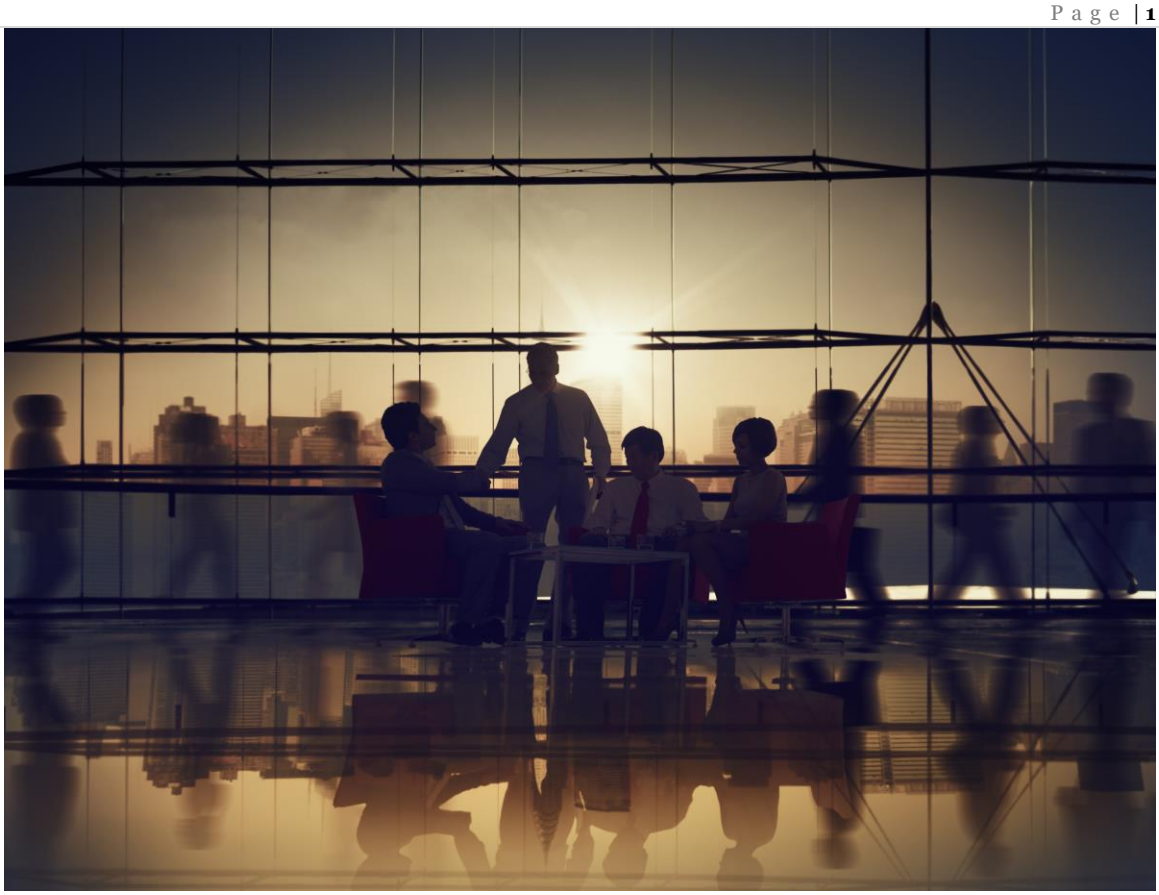


News for the Board of Directors, November 2023

The UK Secretary of State for Science, Innovation, and Technology the Rt Hon Michelle Donelan MP took the decision to establish the UK-US data bridge and lay adequacy regulations in Parliament to this effect.

The Secretary of State took this decision, under Section 17A of the Data Protection Act 2018, to establish a data bridge with the United States of America through the UK Extension to the EU-US Data Privacy Framework.

The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US.

This decision was based on their determination that the framework maintains high standards of privacy for UK personal data.

Adequacy regulations have been laid in Parliament today (21 September 2023) to give effect to this decision.

UK businesses and organisations will be able to make use of this data bridge to safely and securely transfer personal data to certified organisations in the US, once the regulations come into force from the 12 October.

Supporting this decision, the US Attorney General, on the 18 September, designated the UK as a 'qualifying state' under Executive Order 14086.

This will allow all UK individuals whose personal data has been transferred to the US under any transfer mechanisms (i.e. including those set out under UK GDPR Articles 46 and 49) access to the newly established redress mechanism in the event that they believe that their personal data has been accessed unlawfully by US authorities for national security purposes.

The laying of the SI today follows on from an announcement earlier in the year which highlighted the data bridge as a key deliverable for 2023 under the UK-US Comprehensive Dialogue on Technology and Data.

A commitment in principle to establish the data bridge was also announced by the Prime Minister and President Biden in June this year as part of the Atlantic Declaration.

Data bridges

1. The term 'data bridge' is our preferred public terminology for 'adequacy', and describes the decision to permit the flow of personal data from the UK to another country without the need for further safeguards. It symbolises the connection between destinations that is established by these decisions and encapsulates the UK's collaborative approach with our international partners.

2. Data bridges are not reciprocal, therefore they do not allow the free flow of data from other countries to the UK. Instead, a data bridge ensures that the level of protection for UK individuals' personal data under UK GDPR is maintained.

3. A data bridge assessment takes into account, amongst other things, the protection the country provides for personal data, the rule of law, respect for human rights and fundamental freedoms, and the existence and effective functioning of a regulator.

4. Data bridges secure the free and safe exchange of personal data across borders, from the UK to another country. They unlock growth for businesses, allow us to share crucial information for life-saving research, and encourage science and innovation across borders.

   Reducing barriers to data sharing also makes things better for consumers, opening up opportunities for higher-quality services and lower prices on things they pay for.

Data Privacy Framework

1. The EU-US Data Privacy Framework is a bespoke, opt-in certification scheme for US companies, enforced by the Federal Trade Commission (FTC) and Department of Transportation (DoT), and administered by the Department of Commerce (DoC).

2. The Data Privacy Framework includes a set of enforceable principles and requirements that must be certified to, and complied with, in order for US organisations to be able to join the Data Privacy Framework. These principles take the form of commitments to data protection and govern how an organisation uses, collects and discloses personal data.

3. This replaces the previous Privacy Shield framework, established in 2016 to provide a legal basis for companies to comply with EU data protection requirements when transferring personal data to the US.

4. The UK has established a data bridge for the "UK Extension to the Data Privacy Framework" that allows certified US companies to sign-up to be able to receive UK personal data through the framework.

5. We will continue to monitor the Data Privacy Framework to ensure that it functions as intended, as part of the Department for Science, Innovation and Technology (DSIT's) requirement to monitor data bridges.

6. The US 'designation' of the UK relates to the US Executive Order 14086 ("Enhancing Safeguards for United States Signals Intelligence Activities") which created an independent and binding redress mechanism which can be accessed by individuals whose personal data is transferred from qualifying states.

7. The UK's designation as a qualifying state therefore allows UK individuals to seek redress if they believe their personal data was collected or processed through US signals intelligence in a manner that violated applicable US law.

8. This is a new and important safeguard that the US introduced to address the concerns raised in the 2020 Schrems II judgment, in preparation for the operationalisation of the new Data Privacy Framework.

9. Designation by the US of the UK was an important factor that led to the data bridge assessment being successful, providing increased safeguards and redress mechanisms for UK individuals.

Privacy

1. A data bridge ensures high protection for UK individuals when their data is transferred to another country. As discussed above, the US has introduced new rules and practices relating to government access to data which the UK has access to as a designated country.

2. In establishing this data bridge, we have taken steps to ensure the level of protection people in the UK enjoy under the UK GDPR is not undermined.

   That includes closely assessing the level of protection of personal data under the Data Privacy Framework, as well as the wider legal and regulatory system.

The US data bridge will ensure that high standards of protection for personal data are maintained when the data is sent to certified US organisations.

Any US company that elects to receive UK data under the data bridge will be required to maintain those standards.

3. Protecting individuals' privacy – particularly when it comes to their most sensitive information – is paramount. Under the data bridge, the level of protection your personal data has within UK GDPR will be maintained.

4. The data bridge will not remove the obligations of UK companies under UK data protection law to ensure that data, especially sensitive health data, is properly protected and the rights of data subjects upheld, including when they make decisions about transferring data to other organisations.

   The data bridge will ensure that these high standards of protection and privacy travel with the data when it leaves the UK to reach certified US organisations.

To read more: https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer

https://assets.publishing.service.gov.uk/media/650c4c7efbd7bc000de54786/factsheet_for_uk_organisations.pdf

Openness beats fragmentation

Andrew Bailey, Governor of the Bank of England, at the Central Bank of Ireland's 2nd Financial Services Conference, Dublin

It's a great pleasure to be in Dublin today, at the Financial System Conference, and at the Aviva Stadium – though the old-time rugby fan in me has to be reminded not to say Lansdowne Road.

I am going to use my time today to talk about openness and the risk of fragmentation, both in the world economy and the financial system. Ireland is one of the most open economies in the world, and the UK is also an open economy. I will say at the outset, to avoid any doubt, that I am a strong advocate of free trade and open economies.

It can sometimes be challenging when the economy is exposed to big external shocks – and we have been experiencing, and sadly continue to do so, some very big ones of late - but there are very substantial and continuous benefits from free trade, investment and open markets both in goods and in financial services.

