Sarbanes Oxley News, November 2023

The staff of the Public Company Accounting Oversight Board (PCAOB) has posted revised standard-setting, research, and rulemaking agendas, following record action in 2023.

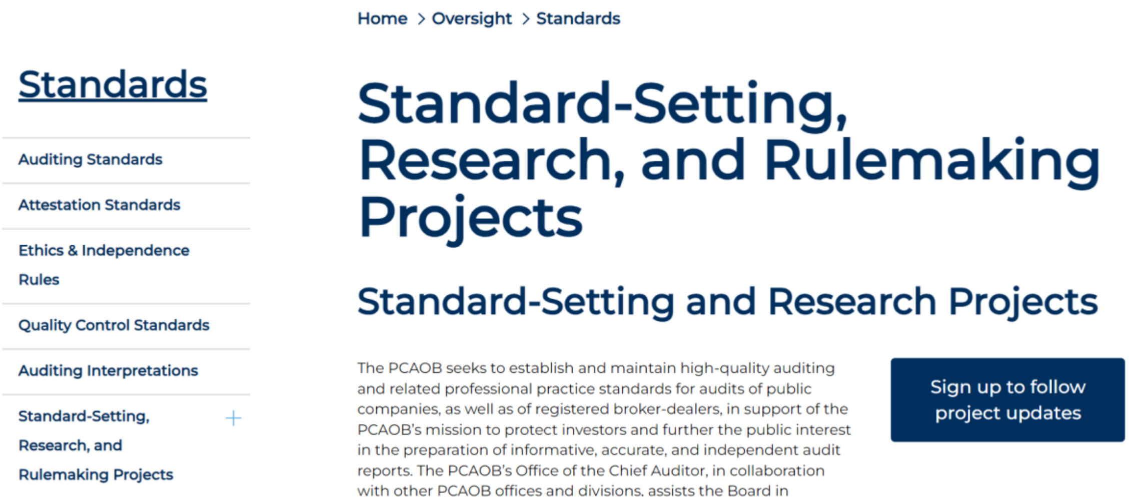
- In 2023, the Board has taken more formal actions on standard setting and rulemaking than any year in the last 10 years, issuing four proposals – with one more expected to be considered before year's end – and adopting a final confirmation standard and related amendments that had previously been stalled since 2010.

- By the end of 2023, it is anticipated the Board will have considered five proposals – more than any single year in PCAOB history since the first set of standards and rules were proposed in 2003.

- Over the past two years, the Board has issued six proposals – with one more expected later this year – and adopted two standards and related amendments.

"We have made incredible progress for investors thanks to the hard work of the talented PCAOB staff, and we are just getting started," said PCAOB Chair Erica Y. Williams. "Our commitment to modernizing our standards and rules remains stronger than ever as we continue working to get these agendas done and done right for investors."

The standard-setting, research, and rulemaking projects can be found on the Standard-Setting, Research, and Rulemaking Projects page at: https://pcaobus.org/oversight/standards/standard-setting-research-projects



Home > Oversight > Standards
Standards
Auditing Standards
Attestation Standards
Ethics & Independence Rules
Quality Control Standards
Auditing Interpretations
Standard-Setting, Research, and Rulemaking Projects
Sign up to follow project updates

Standard-Setting, Research, and Rulemaking Projects

Standard-Setting and Research Projects

The PCAOB seeks to establish and maintain high-quality auditing and related professional practice standards for audits of public companies, as well as of registered broker-dealers, in support of the PCAOB's mission to protect investors and further the public interest in the preparation of informative, accurate, and independent audit reports. The PCAOB's Office of the Chief Auditor, in collaboration with other PCAOB offices and divisions, assists the Board in

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-revises-standard-setting-research-and-rulemaking-agendas-following-record-setting-action-in-2023

2023 Bank Failures - Preliminary lessons learnt for resolution

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

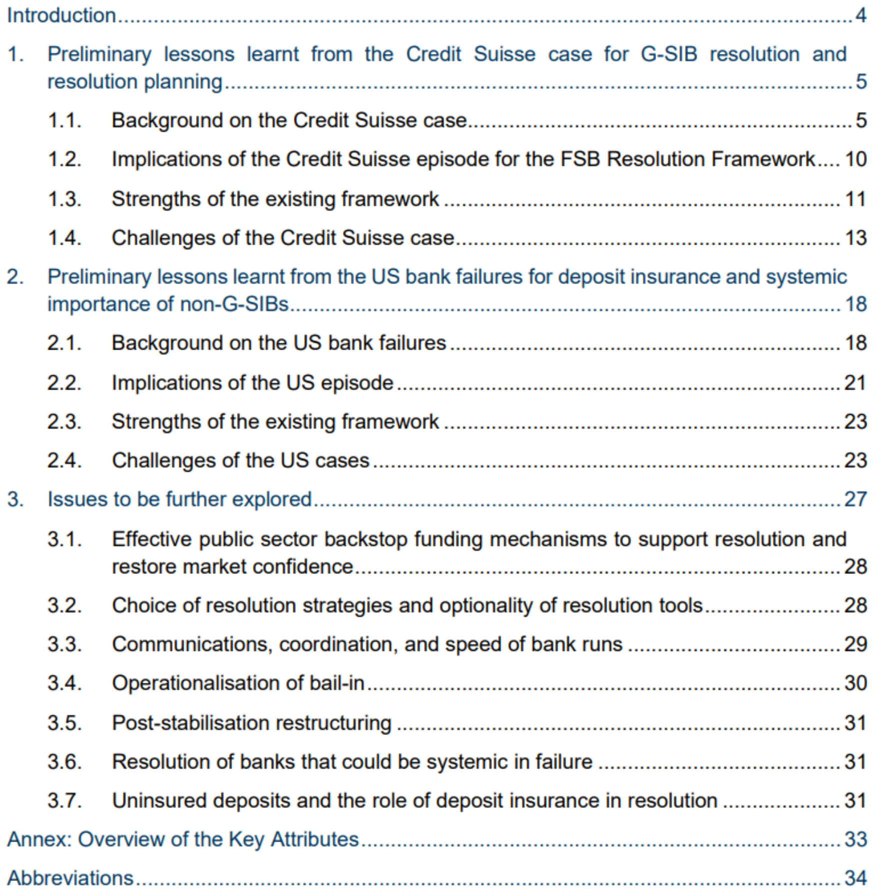
Preliminary lessons learnt for resolution

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.



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

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.

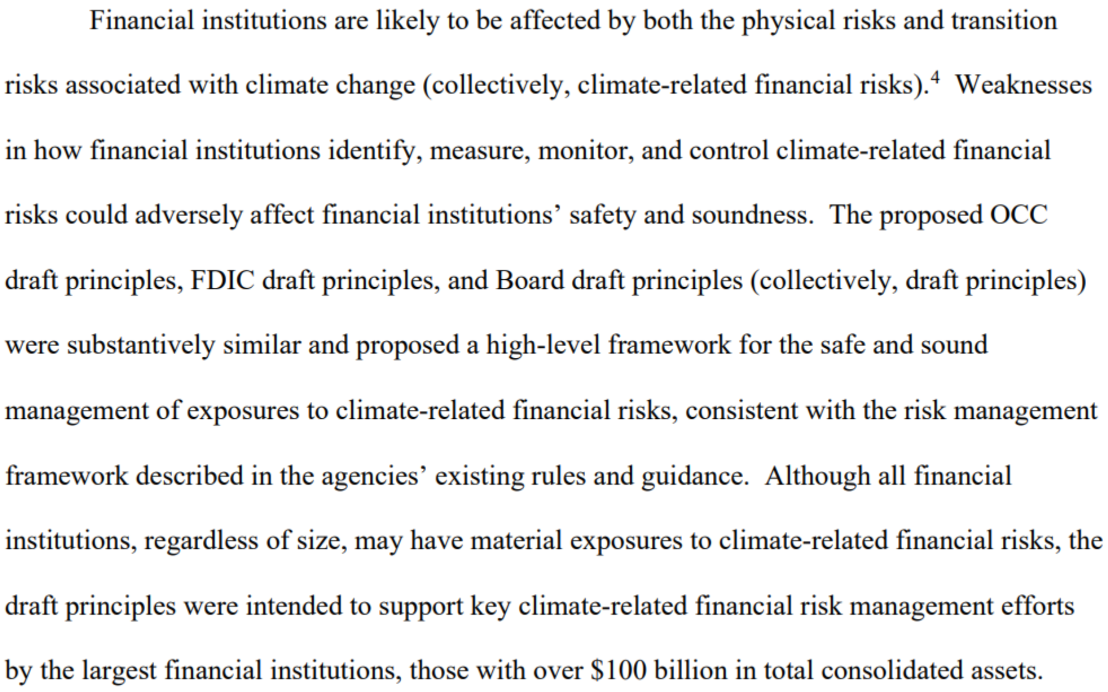
To read more:
https://www.federalreserve.gov/newsevents/speech/barr20231019a.htm

