g. APAC, EU) remain fragmented and detract from the security and resilience of financial networks against targeted state-sponsored attacks.[156]

Multilateral efforts

- Global data sharing approaches will only be effective when there is consistency in risk taxonomies and reasonable quality in underlying data. These are currently lagging and preventing enhanced data sharing.[157]
- Inconsistent application of global AML/CFT standards can lead to conflict between rules and arbitrage (e.g. legal loopholes) that can be exploited by financial criminals.[158]
- Appropriately attributing sophisticated cyber events, both legally and digitally, remains challenging as attackers adeptly protect their anonymity and deploy technology to shield the attack source.[159]

Private sector players

- Many private sector players fail to examine the broader strategic landscape (as it pertains to the intersection of technology and geopolitical tensions) that could directly or indirectly impact operations.
- While incumbents are modernizing AML/CFT mechanisms, the benefits of such initiatives remain minimal due to legacy systems and cost aversion motives (e.g. meeting the minimum bar for compliance).[160]
- Individual entities are unable to adequately monitor and defend themselves from sophisticated cyberattacks through existing threat intelligence systems (as indicated in Risk Topic 1).[161]

KEY MITIGATION UNCERTAINTIES

1 *Despite the growing importance and necessity of cross-border data flows, will the proliferation of global policies that restrict the movement of data across borders heighten jurisdictional conflicts between compliance and security efforts in the public sector?*

2 *As inherent geopolitical tensions rise (e.g. trade barriers), will heightened political pressures hamper multilateral and cross-border progress against systemic risks?*

3 *Can financial institutions operating in silos detect suspicious activities and meaningfully contribute to global AML/CFT efforts if a holistic picture of the customer(s) involved is unattainable?*

To lessen their direct exposure to harmful activities stemming from conflicting national interests, individual players can seek data-driven risk prevention mechanisms.

How can current mitigation efforts be improved? What more can be done by individual entities* to address this risk?

Risk prevention

- Embedded digital geostrategy: Players can integrate geopolitical risk assessments into their ongoing risk management and governance initiatives by layering additional external data (e.g. vendor and trade dependencies) onto their operational footprint to improve enterprise-level resilience and preparedness.[162]
- Analytics-focused data screening: Financial institutions can use analytics to detect anomalies and identify patterns indicative of illicit financial transactions in real time. Such capabilities can be enabled by investments in high-speed computing to process large volumes of data, coupled with dynamic alert triggers.[163]
- Payment systems modernization: Jurisdictions can contribute to global cross-border payment efficiencies by modernizing their core infrastructure for easier payment tracking and system reconciliation.
- Cyber detection neural networks: By extending existing security investments, players can engage cybersecurity players with AI and deep learning capabilities to prevent and detect sophisticated state-sponsored ransomware and cyberthreats at the pre-execution phase.[164]
- Data modernization to combat illicit finance: For financial institutions to increase their ability to more dynamically assess risks, access data, and deploy technology-based tools (i.e. ML and NLP), data can be re-platformed from legacy systems to increase data accessibility and enable real-time actions.[165]
- AML benchmarking exercises: Financial institutions can consider an independent benchmarking exercise, not only to assess strict compliance with AML/CFT and sanctions rules but also to optimize internal processes for the proactive identification of suspicious activity before requiring regulatory intervention.[165]

POTENTIAL UNINTENDED CONSEQUENCES

While large financial institutions can look to leverage analytics as a critical capability to prevent and detect malicious activity, silos between AML, data, cyber and fraud teams could undermine an accurate understanding of enterprise-wide risk exposure and drive redundant actions.[166]

While these entity-level actions could all prevent the impact and occurrence of geopolitically-driven risk events, these risks cannot be adequately combatted by individual players. Public and private sector players should be cautious of over-investing in short-term individual actions, as they could detract from resource allocations and investments made in more impactful, collaborative efforts.

*Note: Individual nation states are considered to be individual entities.

Although individual mitigation efforts provide some degree of effectiveness, coordinated investment into utility mechanisms and collective governance is required to address digital geopolitical risks.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Cross-border data sharing agreements: Bilateral agreements can be established between jurisdictions for digital trade data portability, enabled by interoperable APIs. Such agreements should explicitly recognize the possibility of alternative models (such as federated learning models and data trusts) that can also fulfil the spirit of cross-border data flows (similar to the data provisions within the recent UK-Japan and UK-Switzerland trade deals).[167]
- Blockchain-enabled cross-border data sharing: Financial institutions and regulators can partner to co-create (or delegate a third-party entity) and establish a secure, objective decentralized database with tokenized data sharing (e.g. personal, transactional) that can aid in risk identification (e.g. cybercrime, fraud, illicit finance).[168]
- Joint TM utility: Financial institutions can develop an objective TM capability, housed in a centralized utility that pools critical transaction data, to better monitor and detect illicit finance threats and issue risk-based alerts (similar to TMNL).[169]
- Private sector-led cybersecurity standards: In the absence of formal regulatory guidance, private sector players can develop technical standards to ensure minimum cyber and data protections are in place for collective resilience.[170]
- Cyber threat hunting and attribution: Financial institutions with digital relationships (e.g. through partnerships or shared third-party vendors) can partner to co-develop a proactive threat-hunting and attribution utility that monitors the connected attack surface of these entities and pools anonymized data for organizations to spot and attribute threats that are attempting to/have already infiltrated their network.[171]

Risk resolution

- Flexible data standards: Governments can incentivize players to adopt technical standards for data without prescribing a single, specific standard. Such actions can improve the consistency and interoperability of data, while also enhancing access to tools and solutions that enable their internal workforce to utilize it more efficiently and effectively.[172]
- Cross-border AML authority: To enhance cooperation across jurisdictional FIUs, a global AML authority can be stood up on behalf of national authorities, integrating supervisory methods and ensuring that the financial sector correctly and consistently applies AML standards (similar to the EU AML Authority).[173]
- Linked payments systems: To improve the current state of disparate, nation-based risk management frameworks and compliance checks related to AML, global instant payment systems (gIPS) operating on a common messaging standard can enable secure transactions with real-time monitoring capabilities (e.g. through the Bank for International Settlements' Nexus Gateway blueprint).[174]

POTENTIAL UNINTENDED CONSEQUENCES



While many nation states already collaborate to safeguard the security of the financial system against many critical geopolitical risks, select countries that permit illicit activities are generally less willing to participate in these coordinated activities. If a group of nations establishes global standards, this progress may inadvertently increase tensions and the advent of related attacks.

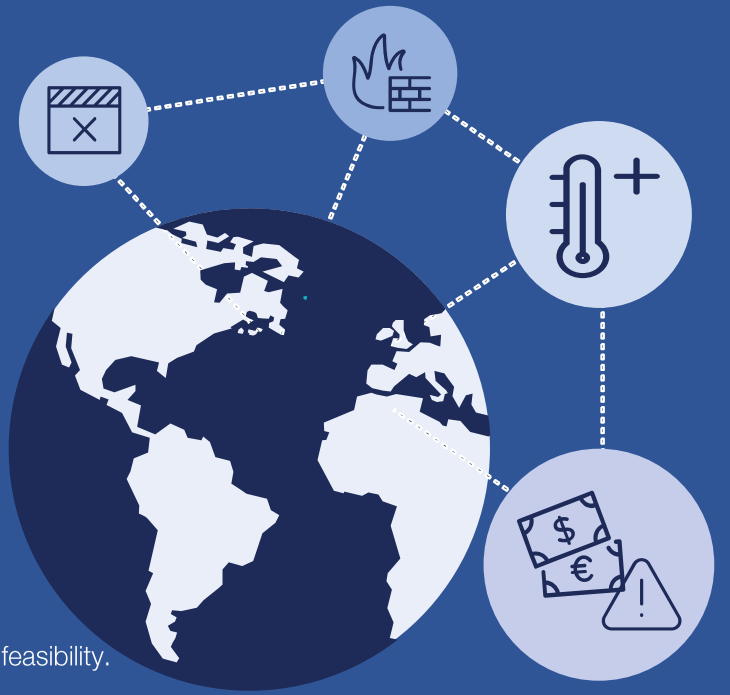


While cybersecurity charters are meant to regulate the cyber conduct of an industry, they could create a false sense of security if they remain very limited in scope and lack a use case-based approach beyond the industry, resulting in gaps for threats posed by the broader economy.



While an interoperable gIPS could facilitate more rapid, accessible and secure cross-border transactions, there may be an increased cybersecurity risk associated with using a critical, centralized cross-border payment system.

Key mitigation applications



Note: The mitigation applications highlighted in the following slides are intended to be considerations and have not been assessed for viability or feasibility.

Table stakes: Global jurisdictions can look to instate a network of financial 'data authorities', enabled by blockchain solutions, to facilitate the secure cross-border transfer of data.

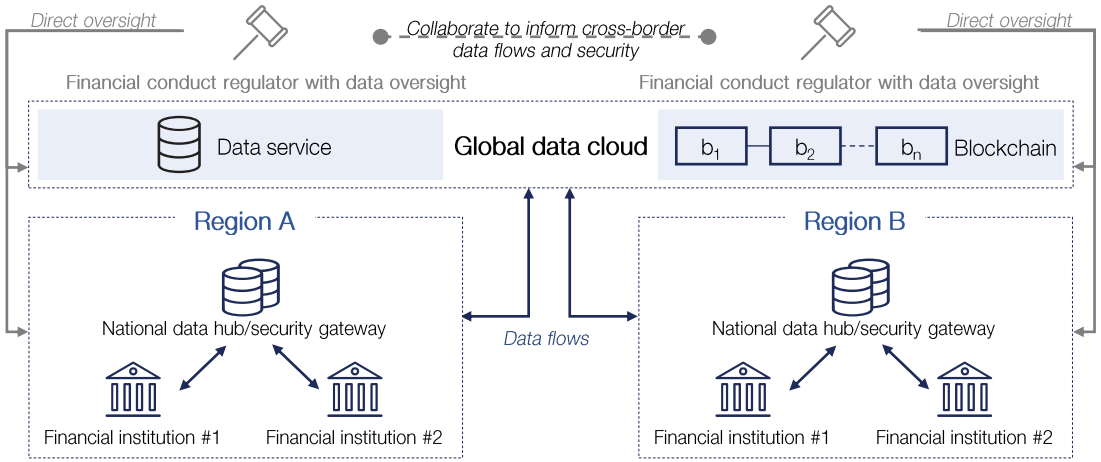
Overview

Cross-border data flows (i.e. transactions, PII) are key enablers for any nation that critically depends on the global trade of capital. Despite their ever-growing importance, there has been a recent proliferation of policies that restrict the free flow of data across borders.

While a network of national data protection authorities with cross-sectoral oversight exists, it typically only has jurisdiction over personal data. Governments can look to bolster the responsibility of existing conduct-oriented or activity-based regulators and empower them with oversight of all inbound and outbound cross-border financial data flows.[175]

Once the necessary appointments are made, technology-based solutions can be explored to enable the optimization of cross-border data flows. Blockchain can tokenize this data to enable its transparent and efficient ownership, portability, and usage to ensure that valuable global data can be properly utilized to solve complex global risks.[176]

How it works



By empowering financial regulators with the power to **oversee cross-border data flows**, global digital interoperability can be pursued through blockchain solutions.

Use in financial services



- By empowering financial supervisors to mandate the safe and efficient flow of cross-border data that pertains to the financial system, purpose-fit rules and legislation can be created to fit the unique data needs of the financial system.
- Once the financial sector is empowered with such oversight at the local level, a clear cooperation mechanism between international authorities should be established to enhance trust.
- Blockchain is one potential solution, where a high level of security is offered within data flows while smart contracts can hard-code agreements between global jurisdictions.[177]
- For more information on a potential cross-border policy roadmap for public sector actors, please visit the Forum's recent white paper on *A Roadmap for Cross-Border Data Flows.*

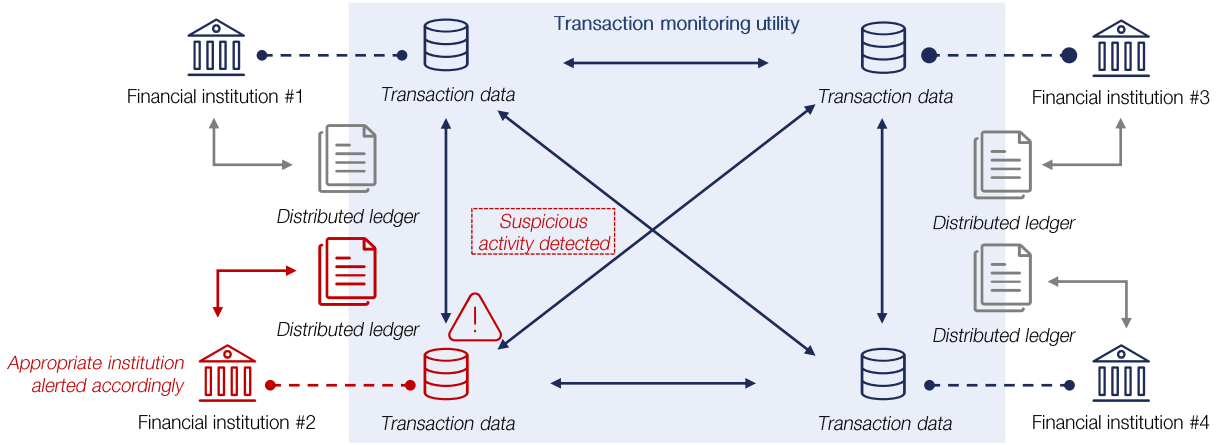
Emerging: A decentralized transaction monitoring (TM) utility can improve collaboration and information sharing between entities to effectively and efficiently combat money laundering.

Overview

Financial crime prevention efforts have been largely led by national and international bodies. Despite the direction of AML, and terrorist financing efforts being set at the public sector level, private sector financial institutions have become increasingly challenged by costly compliance expectations to screen for, monitor and report suspicious activity. This dilemma becomes increasingly challenging when a financial institution operates multi-nationally and must contend with varying regulations and requirements across the jurisdictions in which it operates.

There is an opportunity for public and private sector bodies to collaborate within and across jurisdictions to respond to the risk. A cooperative, technology-driven TM approach would provide an industry-level view of financial activities to better detect complex relationships and transactional patterns, and improve how players signal, monitor and detect illicit activities. Multiple players can share their TM data through a utility that monitors aggregated data to better detect behavioural patterns across traditional institutional silos, providing alerts to the designated financial institution(s) when a suspicious event is detected.[178]

How it works



An integrated and streamlined approach to TM will better **prevent and detect fraud and money laundering** across players and, potentially, jurisdictions.

Use in financial services

Monitor — Avoid — Assume — Control

- While there are instances of successful centralized utilities (e.g. TMNL) with a single controlling entity, a decentralized model would ensure the sharing of ownership and resources, with transactional data and monitoring responsibilities remaining impartial.[178]
- DLT could play a meaningful role as an alternative facilitator, giving financial institutions a trusted, up-to-date record of suspicious transactions rather than relying on disparate databases.[179]
- While DLT is decentralized, its corporate organization may not be decentralized, enabling the flexibility to collectively stand up a fit-for-purpose entity to monitor transactions. Alternatively, a blockchain solution can be deployed where the organization is also distributed.[179]

Novel: A designated, multilateral cyberthreat hunting and attribution (CTHA) utility can enable public and private sector players to better monitor and attribute cyberattacks across the ecosystem.

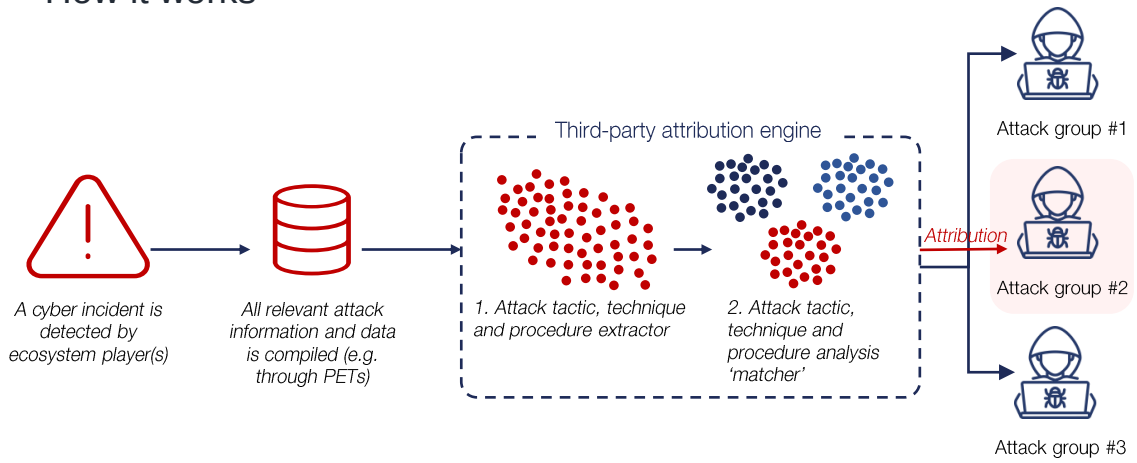
Overview

In recent years, certain nation states have become increasingly bold in their use of cyber tactics to target and attack adversaries. One of the most prominent ways to deter state-sponsored cyberattacks is through attribution, however, upwards of 30% of cyberattacks observed between 2010-2020 were of uncertain or unattributable origin.[180]

Given the increasing sophistication and impact of state-sponsored cyberattacks, the industry has a meaningful role to play in the attribution of these events. As state-sponsored hacking groups typically follow a set of tactics, techniques, and procedures, players in the industry can amalgamate data from incumbents and their key service providers (e.g. Big Techs) to inform a multilateral utility.