That said, we have to recognise that today we live in a world economy which is experiencing fragmentation, and that is at risk of further such pressure.

The World Trade Organisation has recently reported that the share of so-called intermediate goods in world trade – these are the goods that form inputs to the final product – fell to 48.5% in the first half of this year, compared to an average of 51% in the previous 3 years. This is an indicator of pressure on global supply chains.

Covid was an important first shock to the supply chain system, and I will include in this the disruption to global supply chains that we saw in the early part of the recovery from the severe initial impact of Covid on the world economy. It means that extended just-in-time supply chains have moved from being a perceived source of strength to a perceived vulnerability, hence the reduction in the share of trade accounted for by intermediate goods.

This is not, however, the end of the story on fragmentation in the world economy.

Russia's illegal and utterly reprehensible invasion and war on Ukraine has been a further source of economic disruption and fragmentation – notably in energy and food supplies – which has seriously disrupted supply chains and economic conditions.

Let me also add a comment which relates to events nearer to home. As a public official I take no position on Brexit per se. That was a decision for the people of the UK. It has led to a reduction in the openness of the UK economy, though over

time new trading relationships around the world should, and I expect will, be established. Of course, that requires a commitment to openness and free trade.

To sum up this part of the story: we have moved from a state of affairs where the orthodoxy was to open up the world economy, to increase trade flows, and increase the flows of finance to support this trade. In doing so, yes there was an increase in interlinkages and dependencies around the world economy. Some of those interlinkages turned out to be less resilient than we had expected.

We can't ignore that for the sake of free trade idealism, because the threats that are behind it are sadly real. But, nor must we give up on openness. Diversifying supply chains to increase resilience does not need to involve protectionism. Let me end this part of my remarks on a note of optimism. Recently, as part of my regular visits around the country, I was in Newry in Northern Ireland meeting firms and schools.

It was a most enjoyable day, and I came away with a real sense of optimism of businesses taking up the opportunities of open economies.

This conference is about the financial system, so in the rest of my remarks I am going to focus on openness in the world of financial services. The theme will however be the same, openness is a good thing. But in the world of regulated industries, we have to set out carefully what we mean and how it works.

Just as reducing openness does the same thing to economic growth, so fragmentation damages financial markets. But it doesn't just reduce the size of markets, it makes them inherently less stable. Fragmentation is a risk to financial stability.

Put simply, large markets and their infrastructures, which are run safely and to high standards, will support rather than endanger financial stability. A very good example of this is clearing and central counterparties. Fragmenting this type of market infrastructure creates rather than reduces risks in markets. It also increases the cost of market functioning.

I want to focus a little bit on the point about whether there is, or is not, good reason to restrict and fragment. Inevitably, with such financial infrastructures, they have to be located in a single place, and become the responsibility of that place in terms of their safety, soundness and stability. Yet they are, as the IMF has rightly said, a global public good.

So, the responsibility of those who operate and regulate such infrastructures is a large one, and one that must hold good at all times. This requires accountability and transparency.

Likewise, it is important to have global standards for the operation and oversight of such infrastructures, and strong co-operation among the interested countries – not just where the operator is located but also those where firms which use the infrastructure and depend on it are located.

The UK – as home to multiple financial infrastructures which are systemic outside the UK, including some of the world's largest clearing houses – takes these responsibilities very seriously. And we have recently enshrined in law our commitment to consider the effects of UK standards on the financial stability of countries where our clearing houses provide services.

A necessary foundation for such openness in the financial system more broadly is robust global standards and trust. I think we have made huge steps forward on this front since the global financial crisis. The standards and expectations are stronger, and the co-operation is real and deep-seated.

At the heart of this is the global Financial Stability Board, and the so-called standard setting bodies, the Basel Committee for banks, CPMI and IOSCO for payments, infrastructure, securities and investment markets, and the IAIS for insurance. Our two central banks, in Ireland and the UK, work very closely together in these bodies.

The consequence of all this activity is much stronger standards, and in my view an overwhelming case for rejecting the false allure of fragmentation.

To read more:
https://www.bankofengland.co.uk/speech/2023/november/andrew-bailey-keynote-address-at-the-central-bank-of-ireland

Financial stability - resilience and challenges

Lisa D Cook, Member of the Board of Governors of the Federal Reserve System, at Duke University, Durham, North Carolina.

I am delighted to be back at Duke University after spending many summers of my childhood here with my family visiting my uncle and his family.

As you might know, my uncle Samuel DuBois Cook was a political theorist and the first African American professor tenured at Duke and at a major southern university.

My family and I have many fond memories on this campus. I am also happy to be with you in the Economics Department today to discuss financial stability.

My own work as an academic has frequently reinforced the importance of financial stability in the United States and abroad.

Early in my career, I examined the impact of underdevelopment in the Russian banking system on growth in post-Soviet Russia and the instability that can occur in a poorly regulated financial system.

Years later, as an economist on the Council of Economic Advisers, I saw how weaknesses in the financial system contributed to instability in the euro area.

These formative experiences shaped my view that the Federal Reserve's work on financial stability is critical to the well-being of households, businesses, and the broader economy.

This is one reason I particularly value the opportunity to serve on the Board's Committee on Financial Stability.

I will focus my remarks on my assessment of financial stability risks, based on the Federal Reserve's framework for monitoring vulnerabilities in the financial system.

In my view, our financial system is substantially more resilient than it was in the mid-2000s, reflecting progress by regulators and the private sector in boosting resilience.

That said, we cannot be complacent, and I see some important risks.

Achieving the Federal Reserve's dual mandate of maximum employment and stable prices depends on a stable financial system.

We all saw how the Global Financial Crisis triggered the Great Recession and brought misery to countless millions who lost their jobs, homes, or investments.

A stable financial system provides households, communities, and businesses with the financing they need to invest, grow, and participate in a well-functioning economy— even when hit by adverse events or "shocks."

Consistent with this view of financial stability, our framework for how we think about this goal—as laid out in our Financial Stability Report (FSR), which was just released in October—distinguishes between shocks to, and vulnerabilities of, the financial system.

Importantly, and as we economists know, we cannot predict exogenous shocks, which are, by definition, the surprise events that will hit the financial system and economy.

By contrast, vulnerabilities—the aspects of the financial system that would exacerbate stress—tend to build up over time and can be identified, assessed, and monitored.

In the example of the Global Financial Crisis, although it was widely recognized that housing valuations were high, the magnitude of the ensuing price drop was unexpected, or a shock.

That shock was amplified by vulnerabilities that had built up within the financial system over time, including weak bank capital, excessive household debt, lax lending standards, and fragile short-term wholesale funding.

To read more:
https://www.federalreserve.gov/newsevents/speech/cook20231106a.htm

2023 Bank Failures - Preliminary lessons learnt for resolution

FSB FINANCIAL STABILITY BOARD

Executive summary

The bank failures of the first quarter of 2023 constitute the first real test at a larger scale of the international resolution framework established by the Key Attributes of Effective Resolution Regimes for Financial Institutions ("Key Attributes") in the aftermath of the Global Financial Crisis.

The Financial Stability Board (FSB) announced publicly that it would review the lessons to be learnt from the recent actions taken by the authorities to resolve financial institutions for the operation of the international resolution framework.

FSB FINANCIAL STABILITY BOARD

2023 Bank Failures

Preliminary lessons learnt for resolution

Over the period between March and September 2023, the FSB has reviewed the recent events in Switzerland, the United States (US), and the United Kingdom (UK) and assessed potential implications for the FSB's resolution framework as set out in the FSB Key Attributes.

This report identifies preliminary lessons learnt regarding the FSB Key Attributes' framework for

(i) resolving a global systemically important bank (G-SIB), drawing on an analysis of the Credit Suisse case; and

(ii) the resolution of systemically important banks more broadly, drawing on the recent bank failure episodes in the US.

Introduction 4
1. Preliminary lessons learnt from the Credit Suisse case for G-SIB resolution and resolution planning 5
1.1. Background on the Credit Suisse case 5
1.2. Implications of the Credit Suisse episode for the FSB Resolution Framework 10
1.3. Strengths of the existing framework 11
1.4. Challenges of the Credit Suisse case 13
2. Preliminary lessons learnt from the US bank failures for deposit insurance and systemic importance of non-G-SIBs 18
2.1. Background on the US bank failures 18
2.2. Implications of the US episode 21
2.3. Strengths of the existing framework 23
2.4. Challenges of the US cases 23
3. Issues to be further explored 27
3.1. Effective public sector backstop funding mechanisms to support resolution and restore market confidence 28
3.2. Choice of resolution strategies and optionality of resolution tools 28
3.3. Communications, coordination, and speed of bank runs 29
3.4. Operationalisation of bail-in 30
3.5. Post-stabilisation restructuring 31
3.6. Resolution of banks that could be systemic in failure 31
3.7. Uninsured deposits and the role of deposit insurance in resolution 31
Annex: Overview of the Key Attributes 33
Abbreviations 34

G-SIB resolution and the Credit Suisse case

Following long-standing difficulties and extreme episodes of liquidity stress in October 2022 and March 2023, Credit Suisse was acquired by UBS, supported by ample liquidity facilities including a public liquidity backstop, a second-loss guarantee from the Swiss government, and a write-down of Additional Tier 1 (AT1) bonds.