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.

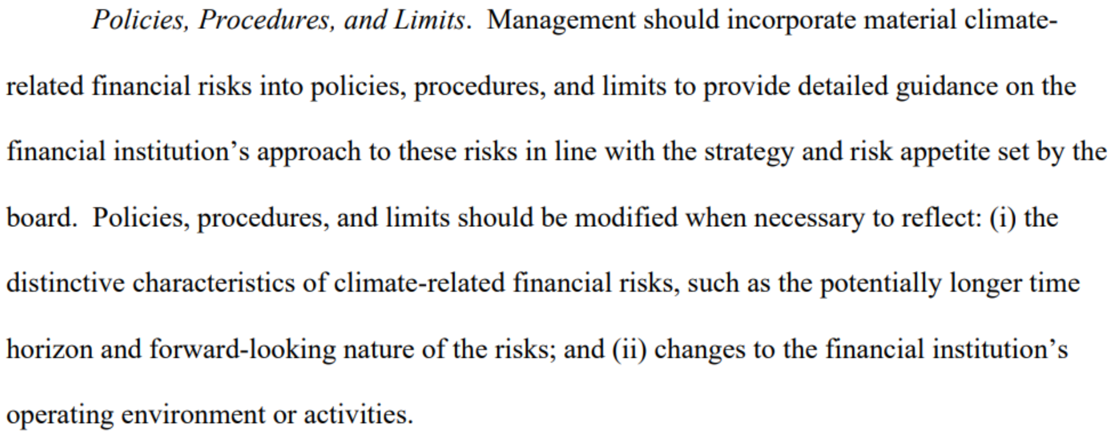
The principles are intended to support efforts by the largest financial institutions to focus on key aspects of climate-related financial risk management.

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.

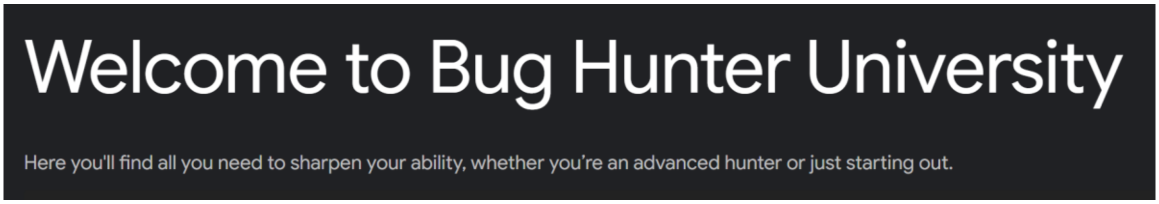
To read more: https://www.sec.gov/news/speech/gensler-remarks-securities-enforcement-forum-102523

Acting on our commitment to safe and secure AI

Bug bounty program specific to generative AI, and new ways to support open source security for AI supply chains

Google

Cyberthreats evolve quickly and some of the biggest vulnerabilities aren't discovered by companies or product manufacturers — but by outside security researchers. That's why we have a long history of supporting collective security through our Vulnerability Rewards Program (VRP), Project Zero and in the field of Open Source software security. It's also why we joined other leading AI companies at the White House earlier this year to commit to advancing the discovery of vulnerabilities in AI systems.



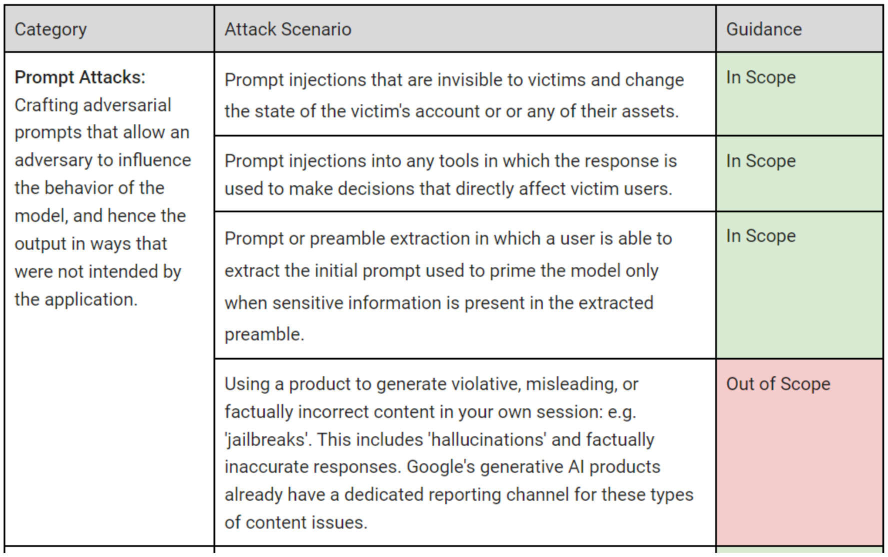
Welcome to Bug Hunter University

Here you'll find all you need to sharpen your ability, whether you're an advanced hunter or just starting out.

Today, we're expanding our VRP to reward for attack scenarios specific to generative AI. We believe this will incentivize research around AI safety and security, and bring potential issues to light that will ultimately make AI safer for everyone. We're also expanding our open source security work to make information about AI supply chain security universally discoverable and verifiable.

New technology requires new vulnerability reporting guidelines

As part of expanding VRP for AI, we're taking a fresh look at how bugs should be categorized and reported.



Category	Attack Scenario	Guidance
Prompt Attacks: Crafting adversarial prompts that allow an adversary to influence the behavior of the model, and hence the output in ways that were not intended by the application.	Prompt injections that are invisible to victims and change the state of the victim's account or or any of their assets.	In Scope
	Prompt injections into any tools in which the response is used to make decisions that directly affect victim users.	In Scope
	Prompt or preamble extraction in which a user is able to extract the initial prompt used to prime the model only when sensitive information is present in the extracted preamble.	In Scope
	Using a product to generate violative, misleading, or factually incorrect content in your own session: e.g. 'jailbreaks'. This includes 'hallucinations' and factually inaccurate responses. Google's generative AI products already have a dedicated reporting channel for these types of content issues.	Out of Scope

Generative AI raises new and different concerns than traditional digital security, such as the potential for unfair bias, model manipulation or misinterpretations of data (hallucinations).

As we continue to integrate generative AI into more products and features, our Trust and Safety teams are leveraging decades of experience and taking a comprehensive approach to better anticipate and test for these potential risks. But we understand that outside security researchers can help us find, and address, novel vulnerabilities that will in turn make our generative AI products even safer and more secure.