Whenever a cyberattack is detected, ecosystem players can pool relevant data (e.g. through PETs) into the CTHA utility where ML techniques will routinely be assessed, and attacks can be attributed to specific criminal groups (e.g. by gaining context on historic behaviour). The private sector will be better equipped to inform governments with critical attack insights, and insights from the attribution engine will enable players to better understand and respond, bolstering the overarching cybersecurity of the ecosystem.[180]

How it works



A shared CTHA utility would enable the **unbiased** attribution of cyberthreats, benefiting all participating private and public sector players with system-wide cybersecurity.[181]

Use in financial services



- The average time for an individual player or regulator to detect a cyberattack and respond to sophisticated state-sponsored threats is often too long given the intensity of siloed investigation and the necessity of reverse-engineering the attack.
- By consolidating efforts across the private and public sector, the ecosystem will be better equipped to attribute attacks, not only accelerating the time taken to respond, but also lessening the financial and reputational impact of the attack on impacted players.
- Through this utility, global cybersecurity bodies could seek to strengthen their existing network of national or industrial cybersecurity groups with the ultimate goal of reaching full global cooperation around state-sponsored cyberattack attribution.



1 2 3 4 5 6

Emerging sources of influence

New sources of influence are using social media platforms to drive activities and behaviours that pose risks to consumer protection and market stability.

Overview



Democratized market access

Digital offerings have played a key role in democratizing financial services, providing retail consumers with **entry to domains that have traditionally been exclusive to sophisticated or institutional market participants** (e.g. investing, trading, information sharing).

This dynamic has also increased access to participants without requiring agency supervision (e.g. licensed advisories) and niche expertise (e.g, fundamental analysis) in retail financial activities.[182]



Coordination of activity

As a result, there has been an uptake in emerging digital sources of influence (e.g. social media platforms such as Reddit) that enable the broad **evaluation, distribution and coordination of financial activities.**[183]

Public financial information sharing is a key prerequisite of sound market access and participation, which was once only conducted within accredited institutions, or through investors and media outlets (e.g. Reuters).



Influential sources of harm

Conversely, **misinformation can easily spread through digital channels and reach countless users without impartial checks and balances.** Certain individual actors and malicious programs (e.g. social bots) can influence public sentiment and behaviour to create stock-buying and -selling frenzies.[184]

Such growing opportunities for market manipulation could result in **financial or reputational harm to market participants and erode public trust in financial services.**[185]



Channels of coordination

Low-cost digital financial platforms and brokerages (e.g. Robinhood, eToro, Futu, Coinbase) **have made retail financial participation relatively frictionless.** There are also digital tools that exist at the intersection of social media and finance (e.g. automated trading algorithms, alternative data platforms, screen scrapers).[186]

In combination with **non-traditional sources of influence, platforms can amplify the effects of risky investor behaviour.**

Why is it important?



Challenged protection

Whether malicious or not, emerging sources of influence are driving imprudent actions that can **put participants' financial wellbeing at risk** (e.g. digital-natives conducting margin trading) and **potentially strain the operations of certain existing market mechanisms** (e.g. brokers, clearing houses).

This change in dynamics can result in **unprecedented market volatility, coupled with the potential loss of money and trust for many across financial markets.**

PRIMARY SOURCES OF THIS RISK

- Dissemination of verbose and false information
- Undefined regulatory oversight for new entities/business models
- Growing social inequities and fragmentation
- New and emerging drivers of market movement

Given the proliferation of digital offerings in financial services, a variety of new sources and channels of influence have emerged as the drivers of change within the ecosystem.



Social media platforms

Major social media platforms (e.g. Instagram, Youtube, Twitter, TikTok) facilitate the sharing of ideas, thoughts and information through virtual networks. These platforms serve as vehicles for effective and expansive coordination and are vulnerable to the spread of misinformation among the masses that influence perceptions of, and interactions with, the financial system.[187]



Influential individuals

The financial opinions and investment decisions of prominent individuals within the ecosystem have always been closely followed (e.g. Warren Buffet). However, today's influential individuals are enabled by large followings on social media channels, where digital 'endorsements' influence almost immediate financial market movements (e.g. Elon Musk's tweets about certain crypto assets).



Web-based forums and communities

Online forums (e.g. Reddit) facilitate open online communication, within which specific communities (e.g. wallstreetbets) bring together groups of people with shared interests. Prominent message boards that facilitate finance-oriented discussions can become the epicentre for crowdsourced, high-risk market speculation and analysis.[187]



Private messaging platforms

Apps that host live, and often locked, chatrooms (e.g. Telegram, Discord, Clubhouse) are dedicated to exchanging information regarding specific finance-oriented topics. These platforms are drawing users looking for real-time conversations with other participants and are enabling users to share knowledge and seek investment advice within their closed digital forums.[188]

CHANNELS OF INFLUENCE

While each of these sources of influence impact consumer, institutional and market sentiment in a variety of ways across the ecosystem, there are three primary channels of financial activity that are majorly influenced by a combination of these sources:

1. Online investment decisions: Enabled by the advent of digital retail investment brokerage firms and platforms, consumers can more easily and directly make investing decisions through seamless digital applications and platforms.

2. Financial market dynamics: While influenced by crowdsourced investment decisions, dis- and misinformation can impact the sound functioning of markets.

3. DeFi Applications: New digital tools, marketplaces and asset classes (e.g. cryptocurrencies) within DeFi are predicated on the influence of decentralized sources.

There are limited financial incentives for platforms to prevent misinformation and this can result in market manipulation, causing significant financial harm and concerns around market stability.

Scenario example

Rogue actors deliberately spread false information, coercing consumers' financial buying decisions and, ultimately, driving the widespread loss of public trust in financial services and markets.

What if…?

A group of anonymous actors spreads false and misleading claims about a looming financial crisis through a sophisticated misinformation campaign on social media platforms and online forums.

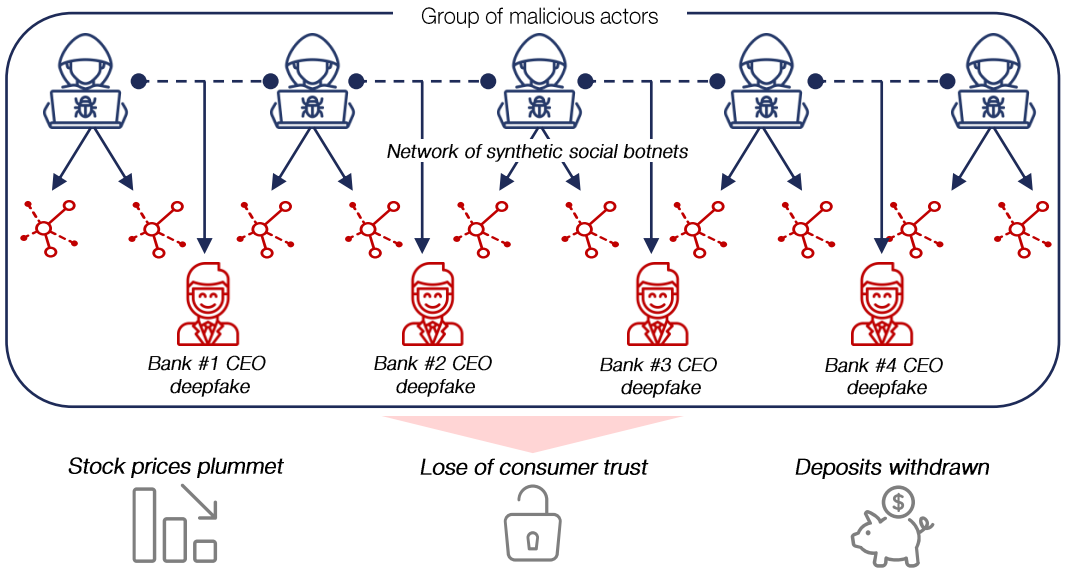
The group deploys many synthetic social botnets (i.e. fake social media accounts made from AI-generated photographs and text) to spread false information on the state of the economy and deepfake videos of bank CEOs acknowledging a financial crisis. These synthetic social bots have operated with minimal supervision for years to build credibility and clout on social platforms.[189]

Then this happens…

When combined, these tactics persuade large groups of retail investors to sell their stock holdings, triggering a widespread sell-off. This sophisticated misinformation campaign generates quick profits for the bad actors (i.e. 'short and distort').

Public trust across the financial market deteriorates. This doubt is further amplified as it becomes more difficult to distinguish false sentiment from the truth across social media platforms, and widespread consumer panic and other financial runs ensue.

Process flow *(illustrative)*



If incumbents and regulators, alongside social media providers, are unable to prevent the proliferation of false information that impacts markets, certain actors will continue to take advantage of misinformation sharing to the detriment of consumer wellbeing and market stability, as seen in the global political sphere to-date.

Emerging sources of influence can manifest into instances of market manipulation and scams that are transposed to the broader financial system.

What does this mean for the financial services ecosystem?



The potential for consumer harm is increasing: Emerging sources of influence have created a new source of information asymmetry. Currently, there are limited mechanisms to disclose or prevent the dissemination of false or misleading information and consumers may have a limited understanding of the underlying risks of participation. When combined, these factors lead to uninformed consumer decision-making with potential financial consequences.[190]



Institutions are caught in the crossfire: The advent of social media-fueled retail investing presents a fundamental change to market dynamics, which has impacted both large and small traders, brokerage firms and clearing houses. Traditional market infrastructure and institutional operations may not be adequately prepared to manage unprecedented high-volume, high-margin and large derivative trading. Such trading activity can result in financial, reputational or operational risks for players.[191]



Resulting systemic implications: The risks created by increased access and misinformation, coupled with lagging protection mechanisms (e.g. margin requirements, circuit breakers), can impair critical activities within the financial system. The resulting impacts can be of systemic proportions, where the stability of financial markets is harmed by widespread market manipulation and/or the erosion of public confidence.[192]



Rethinking protection mechanisms: As mass participation in financial markets continues to grow, greater end-to-end visibility and balanced considerations for responsible access (e.g. consumer education vs. open inclusion) must be explored by private and public sector players to protect all participants within the system, alongside the functioning of the system itself. Inadequate oversight of emerging sources of influence leaves the system exposed to manipulation and negative influence.

CASE STUDY

In May 2021, the Securities and Exchange Commission (SEC) sued key promoters of 'BitConnect', a cryptocurrency Ponzi scheme that promised outsized returns through YouTube testimonials. The project raised over $2 billion from retail investors before the cryptocurrency lost its value in 2018. Events like BitConnect highlight the necessity for greater regulation and scrutiny on new tech-enabled products and sources of influence to ensure consumers are adequately protected moving forward.[193]

The limitations of current consumer protection mechanisms can be exacerbated where information gaps exist (e.g. limited financial literacy, false information). While this event had systemic implications, imagine if a similar event occurred with a greater magnitude of impact…

What if misleading information about a cryptocurrency spreads and millions of consumers blindly purchase it, days before a 'rug pull' that creates a panic sell-off?

Both the protectors and enablers of financial access have a role to play in safeguarding the system against emerging sources of influence.

What are some key efforts that ecosystem players have undertaken to mitigate this risk?

Public sector players

- Issuing enforcement actions to online retail brokerages that are found to be misleading customers or approving ineligible traders for risky strategies (e.g. failing to exercise due diligence on consumer suitability).[194]
- Exploring the ability to enforce social media safeguarding mechanisms, where platforms could be mandated to moderate online financial market-related postings with flags or warning messages.[195]
- Creating policies and tools to counter online falsehood and protect consumers from internet-based manipulation, including ensuring that internet and digital advertising intermediaries have adequate systems in place to prevent and counter the misuse of online accounts by malicious actors.[196]

Multilateral efforts

- Securities market regulators are suspending the trading of stocks where their prices have been identified as driven by 'suspect social media activity', based on the recommendations of exchanges.[197]
- Regulators are soliciting public feedback regarding the digital engagement practices employed by retail investment platforms (e.g. investment gamification) that influence investment decisions.[198]
- Driven by supervisory pressures, Big Tech and social media platform providers are amending internal policies to ensure only financial services that are verified by conduct regulators can be advertised.[199]

Private sector players

- Offering comprehensive 'education' libraries on retail investment platforms, where consumers can access a variety of informative tools (e.g. financial market guides, blogs, podcasts, tutorials) to help narrow the knowledge gap between institutional/accredited and retail investors.[200]
- Monitoring and mining opinion data from social media platforms to deliver insights based on aggregated sentiment analysis for more effective, real-time trading surveillance.[201]
- Building algorithms to screen scrape or scan discussions on prominent social media platforms, online forums and online brokerage platforms for effective market sentiment analysis.

RELEVANT CASE STUDIES

FINRA

In June 2021, the US Financial Industry Regulatory Authority (FINRA) issued Robinhood Financial LLC a $57 million fine and handed out $12.6 million in compensation to harmed investors. The regulatory allegations against the online brokerage included account opening and trading strategy automation issues and customer misinformation.[202]

Google Ads FCA FINANCIAL CONDUCT AUTHORITY

In August 2021, Google updated its UK Financial Products and Services advertising policy so that purveyors of online financial scams transmitted through ad networks will now be blocked. This change follows collaborative anti-scam campaigns and screening warnings from the UK's FCA.[203]

Nasdaq

Nasdaq's US market surveillance team deployed StockPulse, an investment news aggregator, to incorporate social media analytics into their surveillance system and develop processes tailored for exchange trading that can detect potential market manipulation (e.g. spam, bots) across social media platforms.[204]

However, the definition of consumer protection and modernized institutional and infrastructural requirements have yet to be fully reinterpreted in today's digital and social context.

What gaps exist in current mitigation efforts?

Public sector players

- Regulatory bodies have been slow to create effective social media safeguarding approaches in financial markets, where clear rules of engagement and conduct for social media have yet to be articulated. [205]
- The attribution of 'flash crashes', where US regulators can pinpoint the buying and selling of securities to better monitor automated trading, is enabled by the Consolidated Audit Trail and has not been adapted to fit current market dynamics.[205]
- While authorities can intervene in insider trading and market manipulation incidents, oversight mechanisms are unclear as these activities pertain to the free, but coordinated, sharing of individual opinions on a specific stock.[205]

Multilateral efforts

- A lack of comprehensive training and education from public and private sector players mean that consumers may not understand the underlying risks of receiving unregulated financial advice.[206]
- Identifying and removing malicious actors and posts on social media channels is a difficult and fraught task, even when players have access to large data sets and sophisticated AI activity-tracking algorithms.[207]
- Conflicting multilateral interests (e.g. public vs. private) are preventing an effective system-wide balance between consumer protection through regulation and free market access.[208]

Private sector players

- Certain social media platforms and communities promote risky trading activity without fully disclosing potential downsides and the validity of information (e.g. Twitter has no explicit policy banning misinformation on stocks).[209]
- If retail investing platforms, brokerages and clearing houses continue to face unprecedented trading volume caused by sentiment-driven activity, this may place an increasing strain on market infrastructure.[210]

KEY MITIGATION UNCERTAINTIES

1 *Can the bounds of financial market oversight extend to cover these adjacent activities that impact other industries in varying ways (e.g. false information transmitted through social media platforms)?* [211]

2 *As many regulators and private sector players prioritize objectives differently (e.g. consumer protection, pursuit of profit), how will misalignments prevent clear opportunities for mutual understanding and multilateral mitigation?* [211]

3 *Do existing, misaligned financial incentives (e.g. how some online brokerages generate revenue through payment for order flow) have the potential to drive riskier investor trading decisions and harm consumers?* [212]

To safeguard the system from the risks posed by prevalent and emerging sources of influence, players can explore technology-based consumer and market protection policies, tools and mechanisms.

How can current mitigation efforts be improved? What more can be done by individual entities to address this risk?

Risk prevention

- Identity verification requirements: Social media platforms or specific online communities (e.g. wallstreetbets) can require participants to provide identity verification to easily attribute orchestrated or mass-scale misinformation campaigns by bad actors.[213]
- Digital disclosure adaptations: To alleviate information asymmetries posed by digital channels that host discussions on financial market activity, regulators can look to mandate consistent disclosure formats that ensure transparent information flows.[214]
- Social media moderation: Social media platforms can be mandated to moderate online postings by flagging financial recommendations, opinions and investing tips from individuals and influencers as 'unverified claims' to prevent retail investors from making uninformed decisions.[215]
- Mandated retail investor training: Retail investing platforms can be mandated to require all individuals to complete an online training and education programme before approving riskier trading activities (e.g. leveraged stock options trading).