The actions by the Swiss authorities to facilitate a commercial transaction outside of resolution supported financial stability and the global operations of Credit Suisse. At the same time, it raises the question why resolution was not the chosen path despite it being an executable alternative at that time in light of preparations made.

The Swiss authorities had concerns about the ability of the prepared resolution strategy to address the crisis of confidence at Credit Suisse.

This report seeks to set out a clear understanding of the Swiss authorities' actions with a view to drawing lessons for the international resolution framework.
Since the summer of 2022, the Swiss Financial Market Supervisory Authority (FINMA) had initiated intensive meetings of the Crisis

Management Group (CMG), which included home and key host authorities of Credit Suisse.

In collaboration with the CMG, FINMA had conducted two valuations for the purpose of bail-in resolution (in November 2022 and March 2023), suggesting that if FINMA had pursued a full bail-in, Credit Suisse would have reopened with a consolidated Common Equity Tier 1 (CET1) ratio of about 44% of risk weighted assets (RWAs).

It was also established that Credit Suisse did not have any known retail Total Loss-Absorbing Capacity (TLAC) bond holders. FINMA had addressed, in good cooperation with the Bank of England (BoE), Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC) and Securities and Exchange Commission (SEC), several technical issues to prepare for resolution.

CMG members worked on recognition aspects, as applicable, and the near-final draft documents were distributed to the CMG members.

Based on the review conducted by the FSB, it appears that the resolution planning work of the past decade, the availability of loss-absorbing resources, the collaboration that took place within the CMG in the months leading up to the failure of Credit Suisse, and the efforts of Swiss and host authorities to address remaining obstacles had put authorities in a position to conduct a single point-of-entry (SPE) resolution, if desired.

Indeed, the host authorities involved confirmed their readiness to support the execution of the SPE resolution and their confidence that resolution could be undertaken.

At the same time, the Credit Suisse case highlighted a number of important issues for the effective implementation of the international resolution framework that merit further attention as part of the future work of the FSB. Among these are the need for an effective public sector liquidity backstop and operational readiness of banks to access it as a last resort. In addition, firms and authorities need to:

(i) address the legal issues identified in the execution of bail-in across borders in the course of resolution planning,

(ii) better operationalise a range of resolution options such as transfer and sale of business tools alone or in combination with bail-in, and

(iii) understand the impact of bail-in on financial markets.

Additionally, the Credit Suisse case shows that authorities should continue to prioritise testing and simulating effective decision making and execution at domestic and international levels.

They should also extend their communication and coordination efforts outside of the core CMG.

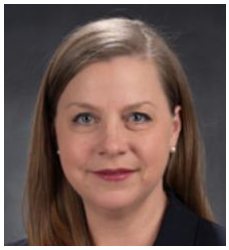
This review reaches the conclusion that recent events demonstrate the soundness of the international resolution framework in that it provided the Swiss authorities with an executable alternative to the solution that they deemed preferable in this particular case.

While the report identifies several areas for further analysis and improvements in the operationalisation and implementation of the G-SIB resolution framework, this review upholds the appropriateness and feasibility of the framework, rather than presenting issues that would question the substance of the Key Attributes themselves.

To read more: https://www.fsb.org/wp-content/uploads/P101023.pdf

Responsible Innovation in Money and Payments

Governor Michelle W. Bowman, at Roundtable on Central Bank Digital Currency, Harvard Law School Program on International Financial Systems, Washington, D.C.



Thank you for the opportunity to speak with you today on the important topic of innovations in money and payments. These issues continue to be of primary importance to the Federal Reserve.

As part of its key functions, the Federal Reserve carries out a number of different responsibilities that include

- fostering a safe and efficient payment system and providing services that support U.S. financial markets and private-sector payment, clearing, and settlement arrangements;
- promoting the safety and soundness of individual financial institutions and monitoring their impact on the financial system as a whole;
- setting U.S. monetary policy; and
- helping to maintain the overall stability of the U.S. financial system and the economy.

As a policymaker, I view responsible innovation through the lens of accomplishing these policy goals.

Innovation in money and payments can take many forms. We have continued to see interest in digital assets, such as crypto-assets, stablecoins, central bank digital currency (CBDC), and programmable payment platforms, including those built on distributed ledger technology (DLT).

Alongside these innovations, we have embraced opportunities to improve the existing payment infrastructure by adopting and developing instant payments, planning for future technology upgrades and improvements, and considering other more straightforward changes like expanding operating hours for the wholesale payment infrastructure.

Today I will share my views on several of these potential improvements, including CBDC, other digital assets, and wholesale payments innovations. I will also discuss the importance of determining whether the benefits of innovation flow from the new technology itself or, rather, result from policy choices that require new technology adoption.

Throughout, I will lay out a vision for responsible innovation, which recognizes the important role of private-sector innovation and leverages the strengths of the U.S. banking system supported by clear prudential supervision and regulation, and I will discuss how policy can support the continued development of the payment system and broader financial system.

Digital Assets

Often, discussions about the evolution of the payments landscape focus on novel forms of payment, including CBDC, stablecoins, and other forms of digital assets.

Central Bank Digital Currency

First, I will touch on CBDC. For the purposes of this discussion, I will define CBDC as a new, digital form of central bank money widely available to the general public.

Some refer to this as a "general purpose" or "retail" CBDC. There are meaningful differences between this type of retail CBDC and what is commonly referred to as a wholesale CBDC, which is a term some use to refer to digital central bank money used to settle large-value transactions among banks.

While I will return to the concept of a wholesale CBDC in a moment, I would like to share my thoughts on the debate about the introduction of a retail CBDC in the United States.

As I have noted before in other venues, there are two threshold questions that a policymaker should ask when contemplating a CBDC.

First: what problem is the policymaker trying to solve, and is there a more efficient way to solve it?

Second: what features and considerations, including unintended consequences, should a policymaker think about before deciding to adopt a CBDC and in designing the operation of a CBDC?

On the first question, we have seen a range of arguments in the public debate about issuing a CBDC, including addressing frictions within the

payment system, promoting financial inclusion, and providing the public with access to safe central bank money.

These are all important issues. I have yet to see a compelling argument that a U.S. CBDC could solve any of these problems more effectively or efficiently than alternatives, or with fewer downside risks for consumers and for the economy.

Yet in the United States, we have a safe and efficient payment system that continues to evolve with responsible innovations, like the FedNow Service, which is the Federal Reserve's new interbank system for instant payments that launched in July of this year.

Through FedNow, participating banks, businesses, and consumers can send and receive instant payments in real time, around the clock, every day of the year, with immediately available funds.

FedNow, and a similar private sector service, is designed to help make everyday payments faster and more convenient, allowing consumers to instantly receive funds with same-day access, and enabling small businesses to more efficiently manage cash flows without processing delays.

Future innovations may further build upon these services to more effectively address payment systems frictions and financial inclusion. It is quite possible that other proposed solutions may address many or all of the problems that a CBDC would address, but in a more effective and efficient way.

Further, the potential benefits of a U.S. CBDC remain unclear, and the introduction of a U.S. CBDC could pose significant risks and tradeoffs for the financial system. These risks and tradeoffs include potential unintended consequences for the U.S. banking system and considerable consumer privacy concerns.

The U.S. banking system is a mature, well-functioning, and effective system that delivers important benefits to our economy. Within this system, banks play a number of important roles, including providing consumers with access to credit and other banking and payments services, all within an established regulatory perimeter.

In addition, bank compliance and reporting programs support important public policies, like deterring criminal activity and protecting consumer financial data. Banks also play an essential role in the transmission of monetary policy, and they provide the foundation for a well-functioning economy and financial system.

The U.S. intermediated banking model helps to insulate consumer financial activities from unnecessary government overreach, and I believe this is an appropriate model for future financial innovation.

If not properly designed, a CBDC could disrupt the banking system and lead to disintermediation, potentially harming consumers and businesses and presenting broader financial stability risks.

As policymakers, we would need to carefully consider how an intermediated CBDC, with private-sector service providers, could be designed in a way that maintains financial institution involvement and minimizes, or ideally, eliminates related disruptions to the broader U.S. financial system.

I believe it is important to continue to research the possible benefits, risks, and tradeoffs of a potential U.S. CBDC, and to follow international CBDC developments that could have implications for the United States.

However, given that we have a safe and efficient payment system and a well-functioning banking system, the potential uses of a U.S. CBDC remain unclear and, at the same time, could introduce significant risks and tradeoffs.

That said, recognizing the interconnected and global nature of the financial system, I see value in continuing to research and understand the underlying technology and associated policy implications as other jurisdictions continue to actively pursue CBDCs.

Doing so ensures we are aware of and can be responsive to any developments and can continue to support a safe and efficient financial system into the future.

Stablecoins

But a CBDC is just one potential piece of the evolving payments landscape. Another alternative to traditional forms of money and payment, or to a CBDC, is stablecoins.

This form of payment emerged primarily to support the trading of crypto-assets but increasingly has been proposed as an alternative to traditional payments and as a store of value. Stablecoins purport to have convertibility one-for-one with the dollar, but in practice have been less secure, less stable, and less regulated than traditional forms of money.

Digital assets used as an alternative form of money and payment, including stablecoins, could pose risks to consumers and the U.S. banking system.