In August, we joined the White House and industry peers to enable thousands of third-party security researchers to find potential issues at DEF CON's largest-ever public Generative AI Red Team event.

Now, since we are expanding the bug bounty program and releasing additional guidelines for what we'd like security researchers to hunt, we're sharing those guidelines so that anyone can see what's "in scope." We expect this will spur security researchers to submit more bugs and accelerate the goal of a safer and more secure generative AI.

Two new ways to strengthen the AI Supply Chain

We introduced our Secure AI Framework (SAIF) — to support the industry in creating trustworthy applications — and have encouraged implementation through AI red teaming.

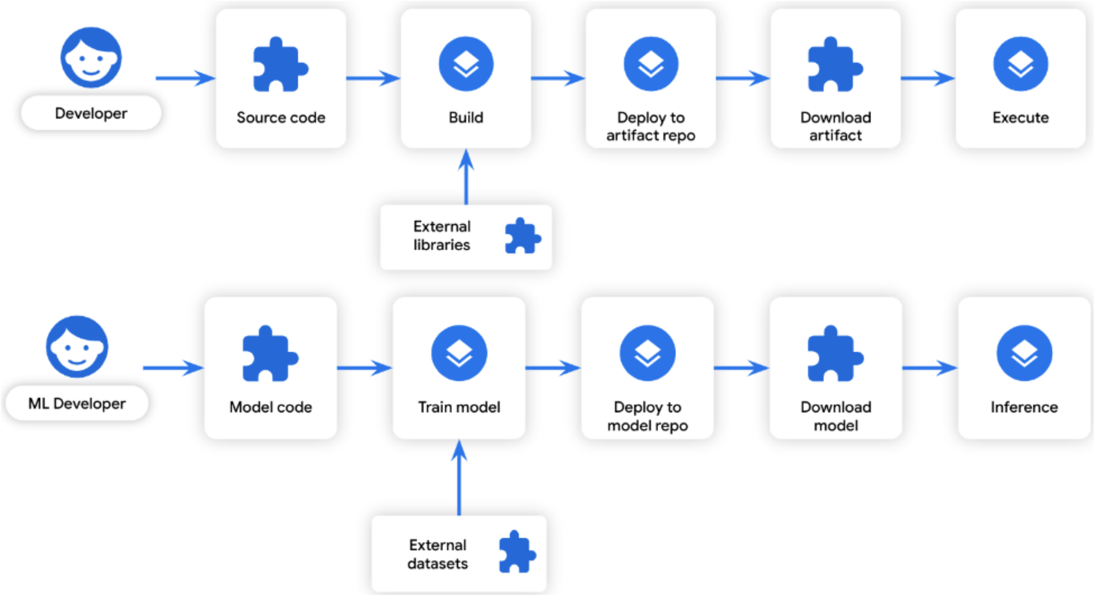
The first principle of SAIF is to ensure that the AI ecosystem has strong security foundations, and that means securing the critical supply chain components that enable machine learning (ML) against threats like model tampering, data poisoning, and the production of harmful content.

Today, to further protect against machine learning supply chain attacks, we're expanding our open source security work and building upon our prior collaboration with the Open Source Security Foundation.

The Google Open Source Security Team (GOSST) is leveraging SLSA and Sigstore to protect the overall integrity of AI supply chains.

SLSA involves a set of standards and controls to improve resiliency in supply chains, while Sigstore helps verify that software in the supply chain is what it claims to be. To get started, today we announced the availability of the first prototypes for model signing with Sigstore and attestation verification with SLSA.

These are early steps toward ensuring the safe and secure development of generative AI — and we know the work is just getting started. Our hope is that by incentivizing more security research while applying supply chain security to AI, we'll spark even more collaboration with the open source security community and others in industry, and ultimately help make AI safer for everyone.



Similarities between software development and ML model development

To read more: https://blog.google/technology/safety-security/google-ai-security-expansion/

Hiroshima Process - International Guiding Principles for Organizations Developing Advanced AI Systems

The Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems aims to promote safe, secure, and trustworthy AI worldwide and will provide guidance for organizations developing and using the most advanced AI systems, including the most advanced foundation models and generative AI systems (henceforth "advanced AI systems").

Organizations may include, among others, entities from academia, civil society, the private sector, and the public sector.

This non-exhaustive list of guiding principles is discussed and elaborated as a living document to build on the existing OECD AI Principles in response to recent developments in advanced AI systems and are meant to help seize the benefits and address the risks and challenges brought by these technologies.

These principles should apply to all AI actors, when and as applicable to cover the design, development, deployment and use of advanced AI systems.

We look forward to developing these principles further as part of the comprehensive policy framework, with input from other nations and wider stakeholders in academia, business and civil society.

We also reiterate our commitment to elaborate an international code of conduct for organizations developing advanced AI systems based on the guiding principles below.

Different jurisdictions may take their own unique approaches to implementing these guiding principles in different ways.

We call on organizations in consultation with other relevant stakeholders to follow these actions, in line with a risk-based approach, while governments develop more enduring and/or detailed governance and regulatory approaches.

We also commit to develop proposals, in consultation with the OECD, GPAI and other stakeholders, to introduce monitoring tools and mechanisms to help organizations stay accountable for the implementation of these actions.

We encourage organizations to support the development of effective monitoring mechanisms, which we may explore to develop, by contributing best practices. While harnessing the opportunities of innovation, organizations should respect the rule of law, human rights, due process, diversity, fairness and non-discrimination, democracy, and humancentricity, in the design, development and deployment of advanced AI systems.

Organizations should not develop or deploy advanced AI systems in a way that undermines democratic values, are particularly harmful to individuals or communities, facilitate terrorism, enable criminal misuse, or pose substantial risks to safety, security, and human rights, and are thus not acceptable.

States must abide by their obligations under international human rights law to promote that human rights are fully respected and protected, while private sector activities should be in line with international frameworks such as the United Nations Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises.

Specifically, we call on organizations to abide by the following principles, commensurate to the risks:

1. Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle.

This includes employing diverse internal and independent external testing measures, through a combination of methods such as red-teaming, and implementing appropriate mitigation to address identified risks and vulnerabilities.

Testing and mitigation measures should for example, seek to ensure the trustworthiness, safety and security of systems throughout their entire lifecycle so that they do not pose unreasonable risks.

In support of such testing, developers should seek to enable traceability, in relation to datasets, processes, and decisions made during system development.

2. Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.

Organizations should use, as and when appropriate commensurate to the level of risk, AI systems as intended and monitor for vulnerabilities, incidents, emerging risks and misuse after deployment, and take appropriate action to address these.

Organizations are encouraged to consider, for example, facilitating third-party and user discovery and reporting of issues and vulnerabilities after deployment.

Organizations are further encouraged to maintain appropriate documentation of reported incidents and to mitigate the identified risks and vulnerabilities, in collaboration with other stakeholders.

Mechanisms to report vulnerabilities, where appropriate, should be accessible to a diverse set of stakeholders.

3. Publicly report advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability.

This should include publishing transparency reports containing meaningful information for all new significant releases of advanced AI systems. Organizations should make the information in the transparency reports sufficiently clear and understandable to enable deployers and users as appropriate and relevant to interpret the model/system's output and to enable users to use it appropriately, and that transparency reporting should be supported and informed by robust documentation processes.

4. Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.

This includes responsibly sharing information, as appropriate, including, but not limited to evaluation reports, information on security and safety risks, dangerous intended or unintended capabilities, and attempts by AI actors to circumvent safeguards across the AI lifecycle.

5. Develop, implement and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in particular for organizations developing advanced AI systems.

This includes disclosing where appropriate privacy policies, including for personal data, user prompts and advanced AI system outputs.

Organizations are expected to establish and disclose their AI governance policies and organizational mechanisms to implement these policies in accordance with a risk-based approach.