Risk intervention

- Stock market mediation: While markets are currently tasked with monitoring for 'suspicious activities' and issuing warnings to investors, incumbents and brokerages can temporarily halt highly-leveraged retail stock purchasing frenzies.[216]
- Algorithm-driven detection: Retail investing platforms or exchanges can augment existing social media trade surveillance algorithms with big data and ML capabilities to detect misinformation and proactively uncover potential 'pump and dump' schemes.[217]

Risk resolution

- Index volatile 'meme' stocks: To avoid imposing risk to mainstream indices (e.g. a stock being added to the S&P 500 index) and to address emerging consumer demand, high-performing stocks that are attributed to speculation from consumer sentiment can be separately indexed, enabling benchmarks and exposures against a high-risk fund.[218]
- Prescriptive platform policies: Big Techs and social media platforms can consider taking a more proactive approach prior to regulatory intervention by implementing explicit policies that ban market manipulation, based on mutually developed criteria with regulators.

POTENTIAL UNINTENDED CONSEQUENCES



While more active social media moderation from platforms could be a very useful tool to curb the distribution of false or misleading information, questions regarding free speech have already emerged. These views are likely to build momentum as not all social media accounts violate platform policies. Moderation algorithms would need to be designed so that consumers are adequately protected and informed, but the information being shared is not strictly 'policed'.



While there are compelling arguments that call for financial markets to enhance their oversight and more closely monitor entities to actively protect consumers beyond the issuance of warnings, markets may not have the resource capacity or technical capabilities to intervene in significantly volatile events. Market participants could operate with a false sense of confidence regarding the actual safeguarding of markets.

Only through multilateral efforts can adequate consumer, institutional and systemic protection be achieved amidst the growing influence of new sources and channels of influence.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Refreshed financial regulatory frameworks: Regulators and policy-makers can reassess existing consumer protection mechanisms and consider new guardrails for retail trading activities (e.g. aligning financial incentives for retail platforms with consumer protection outcomes). This would likely require the monitoring of retail trade forums to better understand the nature and extent to which they influence market activity.[219]
- Coordinated consumer education platform: Regulators and financial institutions in jurisdictions can look to create a cross-border education platform that crowdsources course creation to include relevant and topical resources around investing and risk.[219]

Risk intervention

- Augmented social media monitoring: Players can look to use advanced ML models and NLP to scan social media comments in real time and relay findings on market sentiment to their customers before significant price volatility occurs.
- Multilateral financial market alert system: Big Techs and regulators can collaborate to develop an advanced false information detection system with a shared live feed, which can be leveraged for the identification of 'red flag events' and broader market warnings.
- Social media risk reporting: Akin to the current process of AML incident reporting, regulators can consider mandating social media platforms to automatically report any material cases of false information that could generate market volatility.

Risk resolution

- Consequence management strategy: Regulators and social media platform operators (e.g. Big Techs) can collaborate to develop a consequence management strategy that introduces greater financial punishments for the deliberate or malicious spread of false information deemed to drastically influence asset price volatility and market movements.

POTENTIAL UNINTENDED CONSEQUENCES

Beyond free speech, limitations on investment and trading activity may present new accessibility issues. The Reddit-driven stock buying frenzy in January 2021 saw certain brokers restrict transactions on implicated stocks and raise margin requirements. While these investing platforms attributed their decisions to volatility and regulatory capital requirements, retail investors may have been subject to asymmetric, and potentially undue, disadvantages compared to institutional investors.[220]

Intelligent social media monitoring can be a useful tool to preemptively foresee significant stock price volatility events. While this can limit the full level of impact that market manipulation could have on consumers, financial institutions and markets, it can also create another signal for insider trading and lead to sentiment manipulation due to information asymmetries.

Key mitigation applications



Note: The mitigation applications highlighted in the following slides are intended to be considerations and have not been assessed for viability or feasibility.

Table stakes: Algorithm-driven monitoring of social media comments can help private sector players to understand market sentiment and anticipate significant movements.

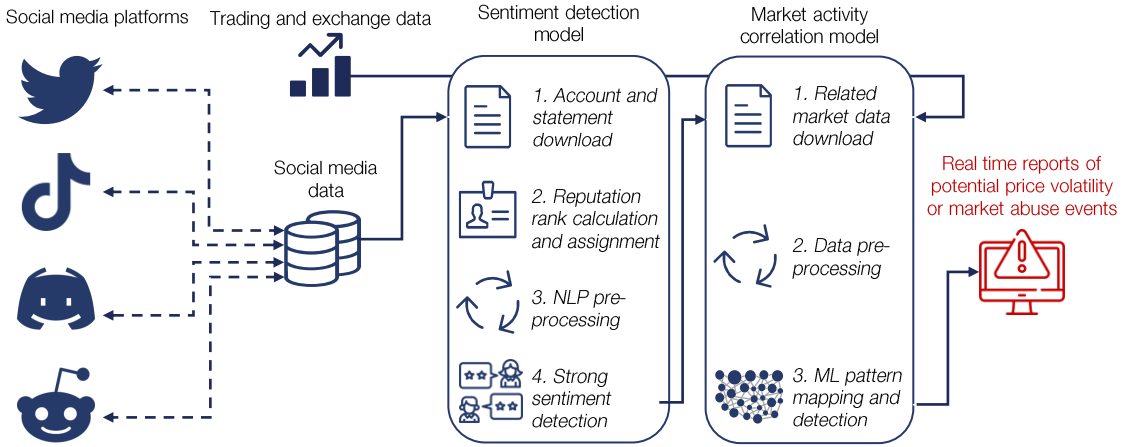
Overview

Information disseminated through social media channels is expected to continue playing a significant role in influencing financial market activities. To prevent instances of market manipulation, social media platforms and digital brokerage firms can co-develop a sentiment detection model that leverages ML and NLP capabilities.

Social media data (e.g. online discussion posts) can be captured through screen scraping technology and mapped to emerging market activity (e.g. anomalies, preemptive patterns of buying or selling frenzies). NLP capabilities are useful in deconstructing messages based on key words (e.g. stock names, actions) that would indicate a potential market movement.

This provides financial players with the ability to forecast material changes in stock price and identify instances of manipulation; such findings can be shared with end-users (e.g. retail consumers, institutions) to better inform risk-reward decisions. Coupled with the appropriate regulatory safeguards, this can support efficient market participation.[221]

How it works



Sophisticated social media monitoring algorithms can detect social media **sentiment and patterns** to proactively forecast market volatility and potential manipulation.[222]

Use in financial services



- The model can be used to closely analyze financial accounts and online communities, including relationships between users (e.g. influential individuals and their follower networks) to calculate a ‘reputation rank’.
- Flagged posts and accounts (i.e. investor sentiments) are then mapped to stock market and trading data, where the ML algorithm detects potential market activity patterns or anomalies that could indicate market manipulation.[223]
- While this application cannot prevent instances of market manipulation, it provides diverse data points for private sector players to account for in their decision-making processes and models.

Emerging: Financial players can crowdsource resources through a digital education platform that helps to reduce the risk-taking knowledge gap among retail investors.

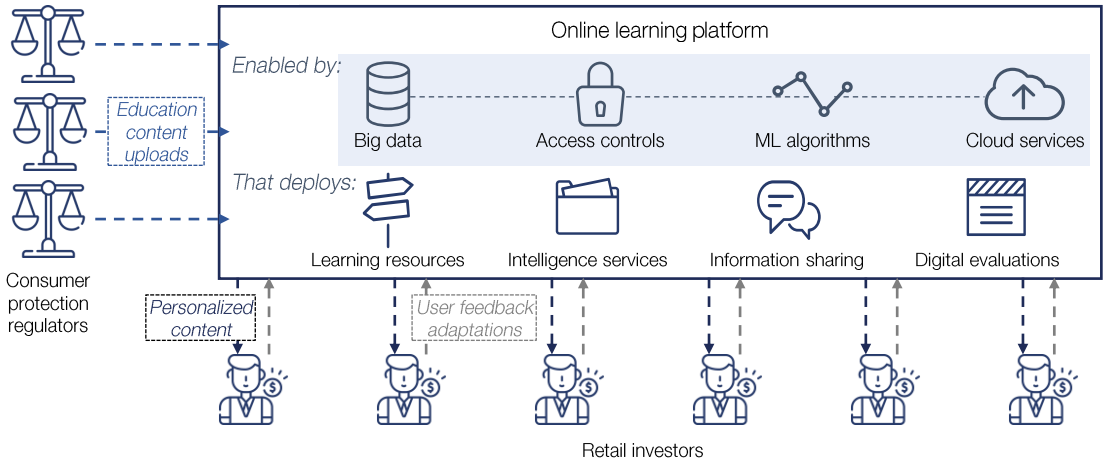
Overview

More than ever, consumers must understand risk-reward decisions, fee-based pricing, the impact of false information, and other key investing concepts that are fundamental to safeguarding their participation in financial markets.

Regulators can explore the opportunity to create a cloud-based digital education platform, augmented by big data, access controls and ML algorithms to ensure secure and personalized consumer access. Through on-demand availability and curated learning paths, retail investors will have access to a tailored platform with relevant and meaningful content based on their existing financial knowledge level and risk appetite.[224]

Regulators can explore supplementary legislation to mandate that any user of a digital brokerage platform must create an account and complete certain learning modules to engage in more complex or risky financial activities. By combining educational tools and policy measures that align with how retail investors are consuming content and participating in financial markets today, investors will be more empowered to navigate financial markets.[225]

How it works



An innovative and engaging investor education platform can support the **effective delivery of financial education** to inform consumers of potential harm.[226]

Use in financial services



- Educational tools and content can be tailored to each investor based on their existing knowledge base, performance on digital evaluations, and appetite for engaging with novel or volatile asset classes.
- Consumer protection authorities and related regulators across jurisdictions can solicit regulatory best practices while crowdsourcing educational content.
- Data and feedback attained from such a platform can equip regulators with insights on a population's financial literacy and support the mitigation of adjacent issues such as financial exclusion.

Novel: By establishing a multilateral alert system, public and private sector players can collaborate to detect false information and diminish information asymmetry.

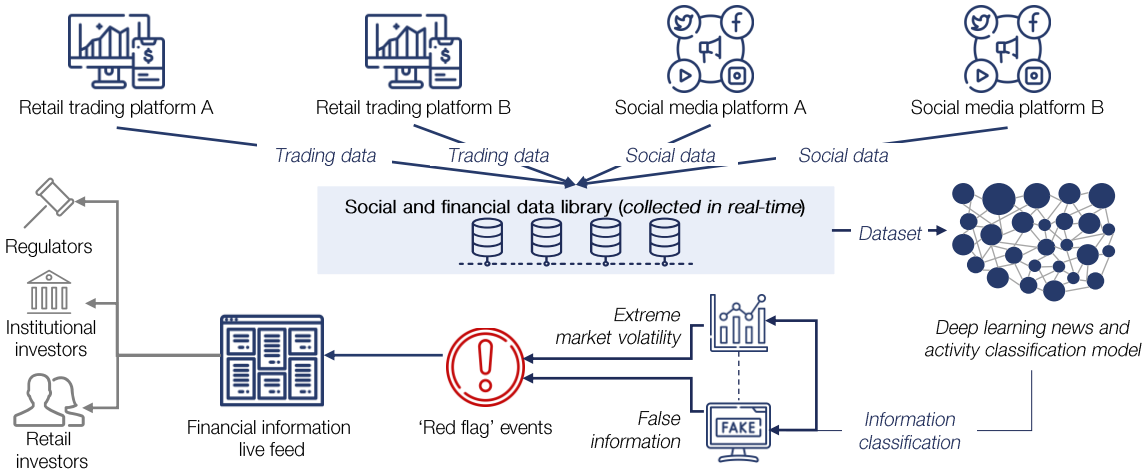
Overview

Detecting false or misleading information on social media which is directly followed by material stock price changes is an increasingly important objective in trading surveillance and investment due diligence.

The automated detection of misinformation remains difficult as it requires highly advanced models to demystify information based on what is deemed 'true' and 'false', especially as misinformation grows in complexity. This challenge is further exacerbated by the locus of responsibility being spread beyond the financial services domain (i.e. social media platforms collect data sets and regulators penalize misuse).[227]

Players can begin to explore deep learning techniques that can lead to the development of an advanced false-information detection system (e.g. to determine whether information is truthful or misleading). These insights can support the identification and sharing of 'red flag events', or market warnings grounded upon false information and made accessible through a live feed. [228]

How it works



Deep learning techniques are robust and well equipped to deal with **complex interaction patterns** between social networks and financial markets.

Use in financial services

Monitor — **Avoid** — Assume — **Control**

- Social media platforms can use insights derived from the system to halt the dissemination of false information throughout their networks, whereas regulators and investing platforms are better equipped to halt trading activities connected to market manipulation.[228]
- Both retail and institutional investors' investment decisions can also be better informed if model outputs are disclosed through a public live feed.
- This solution requires significant coordination between the financial sector and broader economy; Big Techs and financial brokerage firms would need to securely pool data to generate a clear, real-time picture of social media and financial market activities.



1 2 3 4 5 6

New drivers of financial exclusion

While technology has been instrumental in reducing the global financial inclusion gap, it has also created new areas of exclusion that must be addressed to ensure a well-functioning financial system.

Overview



Impetus for inclusion

Globally, an estimated **1.7 billion people remain unbanked**[229] and still more lack access to affordable financial services, which provide greater wellbeing; inclusion of these groups is a key building block for poverty reduction and a facilitator of economic development.

Financial inclusion is not just a public sector issue; incumbents and FinTechs alike can discover vast and largely untouched markets to accelerate economic growth.



Inaccessibility barriers

Financial inclusion is on the rise globally, accelerated by mobile phones and the internet, but **access remains uneven across nations.**[230]

Technology-driven inaccessibility takes many forms. For example, digital shifts have led to bank branch closures which disproportionately impact **older, remote, and disabled populations. Gender gaps** have also emerged, with women having lower access to financial accounts than men.



Biases and automation

Despite enhancements to algorithms to remove human subjectivity, **discriminatory biases** in product decision-making remain a point of industry-wide scrutiny.

Highly automated business functions fall under similar inspection, as **standardization is giving rise to unsuitable products.** While this may not be intentionally predatory, cases of overlending, overspending and unaffordable loans are growing in prevalence across both developed and emerging markets.



Fraud and cybercrime

The rate of digitalization in emerging markets often outpaces **digital and financial literacy** for those who are newly 'financially included'.

Growing adoption means that existing weaknesses (e.g. governance frameworks, consumer awareness) are being increasingly **exploited by malicious actors** who target victims with unmanaged, unsecured information assets (e.g. mobile phones).[231]

Why is it important?



Vulnerable populations

Without a **stronger understanding of technology-driven financial exclusion**, the potential for global economic development, financial prosperity and general financial stability will remain hindered. According to a World Bank study, a 1% increase in financial inclusion can contribute to an annual GDP growth per capita of ~0.03%.[232]

The global financial system must **work for all** to be considered sound and successful.

PRIMARY SOURCES OF THIS RISK



Social inequities and fragmentation



Algorithmic and model deficiencies



Inexplicable machine- and model-led outputs



Undefined regulatory oversight

When observing issues of consumer suitability, scaled and highly automated business models may expose customers and investors to misaligned financial outcomes

Scenario example

Several peer-to-peer (P2P) lending platforms facilitate unaffordable loans, resulting in soaring default rates and cases of business insolvency.

What if…?

New digital platforms and applications offering P2P lending emerge in a developing market, directly connecting hundreds of lenders with millions of borrowers without an agency-led intermediary. To expedite the onboarding of millions of clients, many of these players take on the responsibility of performing identity verification and credit-worthiness assessments.

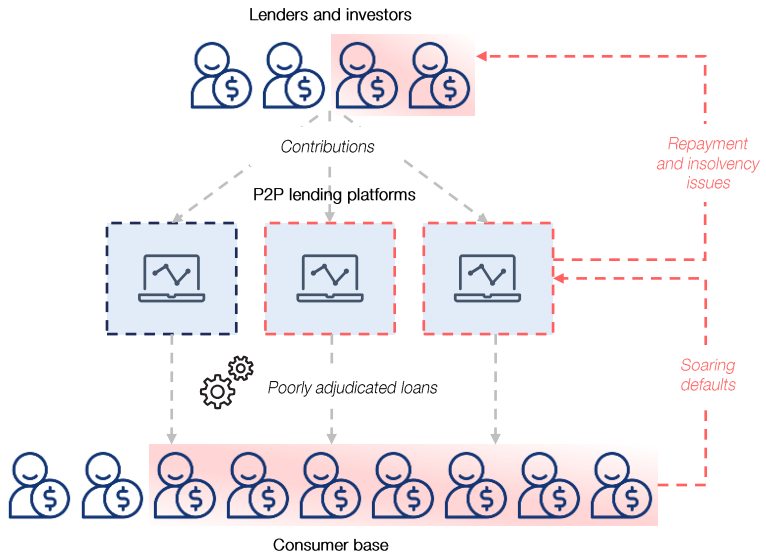
Given a jurisdiction-wide aversion to accredit new entrants or to facilitate partnerships with incumbents, these players are unable to reference regulator-operated personal credit systems and must exclusively rely on internal assessments that lack formal, credit-related data. Despite these limitations and given a large dependency on fee revenue, players facilitate billions of transactions.

Then this happens…

Inadequate assessments and limited insight into suitability drive the creation of unaffordable loans for thousands of consumers in financial need, resulting in soaring default rates and the insolvency of several players. Furthermore, investors and lenders suffer considerable harm due to lagging repayments.

To mitigate further financial contagion, regulators mandate these players to immediately cease operations. They also implement reactive measures through new consumer protection mechanisms and risk profiling obligations. This leads to the entire collapse of a once-booming alternative sector.