Therefore, it is important to understand risks and tradeoffs associated with digital assets and new arrangements used for banking and payments.

While I support responsible innovation that benefits consumers, I caution against solutions that could disrupt and disintermediate the banking system, potentially harming consumers and contributing to broader financial stability risks.

And, where the activity happens outside the regulatory perimeter, consumers would be left without the adequate protections that our regulated and supervised banks provide today in the United States.

A Comprehensive Regulatory Framework

For these reasons, my vision for responsible innovation includes a clear and sensible regulatory framework, where we incorporate what works well today in the U.S. banking system, allowing for private sector innovations within established guardrails.

Within this framework, it is imperative that the same activities that present the same risks are subject to the same regulations—regardless of what a product is called and by whom it is offered. I think the desire for "new" often leads us to overlook existing success, both in terms of regulatory approach and financial services.

Rather than speculate about the composition of alternative regimes, we should ask how these new products and providers can be held to the same standards as banks, especially with respect to consumer protection.

As an example, stablecoin issuers today typically are licensed or chartered at the state level as money service businesses or trust companies, and, in some cases, offer bank-like services, including the ability to store funds.

However, while many of these issuers are subject to state supervision, they are not subject to the full complement of prudential regulation applicable to banks like capital requirements and prudential supervision.

They also do not benefit from the backstops and protections available to banks like deposit insurance coverage and access to central bank liquidity in times of stress.

In order to protect consumers, it is imperative that activities that present the same risks are subject to the same regulations and offer the same protections.

This approach would also allow banks to compete on a level playing field in introducing products and services to benefit consumers. This type of regulatory clarity can provide support for responsible innovation.

Wholesale Payments Innovation

Next, I will speak to potential improvements, including technological innovations, in wholesale payments. Wholesale payments generally refer to large-value, interbank transactions, and not consumers sending money to other consumers. This refers to the financial plumbing that banks use behind the scenes to settle payments.

The Federal Reserve continues to speak to a broad range of stakeholders and conduct research regarding emerging technologies, including those that could enable or be supported by future Federal Reserve-operated payment infrastructures.

The goal is to better understand potential opportunities and risks of new wholesale payment platforms, including those built on DLT, as well as the associated risks and benefits of depository institutions transacting on these platforms with "tokenized" forms of digital central bank money, sometimes called wholesale CBDC.

In my view, the term "wholesale CBDC," despite its wide use, is generally a misnomer that leads to confusion since we already have central bank money in digital form that is available to banks for wholesale transactions.

Today, banks and other eligible entities hold central bank money as digital balances at the Federal Reserve—frequently referred to as reserves. These reserves are held for a number of purposes, including settling large-value interbank payments.

Interbank payment services, like the Fedwire Funds Service and other private sector services, are critical to the functioning and stability of the financial system, and the economy more broadly, as they enable important financial market functions.

Wholesale payment infrastructures operated by the central bank tend to underpin domestic and international financial activities by serving as a foundation for payments and the broader financial system.

This infrastructure allows payments to flow safely between consumers and businesses within the United States and internationally. Since this infrastructure is so critical to the payments system, it is necessary that we investigate and understand the potential opportunities, risks, and tradeoffs for wholesale payments innovation to support a safe and efficient U.S. payment system.

These wholesale systems function safely and efficiently today, but we have seen new payment platforms built on innovative technologies that have generated interest in new capabilities. This includes transacting "tokenized" forms of money and assets and enhancing the programmability of payments through the transfer of money using so-called smart contracts.

These platforms are also being explored as a way to improve the efficiency of payment, clearing, and settlement of certain financial transactions, including for cross-border purposes.

Policymakers should be mindful of the specific features innovative wholesale platforms could include, and the risks, tradeoffs, and other considerations they could entail.

For example, one potential model under consideration is the concept of a common platform or shared ledger that could facilitate digital asset transactions, including commercial bank and central bank liabilities.

This type of ledger could be specific to one jurisdiction (such as U.S. dollar transactions only among regulated financial institutions) or across jurisdictions and containing multiple currencies.

While there is interest in new capabilities and efficiencies that a shared ledger could offer, transacting central bank money on a shared ledger may introduce additional risks and operational complexities.

This would depend on how a platform would be governed, and which entities would be allowed to participate. In the United States for example, this technology would introduce risks and complexities that do not exist today because a shared ledger might allow central bank money to circulate on a platform that is not owned and operated by the central bank.

Important legal, policy, and operational questions would need to be thoroughly considered alongside an assessment of potential benefits.

Another potential model is one where central banks maintain their own ledgers—just as they do today—and use DLT as a bridge between distinct ledgers to achieve interoperability and facilitate cross-border, cross-currency payments.

Still other models exist across both wholesale and retail payments that would leverage existing infrastructure. Examples include experiments that look at interlinking faster domestic payment systems to facilitate cross-border payments, or even exploring how existing domestic payment infrastructures could be incrementally improved.

Each model contains its own set of potential features and tradeoffs. While my vision for responsible innovation includes a broad understanding of different options, I continue to emphasize that to help focus efforts, we must begin by asking "What specific problem are we trying to solve?"

To read more:
https://www.federalreserve.gov/newsevents/speech/bowman20231017a.htm

The European Commission adopts the 2024 Commission Work Program

European Commission

'Together, we have shown that when Europe is bold, it gets things done. And our work is far from over, so let's stand together. Let's deliver today and prepare for tomorrow.'
European Commission President Ursula von der Leyen, State of the Union speech, 13 September 2023.

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Commission work programme 2024

Delivering today and preparing for tomorrow

Next June, Europeans will take part in the continent's biggest democratic exercise. Among the more than 400 million people eligible to vote for the new European Parliament will be many young people who are exercising their democratic rights for the first time – including, in five Member States, 16- and 17-year-olds.

The results will set Europe on its path for the subsequent five years and beyond, with the election coming at a crucial juncture in Europe's history.

We are faced with a number of epoch-making challenges and opportunities. From the climate and biodiversity crises to the digital revolution and artificial intelligence; from Russia's brutal invasion of Ukraine to the ensuing energy price and cost of living crises; from migration to ensuring economic growth and competitiveness.

At the start of the mandate, this Commission laid out an ambitious agenda for a stronger and more resilient Union.

We committed to bold action to be the first climate-neutral continent and preserve Europe's natural environment, to lead the way towards a human-centered and innovative digital transition, to boost our economy while ensuring social fairness, inclusion and prosperity, to reinforce our responsible global leadership, to protect our citizens and our values, and to nurture and strengthen our democracy.

The world is a very different place compared to 2019, however. As a Union, we have had to react and adapt in the face of unprecedented challenges, remaining united in our responses and refusing to back away from delivering on our ambitions.

We have accelerated the twin green and digital transitions, put in place the landmark NextGenerationEU, strengthened the EU's role as a global leader and promoted the values that lie at the heart of our societies, such as democracy and the rule of law.

Through our Economic Security Strategy, we seek to reap the benefits of the EU's economic openness, while minimising risks arising from increased geopolitical tensions and accelerated technological shifts.

The clock is now ticking on our work to finalise the remaining key legislative proposals presented by this Commission to ensure that citizens and businesses can take full advantage of our policy actions.

To this end, in the coming months, the Commission will support the European Parliament and the Council in their efforts to reach agreement on pending legislative proposals.

To allow sufficient focus for this task, and with most of the necessary legislative framework promised under this mandate already in place, this work programme contains a limited number of new initiatives that deliver on existing commitments or respond to emerging challenges.

The EU's economy has continued to show resilience despite the challenges we have faced supported by our efforts to strengthen our energy security, a resilient labour market and the easing of supply constraints.

The European Green Deal, our world-leading effort to tackle climate change and biodiversity loss and Europe's growth agenda, remains a central part of the Commission's work.

While the main focus is now on implementation, we are coming forward still this year with proposals on the protection of animals during transport, preventing microplastic pollution, improving forest monitoring and a mobility package.

We will also maintain our efforts to set the course towards a human-centered, sustainable and more prosperous digital future with the Digital Decade.

NextGenerationEU will remain key to ensuring secure, affordable and clean supplies of energy, the competitiveness of European industry, social

and territorial cohesion and the transition to a net-zero, circular and nature-positive economy.

The Commission will support all Member States in accelerating the implementation of their recovery and resilience plans, in line with the country-specific recommendations under the European Semester, including their REPowerEU chapters.

Early next year we will present an interim evaluation on the implementation of the Recovery and Resilience Facility.

To promote more jobs and investments in Europe we will also continue work to accelerate the deployment of renewable energy while keeping energy prices under control, to ensure supplies of key strategic commodities such as critical raw materials and clean hydrogen, and to reduce administrative burden, in particular in relation to reporting in line with our strategy to boost the EU's long-term competitiveness.

At the same time, we need to finish building an economic governance framework fit for the challenges ahead.

This means finding agreement on the Commission's proposals on reforming governance rules and strengthening debt sustainability and on promoting sustainable and inclusive growth through reforms and investment.

Together with the Belgian Presidency, the Commission will convene a Social Partner Summit in Val Duchesse to discuss the challenges facing our labour markets, workers and businesses, including from skills and labour shortages, and artificial intelligence.

The challenges over the past years have underlined the strengths and capabilities of our Union. But they have pushed the EU budget to the point of exhaustion despite its in-built flexibilities and extensive reprogramming.