This should include accountability and governance processes to evaluate and mitigate risks, where feasible throughout the AI lifecycle.

6. Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

These may include securing model weights and algorithms, servers, and datasets, such as through operational security measures for information security and appropriate cyber/physical access controls.

7. Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content.

This includes, where appropriate and technically feasible, content authentication such provenance mechanisms for content created with an organization's advanced AI system.

The provenance data should include an identifier of the service or model that created the content, but need not include user information.

Organizations should also endeavor to develop tools or APIs to allow users to determine if particular content was created with their advanced AI system such as via watermarks.

Organizations are further encouraged to implement other mechanisms such as labeling or disclaimers to enable users, where possible and appropriate, to know when they are interacting with an AI system.

8. Prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.

This includes conducting, collaborating on and investing in research that supports the advancement of AI safety, security and trust, and addressing key risks, as well as investing in developing appropriate mitigation tools.

9. Prioritize the development of advanced AI systems to address the world's greatest challenges, notably but not limited to the climate crisis, global health and education.

These efforts are undertaken in support of progress on the United Nations Sustainable Development Goals, and to encourage AI development for global benefit. Organizations should prioritize responsible stewardship of trustworthy and human-centric AI and also support digital literacy initiatives.

10. Advance the development of and, where appropriate, adoption of international technical standards.

This includes contributing to the development and, where appropriate, use of international technical standards and best practices, including for watermarking, and working with Standards Development Organizations (SDOs).

11. Implement appropriate data input measures and protections for personal data and intellectual property.

Organizations are encouraged to take appropriate measures to manage data quality, including training data and data collection, to mitigate against harmful biases.

Appropriate transparency of training datasets should also be supported and organizations should comply with applicable legal frameworks.

To read more:
https://www.mofa.go.jp/files/100573471.pdf

G7 Leaders’ Statement on the Hiroshima AI Process

THE WHITE HOUSE

We, the Leaders of the Group of Seven (G7), stress the innovative opportunities and transformative potential of advanced Artificial Intelligence (AI) systems, in particular, foundation models and generative AI.

We also recognize the need to manage risks and to protect individuals, society, and our shared principles including the rule of law and democratic values, keeping humankind at the center. We affirm that meeting those challenges requires shaping an inclusive governance for artificial intelligence.

Building on the progress made by relevant ministers on the Hiroshima AI Process, including the G7 Digital & Tech Ministers’ Statement issued on September 7, 2023, we welcome the Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems and the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems (https://www.mofa.go.jp/ecm/ec/page5e_000076.html).

In order to ensure both documents remain fit for purpose and responsive to this rapidly evolving technology, they will be reviewed and updated as necessary, including through ongoing inclusive multistakeholder consultations. We call on organizations developing advanced AI systems to commit to the application of the International Code of Conduct.

We instruct relevant ministers to accelerate the process toward developing the Hiroshima AI Process Comprehensive Policy Framework, which includes project based cooperation, by the end of this year, in cooperation with the Global Partnership for Artificial Intelligence (GPAI) and the Organisation for Economic Co-operation and Development (OECD), and to conduct multi-stakeholder outreach and consultation, including with governments, academia, civil society, and the private sector, not only those in the G7 but also in the economies beyond, including developing and emerging economies.

We also ask relevant ministers to develop a work plan by the end of the year for further advancing the Hiroshima AI Process.

We believe that our joint efforts through the Hiroshima AI Process will foster an open and enabling environment where safe, secure, and trustworthy AI systems are designed, developed, deployed, and used to maximize the benefits of the technology while mitigating its risks, for the common good worldwide, including in developing and emerging economies with a view to closing digital divides and achieving digital inclusion. We also look forward to the UK’s AI Safety Summit on November 1 and 2.

To read more: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/g7-leaders-statement-on-the-hiroshima-ai-process/

The European Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence

The Commission welcomes the agreement by G7 leaders on International Guiding Principles on Artificial Intelligence (AI) and a voluntary Code of Conduct for AI developers under the Hiroshima AI process.

These principles and the voluntary Code of Conduct will complement, at international level, the legally binding rules that the EU co-legislators are currently finalising under the EU AI Act.

President of the European Commission, Ursula von der Leyen, was among those who subscribed to the G7 leaders' statement issued by the 2023 Japan G7 presidency.

President von der Leyen, said: "The potential benefits of Artificial Intelligence for citizens and the economy are huge. However, the acceleration in the capacity of AI also brings new challenges. Already a regulatory frontrunner with the AI Act, the EU is also contributing to AI guardrails and governance at global level. I am pleased to welcome the G7 international Guiding Principles and the voluntary Code of Conduct, reflecting EU values to promote trustworthy AI. I call on AI developers to sign and implement this Code of Conduct as soon as possible."

Ensuring safety and trustworthiness of the technology

The eleven Guiding Principles adopted by the leaders of the seven countries and the EU, which make up the G7, provide guidance for organisations developing, deploying and using advanced AI systems, such as foundation models and generative AI, to promote safety and trustworthiness of the technology.

They include commitments to mitigate risks and misuse and identify vulnerabilities, to encourage responsible information sharing, reporting of incidents, and investment in cybersecurity as well as a labelling system to enable users to identify AI-generated content.

Informed by the results of a stakeholder survey, these principles have been jointly developed by the EU with the other G7 members, under the Hiroshima Artificial Intelligence Process.

The Guiding Principles have in turn served as the basis to compile a Code of Conduct, which will provide detailed and practical guidance for organisations developing AI.

The voluntary Code of Conduct will also promote responsible governance of AI globally. Both documents will be reviewed and updated as necessary, including through inclusive multistakeholder consultations, to ensure they remain fit for purpose and responsive to this rapidly evolving technology.

The G7 leaders have called on organisations developing advanced AI systems to commit to the application of the International Code of Conduct.

The first signatories will be announced in the near future.

Background

The G7 Hiroshima Artificial Intelligence Process was established at the G7 Summit on 19 May 2023 to promote guardrails for advanced AI systems on a global level.

The initiative is part of a wider range of international discussions on guardrails for AI, including at the OECD, the Global Partnership on Artificial Intelligence (GPAI) and in the context of the EU-U.S. Trade and Technology Council and the EU's Digital Partnerships.

Since first announcing its intention to work on a Code of Conduct at the TTC Ministerial of 31 May 2023, the European Commission actively worked with key international partners in the G7 to develop the principles and the Code of Conduct on AI.

These international commitments are consistent with the legally binding rules currently being negotiated as part of the more comprehensive Artificial Intelligence Act (EU AI Act), which will apply in the EU.

The proposal for the EU AI Act will guarantee the safety and fundamental rights of people and businesses, while strengthening AI uptake, investment and innovation across the EU.

The AI Act will provide risk-based, legally binding rules for AI systems that are placed on the market or put into service in the Union market.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5379

PHISHING GUIDANCE: STOPPING THE ATTACK CYCLE AT PHASE ONE

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

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.

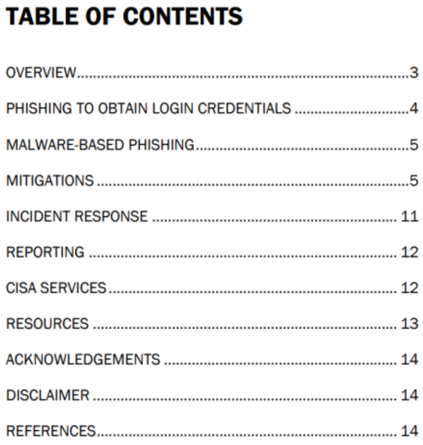


TABLE OF CONTENTS

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

PHISHING GUIDANCE:

STOPPING THE ATTACK CYCLE AT PHASE ONE

Understanding Cognitive Security

CSRL
Cognitive Security Research Lab

Cognitive security is maintaining rational decision-making under adversarial conditions. It entails generally accepting the same shared reality and rules of the game to come to a decision, resisting/mitigating emotional manipulation and protecting individuals and societies to enable collective action to solve problems.