Process flow *(illustrative)*



As decision-making processes leverage alternative sources of data and are increasingly automated, players may feel gradually less responsible for decisions (or lack awareness of their decisions), potentially creating cascading implications to end-users and contributors of the system.

The private and public sectors play crucial roles in the financial wellbeing of individuals, communities and businesses, and cannot overlook the harm that digitization efforts may cause vulnerable groups.

What does this mean for the financial services ecosystem?



Technology's complex role in inclusivity: Without a stronger understanding of the issues surfacing as a result of digital transitions, large population groups will not be able to overcome learning gaps, remain aware of risks or use money as a tool for economic development. Emerging markets often struggle with resources or lack the personnel to remediate broken links with those who are left behind as digital financial services are rolled out. For example, those living in remote places are less likely to get formal identity documents and often cannot access services until provided with them.[232]



Financial inclusion as a key component of financial stability: Beyond supporting national economic development, financial inclusion measures have a direct tie-in to financial stability and can limit exposure to risks associated with financial interlinkages. For example, the expansion of individuals and businesses participating in the formal economy will allow incumbents to diversify their loan portfolios, reducing the size of any single borrower. As new savers enter the system, the size of incumbents' deposit bases increase, alleviating the need to turn to other funding sources to finance lending needs.



Preventing the 'black box' dilemma: Players should also refrain from operating in a 'black box', where decision-making processes and usage of services lack external visibility. Without industry-wide monitoring and detection, risks of inexplicable product rejections, over-lending, fraud and scams may remain relatively unaccounted for. If misconfigured technology applications are not properly scrutinized, negative financial outcomes and exploitative practices will result.

CASE STUDY

Mobile money transactions in Ghana have increased financial inclusion through seamless transfers and remittances. However, rampant cases of e-wallet fraud have put millions of active mobile money accounts at risk.

To prevent fraud, in 2020, the largest mobile money operator in Ghana introduced 'proof of identity' before a customer could withdraw cash. A new inclusion issue then emerged; only 15.5 million people out of a population of 30 million have been registered with formal ID, meaning that just under half of the eligible population were prevented from using these services.[233]

While this event had systemic implications, imagine if a similar event occurred with a greater magnitude of impact…

What if several large insurers utilize a common third-party AI capability that is prone to developing biases, preventing thousands of consumers from affordable protection?

Players are addressing technology-driven financial exclusion by aligning goals with actionable initiatives, such as amended regulations and personalized market offerings.

What are some key efforts that ecosystem players have undertaken to mitigate these risks?

Public sector players

- Establishing comprehensive and measurable strategic approaches to cybercrime, including metrics and dedicated supervisory bodies.[234]
- Strengthening due diligence responsibilities for market players (e.g. transparency of product terms, consent for use of data, dispute resolution mechanisms, illicit activity monitoring).
- Exploring solutions to allow those with limited access to mobile devices and the internet to participate in payments, digital identity and digital currency schemes.

Multilateral efforts

- Public sector players are increasingly understanding the broader impact of technology-driven exclusion through information sharing initiatives between regional authorities and private sector players.
- Cross-industry engagement is being actioned through regulatory sandboxes to pilot innovations and provide an evidence base for creating new policies on fairness, accountability and transparency.[235]
- Incumbents, FinTechs and technology players are increasingly collaborating to launch needs-based offerings (e.g. smart cards) for select financially excluded communities.[236]

Private sector players

- Leveraging big and alternative data (e.g. mobile data, social media activity, internet usage) to tailor offerings that fit the risk profile of those with a limited financial footprint.
- Developing interactive online educational platforms and gamified financial literacy programmes that are intertwined with financial products and services.[237]
- Deploying new proof of identity mechanisms and verifying information about a consumer's financial circumstances before onboarding (for product suitability needs and fraud prevention).

RELEVANT CASE STUDIES

European Commission

The European Commission proposed a revision of the Consumer Credit Directive to ensure that credits (i.e. loans) are presented clearly and adapted to digital devices. The Directive will also improve rules on how creditworthiness is assessed to prevent issues with over-indebtedness.[238]

mastercard.

A joint venture by Mastercard's Community Pass and Paycode aims to capture the biometrics of 30 million individuals in remote parts of Africa over the next three years. Citizens are expected to receive a digital bank account and a smartcard with a biometric digital identity.[239]

Niyo

Niyo Bharat launched a comprehensive financial literacy programme for the Indian labour force. As part of this digital initiative, the company is playing a vital role in educating thousands of blue-collar workers about the benefits and features of branchless banking.[240]

Despite progress made to address financial exclusion, numerous 'building blocks' across schemes, regulation and automation remain absent and must be sought to ensure continued momentum.

What gaps exist in current mitigation efforts?

Public sector players

- Financial inclusion efforts will remain stagnant if hardware needs (e.g. internet, smartphones) remain unaccounted for; over half of the world's population currently does not own a smartphone.[241]
- Identification mechanisms remain inaccessible for certain population groups; 1.1 billion people worldwide do not have the identity documentation that is often required for basic financial account access.[242]
- Gaps in regulatory coverage may leave important players outside the perimeter and create new instances of regulatory arbitrage; activity-based approaches lack applicability if players do not engage appropriate regulators early in the product deployment process to inform systemic challenges.

Multilateral efforts

- Given testing capacity limitations, regulators may not be able to draw reliable insights about the broader impact of certain products or services outside of a sandbox.
- Although effective for risk resolution, disclosure requirements can be ineffective in proactively ensuring that players operate with a responsible business outlook and avoid operating in a 'black box' vacuum.

Private sector players

- While digital financial inclusion increases, more individuals and players are handling more PII, raising privacy concerns for users and security vulnerabilities for data custodians.
- Actions of 'de-risking' as means to address compliance concerns (e.g. money laundering, terrorist financing, sanctions) can lead to a mass revocation of newly financially included population groups.
- New market players are likely to take a 'learning' approach upon deploying automated decision-making that relies on the ongoing capture of data for refinement; this can create lasting product suitability issues for consumers.[243]

KEY MITIGATION UNCERTAINTIES

1 *While technology has created new distribution channels, will barriers to accessing widely used hardware (e.g. smartphones) prevent the deployment of new offerings to certain markets?*

2 *Given that policies to prevent unethical financial practices (e.g. predatory lending) are globally scarce, how can an organization be incentivized to ensure that consumers receive the right outcome, irrespective of legal or regulatory demands?*

3 *As policy responses to evolving risks (e.g. illicit finance) often require players to perform additional due diligence (e.g. provide proof of identity), how can players ensure that these measures do not unintentionally exclude other population groups (e.g. those without identification)?*

Individual players can explore awareness building and new distribution channels to increase access for those who have been displaced by technology.

How can current mitigation efforts be improved? What more can be done by individual players to address this risk?

Risk prevention

- Education and awareness building: Regulators can facilitate financial and digital literacy, educating consumers on the risks of certain financial offerings (e.g. awareness campaigns on cybercrime). Similar approaches can be undertaken to strengthen product suitability (e.g. presenting consumers with warnings regarding costly credit).
- Pre-processing data: Players can increase the accuracy of financial outcomes and decorrelate sensitive information by filtering, transforming and encoding data before intake by ML models. Algorithmic fairness can also be improved through counterfactual fairness techniques.[244]

Risk intervention

- New distribution channels: To counterbalance branch closures, players can proactively explore the introduction of new distribution channels within existing outlets in underserved communities, such as retail stores, grocery stores, pharmacies or postal services locations.
- Proactive investigation: Players can routinely review bias and suitability across each stage of the product decision-making process and document their approach to tackling instances of discrimination. Additionally, players can make better use of AI and ML to automatically detect, flag and temporarily block potential fraudulent behaviour.[245]

Risk resolution

- Cyber liability shift: Regulators in emerging markets can ensure that cybersecurity regulations are keeping up with global standards and/or best practices to reach cybersecurity goals (e.g. preventing targeted exploitative practices by bad actors). This includes ensuring that players without adequate cybersecurity mechanisms are liable to a fine.
- Enterprise-wide explainable AI: Players can adopt an enterprise framework to address 'black box' AI decisions and assess the level of transparency required for each stage of decision-making. Simpler forms of ML may be considered, such as decision trees, Bayesian classifiers, and other algorithms that provide greater traceability when making decisions.[246]

POTENTIAL UNINTENDED CONSEQUENCES



As financial and digital literacy programmes are rolled out to support the usage of digital financial services, consumers may feel over-confident in their knowledge and begin to participate in riskier digital financial activities.



Algorithmic explanations can help to reduce information asymmetry, but these explanations are often incomplete. This presents an opportunity to embed preconceived notions or unconscious biases in how developer teams classify data that may further negatively impact algorithmic outcomes.

Collectively, the industry can overcome new challenges brought on by technology-driven exclusion, with alternative credit scoring and identity scheme enhancements among the most critical.

How can current mitigation efforts be improved? What more can be done multilaterally to address this risk?

Risk prevention

- Innovation networks: Jurisdictions can explore the creation of cross-border, open-architecture collaboration platforms that safely scale FinTech offerings. Multi-jurisdictional thematic sandboxes on responsible AI can enable shared testing programmes with the aim of reducing regulatory arbitrage across participating regions.
- Alternative credit scoring: Rather than exclusively relying on traditional credit scoring models to judge product suitability, players can collaborate with data providers to use alternative data in financial product decision-making. This can better accommodate unbanked and underbanked populations in circumstances where financial data may be limited.[247]

Risk intervention

- Affordable digital access: Regulators can take on specific policy measures to address the underlying issue of a 'digital divide'. Policy- and law-makers can push for ubiquitous and affordable internet access or mobile device subsidies. Such measures are likely beyond the purview of financial services functions and require broader collaboration.
- Big Tech diagnostic tools: Players can utilize Big Techs' capabilities to review algorithmic fairness by testing different hypothetical situations and analyzing the importance of different data features and conceptions of 'fairness'.
- Novel digital identity solutions: Regulators and private sector players can explore complementary mechanisms to ensure the successful roll-out of federated digital identity schemes. Novel biometric solutions, for example, hold the potential to advance national legal identification frameworks and can offer millions of people a legally recognized identity without requiring a smartphone or internet access.[248]

POTENTIAL UNINTENDED CONSEQUENCES



Although identity mechanisms can provide users with the ability to manage their identity information, they also give rise to data privacy and security issues (particularly in federated models). For this reason, strong cybersecurity mechanisms will need to be in place for the proper facilitation of identity schemes.

Key mitigation applications

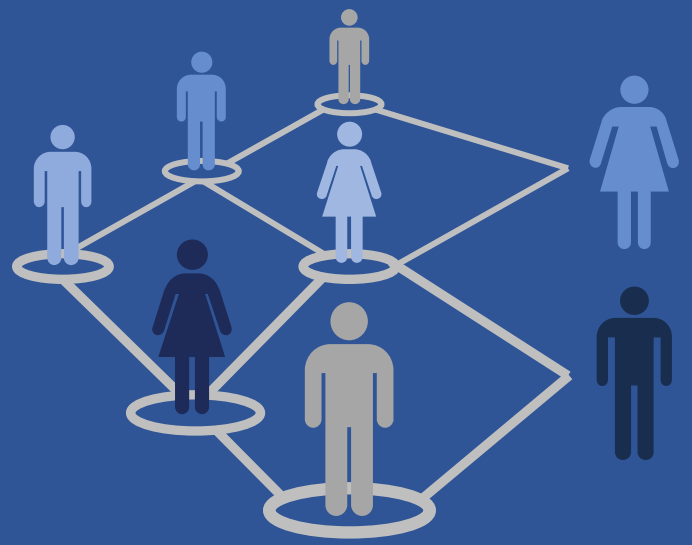


Table stakes: Greater adoption of alternative credit scoring (ACS) mechanisms can improve the accuracy of product suitability assessments by providing an alternative to one-dimensional credit histories.

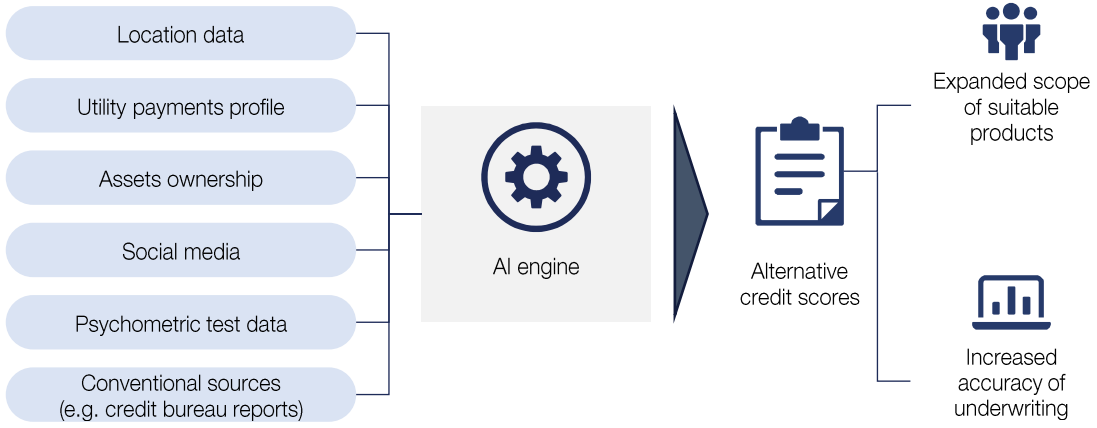
Overview

Traditional credit scoring (e.g. FICO) focuses primarily on financial data consisting of historical information on credit cards, loans and banking usage. Despite the amount of new data available to determine consumers' eligibility for a product or service, significant gaps in the widespread adoption of alternative decision-making methodologies remain.

ACS leverages alternative data in financial product decision-making that can be instrumental in the inclusion of population groups with a limited financial footprint. Rather than conventional verification and hardcoded credit scores, AI and ML capabilities can assess alternative data sources such as social media, electronic transactions and cellular data to build consumer risk profiles.[249]

Although ACS provides a unique channel for financial product accessibility, data privacy and security concerns would need to be addressed (including the interplay with digital identity schemes) at jurisdictional and organizational levels before the deployment of use cases. ACS is not intended to replace traditional credit scoring.[249]

How it works



ACS leverages **unconventional consumer information** in combination with conventional credit sources.

Use in financial services



- Through the ACS method, financial institutions could have better visibility over a potential borrower's capacity to pay back a loan, especially with regards to the underserved segments who lack credit capacity information.
- In turn, this allows digital and traditional lending institutions to identify borrowers' capabilities when they propose the issuance of financial credit, particularly regarding micro and small businesses, which rely extensively on working capital to thrive.[249]
- Although ACS is increasingly being deployed by FinTechs, large-scale adoption by incumbents remains limited.

Emerging: With algorithms increasingly supporting financial services players in product decision-making, fairness needs to be embedded in every step of the process.

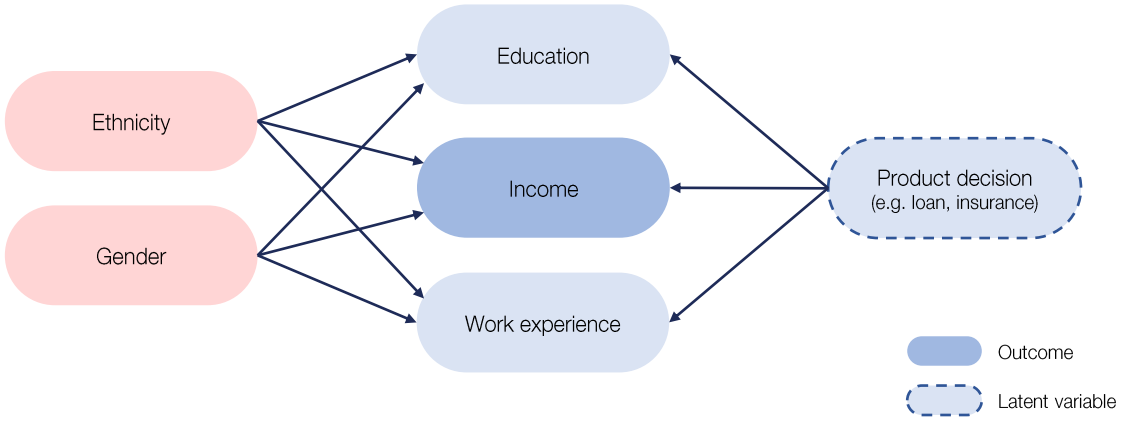
Overview

While players are increasingly utilizing algorithms, if the data used to train the model contains societal biases against certain ethnicities, genders or other demographic groups, then the algorithm will too. Using causal methods, developer teams can ensure algorithmic fairness by effectively accounting and compensating for different social biases.[250]

Algorithmic fairness through causal methods involves decoding whether the same decision outcome is achieved as it would be in a 'counterfactual' world (e.g. if an applicant receives the same decision if they belong to a different demographic). Players can then use these findings to refine their algorithms accordingly.[250]

Frameworks are being developed to provide modelling teams with an idea of how they should structure a problem, what is implied by their assumptions, and how they could evaluate it using a causal model. This includes ensuring that algorithms are designed using expert knowledge about the situations they are being used in.[250]

How it works



Counterfactual fairness determines whether an outcome would be the same in the 'actual' world versus one with different circumstances.