To counter this, we tabled a proposal to reinforce the longterm EU budget to be able to address the most imminent needs, which provides for a targeted increase in EU spending to deepen our support for Ukraine, finance our action on migration, bolster the Union's capacity to respond to heightened economic and geopolitical instabilities, humanitarian crises and natural disasters, and boost investments in strategic technologies to foster long-term competitiveness.

In line with the negotiations on the long-term EU budget for 2021-2027, we put forward an adjusted proposal for new own resources to help finance the repayment of NextGenerationEU borrowing.

The New Pact on Migration and Asylum remains the structural response the EU needs to tackle migration challenges in the future.

Its adoption is a key priority as work needs to start already next year to prepare for its swift implementation.

With the brave resistance of the Ukrainian people against the invading Russian forces continuing unabated, the EU will not waver in its solidarity with Ukraine.

So far, the Union and its Member States have provided, in a Team Europe approach, EUR 82 billion in total support, including humanitarian aid, military equipment and training, material goods for civilian use, including generators, school buses, medical items and evacuations, rebuilding cities in a high-quality, sustainable and inclusive way, help for children and to rehabilitate damaged schools, and economic support.

This support is provided in coordination with our international partners within the Multi-agency Donor Coordination Platform for Ukraine launched in January 2023 following a decision of G7 leaders.

The Commission hosts the secretariat of the platform that facilitates close coordination among international donors and financial organisations and ensures coherent, transparent, and accountable support.

The EU-Ukraine Solidarity Lanes have helped Ukraine export over 57 million tonnes of agricultural goods and almost 45 million tonnes of non-agricultural products, and import goods the country needs.

Through the Joint Coordination Platform, the Commission will spare no efforts to facilitate the timely and stable delivery of Ukrainian agricultural products to global markets.

The Commission condemns Russia's decision to terminate the Black Sea grain initiative and will continue to support all efforts to mitigate security and safety risks to shipping in the Black Sea.

The Council adopted the Commission's proposal to extend the temporary protection for people fleeing Russia's aggression against Ukraine until 3 March 2025.

Together with the CARE and FAST-CARE initiatives, this will provide certainty and support for more than 4 million persons enjoying protection across the EU.

The EU also adopted in record time several emergency initiatives during the course of 2022 to mitigate the effects of the energy crisis on industry and households.

Finally, to underscore the EU's commitment to stand by Ukraine as long as is necessary, we will create a facility to provide support to Ukraine to the tune of up to EUR 50 billion in the period 2024-2027.

This funding will cater for Ukraine's immediate needs, as well as bolstering its recovery, and supporting its modernisation on its path towards EU membership.

Together with our international partners, we have taken steps to ensure war crimes committed in Ukraine by Russia are punished and that Russia compensates for the damage it has done.

The International Centre for the Prosecution of the Crime of Aggression against Ukraine has started its operations in The Hague and will be key to investigating these horrific acts and facilitating the building of cases for future trials.

We will leave no stone unturned to hold those responsible to account. And we are continuing work on the possible use of proceeds from seized Russian assets for Ukraine's reconstruction.

The Union must prepare for its successful enlargement in order to foster long-term peace and stability in Europe.

We will work closely with our partners as they prepare for this momentous step, including opening the Commission's Rule of Law Reports to those accession countries who get up to speed even faster.

The EU also needs to be ready. The Commission will put forward a Communication on preenlargement reforms and policy reviews to see how each policy would be affected by a larger Union and how the European institutions would work.

To read more: https://commission.europa.eu/publications/2024-commission-work-programme-key-documents_en

ENISA Threat Landscape 2023

The ENISA Threat Landscape (ETL) report, now in its eleventh edition, plays a crucial role in understanding the current state of cybersecurity mainly within the European Union (EU).

It provides valuable insights into emerging trends in terms of cybersecurity threats, threat actors' activities as well as vulnerabilities and cybersecurity incidents.

Accordingly, the ETL aims at informing decisions, priorities and recommendations in the field of cybersecurity.

It identifies the top threats and their particularities, threat actors' motivations and attack techniques, as well as provides a deep-dive insight on particular sectors along with a relevant impact analysis.

The work has been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences.

The ongoing war of aggression against Ukraine continued to influence the landscape.

Hacktivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down.

The prime threats identified and analysed include:

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference
- Supply chain attacks

This is the eleventh edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape.

It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis.

It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

For each of the identified threats, we determine impact, motivation, attack techniques, tactics and procedures to map relevant trends and propose targeted mitigation measures.

During the reporting period, key findings include:

• DDoS and ransomware rank the highest among the prime threats, with social engineering, data related threats, information manipulation, supply chain, and malware following.

• A noticeable rise was observed in threat actors professionalizing their as-a-Service programs, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.

• ETL 2023 identified public administration as the most targeted sector (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport.

• Information manipulation has been as a key element of Russia's war of aggression against Ukraine has become prominent.

• State-nexus groups maintain a continued interest on dual-use tools (to remain undetected) and on trojanising known software packages. Cybercriminals increasingly target cloud infrastructures, have geopolitical motivations in 2023 and increased their extortion operations, not only via ransomware but also by directly targeting users.

• Social engineering attacks grew significantly in 2023 with Artificial Intelligence (AI) and new types of techniques emerging, but phishing still remains the top attack vector

To read more: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Some lessons for crisis management from recent bank failures

Agustín Carstens, General Manager of the BIS, at the High-level meeting on banking supervision of the Association of Supervisors of Banks of the Americas (ASBA), the Basel Committee on Banking Supervision (BCBS) and the BIS Financial Stability Institute (FSI), 19 October 2023, Panama.

The recent bank failures

Let me first recall some of the key features of the bank failures and the strategies that were adopted in the United States and in Switzerland.

In early March 2023, the US regional banking sector experienced severe stress. Two banks failed: Signature Bank and Silicon Valley Bank. Both had a high proportion of uninsured deposits.

And both experienced large and rapid deposit outflows amid concerns about the sustainability of their business models.

Over a couple of days, the FDIC took both banks into receivership, created temporary bridge banks and eventually sold the banks in the market.

This resolution strategy was possible only because the US authorities invoked a "systemic risk exception".

This allowed authorities to override the usual limits on the amount of funds the FDIC can use to finance a resolution.

With it, the FDIC could cover all deposits, including the large amounts that were not insured. Shareholders and certain unsecured debtholders were not protected.

A week after the US bank failures, following an acute liquidity crisis at Credit Suisse, the Swiss authorities announced that UBS and Credit Suisse would merge and provided liquidity support for this process.

This was described as a "commercial transaction".

Importantly, the merger was supported by decrees enacted using emergency powers, which allowed the Swiss National Bank to provide liquidity support to UBS and Credit Suisse.

The transaction also involved the contractual writedown, in full, of all the outstanding Additional Tier 1 (AT1) capital instruments issued by Credit Suisse.

However, Credit Suisse shareholders retained some residual equity.

To read more: https://www.bis.org/speeches/sp231019.htm

PHISHING GUIDANCE: STOPPING THE ATTACK CYCLE AT PHASE ONE

Social engineering is the attempt to trick someone into revealing information (e.g., a password) or taking an action that can be used to compromise systems or networks.

Phishing is a form of social engineering where malicious actors lure victims (typically via email) to visit a malicious site or deceive them into providing login credentials.

Malicious actors primarily leverage phishing for:

• *Obtaining login credentials*. Malicious actors conduct phishing campaigns to steal login credentials for initial network access.

• *Malware deployment*. Malicious actors commonly conduct phishing campaigns to deploy malware for follow-on activity, such as interrupting or damaging systems, escalating user privileges, and maintaining persistence on compromised systems.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint guide to outline phishing techniques malicious actors commonly use and to provide guidance for both network defenders and software manufacturers.

This will help to reduce the impact of phishing attacks in obtaining credentials and deploying malware.

The guidance for network defenders is applicable to all organizations but may not be feasible for organizations with limited resources.

Therefore, this guide includes a section of tailored recommendations for small- and medium-sized businesses that may not have the resources to hire IT staff dedicated to a constant defense against phishing threats.

The guidance for software manufacturers focuses on secure-bydesign and -default tactics and techniques.
Manufacturers should develop and supply software that is secure against the most prevalent phishing threats, thereby increasing the cybersecurity posture of their customers.

TABLE OF CONTENTS

OVERVIEW....3
PHISHING TO OBTAIN LOGIN CREDENTIALS....4
MALWARE-BASED PHISHING....5
MITIGATIONS....5
INCIDENT RESPONSE....11
REPORTING....12
CISA SERVICES....12
RESOURCES....13
ACKNOWLEDGEMENTS....14
DISCLAIMER....14
REFERENCES....14

To read more: https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/0/CSI-PHISHING-GUIDANCE.PDF

Multiple Scenarios in Stress Testing

Michael S. Barr, Vice Chair for Supervision, Federal Reserve System, at the Stress Test Research Conference at the Federal Reserve Bank of Boston, Boston, Massachusetts

Thank you for the opportunity to speak today. I'm here to offer my thoughts on the next steps for stress testing, and in particular why using multiple exploratory scenarios will help improve our understanding of risk in the banking system.