Risks to cognitive security include the following:

- Manipulating human decision-making
- Hacking the "human" of the human-machine team
- Person-to-group behavior manipulation
- How to get information to the human (symbiotic human-computer interface)
- Expanding beyond HMI to HME (human-machine environment or human-machine ecosystem)
- Narrative weaponization
- Politicized and monetized information environments

Our research aims to develop new tools and methodologies to protect decision-making in the face of persistent social-cyber adversarial conditions and environments.

We seek to define and detect attacks against individuals, society, etc. meant to confuse, delay, and degrade action, while researching and developing novel tools and methodologies to assess the information space, at all levels (e.g., operational, strategic) and phases (e.g., competition, conflict) of conflict.

Finally, our research investigates and explores over the horizon at emerging and future threats to cognitive security. Some example research lab outputs include developing and maintaining customized social-cyber analysis and analytic capabilities, as well as advising on mitigating/countering/monitoring/etc. social-cyber threats.

Cyber modeling and simulation (M&S) allows the exploration of complex interrelation between humans, software, and hardware systems and how they can lead to vulnerabilities or resilience. The ACI's Cyber Modeling and Simulation Research Lab (CMSRL) enables the exploration of cyber modeling and simulation in decision making and provides context and understanding of cyber risk, allowing for the development of methods and tooling to identify and mitigate vulnerabilities in systems. By creating abstractions of the physical world and using cutting edge tools to support multiple-domain operations, we can examine these interactions and changes in the system overtime and create scalable solutions.

The next-generation battlefield will be populated with a vast number of interconnected, heterogeneous and sometimes autonomous agents including devices, networks, software, and humans.

Defending such complex and/or autonomous systems will be impossible for humans to do alone, making our research key in defending such system.

In response to the challenges facing the Cyber and Information Domain, our research directly supports the Army, Department of Defense, Intelligence Community, and Nation in the research, design, development, experimentation, testing, evaluation and operationalization of computationally intelligent, assured (secure, resilient, robust, trusted), and distributed decision-support models, tools, and systems for autonomous cyber operations in highly-contested, complex battlefield environments.

To build, assess and deploy smart, autonomous cyber-systems that enable intelligent, assured and federated decision-making, our research explores the science of information, computation, learning, and fusion for adaptive, collaborative pattern discovery, reasoning, perception, action and decision-making given heterogenous, complex, disparate data spanning devices, networks, software, and humans.

Our research aims to develop models and tools for collective intelligence, likely augmented by interacting with human cyber analysts and decision-makers. In conducting basic and applied research in the areas of data science, operations research, artificial intelligence, cognitive science, scientific computing and advanced analytics, our research seeks to tackle a multitude of challenges in infrastructure and architecture engineering, individual and collective decision-making, stealth and resilience, as well as society.

Specifically, our research aims to provide new capabilities to:

- Shift emphasis from sensing to information awareness
- Understand the underpinning of autonomy

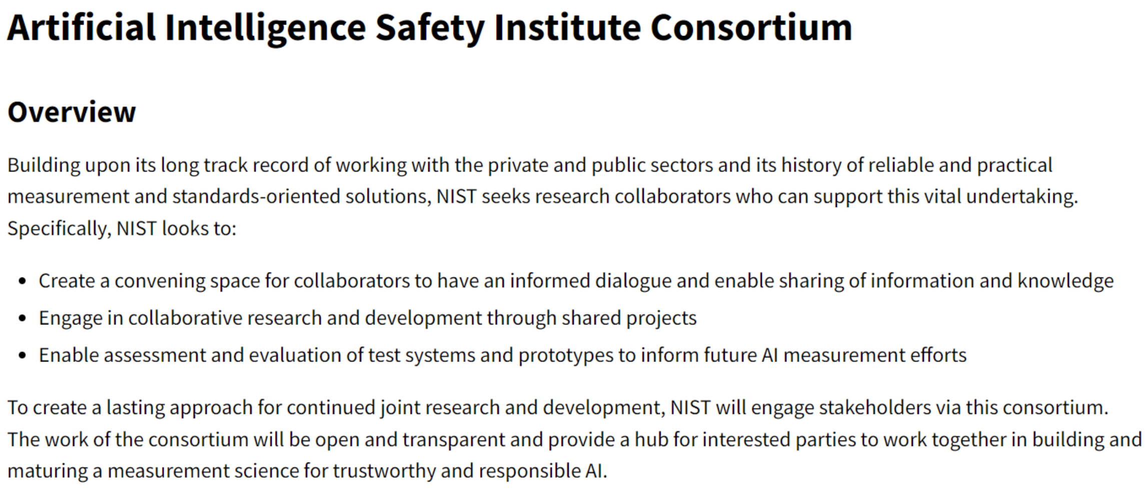
- Relieve human cognitive overload in dealing with the data deluge problem
- Enhance human-machine interface in information processing
- Cope with various complex disparate data/information types
- Integrate a diversity of unique reasoning and learning components collaborating simultaneously
- Bridge correlational with causal discovery
- Determine solutions or obstructions to local-to-global data fusion problems
- Mechanize reasoning/learning and computing in the same computational environment
- Yield provably efficient procedures to enable or facilitate advanced data analytics
- Deal with high-dimensional and massive datasets with provably guaranteed performance

To read more: https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/

NIST Seeks Collaborators for Consortium Supporting Artificial Intelligence Safety

The AI Safety Institute Consortium will help develop tools to measure and improve AI safety and trustworthiness.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) is calling for participants in a new consortium supporting development of innovative methods for evaluating artificial intelligence (AI) systems to improve the rapidly growing technology's safety and trustworthiness. This consortium is a core element of the new NIST-led U.S. AI Safety Institute announced yesterday at the U.K.'s AI Safety Summit 2023, in which U.S. Secretary of Commerce Gina Raimondo participated. You may visit: https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute



Artificial Intelligence Safety Institute Consortium

Overview

Building upon its long track record of working with the private and public sectors and its history of reliable and practical measurement and standards-oriented solutions, NIST seeks research collaborators who can support this vital undertaking. Specifically, NIST looks to:

- Create a convening space for collaborators to have an informed dialogue and enable sharing of information and knowledge
- Engage in collaborative research and development through shared projects
- Enable assessment and evaluation of test systems and prototypes to inform future AI measurement efforts

To create a lasting approach for continued joint research and development, NIST will engage stakeholders via this consortium. The work of the consortium will be open and transparent and provide a hub for interested parties to work together in building and maturing a measurement science for trustworthy and responsible AI.

The institute and its consortium are part of NIST's response to the recently released Executive Order on Safe, Secure, and Trustworthy Development and Use of AI.

OCTOBER 30, 2023

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

The EO tasks NIST with a number of responsibilities, including development of a companion resource to the AI Risk Management Framework (AI RMF) focused on generative AI, guidance on authenticating content created by humans and watermarking AI-generated content, a new initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, and creation of test environments for AI systems. NIST will rely heavily on engagement with industry and relevant stakeholders in carrying out these assignments. The new institute and consortium are central to those efforts.

“The U.S. AI Safety Institute Consortium will enable close collaboration among government agencies, companies and impacted communities to help ensure that AI systems are safe and trustworthy,” said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. “Together we can develop ways to test and evaluate AI systems so that we can benefit from AI’s potential while also protecting safety and privacy.”