Use in financial services



- Algorithms are particularly useful for financial services players to predict the rate of default on a loan and the price (or fee) of a product or service.
- Consistent and fair human decision-making can be hindered by cognitive biases that are challenging to track; by contrast, an algorithm is inherently auditable, and when the ethical and practical objectives are clearly defined, it is possible to test whether it achieves the desired outcome.
- Counterfactual fairness techniques present an opportunity for risk-focused leaders and regulators to meaningfully define and formalize what it means to implement a fair decision-making system.

Novel: Biometric-based identity solutions can complement federated digital identity schemes, offering greater financial services accessibility and security.

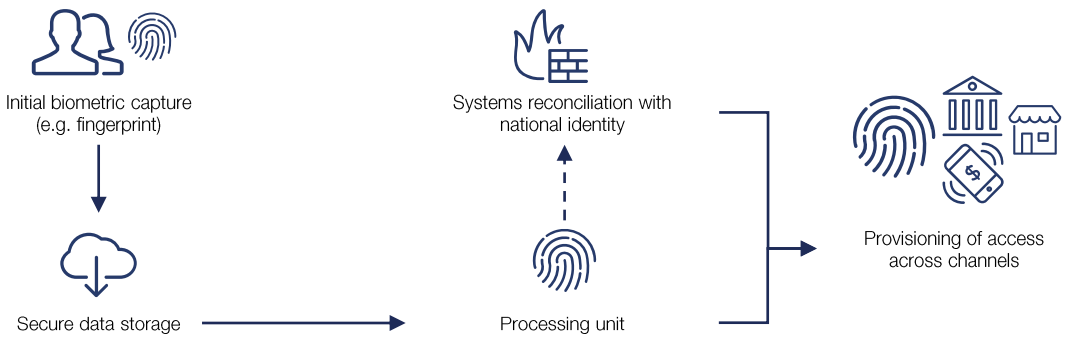
Overview

The weaknesses of fragmented and siloed identity schemes have paved the way for federated nationwide digital identity initiatives. Although these are convenient and require less management of authentication information, federated digital identity schemes do not always account for the millions of people without access to the internet or a smartphone. Biometric solutions have the potential to support national identification frameworks and can offer a recognized identity without restrictions.

Biometric authentication can include recognizing users through their voice, fingerprints, faces, irises or retinas, among other options. Such solutions have the potential to make financial services more accessible to individuals through a secure database of biometric information that players can access to verify a customer's identity. They also have the potential to operate 'offline' to ensure full population coverage without dependency on an internet connection.[251]

Given that digital identity frameworks are an evolving initiative for many global jurisdictions, the widespread adoption of such solutions (particularly those that possess offline interoperability) will likely remain nascent in the near future. Certain private sector players, however, are getting ahead of this issue (e.g. Mastercard and Paycode partnership).[252]

How it works



Biometric capture presents a unique opportunity to **reach the 'last mile'** as nation states accelerate the digital adoption of identity mechanisms and financial services.

Use in financial services

Monitor — Avoid — Assume — Control

- Additional channels of authentication will allow for quick onboarding, with the necessary checks and balances to accurately prove an individual's identity significantly increasing trusted access and preventing instances of fraud.
- Policy-makers need to be able to move as quickly as the technology and times in which they live; data protection authorities must offer sufficient legal bases to enable biometric digital identity to function.
- Initiatives such as India's Aadhaar and players such as Paycode are advancing biometric identity solutions by offering a simple, reliable way for individuals to prove who they are by using their fingerprints.[252, 253]

Conclusion

A new risk agenda is encouraged, where public and private sector players look to understand and proactively mitigate against global technology-driven systemic risks.

Key takeaways for financial services players

Weighing up technology risks

Keeping pace with change in the industry, particularly with the acceleration of digital transformation stemming from COVID-19, necessitates a strong understanding of how innovations and vendor relationships can have unintended consequences.

Players seeking to adopt emerging technology or create relationships with other innovators will need to think pragmatically; the benefits of new capabilities will need to be weighed against known (and potentially unknown) risks.

Enhancing internal capabilities

Private sector players are more pressed than ever to manage risk in a cost-effective manner while meeting evolving regulatory and stakeholder expectations.

In order to respond, players can look to source new data that exists beyond their walls. Resilient risk management can subsequently be realized by mapping new data-rich capabilities (e.g. AI) to a well-defined set of priority risks.

Pursuing collective action

The blurring of traditional industry lines and longstanding regulatory nuances between nations means that action at the entity level will not be enough to tackle complex issues.

Regulators and industry players will need to have a symbiotic relationship that fosters a common understanding of risk and informs new investments to mitigate it. Jointly navigating uncertainty will also require a forward-looking perspective that is not always predicated on past risk events.

Enlisting the right people

Risk management teams can become more strategic to support enterprise goals. To enable this, players need to actively train and recruit leaders who have bold perspectives on the future, an acute awareness of the intersection between technology and risk, and the ambition to translate their visions into reality.

Players also need to attract a strong pipeline of talent that can bring a mix of risk-focused thinking and technology-focused expertise to best understand, assess and prepare for the industry's emerging systemic risks.

When considering how current risk management capabilities will fare against systemic risks now and in the and future, leaders must question their organization's capabilities and resilience.

What key questions should risk-focused public and private sector leaders be asking themselves?

Public sector players

- **Is the organization appropriately considering technology-driven systemic risks, both internally and externally?** Are the right investments in technology being made to monitor these risks? Is your in-house technology expertise being strengthened to understand leading risk indicators?
- **Is the organization linked with global standard- and policy-setting bodies to ensure the most consistent understanding of risk mitigation?** Does the body actively hold consultations to supplement its ability to respond to technology-driven systemic risks? From this collective understanding, are regional regulators able to appropriately tailor regulatory responses based on their jurisdictional nuances?
- **Has the organization deconstructed the full range of emerging financial activities to ensure existing regulations have an appropriate level of coverage?** Has it considered expanding its regulatory or supervisory scope to meet the requirements of the system's new activities?

Private sector players

- **Is the organization taking an offensive or defensive stance towards risk?** Is the organization both defending against entity-level risks (i.e. idiosyncratic risks or individual SoR) and proactively preventing ecosystem-level threats (i.e. accumulation of SoR that can form systemic risks)?[254]
- **Is risk management considered to be a core investment lever in the organization's enterprise strategy?** Is the risk management team able to effectively plan, assess and manage increased demands from regulators while simultaneously deploying resources to mitigate other impactful risks?[255]
- **Is the organization deploying novel, forward-looking tools to monitor and anticipate risk?** How can risk management be transformed through further digitization (e.g. ML applications) and targeted ecosystem partnerships (e.g. vendor risk management platforms)?

The second phase of this initiative will delve deeper into the role that technology plays in increasing systemic risk and explore persistent questions around technology-driven mitigation approaches.

This report identified the most pertinent systemic risks created or amplified by technology, outlined their broader implications to the financial services ecosystem and began to uncover relevant technology-driven approaches to risk mitigation.
In the second phase of the Technology, Innovation and Systemic Risk initiative, the World Economic Forum will aim to answer the following outstanding questions:



What nuances related to the varying impact of systemic risks and mitigation approaches should be explored further?

The following opportunities will be explored:

A Sector-based dynamics (e.g. banking, insurance, investment management)

B Entity-based implications (e.g. incumbents, regulators, FinTechs, Big Techs)

C Jurisdiction-based differences (e.g. Americas, UK, EU, APAC)



What other non-technology-driven systemic risks within financial services can technology can play a primary role in mitigating (e.g. financial fallout, climate change)?

Acronyms and abbreviations

Acronyms and abbreviations used in this report

AI	Artificial intelligence
AML	Anti-money laundering
API	Application programming interfaces
CaaS	Capabilities as a service
CBDC	Central bank digital currency
CDD	Customer due diligence
CFT	Combatting the financing of terrorism
CTHA	Cyberthreat hunting and attribution
DeFi	Decentralized finance
DLT	Distributed ledger technology
DRA	Dynamic risk assessments
DRR	Digital regulation reporting
ECB	European Central Bank
ESG	Environmental, social and governance
FCA	Financial Conduct Authority
FinTech	Financial technology
FIU	Financial intelligence units
gIPS	Global instant payment systems
GIS	Geographic information systems
KYC	Know your customer
MER	Machine executable regulation
ML	Machine learning
MRR	Machine readable regulation
NIS	Network and information security directive
NLP	Natural language processing
P2P	Peer-to-peer
PET	Privacy enhancing technology
PII	Personal identifiable information
QKD	Quantum key distribution
RegTech	Regulatory technology
RPA	Robotic process automation
SaaS	Software as a service
SEC	Securities and exchange commission
SoR	Sources of risk
SupTech	Supervisory technology
TM	Transaction monitoring
TMNL	Transaction Monitoring Nederlands

Acknowledgements

Contributors (1 of 3)

The project team would like to express their gratitude to the following subject matter experts who contributed valuable perspectives through interviews and by participating in workshop and roundtable discussions (in alphabetical order):

Abdullah Mohiuddin	OMERS
Abhishek Chatterjee	Tookitaki
Addie Wagenknecht	Algorand Foundation
Adewale Ayantoye	Flutterwave
Aditya Narain	International Monetary Fund (IMF)
Aidan Murphy	Financial Conduct Authority (FCA)
Ali El Kaafarani	PQShield
Ana Predojević	Stockholm University
André Bastos	Open Co
Andrew Fursman	1QB Information Technologies (1QBit)
Andrew Wiebe	RiskThinking.AI
Aneesh Varma	Aire Labs
Anna Celner	Deloitte Switzerland
Anton Moiseienko	Royal United Services Institute (RUSI)
Austan D. Goolsbee	The University of Chicago, Booth School of Business
Blair Radbourne	OMERS
Brendan Reilly	RiskThinking.AI
Brian LaMacchia	Microsoft
Bruce Schneier	Harvard Kennedy School of Government
Bryan Ware	Next5
Bushra AlBlooshi	Dubai Electronic Security Center (DESC)
Carl J. Williams	National Institute of Standards and Technology (NIST)
Carrie Suen	Ant Group
Charmaine Wong	HSBC
Chi Xiangting	China Construction Bank
Chris Cheatham	RiskGenius (acquired by Bold Penguin)
Christopher Wilson	International Monetary Fund (IMF)
Damien Pang	Cyber Security Agency of Singapore (CSA)
Daniel Cuthbert	Banco Santander SA
Danielle Winandy	BNP Paribas
Daragh Morrissey	Microsoft
Diana Paredes	Suade Labs
Dimitri Tsopanakos	Deloitte UK
Douglas W. Arner	The University of Hong Kong (HKU)
Duncan Jones	Cambridge Quantum Computing
Edwin Lacierda	PayMongo
Elizabeth Rossiello	AZA Finance
Emilios Avgouleas	The University of Edinburgh
Evgueni Ivantsov	European Risk Management Council
Fabiana Melo	International Monetary Fund (IMF)
Francis Plaza	Paymongo
Gabrijela Dreo Rodosek	University of the German Federal Armed Forces
George Marangoly	Australian Securities and Investment Commission (ASIC)
George Miao	Credit Suisse
Guy Caspi	Deep Instinct
Haimera Workie	Financial Industry Regulatory Authority (FINRA)
Harish Natarajan	World Bank Group
Hanna Helin	London Stock Exchange Group (LSEG)
Harqs Singh	BlackRock
Hideo Yamamoto	NTT Data

Contributors (2 of 3)

The project team would like to express their gratitude to the following subject matter experts who contributed valuable perspectives through interviews and by participating in workshop and roundtable discussions (in alphabetical order):

Hoda Alkhzaimi	New York University Abu Dhabi
Ibrahim Almosallam	Saudi Information Technology Company
Illah Nourbakhsh	Carnegie Mellon University
Inma Martinez	Global Partnership on Artificial Intelligence (GPAI)
Jacques Francoeur	International Telecommunication Union (ITU)
James Cemmell	Inmarsat Global Ltd
Jason Lau	Crypto.com
Jason Lee	Algorand Foundation
Jaya Baloo	Avast
Jayne Plunkett	AIA Group Limited - Pan-Asian Life Insurance Company
Jennifer Stott	Royal Bank of Canada (RBC) Financial Group
Jeremy Annis	Ripjar
Jesse Spiro	PayPal
John Beric	Mastercard
John Lowes	OMERS
John Stewart	NatWest Group
Jon Frost	Bank for International Settlements (BIS)
Jonathan Hatch	Australian Securities and Investment Commission (ASIC)
Jonathan Welburn	RAND Corporation
Jong Chin Foo	Cyber Security Agency of Singapore (CSA)
Julian Leake	Deloitte UK
Karen Croxson	Financial Conduct Authority (FCA)
Katharine Preston	OMERS
Kayla Izenman	Royal United Services Institute (RUSI)
Ken Watanabe	NTT Data
Kirk Bresniker	Hewlett Packard Enterprise
Laura Scarpa	Deloitte UK
Laurent Berliner	Deloitte EMEA
Leeanne Barnes	OMERS
Leonie Beyrle	Harvard Kennedy School of Government
Lesly Goh	World Bank Group
Tong Lee Lim	Monetary Authority of Singapore
Lisa Blenkinsop	Protiviti
Luan Cox	FinMkt
Luis Lasso	Banco Nacional de Panama (Banconal)
Lukas Petrikas	Hong Kong Exchanges and Clearing (HKEX)
Luther Bian	China Construction Bank
Marcos Allende López	Inter-American Development Bank (IDB) Asia
Marek Stanislawski	Allianz SE
Mark Adams	Australian Securities and Investment Commission (ASIC)
Mark Carney	Banco Santander SA
Martin K. Hess	Swiss Bankers Association
Maryam Golnaraghi	The Geneva Association
Matthew Osborne	Bank of England
Max von Bismarck	Deposit Solutions GmbH
Maximilian Dyck	Suade Labs
Michael Crumpler	Credit Benchmark
Michael Daniel	Cyber Threat Alliance

Contributors (3 of 3)

The project team would like to express their gratitude to the following subject matter experts who contributed valuable perspectives through interviews and by participating in workshop and roundtable discussions (in alphabetical order):

Michele Mosca	University of Waterloo
Mike Wilkes	SecurityScorecard
Mobolaji 'Mo' Bammeke	Flutterwave
Nick Maxwell	Royal United Services Institute (RUSI)
Nicolas Brand	Lakestar
Nidhi Sharma	Honeywell International Inc.
Nobuyasu Sugimoto	International Monetary Fund (IMF)
Oleksiy Rachok	Aegon N.V.
Parma Bains	International Monetary Fund (IMF)
Pascal Millaire	CyberCube
Paul D. Fabara	VISA Inc
Paul Hiebert	European Central Bank (ECB)
Paul Huston	ComplyAdvantage
Paul Tierno	Federal Reserve Bank of San Francisco
Pavle Avramovic	Financial Conduct Authority (FCA)
Pedro Bizarro	Feedzai
Randall Bartlett	OMERS
Renan Borne	Natixis
Richard McMahon	Australian Securities and Investment Commission (ASIC)
Rick Carey	UBS
Roddy Kok	Cyber Security Agency of Singapore (CSA)
Ron Dembo	RiskThinking.AI
Ronen Assia	Team8
Ross P. Buckley	University of New South Wales
Salvador E. Venegas-Andraca	Tecnológico de Monterrey
Sam Tidswell-Norrish	Motive Partners
Sandro Reiss	Open Co
Sara AlGhunaim	Saudi Information Technology Company
Sarah Zhang Jiachen	Guangzhishu Technology (points.org)
Sarkis Mazmanian	Deutsche Bank
Sean Hunter	OakNorth Bank
Sean Lee	Algorand Foundation
Shinji Setoriyama	NTT Data
Sigmund Kristiansen	Aker BP
Solveig Bachellery	BNP Paribas
Soon Chia Lim	Cyber Security Agency of Singapore (CSA)
Stacey Jeffery	QuSoft
Stan Sadovski	Credit Benchmark
Steven McWhirter	Financial Conduct Authority (FCA)
Syam Nair	Gojo & Company
Takuya Miyamoto	NTT Data
Theresa Yurkewich Hoffmann	City of London
Tony Wood	Deloitte Hong Kong and China
Trisha Kothari	Unit21
Tse Gan Thio	Deloitte Singapore
Vikram Sharma	QuintessenceLabs
Werner de Wit	Credit Benchmark
William Dixon	Istari Global
Yoshiharu Akahane	NTT Data
Zack Zhan Yang	FOMO Pay

Endnotes

References (1 of 18)

Introduction:

1. Cover / Inside art: Spratt, Annie, *Iceberg at Scoresby Sund, Greenland from above*, [Photograph], https://unsplash.com/photos/U1mQ3wGcvtQ.

Context and approach:

2. "Idiosyncratic Risk", *Corporate Finance Institute*, accessed 18 Oct 2021, https://corporatefinanceinstitute.com/resources/knowledge/other/idiosyncratic-risk/.
3. Nguyen, Joseph "Systemic Risk vs. Systematic Risk: What's the difference?" *Investopedia*, 29 September 2021, https://www.investopedia.com/ask/answers/09/systemic-systematic-risk.asp.
4. Welburn, Jonathan and Aaron Strong, "Too Interconnected to Fail", *The Wall Street Journal*, 23 July 2020, https://www.wsj.com/articles/too-interconnected-to-fail-11595523324.