The stress test as we know it today grew out of the 2009 Supervisory Capital Assessment Program, or SCAP, conducted in the heat of the global financial crisis. In the winter of 2008–09, markets had lost confidence in banks amid wide uncertainty about the future path of the economy and the losses banks could face.

This prompted the Federal Reserve and Treasury to conduct a stress test to determine the health of the 19 largest banks under a severely adverse economic scenario and to publish the findings.

The release of the results provided transparency about the status of the largest banks, made it easier for firms to re-capitalize themselves, and restarted the provision of credit to the economy that began the process of recovery.

Following the success of this stress test, Congress mandated in the Dodd-Frank Act that the Federal Reserve conduct an annual stress test of large banks to determine whether those banks have sufficient capital to absorb losses under adverse economic conditions.

And today this test—as well as the data collection that supports it—is one of our primary tools to assess and to help ensure banks' resilience, in good times and bad. During periods of economic or financial uncertainty, stress tests can provide critical assessments of bank resilience to supervisors, the market, and policymakers. This transparency helps enable markets to function better in times of stress.

Outside of stressful periods, stress tests can help to assess sufficient capitalization and improve supervisory insight into risks. The stress test also can provide transparency into the build-up of risks across banks.

In our experience, the test results have given supervisors valuable information to provide feedback to individual firms and helped the Board assess the stability of the financial system. A recent study confirms this experience, finding that banks subject to the stress test were less exposed to common systemic risks.

In addition, the stress test helps to make capital requirements less susceptible to gaming by firms and therefore more likely to be set at adequate levels.

This is so because the design of the scenario can change based on our observations of growing risks in the system. The scenario framework, by using parameters that become stricter when the economy is stronger, also helps to avoid exacerbating the natural tendency for banks to take larger risks during good times and become highly risk averse during bad times.

Furthermore, stress tests change in response to improved modeling and evolving risks, so that the tests better estimate potential losses in a downturn.

Over the past 14 years, we have learned from our experiences and continued to evolve the stress testing program. We have taken steps to increase the transparency of the stress testing program, including to publish an extensive description of our approach to model development, implementation, and validation, as well as our approach to scenario design.

In connection with each stress test, we disclose a detailed summary of the stress test methodology, and for several key portfolios, disclose our approach to modeling loss rates, summary statistics, and modeled loss rates.

In 2020, we adopted the stress capital buffer, which uses the results of the stress test to inform a firm's capital buffer requirements.

The program also provides banks with the opportunity to request reconsideration of their stress capital buffer.

While our stress test is an important measure of the strength and resilience of the banking system, we must recognize that it does have limitations, as does any exercise.

I'll walk through three limitations and explain how they can be at least partially mitigated by incorporating multiple exploratory scenarios into our stress test program.

What I mean by an exploratory scenario is a scenario that is not used to set a firm's stress capital buffer requirement. I'll then describe how the Federal Reserve could use the results of exploratory scenarios to help ensure the banking system remains strong and resilient, by allowing us to better understand potential risks and improve our supervision of those banks.

As we move forward, we must remain cognizant that none of us can predict future stressful events and their consequences with confidence.

Limitations of Stress Testing

First, the current stress test uses a single scenario that is focused on a credit-driven recession and single global market shock to test the financial condition of firms.

A single scenario cannot cover the range of plausible risks faced by all large banks. This has been confirmed time and time again, including in recent experience.

The failures of three large banks last spring showed that acute banking strains can emerge even without a severe recession. Yet, conditions such as those recently experienced presented challenges for the design of the supervisory stress scenario.

Most notably, the Federal Reserve's stress testing policy statement—which governs how the hypothetical scenarios are determined—requires that the severely adverse scenario include a rapid increase in the unemployment rate to at least 10 percent, as well as steep declines in house prices.

Such conditions are historically associated with subdued inflation and a fall in interest rates. The fact that significant banking stress emerged in very different conditions underscores the limitations of our current stress testing processes.

We also do not take into account second-order effects of stress within the financial system, which are channels that amplify the effects of the shocks hitting bank's balance sheets, leading to losses spreading throughout the financial system.

A good example of this is the reaction of funding markets to stress at an individual firm or many firms. These network effects may result in losses across the system not fully captured by our stress tests.

While the severely adverse scenario is calibrated to historical recessions that have included contagion, our stress tests may not fully capture the evolving interconnections in today's financial system.

The second limitation involves our models. In developing supervisory models, Federal Reserve staff draw on economic research and industry practice; the models are also independently validated by a group of experts outside of the stress testing program.

However, all models have limitations—they are generally trained on historical data and therefore may not be robust to structural breaks, such as a once-in-a-lifetime pandemic, or important changes in technology.

Expanding the range of risks captured in the stress test makes models more robust to these limitations but will not address them completely.

The third limitation is how the stress test affects bank behavior. Using scenarios that test for the same underlying risks year after year could disincentivize firms from investing in their own risk management as the test becomes predictable, and may encourage concentration across the system in assets that receive comparably lighter treatment in the test. Additional exploratory stress test scenarios could allow supervisors to better probe the internal risk management of firms and assess whether they are holding sufficient capital for their risks.

We find that firms often use a large number of scenarios and shocks when running their own internal stress testing processes, and our regulatory counterparts use a number of scenarios as well.

Expanding the Risks Captured in the Stress Test

Exploratory stress test scenarios could mitigate these and other risks. The goal of stress testing should be to provide sufficient coverage of the types of severe but plausible scenarios that could adversely impact a bank's operations, and the combination of scenarios and shocks should be curated to achieve this goal.

This doesn't imply a large number of scenarios. Given the limited number of unique bank business models and variables that drive losses, a relatively small number of scenarios may be all that is required to capture a wide range of outcomes for the banking system.

On the macroeconomic side, additional scenarios could be used to explore the effects of qualitatively different macroeconomic and financial environments. For example, instead of the usual demand-driven recession, a scenario could explore the impact of an inflationary shock to supply.

Potentially, an exploratory scenario could probe the interplay between capital and liquidity, to help ensure firms understand their capital exposure to rapid changes in the composition or pricing of their liabilities.

With respect to market risk, the current single market shock used in the test is a one-time shock to several thousand variables in bank trading books. This is just one realization of a large set of risk factors that determine changes in market values.

Using additional market shocks would help us understand how the trading books and counterparty concentrations of firms would change under a range of financial conditions. This could include testing the exposure of firms to different directional risks, such as a sudden rise or fall in certain asset values, or to an unexpected divergence in values of correlated assets.

It is particularly important for us to consider a range of market shocks because some concentrated counterparty exposures may be revealed only under certain scenarios.

To advance the goal of improved testing of market risk, last year, for the first time, we introduced an additional, exploratory market shock component. As compared to the global market shock, the exploratory market shock was characterized by a less severe recession with greater inflationary pressures. As we explained in our results disclosure, banks generally looked better under the exploratory market shock, experiencing smaller trading and counterparty losses in the exploratory market shock than under the global market shock.

This is valuable information to us and the public, since it suggests that these banks' trading and counterparty exposures may not be an unexpected source of

vulnerability during a rising inflation scenario (although that test did not explore the effects of unrealized losses from interest rate risk).

The exercise also provided important insight into banks' counterparty exposures in varying conditions, since banks' largest counterparties differed between the exploratory market shock and the global market shock.

Building on these experiences, the Federal Reserve is developing both exploratory macroeconomic scenarios and exploratory market shocks for next year's stress test. As I noted above, an exploratory scenario would not be used to set a firm's stress capital buffer requirement. Instead, the exploratory scenarios will be used to inform the Board's supervisory assessments of firms' risk management and our understanding of different risks in the banking system.

Using the Additional Stress Test Results

Let me speak to how we currently use the stress test, and how we could use exploratory scenarios going forward. A current use of the stress test is to help set capital requirements for large banks to help prepare firms to withstand a severe economic recession and continue to lend and operate. The key features of the scenario used to calculate the capital requirements are generally similar from year to year.

Since the stress test is used to set each firm's stress capital buffer requirement, there is a benefit to predictability so that firms are better able to conduct capital and business planning. To the extent we were to adjust key features of the scenario used to set the capital requirements, we would do so through a transparent, public process.

However, a tradeoff with producing predictable scenarios is stifling creativity in scenario design and less bank resilience to a range of potential scenarios, and this is where exploratory scenarios can help. The use of stress scenarios and shocks that do not set a firm's stress capital buffer requirement can provide room to explore a wider range of vulnerabilities to inform risk-based supervision.

For example, if the purpose of the exploratory scenario is to inform the Board or the public about new or underappreciated risks, the Board could explore the impact of a scenario using a different set of variables than the ones it has currently defined in its policy statement.

Additional exploratory stress test scenarios could allow supervisors to better probe the internal risk management of firms and assess whether they are holding sufficient capital for their risks. For example, the 2018 stress test revealed that one firm had highly concentrated counterparty exposures that would materialize under the hypothetical stress scenario. This led to supervisory feedback to that firm and its prompt mitigation of the concern. We should continue to enhance the feedback loop between supervision and stress testing.

We can also learn from our international counterparts, who have effectively employed exploratory stress tests. Since 2017, the Bank of England has run a biennial exploratory scenario designed to explore risks not covered by their

annual capital stress test. The results of their exploratory tests are used to improve supervisory feedback related to the risk management of firms.