The U.S. AI Safety Institute will harness work already underway by NIST and others to build the foundation for trustworthy AI systems, supporting use of the AI RMF, which NIST released in January 2023. The framework offers a voluntary resource to help organizations manage the risks of their AI systems and make them more trustworthy and responsible. The institute aims to measurably improve organizations’ ability to evaluate and validate AI systems, as detailed in the AI RMF Roadmap.

“The institute's collaborative research will strengthen the scientific underpinnings of AI measurement so that extraordinary innovations in artificial intelligence can benefit all people in a safe and equitable way,” said NIST’s Elham Tabassi, federal AI standards coordinator and a member of the National AI Research Resource Task Force.

Building on its long track record of working with the private and public sectors as well as its history of measurement and standards-oriented solutions, NIST is seeking collaborators from across society to join the consortium.

The consortium will function as a convening space for an informed dialogue and the sharing of information and insights. It will be a vehicle to support collaborative research and development through shared projects, and will promote the assessment and evaluation of test systems and prototypes to inform future AI measurement efforts.

“Participation in the consortium is open to all organizations interested in AI safety that can contribute through combinations of expertise, products, data and models,” said Jacob Taylor, NIST’s senior advisor for critical and emerging technologies. “NIST is responsible for helping industry understand how to manage the risks inherent in AI products. To do so, NIST intends to work with stakeholders at the intersection of the technical and the applied. We want the U.S. AI Safety Institute to be highly interactive because the technology is emerging so quickly, and the consortium can help ensure that the community’s approach to safety evolves alongside.”

In particular, NIST is soliciting responses from all organizations with relevant expertise and capabilities to enter into a consortium cooperative research and development agreement (CRADA) to support and demonstrate pathways to enable safe and trustworthy AI. Members would be expected to contribute:

- Expertise in one or more of several specific areas, including AI metrology, responsible AI, AI system design and development, human-AI teaming and interaction, socio-technical methodologies, AI explainability and interpretability, and economic analysis;

- Models, data and/or products to support and demonstrate pathways to enable safe and trustworthy AI systems through the AI RMF;

- Infrastructure support for consortium projects; and

- Facility space and handling of hosting consortium researchers, workshops and conferences.

Interested organizations with relevant technical capabilities should submit a letter of interest by Dec. 2, 2023. More details on NIST's request for collaborators are available in the Federal Register. NIST plans to host a workshop on Nov. 17, 2023, for those interested in learning more about the consortium and engaging in the conversation about AI safety.

The U.S. AI Safety Institute will partner with other U.S. government agencies on evaluating AI capabilities, limitations, risks and impacts and coordinate on building testbeds. The institute will also work with organizations in ally and partner countries to share best practices, align capability evaluation, and red-team guidance and benchmarks.

To read more: https://www.nist.gov/news-events/news/2023/11/nist-seeks-collaborators-consortium-supporting-artificial-intelligence

NIST's Responsibilities Under the October 30, 2023 Executive Order

The President's Executive Order (EO) on Safe, Secure, and Trustworthy Artificial Intelligence issued on October 30, 2023, charges multiple agencies – including NIST – with producing guidelines and taking other actions to advance the safe, secure, and trustworthy development and use of Artificial Intelligence (AI).

The EO directs NIST to develop guidelines and best practices to promote consensus industry standards that help ensure the development and deployment of safe, secure, and trustworthy AI systems. Specifically, NIST is to:

1. Develop a companion resource to the AI Risk Management Framework focused on generative AI

2. Develop a companion resource to the Secure Software Development Framework to incorporate secure-development practices for generative AI and dual-use foundation models

3. Launch a new initiative to create guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities that could cause harm

4. Establish guidelines and processes – except for AI used as a component of a national security system – to enable developers of generative AI, especially dual-use foundation models, to conduct AI red-teaming tests for deployment of safe, secure, and trustworthy systems. This includes:

4.1. Coordinating or developing guidelines related to assessing and managing the safety, security, and trustworthiness of dual-use foundation models and related to privacy-preserving machine learning

4.2. In coordination with the Secretary of Energy and the Director of the National Science Foundation (NSF), developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies, as well as support the design, development, and deployment of associated privacy-enhancing technologies (PETs)

5. Engage with industry and relevant stakeholders to develop and refine (for possible use by synthetic nucleic acid sequence providers):

5.1. Specifications for effective nucleic acid synthesis procurement screening

5.2. Best practices, including security and access controls, for managing sequence-of-concern databases to support such screening

5.3. Technical implementation guides for effective screening

5.4. Conformity assessment best practices and mechanisms

6. Develop a report to the Director of OMB identifying existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques, for:

6.1. Authenticating content and tracking its provenance

6.2. Labeling synthetic content (e.g., watermarking)

6.3. Detecting synthetic content

6.4. Preventing generative AI from producing Child Sexual Abuse Material or producing non-consensual intimate imagery of real individuals

6.5. Testing software used for the above purposes

6.6. Auditing and maintaining synthetic content

7. Create guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI.

8. Develop guidelines, tools, and practices to support agencies' implementation of minimum risk-management practices.

9. Assist the Secretary of Commerce in coordinating with key international partners and standards development organizations to drive the development and implementation of AI-related consensus standards, cooperation, and information sharing.

Then the Secretary of Commerce (coordinating with the Secretary of State and heads of other Federal agencies) will establish a plan for global engagement to promote and develop AI standards.

These efforts are to be guided by principles set out in the NIST AI Risk Management Framework and the US Government National Standards Strategy for Critical and Emerging Technology, which is led by NIST.

In some assignments, NIST will be working on behalf of the Secretary of Commerce.

NIST is to consult with other agencies in producing some of its guidance; in turn, several of those agencies are directed to consult NIST (directly or through the Secretary of Commerce) in accomplishing their actions under the EO.

Most of the EO tasks to NIST have a 270 day deadline.

In addition to working with government agencies, NIST intends to engage with the private sector, academia, and civil society as it produces guidance called for by the EO.

NIST will build and expand on current efforts in several of these areas.

That includes the Generative AI Public Working Group established in June 2023.

To read more: https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence

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

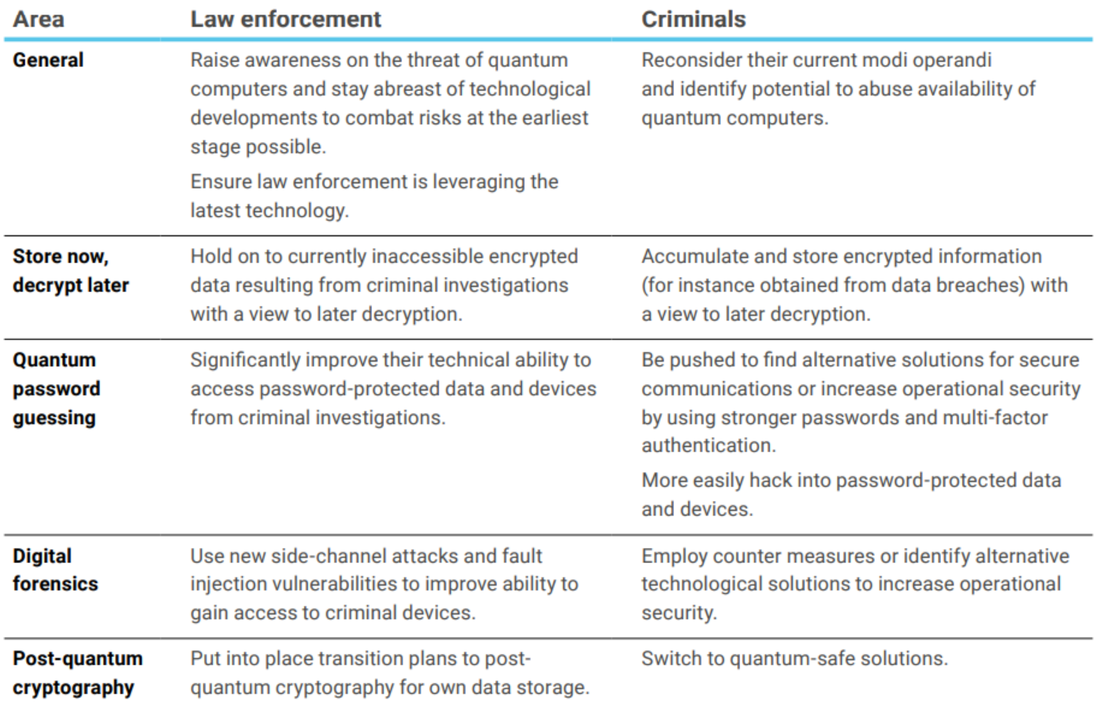
Quantum computing and quantum technologies hold significant potential to improve a wide range of applications and tasks.

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.

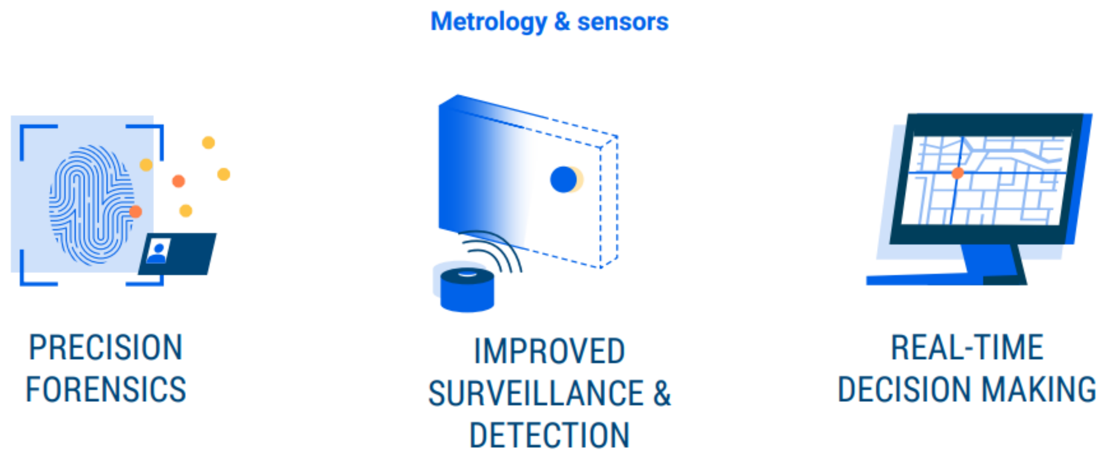
In offering an extensive look at the wide range of potential applications in this context, this report is the first of its kind.

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.

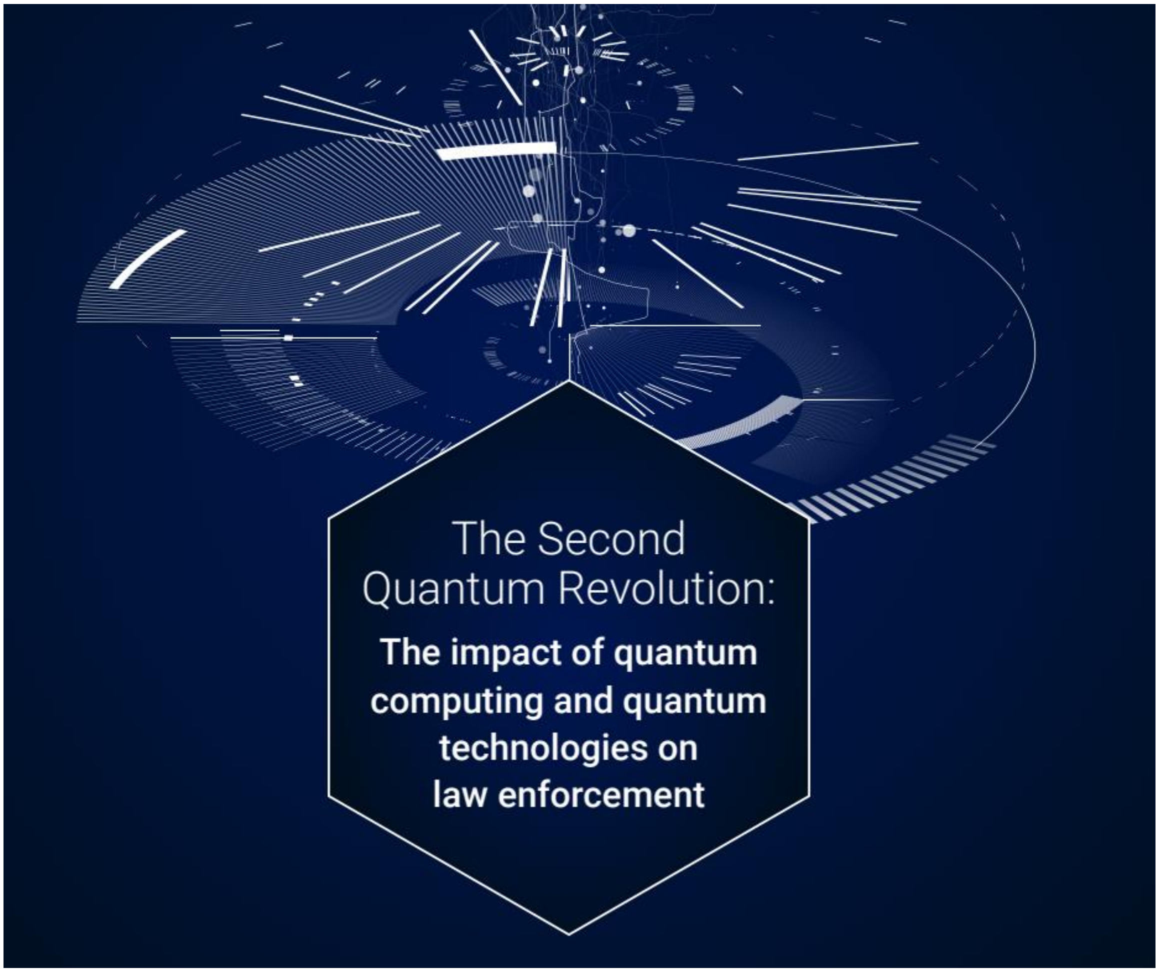
From the perspective of law enforcement, post-quantum cryptography has two major areas of impact.

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 Sarbanes-Oxley Compliance Professionals Association (SOXCPA) (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.

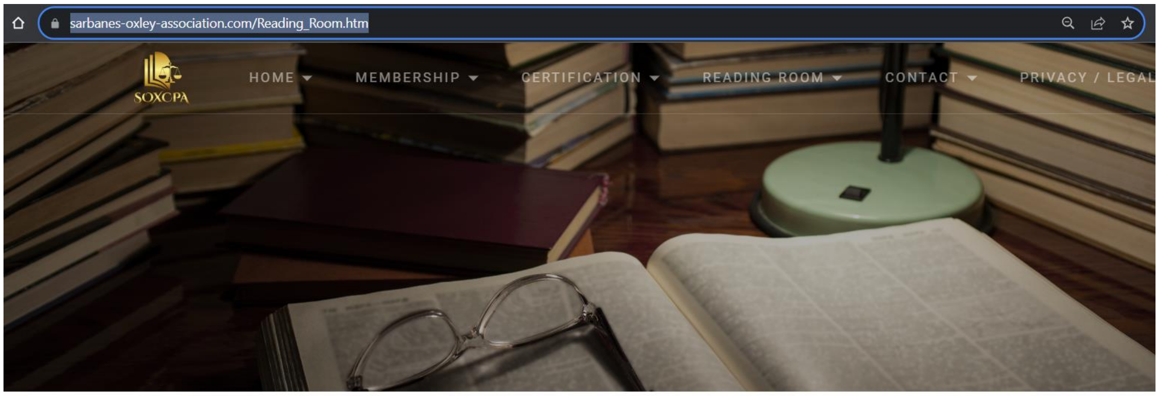
Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Welcome to the Sarbanes-Oxley Compliance Professionals Association (SOXCPA), the largest Association of Sarbanes-Oxley professionals in the world.

The Sarbanes-Oxley Compliance Professionals Association (SOXCPA) 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 and provide independent evidence that you are a Sarbanes-Oxley expert.

Our reading room:
https://www.sarbanes-oxley-association.com/Reading_Room.htm



Reading Room, Sarbanes-Oxley Compliance Professionals Association (SOXCPA)

Our monthly newsletter:

Our training and certification programs.

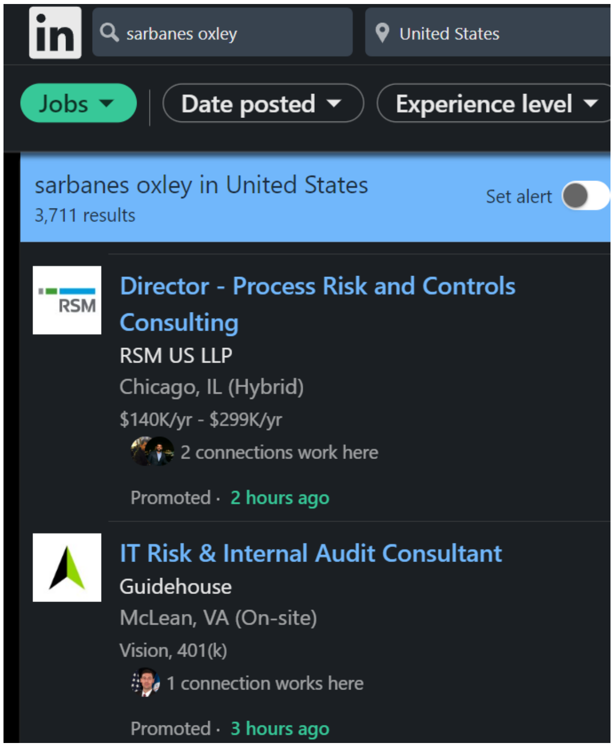
1. Certified Sarbanes-Oxley Expert (CSOE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

2. Certified Japanese Sarbanes-Oxley Expert (CJSOXE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

3. Certified EU Sarbanes-Oxley Expert (CEUSOE), distance learning and online certification program. You may visit: https://www.sarbanes-oxley-association.com/CEUSOE_Distance_Learning_and_Certification.htm

Sarbanes-Oxley is a hot skill that makes a manager or an employee an indispensable asset to a company or organization. There are thousands of new Sarbanes-Oxley jobs advertised in many countries.

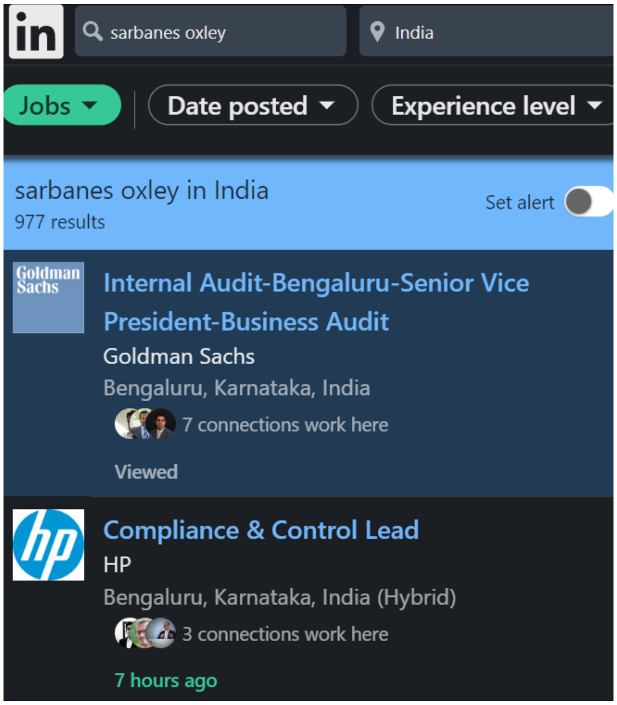
Some examples from LinkedIn:



sarbanes oxley in United States
3,711 results

Director - Process Risk and Controls Consulting
RSM US LLP
Chicago, IL (Hybrid)
$140K/yr - $299K/yr
2 connections work here
Promoted · 2 hours ago

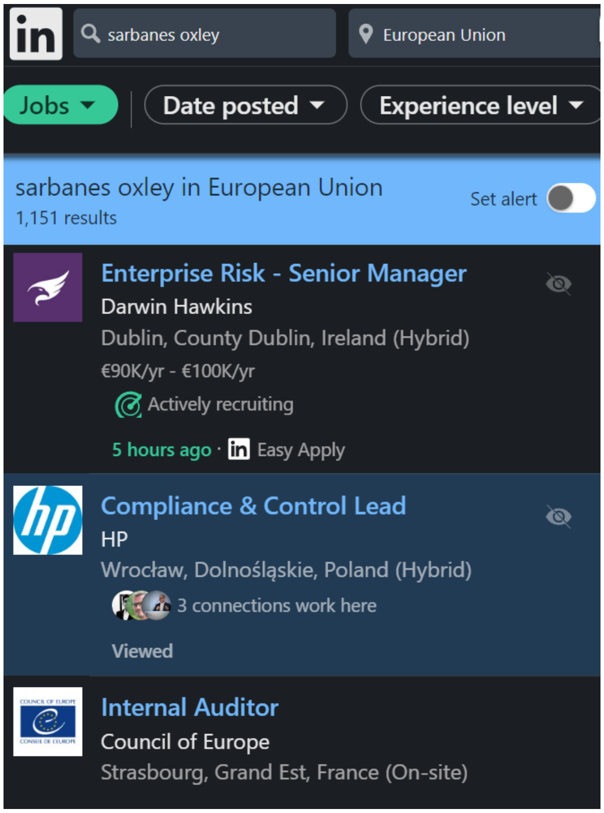
IT Risk & Internal Audit Consultant
Guidehouse
McLean, VA (On-site)
Vision, 401(k)
1 connection works here
Promoted · 3 hours ago



sarbanes oxley in India
977 results

Internal Audit-Bengaluru-Senior Vice President-Business Audit
Goldman Sachs
Bengaluru, Karnataka, India
7 connections work here
Viewed

Compliance & Control Lead
HP
Bengaluru, Karnataka, India (Hybrid)
3 connections work here
7 hours ago



sarbanes oxley

European Union

Jobs

Date posted

Experience level

sarbanes oxley in European Union

1,151 results

Set alert

Enterprise Risk - Senior Manager
Darwin Hawkins
Dublin, County Dublin, Ireland (Hybrid)
€90K/yr - €100K/yr
Actively recruiting
5 hours ago · Easy Apply

Compliance & Control Lead
HP
Wrocław, Dolnośląskie, Poland (Hybrid)
3 connections work here
Viewed

Internal Auditor
Council of Europe
Strasbourg, Grand Est, France (On-site)

Contact Us

Lyn Spooner
Email: lyn@sarbanes-oxley-association.com

George Lekatis
President of the SOXCPA
1200 G Street NW Suite 800,
Washington DC 20005, USA
Email: lekatis@sarbanes-oxley-association.com
Web: www.sarbanes-oxley-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA

Our reading room:
https://www.sarbanes-oxley-association.com/Reading_Room.htm