Executive summary:

5. Zetzsche, Dirk A., et al. "Digital Finance Platforms: Toward a New Regulatory Paradigm", *European Banking Institute (EBI) Working Paper Series*, no. 58, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975.
6. Massari, Jai, and Christian Catalini, "DeFi, Disintermediation, and the Regulatory Path Ahead", *The Regulatory Review*, 10 May 2021, https://www.theregreview.org/2021/05/10/massari-catalini-defi-disintermediation-regulatory-path-ahead/.
7. "Infographic: What Is a G-SIB?", *Government of Canada, Office of the Superintendent of Financial Institutions*, 22 Nov 2019, https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/Pages/nr_20191122_ig.aspx.
8. "EC Unveils Drafts of the Digital Services Act and the Digital Markets Act" *digwatch*, 15 December 2020, https://dig.watch/updates/ec-unveils-drafts-digital-services-act-and-digital-markets-act.
9. Welburn, Jonathan, et al. "Systemic Risk: It's Not Just in the Financial Sector", *RAND Corporation*, 3 February 2020, https://www.rand.org/pubs/research_briefs/RB10112.html.
10. Terdiman, Daniel, "The Rise of Nth Party Risk: What You Need to Know" *Mastercard*, 24 May 2021, https://www.mastercard.com/news/perspectives/2021/the-rise-of-nth-party-risk/.
11. "FCA to Use Blockchain to Speed up Regulatory Reporting", *Finextra*, 23 September 2021, https://www.finextra.com/newsarticle/38891/fca-to-use-blockchain-to-speed-up-regulatory-reporting?utm_medium=newsflash&utm_source=2021-9-23&member=130235.
12. Zimmer, Sabine, "Nth Party Risk Concepts - How Low Should You Limbo?", *Shared Assessments*, 20 February 2021, https://sharedassessments.org/blog/nth-party-risk-concepts-how-low-should-you-go.
13. Wilson, H. James, et al. "The Future of AI Will Be about Less Data, Not More,", *Harvard Business Review*, 14 January 2019, https://hbr.org/2019/01/the-future-of-ai-will-be-about-less-data-not-more.
14. Ferreira, Leonardo N., et al. "Spatiotemporal Data Analysis with Chronological Networks", *Nature Communications*, vol. 11, no. 4036, 2020, https://www.nature.com/articles/s41467-020-17634-2.

References (2 of 18)

Defining systemic risk:

15. Refinitiv, *Revealing the True Cost of Financial Crime*, 2018, https://www.refinitiv.com/content/dam/marketing/en_us/documents/reports/true-cost-of-financial-crime-latin-america-focus.pdf.
16. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment: Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
17. Partz, Helen, "Beijing Investigates Crypto Mining Farms to Improve Energy Efficiency", *Cointelegraph*, 29 April 2021, https://cointelegraph.com/news/beijing-investigates-crypto-mining-farms-to-improve-energy-efficiency.
18. Financial Stability Board, *The Implications of Climate Change for Financial Stability*, 2020, https://www.fsb.org/wp-content/uploads/P231120.pdf.
19. Hayes, Mike and Tegan Keele, "Blockchain Breaks New Ground on Climate Risk and Performance", *KPMG*, 4 March 2021, https://home.kpmg/xx/en/home/insights/2021/03/blockchain-breaks-new-ground-on-climate-risk-and-performance.html.
20. Wolfson, Rachel, "Measuring Success: Offsetting Crypto Carbon Emissions Necessary for Adoption?", *Cointelegraph*, 11 August 2021, https://cointelegraph.com/news/measuring-success-offsetting-crypto-carbon-emissions-necessary-for-adoption.

Exploring and mitigating technology-led systemic risks - Risk theme #1 – Digital interdependencies:

21. Merle, Renae, "A Guide to the Financial Crisis - 10 Years Later", *The Washington Post*, 10 September 2018, https://www.washingtonpost.com/business/economy/a-guide-to-the-financial-crisis--10-years-later/2018/09/10/114b76ba-af10-11e8-a20b-5f4f84429666_story.html.
22. "Post-2008 Financial Crisis Reforms", *Financial Stability Board*, 9 November 2020, https://www.fsb.org/work-of-the-fsb/market-and-institutional-resilience/post-2008-financial-crisis-reforms/.
23. "Big Banks, Bigger Techs?", *Oliver Wyman*, 15 July 2020, https://www.oliverwyman.com/our-expertise/insights/2020/jul/big-banks-bigger-techs.html.
24. Langford, Ronan and Steffen Pietz, "Harnessing Third-Parties for Value Creation", *Deloitte*, 11 May 2018, https://www2.deloitte.com/ch/en/pages/risk/articles/harnessing-third-parties-for-value-creation.html.
25. Leprince-Ringuet, Daphne, "Banks Now Rely on a Few Cloud Computing Giants. That's Creating Some Unexpected New Risks", *ZDNet*, 16 July 2021, https://www.zdnet.com/article/banks-now-rely-on-a-few-cloud-computing-giants-thats-creating-some-unexpected-new-risks/.
26. Watts, Stephen and Muhammad Raza, "Saas vs Paas vs Iaas: What's the Difference and How to Choose", *bmc blogs*, 15 June 2019, https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.
27. Zetzsche, Dirk A., et al. "Digital Finance Platforms: Toward a New Regulatory Paradigm", *European Banking Institute (EBI) Working Paper Series*, no. 58, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975.
28. Brühl, Volker, "How to Define a Systemically Important Financial Institution – A New Perspective", *Intereconomics*, vol. 52, no. 2, 2017, pp. 107-110, https://www.intereconomics.eu/contents/year/2017/number/2/article/how-to-define-a-systemically-important-financial-institution-a-new-perspective.html.

References (3 of 18)

Risk theme #1 – Digital interdependencies (continued):

29. Financial Stability Board, *Evaluation of the Effects of Too-Big-To-Fail Reforms*, 2021, https://www.fsb.org/wp-content/uploads/P010421-1.pdf.
30. Constantin, Lucian, "SolarWinds Attack Explained: And Why It Was so Hard to Detect", *CSO*, 15 Decembder 2020, https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html.
31. Makortoff, Kalyeena, "Why the Bank of England Has Its Head in the Cloud over Data Security", *The Guardian*, 21 July 2021, https://www.theguardian.com/business/2021/jul/21/why-the-bank-of-england-has-its-head-in-the-cloud-over-data-security
32. "Proposed Interagency Guidance on Third-Party Relationships: Risk Management", *Federal Register*, 19 July 2021, https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.
33. Appaya, Sharmista and Mahjabeen Haji, "Four Years and Counting: What We've Learned from Regulatory Sandboxes", *World Bank Blogs*, 18 November 2020, https://blogs.worldbank.org/psd/four-years-and-counting-what-weve-learned-regulatory-sandboxes.
34. "Proposed Interagency Guidance on Third-Party Relationships: Risk Management", *Federal Register*, 19 July 2021, https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management.
35. "Taking a Prevention-First Approach to Preventing Critical Banking Services and Customer Data", *DeepInstinct*, 2020, https://www.deepinstinct.com/pdf/case-study-financial-services-institution.
36. De Moura, Georges and Christophe Blassiau, "3 Principles to Reinforce Digital Trust in Supply Chains" *World Economic Forum*, 5 July 2021, https://www.weforum.org/agenda/2021/07/cybersecurity-hacker-proofing-digital-supply-chains/.
37. Groenfeldt, Tom, "Multi Cloud Becomes the New Norm for Banking", *Forbes*, 29 June 2020, https://www.forbes.com/sites/tomgroenfeldt/2020/06/29/multi-cloud-becomes-the-new-norm-for-banking/?sh=7694489814bc.
38. Evans, Steve, "Parametric Cyber Business Interruption Cover Launched at Lloyd's", *Artemis*, 30 September 2020, https://www.artemis.bm/news/parametric-cyber-business-interruption-cover-launched-at-lloyds/.
39. Bray, Chad, et al. "China's Ant Group to form a financial holding company after regulatory lockdown", *South China Morning Post*, 12 April 2021, https://www.scmp.com/business/banking-finance/article/3129251/chinas-ant-group-unveils-overhaul-after-regulatory.
40. Tung, Liam, "Cloud Computing: Microsoft Sets out New Data Storage Options for European Customers," *ZDNet*, 6 May 2021, https://www.zdnet.com/article/cloud-computing-microsoft-sets-out-new-data-storage-options-for-european-customers/.
41. "American Express, Bank of America, JPMorgan Chase and Wells Fargo form Industry Consortium to Transform Third-Party Risk Management", *TruSight (via Cision PR Newswire),* 14 November 2017, https://www.prnewswire.com/news-releases/american-express-bank-of-america-jpmorgan-chase-and-wells-fargo-form-industry-consortium-to-transform-third-party-risk-management-300555177.html.
42. Restoy, Fernando, *Regulating FinTech: Is an Activity-Based Approach the Solution?,* 16 June 2021, speech presented virtually to the fintech working group at the European Parliament, https://www.bis.org/speeches/sp210616.htm.

References (4 of 18)

Risk theme #1 – Digital interdependencies (continued):

43. Zetzsche, Dirk A., et al. “Digital Finance Platforms: Toward a New Regulatory Paradigm”, *European Banking Institute (EBI) Working Paper Series*, no. 58, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975.
44. “Automation of Regulatory Reporting in Banking And Securities”, *Deloitte*, accessed 18 October 2021, https://www2.deloitte.com/us/en/pages/regulatory/articles/automating-regulatory-reporting-banking-securities.html.
45. Dahl, Katharine, “3 Reasons Why Automating Vendor Risk Management Fails”, *SecurityScorecard*, 30 June 2020, https://securityscorecard.com/blog/3-reasons-why-automating-vendor-risk-management-fails.
46. Zetzsche, Dirk A., et al. “Digital Finance Platforms: Toward a New Regulatory Paradigm”, *European Banking Institute (EBI) Working Paper Series*, no. 58, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975.
47. World Economic Forum, *The next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, 2019, https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value.
48. Finney, George, “The Solarwinds Hack: Why We Need Zero Trust More than Ever”, *SecurityRoundtable.org*, accessed 18 October 2021, https://www.securityroundtable.org/the-solarwinds-hack-why-we-need-zero-trust-more-than-ever/.
49. Partida, Devin, “The Role of Geospatial Data in Cybersecurity”, *isBuzz news*, 24 September 2020, https://informationsecuritybuzz.com/articles/the-role-of-geospatial-data-in-cybersecurity/.
50. World Economic Forum, *The next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, 2019, https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value.
51. Finney, George, “The Solarwinds Hack: Why We Need Zero Trust More than Ever”, *SecurityRoundtable.org*, accessed 18 October 2021, https://www.securityroundtable.org/the-solarwinds-hack-why-we-need-zero-trust-more-than-ever/.
52. “What Is a Zero Trust Architecture”, *Palo Alto Networks*, accessed 18 October 2021, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.
53. Finney, George, “The Solarwinds Hack: Why We Need Zero Trust More than Ever”, *SecurityRoundtable.org*, accessed 18 October 2021, https://www.securityroundtable.org/the-solarwinds-hack-why-we-need-zero-trust-more-than-ever/.
54. Peters, Jeff, “Putting the Geospatial in Cybersecurity”, *Federal News Network*, 12 April 2018, https://federalnewsnetwork.com/commentary/2018/04/putting-the-geospatial-in-cybersecurity/.
55. Kumar, Vivek, “Powering the Role of Cybersecurity with Geospatial Data”, *Analytics Insight*, 18 November 2020, https://www.analyticsinsight.net/powering-the-role-of-cybersecurity-with-geospatial-data/.
56. Partida, Devin, “The Role of Geospatial Data in Cybersecurity”, *isBuzz news*, 24 September 2020, https://informationsecuritybuzz.com/articles/the-role-of-geospatial-data-in-cybersecurity/.

References (5 of 18)

Risk theme #1 – Digital interdependencies (continued):

57. Christiaen, Christophe, "Using Spatial Finance for Sustainable Development", *Refinitiv Perspectives*, 10 June 2020, https://www.refinitiv.com/perspectives/ai-digitalization/using-spatial-finance-for-sustainable-development/.
58. Hayford, Don, "The Future of Security: Zeroing in on Un-Hackable Data with Quantum Key Distribution", *Wired*, accessed 18 Oct 2021, https://www.wired.com/insights/2014/09/quantum-key-distribution/.
59. Prisco, John, "Council Post: Quantum Commercialized: Financial Services Likely First Industry to Take Advantage", *Forbes*, 19 February 2021, https://www.forbes.com/sites/forbestechcouncil/2021/02/19/quantum-commercialized-financial-services-likely-first-industry-to-take-advantage/.

Risk theme #2 – Shared model vulnerabilities:

60. Crespo, Ignacio, et al. "The Evolution of Model Risk Management", *McKinsey & Company*, 10 February 2017, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-evolution-of-model-risk-management.
61. Laurent, Marie-Paule, et al. "Banking Models after COVID-19: Taking Model-Risk Management to the next Level", *McKinsey & Company*, 5 May 2020, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/banking-models-after-covid-19-taking-model-risk-management-to-the-next-level.
62. The Bank for International Settlements, *The Green Swan: Central Banking and Financial Stability in the Age of Climate Change*, 2020, https://www.bis.org/publ/othp31.htm.
63. Guerreri, Federico, "How COVID-19 Is Changing Credit Risk Models", *EY*, 14 August 2020, https://www.ey.com/en_gl/covid-19-financial-services/how-covid-19-is-changing-credit-risk-models.
64. Arnold, Martin, "ECB Cracks down on Deficiencies in Big Banks' Risk Modelling", *Financial Times*, 19 April 2021, https://www.ft.com/content/cf796ff6-759e-47f6-b203-cbc2d44a3056.
65. "Internal Models", *European Central Bank*, accessed 18 October 2020, https://www.bankingsupervision.europa.eu/banking/tasks/internal_models/html/index.en.html.
66. "Model Risk Management", *Deloitte Risk Advisory*, April 2017, https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_model-risk-management_plaquette.pdf.
67. The Bank for International Settlements, *The Green Swan: Central Banking and Financial Stability in the Age of Climate Change*, 2020, https://www.bis.org/publ/othp31.htm.
68. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment | Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
69. World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, 2019, https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value.

References (6 of 18)

Risk theme #2 – Shared model vulnerabilities (continued):

70. "Model Risk Management", *Deloitte Risk Advisory*, April 2017, https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_model-risk-management_plaquette.pdf.
71. UN Environment Programme, *The Climate Risk Landscape: A Comprehensive Overview of Climate Risk Assessment Methodologies*, 2021, https://www.unepfi.org/wordpress/wp-content/uploads/2021/02/UNEP-FI-The-Climate-Risk-Landscape.pdf.
72. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment | Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
73. "Systemic Cyberattack Could Present Material Risk for US. Banks", *Fitch Ratings*, 10 August 2021, https://www.fitchratings.com/research/banks/systemic-cyberattack-could-present-material-risk-for-us-banks-10-08-2021.
74. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment | Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
75. Spratt, David and Ian Dunlop, *Degrees of Risk: Can the Banking System Survive Climate Warming of 3˚C?,* Breakthrough, National Centre for Climate Restoration, 2021, https://52a87f3e-7945-4bb1-abbf-9aa66cd4e93e.filesusr.com/ugd/148cb0_3696c267fcac4eaead397134301c4068.pdf.
76. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment | Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
77. Spratt, David and Ian Dunlop, *Degrees of Risk: Can the Banking System Survive Climate Warming of 3˚C?,* Breakthrough, National Centre for Climate Restoration, 2021, https://52a87f3e-7945-4bb1-abbf-9aa66cd4e93e.filesusr.com/ugd/148cb0_3696c267fcac4eaead397134301c4068.pdf.
78. Golnaraghi, Maryam, "Insurance Industry Perspectives on Regulatory Approaches to Climate Risk Assessment | Issue Brief", *The Geneva Association*, 28 June 2021, https://www.genevaassociation.org/research-topics/climate-change-and-emerging-environmental-topics/insurance-industry-perspectives-regulatory.
79. Evans, Steve, "Oasis Gets Industry Backing for Loss Modelling Framework and Open Source Standards", *Artemis*, 23 March 2021, https://www.artemis.bm/news/oasis-gets-industry-backing-for-loss-modelling-framework-open-source-standards/.
80. Lackey, Brad, et al. "Quantum Impact - Financial Services", *Azure*, 30 October 2020, https://azure.microsoft.com/en-us/resources/quantum-impact-financial-services/.
81. World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value*, 2019, https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value.
82. Evans, Steve, "Oasis Gets Industry Backing for Loss Modelling Framework and Open Source Standards", *Artemis*, 23 March 2021, https://www.artemis.bm/news/oasis-gets-industry-backing-for-loss-modelling-framework-open-source-standards/.
83. Lackey, Brad, et al. "Quantum Impact - Financial Services", *Azure*, 30 October 2020, https://azure.microsoft.com/en-us/resources/quantum-impact-financial-services/.

References (7 of 18)

Risk theme #3 – Gaps in entity-based regulation:

84. Withers, Iain and Huw Jones, “For Bank Regulators, Tech Giants Are Now Too Big to Fail”, *Reuters*, 20 August 2021, https://www.reuters.com/world/the-great-reboot/bank-regulators-tech-giants-are-now-too-big-fail-2021-08-20/.

85. Restoy, Fernando, *Regulating FinTech: Is an Activity-Based Approach the Solution?,* 16 June 2021, speech presented virtually to the fintech working group at the European Parliament, https://www.bis.org/speeches/sp210616.htm.

86. Osipovich, Alexander, “Crypto Frauds Target Investors Hoping to Cash In on Bitcoin Boom”, *The Wall Street Journal*, 7 June 2021, https://www.wsj.com/articles/crypto-frauds-target-investors-hoping-to-cash-in-on-bitcoin-boom-11623058380.

87. World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, 2021, http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.

88. Congressional Research Service, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework*, 2020, https://sgp.fas.org/crs/misc/R44918.pdf.

89. Bank of Canada, *Reinventing the Role of Central Banks in Financial Stability*, 2016, https://www.bankofcanada.ca/wp-content/uploads/2016/11/boc-review-autumn16-lombardi.pdf.

90. Fresh, Adriane and Martin Neil Baily, “What does international experience tell us about regulatory consolidation?”, *The PEW Economic Policy Department*, 2009, "https://www.brookings.edu/wp-content/uploads/2016/06/0921_consolidation_baily.pdf.

91. De Meijer, Carlo R.W., “DeFi and Regulation: The European Approach”, *Finextra*, 28 June 2021, https://www.finextra.com/blogposting/20516/defi-and-regulation-the-european-approach.

92. Sandner, Philipp, “Decentralized Finance Will Change Your Understanding Of Financial Systems”, *Forbes*, 22 February 2021, https://www.forbes.com/sites/philippsandner/2021/02/22/decentralized-finance-will-change-your-understanding-of-financial-systems/.

93. World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, 2021, http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.

94. Kruppa, M. and Gary Silverman, “Regulators begin to grapple with DeFi”, *Financial Times*, 26 June 2021, https://www.ft.com/content/e6e7d9d6-7778-4286-ba6f-e5831fcbc538.

95. Carstens, Agustin, et al. “Regulating Big Techs in finance”, *Bank for International Settlements*, 2021 https://www.bis.org/publ/bisbull45.pdf.

96. Restoy, Fernando, *Regulating FinTech: Is an Activity-Based Approach the Solution?,* 16 June 2021, speech presented virtually to the fintech working group at the European Parliament, https://www.bis.org/speeches/sp210616.htm.

97. Crisanto, Juan C. et al. “Big techs in finance: regulatory approaches and policy options”, *Financial Stability Institute/Bank for International Settlements*, 2021, https://www.bis.org/fsi/fsibriefs12.pdf.

98. Schmidt, Chaz, “Harvest Finance - Industrial Automated Yield Farming for All”, *Defi Pulse*, 13 December 2020, https://defipulse.com/blog/harvest-finance-drop/.

99. Mozur, P. et al. “A Global Tipping Point for Reining In Tech Has Arrived”, *The New York Times*, 20 April 2021, https://www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

100. De Meijer, Carlo R.W., “DeFi and Regulation: The European Approach”, *Finextra*, 28 June 2021, https://www.finextra.com/blogposting/20516/defi-and-regulation-the-european-approach.

101. Broeders, Dirk and Jermy Prenio, “Innovative technology in financial supervision (suptech) – the experience of early users”, *Financial Stability Institute,* 2018, "https://www.bis.org/fsi/publ/insights9.pdf.

References (8 of 18)

Risk theme #3 – Gaps in entity-based regulation (continued):

102. Scott, Tim, "Third-Party Risk Is Becoming a First Priority Challenge", *Deloitte*, accessed 18 October 2021, https://www2.deloitte.com/ca/en/pages/risk/articles/reduce-your-third-party-risk.html.
103. Asif, Chandana, et al. "Financial Services Unchained: The Ongoing Rise of Open Financial Data", *McKinsey & Company*, 11 July 2021, https://www.mckinsey.com/industries/financial-services/our-insights/financial-services-unchained-the-ongoing-rise-of-open-financial-data.
104. "Multi-Cloud in Financial Services." *Finextra*, 9 December 2019, https://www.finextra.com/blogposting/18227/multi-cloud-in-financial-services.
105. "2019 Global AML and Financial Crime TechSprint", *Financial Conduct Authority,* accessed 18 October 2021, https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint.
106. Ackerman, Andrew, "Crypto Firms Want Fed Payment Systems Access—and Banks Are Resisting", *The Wall Street Journal*, 28 August 2021, https://www.wsj.com/articles/crypto-firms-want-fed-payment-systems-accessand-banks-are-resisting-11630143002.
107. Berry, Kate, "Why Data Aggregators Want to Be Regulated by CFPB", *American Banker*, 12 February 2021, https://www.americanbanker.com/news/why-data-aggregators-want-to-be-regulated-by-cfpb.
108. Hodel, Lars and Thiemo Pirani, "The Rise of DeFi: Regulatory Thoughts", *Bitcoin Suisse*, 15 February 2021, https://www.bitcoinsuisse.com/outlook/the-rise-of-defi-regulatory-thoughts.
109. "2019 Global AML and Financial Crime TechSprint", *Financial Conduct Authority,* accessed 18 October 2020, https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint.
110. Berry, Kate, "Why Data Aggregators Want to Be Regulated by CFPB", *American Banker*, 12 February 2021, https://www.americanbanker.com/news/why-data-aggregators-want-to-be-regulated-by-cfpb.
111. Napoletano, E. and John Schmidt, "Decentralized Finance Is Building A New Financial System", *Forbes*, 2 April 2021, https://www.forbes.com/advisor/investing/defi-decentralized-finance/.
112. World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, 2021, http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.
113. Crisanto, Juan Carlos and Johannes Ehrentraud, "The Big Tech Risk in Finance", *International Monetary Fund*, May 2021, https://www.imf.org/external/pubs/ft/fandd/2021/05/big-tech-fintech-and-financial-regulation-crisanto-ehrentraud.htm.
114. Manikandan, Ashwin, "RBI Warns against Allowing Big Tech Firms into Financial Services", *The Economic Times*, 1 July 2021, https://economictimes.indiatimes.com/tech/technology/rbi-warns-against-allowing-big-tech-firms-into-financial-services/articleshow/84044019.cms.
115. Hodel, Lars and Thiemo Pirani, "The Rise of DeFi: Regulatory Thoughts", *Bitcoin Suisse*, 15 February 2021, https://www.bitcoinsuisse.com/outlook/the-rise-of-defi-regulatory-thoughts
116. O'Reilly, Monica, "2021 Banking Regulatory Outlook", *Deloitte*, accessed 18 October 2021, https://www2.deloitte.com/us/en/pages/regulatory/articles/banking-regulatory-outlook.html.
117. Reppel, Oliver, "Digital Regulators Are a New Norm in Financial Services", *Accenture*, 18 June 2020, https://bankingblog.accenture.com/digital-regulators-are-a-new-norm-in-financial-services.

References (9 of 18)

Risk theme #3 – Gaps in entity-based regulation (continued):

118. World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, 2021, http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.
119. Nikolic, Bojana, "Financial Regulation for the Digital Age", *SQLPower*, 14 June 2021, https://www.sqlpower.ca/news/financial-regulation-for-the-digital-age/.
120. Zetzsche, Dirk A., et al. "Digital Finance Platforms: Toward a New Regulatory Paradigm", *European Banking Institute (EBI) Working Paper Series*, no. 58, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532975.
121. Crisanto, Juan Carlos and Johannes Ehrentraud, "The Big Tech Risk in Finance", *International Monetary Fund*, May 2021, https://www.imf.org/external/pubs/ft/fandd/2021/05/big-tech-fintech-and-financial-regulation-crisanto-ehrentraud.htm.
122. Bank of England, *Central Bank Digital Currency: Opportunities, challenges and design*, 2020, https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf.
123. Balz, Burkhard, *Burkhard Balz: Opportunities and Risks of Central Bank Digital Currencies*, 17 June 2021, speech presented virtually at the European Payments Conference, https://www.bis.org/review/r210617c.htm.
124. Reppel, Oliver, "Digital Regulators Are a New Norm in Financial Services", *Accenture*, 18 June 2020, https://bankingblog.accenture.com/digital-regulators-are-a-new-norm-in-financial-services.
125. World Economic Forum, *Decentralized Finance (DeFi) Policy-Maker Toolkit*, 2021, http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.
126. Withers, Iain and Huw Jones, "For Bank Regulators, Tech Giants Are Now Too Big to Fail", *Reuters*, 20 August 2021, https://www.reuters.com/world/the-great-reboot/bank-regulators-tech-giants-are-now-too-big-fail-2021-08-20/.
127. Crisanto, Juan Carlos and Johannes Ehrentraud, "The Big Tech Risk in Finance", *International Monetary Fund*, May 2021, https://www.imf.org/external/pubs/ft/fandd/2021/05/big-tech-fintech-and-financial-regulation-crisanto-ehrentraud.htm.
128. Crisanto, Juan C. et al. "Big techs in finance: regulatory approaches and policy options", *Financial Stability Institute/Bank for International Settlements*, 2021, https://www.bis.org/fsi/fsibriefs12.pdf.
129. Restoy, Fernando, *Regulating FinTech: Is an Activity-Based Approach the Solution?,* 16 June 2021, speech presented virtually to the fintech working group at the European Parliament, https://www.bis.org/speeches/sp210616.htm.
130. Nikolic, Bojana, "Financial Regulation for the Digital Age", *SQLPower*, 14 June 2021, https://www.sqlpower.ca/news/financial-regulation-for-the-digital-age/.
131. PA Consulting, *Digital Regulatory Reporting*, 2020, https://www2.paconsulting.com/rs/526-HZE-833/images/DRR-Report-Sept-2020.pdf.
132. "Ellipse: Regulatory Reporting and Data Analytics Platform", *Bank for International Settlements*, accessed 18 October 2021, https://www.bis.org/about/bisih/topics/suptech_regtech/ellipse.htm.

References (10 of 18)

Risk theme #3 – Gaps in entity-based regulation (continued):

133. "Digital Regulatory Reporting", *Financial Conduct Authority*, 1 November 2017, https://www.fca.org.uk/innovation/regtech/digital-regulatory-reporting.
134. Fresh, Adriane and Martin Neil Baily, "What does international experience tell us about regulatory consolidation?", *The PEW Economic Policy Department*, 2009, "https://www.brookings.edu/wp-content/uploads/2016/06/0921_consolidation_baily.pdf.
135. Silverman, G., "Why US regulation is failing the cryptocurrency test" *Financial Times*, 17 July 2021, https://www.ft.com/content/e196014a-c5bc-4b2e-8455-5b5b8d878209.
136. Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance*, 2019, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf.

Risk theme #4 – Conflicting national priorities:

137. Shepard, Michael, "Illicit Finance Imperils Systemic Stability Globally", *The Wall Street Journal*, 22 January 2020, https://deloitte.wsj.com/riskandcompliance/2020/01/22/illicit-finance-imperils-systemic-stability-globally/.
138. World Economic Forum, *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.
139. Carter, William A., "Forces Shaping the Next Generation of Cyber Threats to Financial Institutions", *Center for Strategic and International Studies*, accessed 18 October 2020, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/financial-sector-cybersecurit-1
140. Forrer, John J., "Secondary Economic Sanctions: Effective Policy or Risky Business?", *Atlantic Council*, 21 May 2018, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/secondary-economic-sanctions-effective-policy-or-risky-business/.
141. "BeagleBoyz" *Masergy*, 9 September 2020, https://www.masergy.com/security-alert/beagleboyz.
142. "Geopolitics and Technology Threaten America's Financial Dominance," *The Economist,* 7 May 2020, https://www.economist.com/special-report/2020/05/07/geopolitics-and-technology-threaten-americas-financial-dominance.
143. McCaffrey, Courtney Rickert, et al. "How to Factor Geopolitical Risk into Technology Strategy", *EY,* 10 September 2021, https://www.ey.com/en_gl/geostrategy/ceo-geopolitics-risk-technology-strategy.
144. Byrne, Dan, "Global Money Laundering 'Drains' $1.6 Trillion Annually from World Resources", *AML Intelligence*, 28 September 2020, https://www.amlintelligence.com/2020/09/global-money-laundering-drains-1-6-trillion-annually-from-world-economy/.
145. "Prudential Regulation Authority Business Plan 2021/22", *Bank of England*, 24 May 2021, https://www.bankofengland.co.uk/prudential-regulation/publication/2021/may/pra-business-plan-2021-22.
146. "NIS Directive", *European Commission*, 2020, https://digital-strategy.ec.europa.eu/en/policies/nis-directive.

References (11 of 18)

Risk theme #4 – Conflicting national priorities (continued):

147. "About Global Risk Institute", *Global Risk Institute*, accessed 18 October 2021, https://globalriskinstitute.org/about/.
148. Mee, Paul and Til Schuermann, "How a Cyber Attack Could Cause the next Financial Crisis", *Harvard Business Review*, 14 September 2018, https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis.
149. "Geopolitical Risk Dashboard", *BlackRock*, September 2021, https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard.
150. "What Is Iso 20022?", *SWIFT*, accessed 18 October 2021, https://www.swift.com/standards/iso-20022.
151. "NIS Directive", *European Commission*, accessed 18 October 2021, https://digital-strategy.ec.europa.eu/en/policies/nis-directive.
152. "What is TMNL?", *Transactie Monitoring Nederland*, accessed 18 October 2021, https://tmnl.nl/summary-eng/.
153. "Geopolitical Risk Dashboard", *BlackRock*, September 2021, https://www.blackrock.com/corporate/insights/blackrock-investment-institute/interactive-charts/geopolitical-risk-dashboard.
154. World Economic Forum, *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.
155. Shepard, Michael, et al. "The Global Framework for Fighting Financial Crime", *Deloitte*, 2019, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html.
156. Carter, William A., "Financial Sector Cybersecurity Requirements in the Asia-Pacific Region", *Center for Strategic and International Studies*, accessed 18 October 2021, https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/financial-sector-cybersecurit-1.
157. World Economic Forum, *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.
158. Shepard, Michael, et al. "The Global Framework for Fighting Financial Crime", *Deloitte*, 2019, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html.
159. Ahaskar, Abhijit, "How Cyberattacks Are Being Used by States against Each Other", *Mint*, 21 June 2019, https://www.livemint.com/technology/tech-news/how-cyberattacks-are-being-used-by-states-against-each-other-1561100711834.html.
160. Stumbauer, Sven, "The Top Challenges in Anti-Money Laundering and Sanctions Compliance", *International Banker*, 31 August 2021, https://internationalbanker.com/finance/the-top-challenges-in-anti-money-laundering-and-sanctions-compliance/.
161. Scroxton, Alex, "Nation-State Cyber Attacks Double in Three Years", *ComputerWeekly.com*, 8 April 2021, https://www.computerweekly.com/news/252499042/Nation-state-cyber-attacks-double-in-three-years.

References (12 of 18)

Risk theme #4 – Conflicting national priorities (continued):

162. Cline, Mary and Courtney Rickert McCaffrey, "Without Understanding Geopolitical Risk, How Can You Successfully Transform?", *EY*, 24 July 2020, https://www.ey.com/en_ca/geostrategy/how-to-manage-political-risk-in-a-post-pandemic-world.

163. Tata Consultancy Services, *Anti-Money Laundering: Challenges and Trends*, 2017, https://www.tcs.com/content/dam/tcs/pdf/Industries/Banking%20and%20Financial%20Services/Anti-Money%20Laundering%20-%20Challenges%20and%20trends.pdf.

164. "Ransomware Prevention", *Deep Instinct*, accessed 18 October 2021, https://www.deepinstinct.com/preventing-ransomware/.

165. Stumbauer, Sven, "The Top Challenges in Anti-Money Laundering and Sanctions Compliance", *International Banker*, 31 August 2021, https://internationalbanker.com/finance/the-top-challenges-in-anti-money-laundering-and-sanctions-compliance/.

166. Shepard, Michael, et al. "The Global Framework for Fighting Financial Crime", *Deloitte*, 2019, https://www2.deloitte.com/global/en/pages/financial-services/articles/gx-global-framework-for-fighting-financial-crime.html.

167. Ungphakorn, Peter, "The United Kingdom-Switzerland Trade Agreements", *EU Relations Law*, 28 January 2021, https://eurelationslaw.com/blog/the-united-kingdom-switzerland-trade-agreements.

168. "Four Belgian Banks Including BNP Paribas, Ing to Share Corporate KYC Data Using Blockchain", *TokenPost*, accessed 18 October 2021, https://tokenpost.com/Four-Belgian-banks-including-BNP-Paribas-ING-to-share-corporate-KYC-data-using-blockchain-4884.

169. "What is TMNL?", *Transactie Monitoring Nederland*, accessed 18 October 2021, https://tmnl.nl/summary-eng/.

170. Mcguire, Michael, *Nation States, Cyberconflict And The Web Of Profit*, HP Wolf Security, 2021, https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf.

171. "How to Prevent Cyber Attacks – Including Escalating Nation State-Sponsored Attacks", *LMG Security*, 27 July 2021, https://www.lmgsecurity.com/how-to-prevent-cyber-attacks-including-escalating-nation-state-sponsored-attacks/.

172. World Economic Forum, *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

173. "Beating Financial Crime: Commission Overhauls Anti-Money Laundering and Countering the Financing of Terrorism Rules", *European Commission*, 20 July 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3690.

174. Bank for International Settlements, *Nexus: A Blueprint for Instant Cross-Border Payments*, 2021, https://www.bis.org/publ/othp39.pdf.

175. World Economic Forum, *A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy*, 2020, http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

References (13 of 18)

Risk theme #4 – Conflicting national priorities (continued):

176. Dascoli, Luke and Nigel Cory, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", *Information Technology and Innovation Foundation*, 19 July 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.
177. Rahman, Shahriar, et al. "Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption", *IEEE Transactions on Engineering* Management, 2021, pp 1-11, https://www.researchgate.net/figure/Cross-border-data-sharing-platform-architecture_fig2_338495342.
178. Kramer, Baldwin, et al. "Deloitte Connects 5 Dutch Banks to Make an Impact with Transaction Monitoring Netherlands (TMNL)", *Deloitte*, accessed 18 October 2021, https://www2.deloitte.com/nl/nl/pages/financial-services/articles/5-dutch-banks-to-make-an-impact-with-transaction-monitoring-netherlands-tmnl.html.
179. "Four Belgian Banks Including BNP Paribas, Ing to Share Corporate KYC Data Using Blockchain", *TokenPost*, accessed 18 October 2021, https://tokenpost.com/Four-Belgian-banks-including-BNP-Paribas-ING-to-share-corporate-KYC-data-using-blockchain-4884.
180. Mcguire, Michael, *Nation States, Cyberconflict And The Web Of Profit*, HP Wolf Security, 2021, https://threatresearch.ext.hp.com/wp-content/uploads/2021/04/hp-bps-web-of-profit-report_APR_2021.pdf.
181. "Kaspersky Threat Attribution Engine", *Kaspersky*, accessed 18 October 2021, https://www.kaspersky.com/enterprise-security/cyber-attack-attribution-tool.

Risk theme #5 – Emerging sources of influence:

182. Feyen, Erik, et al. "Fintech and the digital transformation of financial services: implications for market structure and public policy", *Bank for International Settlements*, July 2021, https://www.bis.org/publ/bppdf/bispap117.pdf.
183. Nann, Stefan, "How Does Social Media Influence Financial Markets?", *Nasdaq*, 14 October 2019, https://www.nasdaq.com/articles/how-does-social-media-influence-financial-markets-2019-10-14.
184. Brauchle, Jan-Philipp, et al. "Cyber Mapping the Financial System", *Carnegie Endowment for International Peace*, 7 April 2021, https://carnegieendowment.org/2020/04/07/cyber-mapping-financial-system-pub-81414.
185. The Alan Turing Institute, *Tackling threats to informed decision-making in democratic societies*, 2020, https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf.
186. Feyen, Erik, et al. "Fintech and the digital transformation of financial services: implications for market structure and public policy", *Bank for International Settlements*, July 2021, https://www.bis.org/publ/bppdf/bispap117.pdf.
187. Murphy, Hannah and Philip Stafford, "How cultish social media accounts fuel trading in penny stocks", *Financial Times*, 18 May 2021, https://www.ft.com/content/0ac9ecba-7408-4466-81ed-ae15f6333e36.
188. Holger, Dieter, "Young Investors Flock to Discord and Telegram for Financial Advice", *The Wall Street Journal*, 4 May 2021, https://www.wsj.com/articles/young-investors-flock-to-discord-and-telegram-for-financial-advice-11620141750.

References (14 of 18)

Risk theme #5 – Emerging sources of influence (continued):

189. Bateman, Jon, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios", *Carnegie Endowment for International Peace*, 8 July 2021, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

190. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.

191. Holmes, Chris, "The Perks and Dangers of the Democratisation of Finance", *Finextra*, 3 March 2021, https://www.finextra.com/blogposting/19968/the-perks-and-dangers-of-the-democratisation-of-finance.

192. Brauchle, Jan-Philipp, et al. "Cyber Mapping the Financial System", *Carnegie Endowment for International Peace*, 7 April 2021, https://carnegieendowment.org/2020/04/07/cyber-mapping-financial-system-pub-81414.

193. Robinson, Matt, "U.S. SEC Sues Crypto Platform BitConnect in US$2B Fraud", *BNN Bloomberg*, 1 September 2021, https://www.bnnbloomberg.ca/u-s-sec-sues-crypto-platform-bitconnect-in-us-2b-fraud-1.1646888.

194. Michaels, Dave, "Robinhood Agrees to Pay $70 Million to Settle Regulatory Investigation", *The Wall Street Journal*, 30 June 2021, https://www.wsj.com/articles/robinhood-agrees-to-pay-70-million-to-settle-regulatory-investigation-11625063765.

195. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.

196. "Codes of Practice", *POFMA Office, Government of Singapore*, accessed 18 October 2021, https://www.pofmaoffice.gov.sg/regulations/codes-of-practice/.

197. Murphy, Hannah and Philip Stafford, "How cultish social media accounts fuel trading in penny stocks", *Financial Times*, 18 May 2021, https://www.ft.com/content/0ac9ecba-7408-4466-81ed-ae15f6333e36.

198. Holmes, Chris, "The Perks and Dangers of the Democratisation of Finance", *Finextra*, 3 March 2021, https://www.finextra.com/blogposting/19968/the-perks-and-dangers-of-the-democratisation-of-finance.

199. Lomas, Natasha, "Google Tightens UK Policy on Financial Ads after Watchdog Pressure over Scams", *TechCrunch*, 30 June 2021, https://social.techcrunch.com/2021/06/30/google-tightens-uk-policy-on-financial-ads-after-watchdog-pressure-over-scams/.

200. "SEC Calls for Feedback on Trading App Gamification", *Finextra*, 30 August 2021, https://www.finextra.com/newsarticle/38728/sec-calls-for-feedback-on-trading-app-gamification.

201. Nann, Stefan, "How Does Social Media Influence Financial Markets?", *Nasdaq*, 14 October 2019, https://www.nasdaq.com/articles/how-does-social-media-influence-financial-markets-2019-10-14.

202. Michaels, Dave, "Robinhood Agrees to Pay $70 Million to Settle Regulatory Investigation", *The Wall Street Journal*, 30 June 2021, https://www.wsj.com/articles/robinhood-agrees-to-pay-70-million-to-settle-regulatory-investigation-11625063765.

References (15 of 18)

Risk theme #5 – Emerging sources of influence (continued):

203. Lomas, Natasha, "Google Tightens UK Policy on Financial Ads after Watchdog Pressure over Scams", *TechCrunch*, 30 June 2021, https://social.techcrunch.com/2021/06/30/google-tightens-uk-policy-on-financial-ads-after-watchdog-pressure-over-scams/.
204. Nann, Stefan, "How Does Social Media Influence Financial Markets?", *Nasdaq*, 14 October 2019, https://www.nasdaq.com/articles/how-does-social-media-influence-financial-markets-2019-10-14.
205. Newmyer, Tory and David J. Lynch, "GameStop Frenzy Leaves behind a Mess for Wall Street Regulators", *The Washington Post*, 3 February 2021, https://www.washingtonpost.com/business/2021/02/03/gamestop-sec-regulation/.
206. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.
207. Bateman, Jon, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios", *Carnegie Endowment for International Peace*, 8 July 2021, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.
208. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.
209. Holmes, Chris, "The Perks and Dangers of the Democratisation of Finance", *Finextra*, 3 March 2021, https://www.finextra.com/blogposting/19968/the-perks-and-dangers-of-the-democratisation-of-finance.
210. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.
211. Bateman, Jon, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios", *Carnegie Endowment for International Peace*, 8 July 2021, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.
212. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.
213. The Alan Turing Institute, *Tackling threats to informed decision-making in democratic societies*, 2020, https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf.
214. Boeddu, Gian, et al. "Addressing Consumer Risks in FinTech to Maximize Its Benefits", *World Bank Blogs*, 26 May 2021, https://blogs.worldbank.org/psd/addressing-consumer-risks-fintech-maximize-its-benefits.
215. Khan, Roomy, "Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected", *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.

References (16 of 18)

Risk theme #5 – Emerging sources of influence (continued):

216. Murphy, Hannah and Philip Stafford, “How cultish social media accounts fuel trading in penny stocks”, *Financial Times*, 18 May 2021, https://www.ft.com/content/0ac9ecba-7408-4466-81ed-ae15f6333e36.

217. Bateman, Jon, “Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios”, *Carnegie Endowment for International Peace*, 8 July 2021, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237

218. Levine, Matt, “Money Stuff: Putting the Meme Stocks in the Index”, *Bloomberg*, 1 September 2021, https://www.bloomberg.com/news/newsletters/2021-09-01/putting-meme-stocks-like-gamestop-in-the-sp-500-index.

219. Glossman, Diane, et al, “Robinhood and GameStop: Essential Issues and Next Steps for Regulators and Investors”, *The Harvard Law School Forum on Corporate Governance*, 23 February 2021, https://corpgov.law.harvard.edu/2021/02/23/robinhood-and-gamestop-essential-issues-and-next-steps-for-regulators-and-investors/.

220. Gonzalez, Oscar and David Priest, “Robinhood Backlash: What You Should Know about the GameStop Stock Controversy”, *CNET*, 17 March 2021, https://www.cnet.com/personal-finance/investing/robinhood-backlash-what-you-should-know-about-the-gamestop-stock-controversy/.

221. Khan, Roomy, “Social Media Fueled Stock Market Trading: The Unsuspecting Need To Be Protected”, *Forbes*, 8 March 2021, https://www.forbes.com/sites/roomykhan/2021/03/08/social-media-fueled-stock-market-trading-the-unsuspecting-need-to-be-protected/.

222. Aslam, Nida, et al, "Fake Detect: A Deep Learning Ensemble Model for Fake News Detection", *Complexity*, 2021, https://www.hindawi.com/journals/complexity/2021/5557784/.

223. Ehret, Todd, “SEC’s Advanced Data Analytics Helps Detect Even the Smallest Illicit Market Activity”, *Reuters*, 30 June 2017, https://www.reuters.com/article/bc-finreg-data-analytics-idUSKBN19L28C.

224. “Digital delivery of financial education: design and practice”, *OECD*, 2021, https://www.oecd.org/financial/education/Digital-delivery-of-financial-education-design-and-practice.pdf.

225. Glossman, Diane, et al, “Robinhood and GameStop: Essential Issues and Next Steps for Regulators and Investors”, *The Harvard Law School Forum on Corporate Governance*, 23 February 2021, https://corpgov.law.harvard.edu/2021/02/23/robinhood-and-gamestop-essential-issues-and-next-steps-for-regulators-and-investors/.

226. Sun, Xiaomeng, “Exploration and Practice of “Internet + Maker Education” University Innovative Entrepreneurship Education Model From the Perspective of Positive Psychology”, *Frontiers in Psychology*, June 2020, https://www.researchgate.net/figure/The-construction-diagram-for-the-Internet-platform-of-maker-education_fig1_342021712.

227. The Alan Turing Institute, *Tackling threats to informed decision-making in democratic societies*, 2020, https://www.turing.ac.uk/sites/default/files/2020-10/epistemic-security-report_final.pdf.

228. Islam, Md. Rafiqul, et al. “Deep Learning for Misinformation Detection on Online Social Networks: A Survey and New Perspectives”, *Social Network Analysis and Mining*, 29 September 2020, https://link.springer.com/article/10.1007/s13278-020-00696-x.

References (17 of 18)

Risk theme #6 – New drivers of financial exclusion:

229. "The Global Findex Database 2017: The Unbanked", *The World Bank Group*, 2017, https://globalfindex.worldbank.org/chapters/unbanked.
230. Turner, Ash, "How Many Smartphones are in the World?", *BankMyCell*, 1 September 2021, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.
231. Świątkowska, Joanna. Tackling Cybercrime to Unleash Developing Countries' Digital Potential. The Pathways for Prosperity Commission on Technology and Inclusive Development , Jan. 2020, https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf.
232. Kassai, Husayn, "Stop Talking about Financial Inclusion. Identity Inclusion Must Come First", *World Economic Forum*, 11 April 2018, https://www.weforum.org/agenda/2018/04/stop-talking-about-financial-inclusion-identity-inclusion-must-come-first/.
233. Senyo, PK., "Ghana's New Mobile Money Rule Could Derail Financial inclusion. but There Are Answers", *The Conversation*, 18 April 2021, https://theconversation.com/ghanas-new-mobile-money-rule-could-derail-financial-inclusion-but-there-are-answers-158770.
234. Peters, Allison, and Amy Jordan, "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime", *Third Way*, 2 October 2019, https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime.
235. Duff, Schan, "A Growing Trend in Financial Regulation: Thematic Sandboxes", *CGAP*, 14 February 2019, https://www.cgap.org/blog/growing-trend-financial-regulation-thematic-sandboxes.
236. Hersey, Frank, "Mastercard Partnership to Capture Biometrics of 30 million Africans", *BiometricUpdate.com*, 10 September 2021, https://www.biometricupdate.com/202109/mastercard-partnership-to-capture-biometrics-of-30-million-africans.
237. Hall, Christine, "FinTech Startups Target Younger Audiences, Investor Interest in Financial Literacy", *Crunchbase News*, 5 February 2021, https://news.crunchbase.com/news/fintech-startups-target-younger-audiences-investor-interest-in-financial-literacy/.
238. "European Commission Proposes Revisions to Consumer Credit Rules", *Finextra*, 1 July 2021, https://www.finextra.com/pressarticle/88411/european-commission-proposes-revisions-to-consumer-credit-rules.
239. Hersey, Frank, "Mastercard Partnership to Capture Biometrics of 30 million Africans", *BiometricUpdate.com*, 10 September 2021, https://www.biometricupdate.com/202109/mastercard-partnership-to-capture-biometrics-of-30-million-africans.
240. "Niyo Bharat Announces Financial Literacy Initiative for Indians", *The Paypers*, 4 May 2020, https://thepaypers.com/e-invoicing-supply-chain-finance/niyo-bharat-announces-financial-literacy-initiative-for-indians--1242099.
241. Turner, Ash, "How Many Smartphones are in the World?", *BankMyCell*, 1 September 2021, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world.
242. The World Bank, *1.1 Billion 'Invisible' People without ID Are Priority for New High Level Advisory Council on Identification for Development* [Press release], 12 October 2017, https://www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development.

References (18 of 18)

Risk theme #6 – New drivers of financial exclusion (continued):

243. Manyika, James, et al. “What Do We Do about the Biases in AI?”, *Harvard Business Review*, 25 October 2019, https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai.

244. Chen, Haoyu, et al. “Counterfactual Fairness through Data Preprocessing”, *OpenReview.net*, 5 March 2021, https://openreview.net/forum?id=21aG-pxQWa.

245. Schmelzer, Ron, “Understanding Explainable AI”, *Forbes*, 23 July 2019, https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/?sh=272c06577c9e.

246. Scanlon, Luke, “AI in Financial Services: Addressing the Risk of Bias”, *Pinsent Masons*, 8 July 2020, https://www.pinsentmasons.com/out-law/analysis/ai-financial-services-risk-of-bias.

247. Widiyasari, Vira, and Herman Widjaja. “This New Approach to Credit Scoring Is Accelerating Financial Inclusion in Emerging Economies.” World Economic Forum, 20 Jan. 2021, https://www.weforum.org/agenda/2021/01/this-new-approach-to-credit-scoring-is-accelerating-financial-inclusion/.

248. Visa, *Assessing the Role of Biometrics in Advancing Financial Inclusion*, 2019, https://usa.review.visa.com/content/dam/VCOM/regional/na/us/about-visa/documents/assessing-the-role-of-biometrics-in-financial-inclusion-visa.pdf.

249. Widiyasari, Vira, and Herman Widjaja. “This New Approach to Credit Scoring Is Accelerating Financial Inclusion in Emerging Economies.” World Economic Forum, 20 Jan. 2021, https://www.weforum.org/agenda/2021/01/this-new-approach-to-credit-scoring-is-accelerating-financial-inclusion/.

250. “Counterfactual Fairness”, *The Alan Turing Institute*, accessed 18 October 2021, https://www.turing.ac.uk/research/research-projects/counterfactual-fairness.

251. Visa, *Assessing the Role of Biometrics in Advancing Financial Inclusion*, 2019, https://usa.review.visa.com/content/dam/VCOM/regional/na/us/about-visa/documents/assessing-the-role-of-biometrics-in-financial-inclusion-visa.pdf

252. Hersey, Frank, “Mastercard Partnership to Capture Biometrics of 30 million Africans”, *BiometricUpdate.com*, 10 September 2021, https://www.biometricupdate.com/202109/mastercard-partnership-to-capture-biometrics-of-30-million-africans.

253. Sudhir, K., and Shyam Sunder, “What Happens When a Billion Identities Are Digitized?”, *Yale Insights*, 27 March 2020, https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized.

Conclusion:

254. Renjen, Punit, “The Perseverance of Resilient Leadership: Sustaining Impact on the Road to Thrive”, *Deloitte*, 6 August 2020, https://www2.deloitte.com/global/en/insights/economy/covid-19/sustaining-resilient-leadership-covid-19.html

255. Deloitte, *The Future of Risk in Financial Services*, 2017, https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/financial-services/deloitte-cn-fs-future-of-risk-en-171020.PDF.


WORLD
ECONOMIC
FORUM