While the results of our stress test are informative and provide a rigorous measure of resilience, the supervisory stress test is not a replacement for a firm's own risk management or its own stress testing processes. Large banking organizations should maintain a solid line of sight into their own risks and focus their efforts to capture those risks and determine capital needs.

Our stress test is designed to provide a consistent measure of risk across firms, and is not a replacement for comprehensive modeling, risk management, and capital planning by the largest banks that enable them to measure and manage their own unique risks.

The Future Evolution of Stress Testing

Exploratory scenarios would also allow the Board to have more flexibility in its modeling approaches. For example, the Board could explicitly model the behavioral response of depositors to losses, allowing for contagion of the type we saw earlier this year, the interaction of the broader economy and the banking system under stress, or the transmission of stress through nonbank parts of the financial system.

The Bank of England's recent stress tests included a set of models to better understand how feedback and amplification channels during a stress event could drive contagion losses and exacerbate the impact of an initial shock. These feedback loops included a contagion model testing how deteriorating capital positions might impact the market for interbank lending.

Expanding the use of exploratory scenarios in the stress test would allow for more experimentation in the modeling of risks by the Board's supervisory stress test program.

Conclusion

In conclusion, forums such as this research conference are excellent sources of ideas and hypothesis testing. In thinking about the future evolution of stress tests, we would benefit from wide ranging input—from academics, other policymakers, public interest groups, bankers and other market participants.

The stress test needs to continue to evolve. Introducing multiple exploratory scenarios—both for the broader macroeconomic scenario and the global market shock for trading banks—would be beneficial for supervising potential risks on bank balance sheets. These continued adjustments will help to ensure, consistent with the original intent of the Dodd-Frank Act, that the stress test remains a powerful and relevant tool for assessing whether large banks are resilient and our financial system is robust. Thank you.

To read more:
https://www.federalreserve.gov/newsevents/speech/barr20231019a.htm

Agencies issue principles for climate-related financial risk management for large financial institutions

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency

Federal bank regulatory agencies jointly finalized principles that provide a high-level framework for the safe and sound management of exposures to climate-related financial risks for large financial institutions.

The principles are consistent with the risk management framework described in the agencies' existing rules and guidance. The principles are intended for the largest financial institutions, those with $100 billion or more in total assets, and address physical and transition risks associated with climate change.

> Financial institutions are likely to be affected by both the physical risks and transition risks associated with climate change (collectively, climate-related financial risks).[4] Weaknesses in how financial institutions identify, measure, monitor, and control climate-related financial risks could adversely affect financial institutions' safety and soundness. The proposed OCC draft principles, FDIC draft principles, and Board draft principles (collectively, draft principles) were substantively similar and proposed a high-level framework for the safe and sound management of exposures to climate-related financial risks, consistent with the risk management framework described in the agencies' existing rules and guidance. Although all financial institutions, regardless of size, may have material exposures to climate-related financial risks, the draft principles were intended to support key climate-related financial risk management efforts by the largest financial institutions, those with over $100 billion in total consolidated assets.

The principles are intended to support efforts by the largest financial institutions to focus on key aspects of climate-related financial risk management.

General climate-related financial risk management principles are provided with respect to a financial institution's governance; policies, procedures, and limits; strategic planning; risk management; data, risk measurement, and reporting; and scenario analysis. Additionally, the principles describe how climate-related

financial risks can be addressed in the management of traditional risk areas, including credit, market, liquidity, operational, and legal risks.

The final principles neither prohibit nor discourage large financial institutions from providing banking services to customers of any specific class or type, as permitted by law or regulation. The decision regarding whether to make a loan or to open, close, or maintain an account rests with the financial institution, so long as the financial institution complies with applicable laws and regulations.

These final principles are substantively similar to the agencies' draft principles, with clarifications based on commenter feedback.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20231024b1.pdf

Policies, Procedures, and Limits. Management should incorporate material climate-related financial risks into policies, procedures, and limits to provide detailed guidance on the financial institution's approach to these risks in line with the strategy and risk appetite set by the board. Policies, procedures, and limits should be modified when necessary to reflect: (i) the distinctive characteristics of climate-related financial risks, such as the potentially longer time horizon and forward-looking nature of the risks; and (ii) changes to the financial institution's operating environment or activities.

Partners of Honest Business and Prosecutors of Dishonesty

Gary Gensler, Chair of the U.S. Securities and Exchange Commission, remarks before the 2023 Securities Enforcement Forum

I am pleased to join you at the 2023 Securities Enforcement Forum. As is customary, I'd like to note that my views are my own as Chair of the Securities and Exchange Commission, and I am not speaking on behalf of my fellow Commissioners or the SEC staff.

When I spoke with you two years ago, I shared what the SEC's first chair, Joseph Kennedy, said in his first speech: "The Commission will make war without quarter on any who sell securities by fraud or misrepresentation."

In a subsequent speech, just four months later, Kennedy emphasized: "We are not prosecutors of honest business, nor defenders of crookedness. We are partners of honest business and prosecutors of dishonesty. We shall not prejudge, but we shall investigate."

These words remain just as true today.

I am appearing here today in front of an audience of lawyers, accountants, and compliance officials. While you serve your clients, you also have a responsibility to the law and to the public.

William O. Douglas—before serving as the SEC's third chair and a Supreme Court Justice—once said to an audience of lawyers: "Service to the client has been the slogan of our profession. And it has been observed so religiously that service to the public has been sadly neglected."

Thus, as Felix Frankfurter said in advising President Franklin Roosevelt on staffing the newly formed SEC: "You need administrators … who have stamina and do not weary of the fight, who are moved neither by blandishments nor fears, who in a word, unite public zeal with unusual capacity."

That's why we're so fortunate to have the remarkable staff at the SEC. Every day, they work to advance our mission and ensure the markets work on behalf of investors and issuers, not the other way around.

In fiscal year 2023, our staff once again "[did] not weary of the fight."

We filed more than 780 actions, including more than 500 standalone cases. We obtained judgments and orders totaling $5 billion. Our work led to $930 million distributed to harmed investors.

These numbers, though, tell only part of the story. Our philosophy behind them tells a fuller one.

Again, I think of our enforcement program through five themes: Economic Realities, Accountability, High-Impact Cases, Process, and Positions of Trust.

Economic Realities

First, economic realities. In thinking about economic realities, I once again will quote a Supreme Court Justice: Thurgood Marshall.

"Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called." This is not just a talking point. This is the law of the land, as Justice Thurgood Marshall wrote in the Supreme Court's famous Reves decision.

Thus, to effectuate Congress's purpose, we don't enforce the securities laws based on a product's label. Rather, we look to the underlying economic realities.

This is true across all of the securities markets, but let me focus on one of its sectors.

There is nothing about the crypto asset securities markets that suggests that investors and issuers are less deserving of the protections of our securities laws.

Congress could have said in 1933 or in 1934 that the securities laws applied only to stocks and bonds. Yet Congress included a long list of items in the definition of a security, including "investment contract."

Let me ask with a show of hands—how many of you in the audience have clients in the crypto markets?

For those of you who raised your hand, I'm presuming that you entered into an engagement agreement with them. That you know who they are. That most of them have websites. That there's some identifiable person that you're relying on to retain you and pay for the services you provide.

In most cases, that's the economic reality at hand. As the Supreme Court said in the famous Howey decision: An investment contract exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.

As I've previously said, without prejudging any one asset, the vast majority of crypto assets likely meet the investment contract test, making them subject to the securities laws.

Further, it follows that most crypto intermediaries—transacting in these crypto asset securities—are subject to the securities laws as well.

With wide-ranging noncompliance, frankly, it's not surprising that we've seen many problems in these markets. We've seen this story before. It's reminiscent of what we had in the 1920s before the federal securities laws were put in place.

This is a field rife with fraud, scams, bankruptcies, and money laundering. While many entities in this space claim they operate beyond the reach of regulations issued before Satoshi Nakamoto's famous white paper, they also are quick to seek the protections of the law, in bankruptcy court and litigating their private disputes.

We have brought numerous enforcement actions against actors in this space—some settled, and some in litigation.

To read more: https://www.sec.gov/news/speech/gensler-remarks-securities-enforcement-forum-102523

The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement

EUROPOL

Quantum computing and quantum technologies hold significant potential to improve a wide range of applications and tasks.

At the same time, recent technological progress in this field, also referred to as the 'Second Quantum Revolution', is threatening to break the encryption we use to keep our most sensitive information safe.

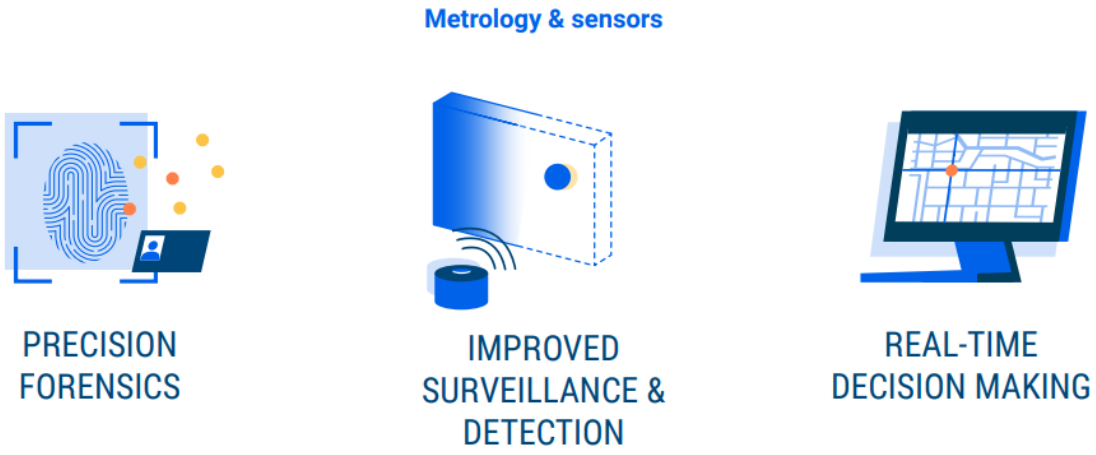
The purpose of this report is to provide a forward-looking assessment of the impact of quantum computing and quantum technologies from the law enforcement perspective.

In offering an extensive look at the wide range of potential applications in this context, this report is the first of its kind.

The report is the result of a collaborative effort of the European Commission's Joint Research Centre (JRC), Europol's European Cybercrime Centre (EC3), and the Europol Innovation Lab.

Area	Law enforcement	Criminals
General	Raise awareness on the threat of quantum computers and stay abreast of technological developments to combat risks at the earliest stage possible. Ensure law enforcement is leveraging the latest technology.	Reconsider their current modi operandi and identify potential to abuse availability of quantum computers.
Store now, decrypt later	Hold on to currently inaccessible encrypted data resulting from criminal investigations with a view to later decryption.	Accumulate and store encrypted information (for instance obtained from data breaches) with a view to later decryption.
Quantum password guessing	Significantly improve their technical ability to access password-protected data and devices from criminal investigations.	Be pushed to find alternative solutions for secure communications or increase operational security by using stronger passwords and multi-factor authentication. More easily hack into password-protected data and devices.
Digital forensics	Use new side-channel attacks and fault injection vulnerabilities to improve ability to gain access to criminal devices.	Employ counter measures or identify alternative technological solutions to increase operational security.
Post-quantum cryptography	Put into place transition plans to post-quantum cryptography for own data storage.	Switch to quantum-safe solutions.

It aims to inform decision-makers, policy-makers, and practitioners on the benefits and threats stemming from quantum computing and quantum technologies.



The report provides an update on the current state-of-play, and offers concrete recommendations to better prepare for the future.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement.

One of the most immediately significant areas quantum computers will impact is cryptography. As such, a large part of the cryptographic protocols currently used are threatened by the arrival of quantum computers. This includes both symmetric and asymmetric cryptography.

While symmetric cryptography can be relatively easily patched, widely used asymmetric cryptography would collapse entirely if subjected to this process.

The realisation that quantum computers pose a significant threat to currently used cryptography has led to post-quantum cryptography, which aims to keep sensitive information secure from this emerging threat.

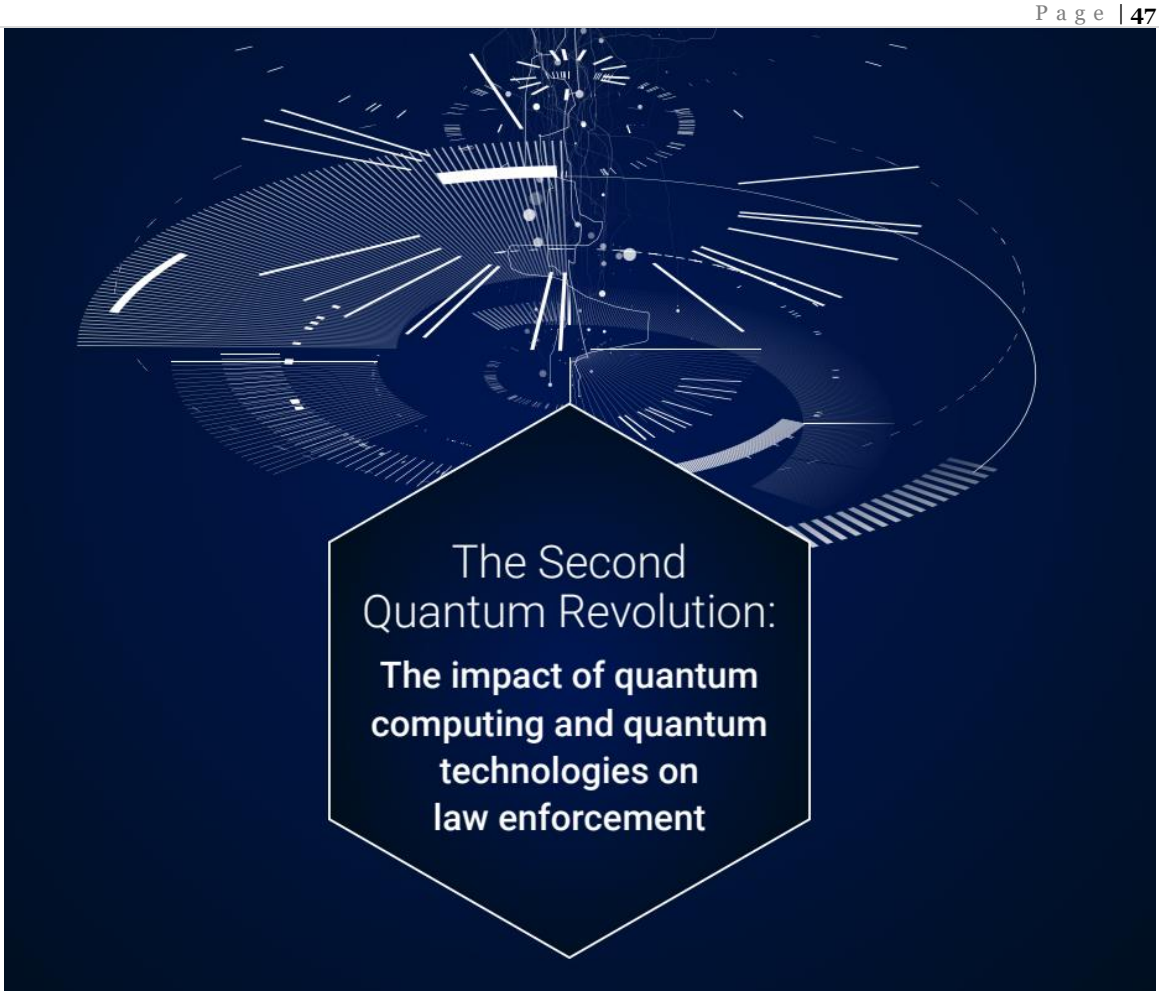
From the perspective of law enforcement, post-quantum cryptography has two major areas of impact.

First, law enforcement agencies need to prepare already to ensure that sensitive information and systems are protected adequately.

Second, the transition to post-quantum cryptography might reveal new vulnerabilities that could be exploited in the future.

At the same time, the impact of quantum computing in this field offers numerous potential advantages for law enforcement.

As such, quantum computers can support the investigation of cold cases, improve password guessing, and allow for new digital forensics techniques.



In addition to the impact quantum computing will have on cryptography, the overall field of quantum technologies is expected to bring significant advancements across several other areas.

This includes improvements in data analysis, machine learning and artificial intelligence, which may benefit from quantum algorithms to process large amounts of data at scale.

Quantum communications can enable the establishment of highly secure communications channels through which sensitive law enforcement data can be transmitted.

Finally, quantum sensors can improve the reliability of evidence, decrease the chance of wrongful convictions, and improve the surveillance and detection of objects.

In order for law enforcement to better prepare for the future of quantum computing and quantum technologies, five key recommendations have been identified.

While the development of universal quantum computers is still a future scenario, important steps can and should already be taken today to ensure better preparedness.

Quantum computing and quantum technologies have the potential to revolutionise the work of law enforcement.

At the same time, these technologies are likely to pose criminal threats that will need to be mitigated.

Only by understanding this impact and taking relevant action, can law enforcement agencies fully leverage these opportunities.

This report aims to provide the first step in this endeavour.

To read more: https://www.europol.europa.eu/publication-events/main-reports/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement

Disclaimer

The International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD) (hereinafter "Association") enhances public access to information. Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided, as these are general information, not specific guidance for an organization or a firm in a specific country.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice;

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the courts might place on the matters at issue.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been

created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems. The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD)

Welcome to the International Association of Potential, New and Sitting Members of the Board of Directors (IAMBD).

The Association is a business unit of Compliance LLC, incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training in 57 countries.

Join us. Stay current. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified.

Our reading room: https://www.iambd.org/Reading_Room.htm

Our training and certification programs

1. Certified Member of the Board of Directors (CMBD), distance learning and online certification program. You may visit: https://www.iambd.org/Distance_Learning_and_Certification.htm

2. Certified Member of the Risk Committee of the Board of Directors (CMRBD), distance learning and online certification program. You may visit: https://www.iambd.org/Distance_Learning_for_the_Risk_Committee_of_the_Board.htm

3. Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD), distance learning and online certification program. You may visit: https://www.iambd.org/Distance_Learning_for_the_Sustainability_Committee_of_the_Board.htm

Contact Us

Lyn Spooner
Email: lyn@iambd.org

George Lekatis
President of the IAMBD
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@iambd.org
Web: www.iambd.org
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA