Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, January 2023

Dear members and friends,

We will start with the joint statement on crypto-asset risks to banking.

Agencies issue joint statement on crypto-asset risks to banking organizations

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing the following statement on crypto-asset1 risks to banking organizations.

The events of the past year have been marked by significant volatility and the exposure of vulnerabilities in the crypto-asset sector. These events highlight a number of key risks associated with crypto-assets and crypto-asset sector participants that banking organizations should be aware of, including:

- Risk of fraud and scams among crypto-asset sector participants.

- Legal uncertainties related to custody practices, redemptions, and ownership rights, some of which are currently the subject of legal processes and proceedings.

- Inaccurate or misleading representations and disclosures by crypto-asset companies, including misrepresentations regarding federal deposit insurance, and other practices that may be unfair, deceptive, or abusive, contributing to significant harm to retail and institutional investors, customers, and counterparties.

- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.

- Susceptibility of stablecoins to run risk, creating potential deposit outflows for banking organizations that hold stablecoin reserves.

- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements. These interconnections may also present concentration risks for banking organizations with exposures to the crypto-asset sector.

- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.

- Heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to, the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.

It is important that risks related to the crypto-asset sector that cannot be mitigated or controlled do not migrate to the banking system. The agencies are supervising banking organizations that may be exposed to risks stemming from the crypto-asset sector and carefully reviewing any proposals from banking organizations to engage in activities that involve crypto-assets.

Through the agencies' case-by-case approaches to date, the agencies continue to build knowledge, expertise, and understanding of the risks crypto-assets may pose to banking organizations, their customers, and the broader U.S. financial system.

Given the significant risks highlighted by recent failures of several large crypto-asset companies, the agencies continue to take a careful and cautious approach related to current or proposed crypto-asset-related activities and exposures at each banking organization.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf

Addressing the risks in crypto: laying out the options

Matteo Aquilina, Jon Frost and Andreas Schrimpf

BIS

Key takeaways

• The recent high-profile failures of FTX and other crypto firms have re-ignited the debate on the appropriate policy response to address the risks in crypto, including through regulation.

• The "shadow financial" functions enabled by crypto markets share many of the vulnerabilities of traditional finance. These risks are exacerbated by specific features of crypto.

• Authorities may consider different – not mutually exclusive – lines of action to tackle the risks in crypto. These include containment or regulation of the crypto sector or an outright ban.

• Central banks and public authorities could also work to make TradFi more attractive. A key option is to encourage sound innovation with central bank digital currencies (CBDCs).

After the failure of several major crypto firms, addressing the risks from crypto markets has become a more pressing policy issue.

Cryptoasset markets have gone through booms and busts before, and so far, the busts have not led to wider contagion threatening financial stability. Yet the scale and prominence of recent failures heighten the urgency of addressing these risks before crypto markets become systemic.

The crypto ecosystem and the "shadow financial" functions it engages in, through centralised financial entities (CeFi) and decentralised finance (DeFi) protocols, share many of the vulnerabilities that are familiar from traditional finance (TradFi).

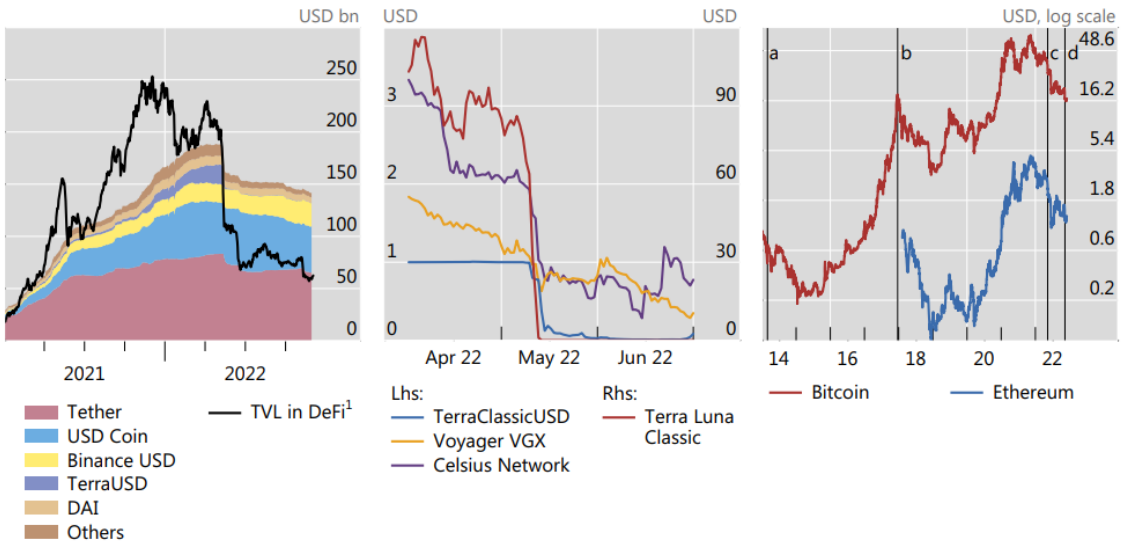
But several factors exacerbate the standard risks. These relate to high leverage, liquidity and maturity mismatches and substantial information asymmetries. Policy responses should consider how to address these sources of risk appropriately, given the borderless nature of crypto.

This bulletin briefly summarises the lessons of the 2022 turmoil. It then outlines three – non-mutually exclusive – lines of action to address the risks in crypto: a ban, containment and regulation, as well as their pros and cons. It also outlines complementary lines of policy action to address inefficiencies in TradFi and curb the demand for crypto.

One key option would be to encourage sound innovation with CBDCs. An online appendix gives a selective overview of ongoing initiatives in crypto regulation.

The recent crypto turmoil: features and lessons

Prices and market capitalisation of crypto assets and the 2022 turmoil — Graph 1



[a] Bankruptcy of Mt Gox on 28 February 2014. [b] Bursting of ICO bubble on 22 December 2017. [c] TerraUSD implosion on 9 May 2022. [d] Bankruptcy of FTX on 11 November 2022.

[1] TVL (total value locked) refers to the total dollar amount of assets that is staked across all DeFi protocols. It does not refer to transaction volumes or the market capitalisation of cryptocurrencies, but rather to the value of reserves that are "locked" into smart contracts. The TVL may vary depending upon the source and is subject to overestimation.

Sources: Bloomberg; CoinGecko; DefiLlama.

After peaking in late 2021, when cryptoasset prices, stablecoin volumes and DeFi activity reached all-time highs (Graph 1, left-hand panel), the crypto ecosystem faced turmoil in 2022.

The decline started early in the year, but problems became acute in May. It was then that a large stablecoin, TerraUSD (UST) – which relied on an algorithm to maintain its peg to the US dollar – collapsed, causing contagion in crypto markets (Graph 1, centre panel).

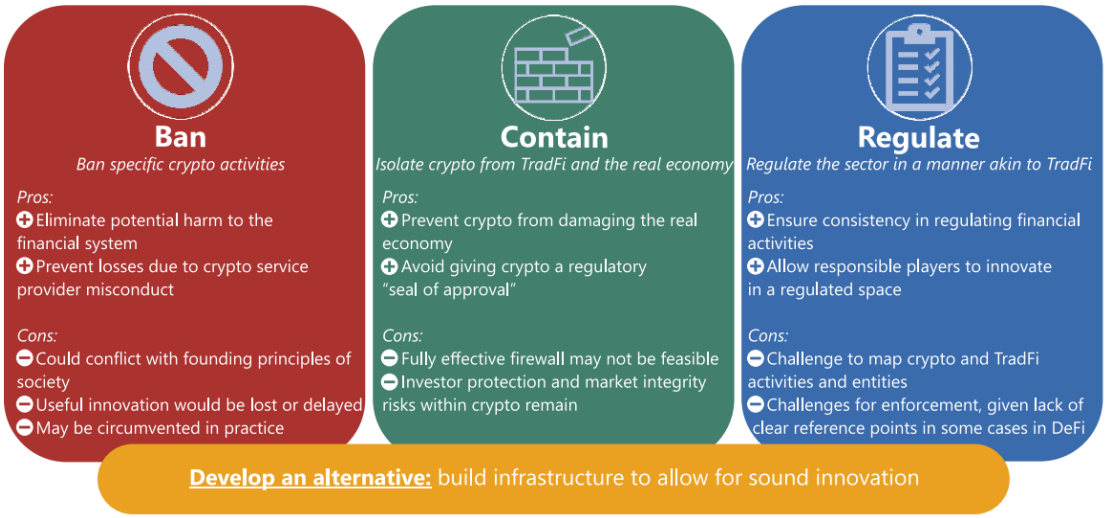
A period of relative calm followed, but crypto markets again saw serious stress in November 2022, when the FTX crypto trading platform declared bankruptcy. In the past, despite repeated turmoil, the crypto ecosystem has survived and prices have often recovered (Graph 1, right-hand panel). There are thus reasons to doubt that crypto will fade away on its own. In particular, a substantial part of the crypto community firmly believes in the ideological pursuit of a decentralised system as an alternative to TradFi.

And in response to recent events, many proponents of crypto claim that decentralisation and the underlying crypto technology are the solution rather than the problem.

They argue that while CeFi entities like FTX were at the epicentre of the stress, DeFi protocols and underlying blockchains continued to function, concluding that only “true” DeFi can be resilient.1

To read more: https://www.bis.org/publ/bisbull66.pdf

Options for addressing the risks in crypto: pros and cons Graph 2



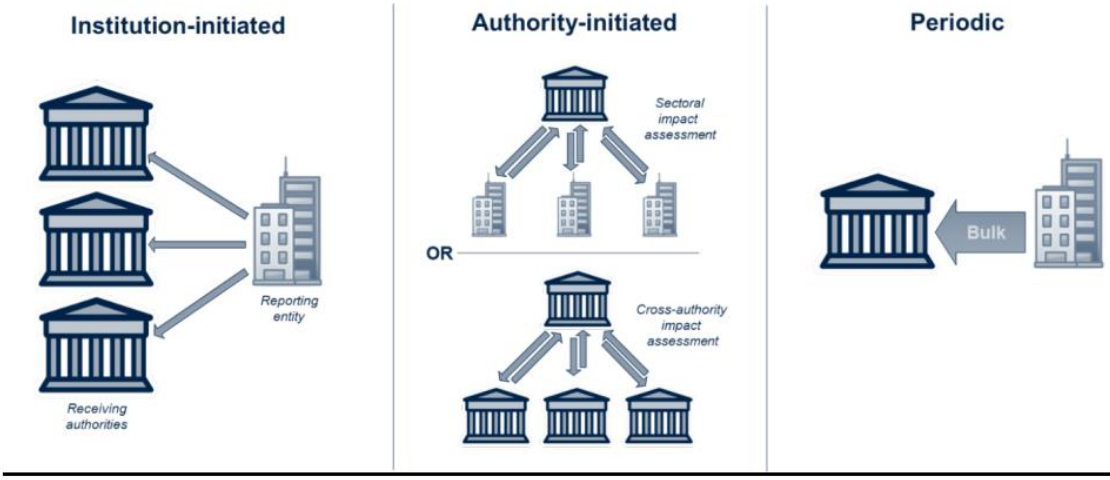
Public responses to consultation on achieving greater convergence in cyber incident reporting

On 17 October 2022, the FSB published Achieving Greater Convergence in Cyber Incident Reporting – Consultative document. You may visit: https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/

Achieving Greater Convergence in Cyber Incident Reporting

Consultative Document

Illustration of reporting types Figure 6

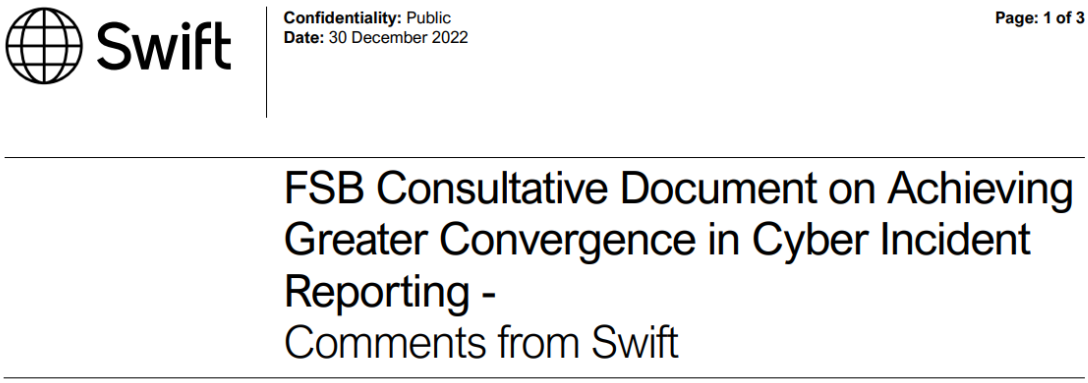


Interested parties were invited to provide written comments by 31 December 2022. The public comments received are available below.

The FSB thanks those who took the time and effort to express their views. The FSB expects to publish the final report in April 2023.

We have very interesting responses from:

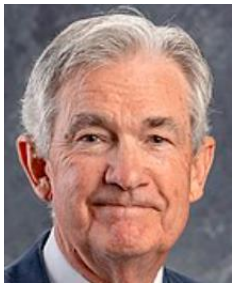
- Banking Association of South Africa
- EBA Clearing
- European Banking Federation
- Financial Services Sector Coordinating Council
- German Banking Industry Committee
- Global Financial Markets Association
- Global Legal Entity Identifier Foundation
- Google Cloud
- Institute of International Finance
- Insurance Europe
- Intesa Sanpaolo
- NASDAQ
- SWIFT
- Swiss Insurance Association
- UK Finance
- Unipol
- World Council
- World Federation of Exchanges



To read more: https://www.fsb.org/2023/01/public-responses-to-consultation-on-achieving-greater-convergence-in-cyber-incident-reporting/

Panel on "Central Bank Independence and the Mandate—Evolving Views"

Chair Jerome H. Powell, at the Symposium on Central Bank Independence, Sveriges Riksbank, Stockholm, Sweden



I will address three main points.

First, the Federal Reserve's monetary policy independence is an important and broadly supported institutional arrangement that has served the American public well.

Second, the Fed must continuously earn that independence by using our tools to achieve our assigned goals of maximum employment and price stability, and by providing transparency to facilitate understanding and effective oversight by the public and their elected representatives in Congress.

Third, we should "stick to our knitting" and not wander off to pursue perceived social benefits that are not tightly linked to our statutory goals and authorities.

Central bank independence and transparency

On the first point, the case for monetary policy independence lies in the benefits of insulating monetary policy decisions from short-term political considerations.

Price stability is the bedrock of a healthy economy and provides the public with immeasurable benefits over time. But restoring price stability when inflation is high can require measures that are not popular in the short term as we raise interest rates to slow the economy.

The absence of direct political control over our decisions allows us to take these necessary measures without considering short-term political factors. I believe that the benefits of independent monetary policy in the U.S. context are well understood and broadly accepted.

In a well-functioning democracy, important public policy decisions should be made, in almost all cases, by the elected branches of government. Grants of independence to agencies should be exceedingly rare, explicit,

tightly circumscribed, and limited to those issues that clearly warrant protection from short-term political considerations.

With independence comes the responsibility to provide the transparency that enables effective oversight by Congress, which, in turn, supports the Fed's democratic legitimacy.

At the Fed, we treat this as an active, not passive, responsibility, and over the past several decades we have steadily broadened our efforts to provide meaningful transparency about the basis for, and consequences of, the decisions we make in service to the American public.

We are tightly focused on achieving our statutory mandate and on providing useful and appropriate transparency.

Sticking to our mandate

It is essential that we stick to our statutory goals and authorities, and that we resist the temptation to broaden our scope to address other important social issues of the day. Taking on new goals, however worthy, without a clear statutory mandate would undermine the case for our independence.

In the area of bank regulation, too, the Fed has a degree of independence, as do the other federal bank regulators. Independence in this area helps ensure that the public can be confident that our supervisory decisions are not influenced by political considerations.

Today, some analysts ask whether incorporating into bank supervision the perceived risks associated with climate change is appropriate, wise, and consistent with our existing mandates.

Addressing climate change seems likely to require policies that would have significant distributional and other effects on companies, industries, regions, and nations. Decisions about policies to directly address climate change should be made by the elected branches of government and thus reflect the public's will as expressed through elections.

At the same time, in my view, the Fed does have narrow, but important, responsibilities regarding climate-related financial risks. These responsibilities are tightly linked to our responsibilities for bank supervision.

The public reasonably expects supervisors to require that banks understand, and appropriately manage, their material risks, including the financial risks of climate change.

But without explicit congressional legislation, it would be inappropriate for us to use our monetary policy or supervisory tools to promote a greener economy or to achieve other climate-based goals.7 We are not, and will not be, a "climate policymaker."

To read more:
https://www.federalreserve.gov/newsevents/speech/powell20230110a.htm

Wi-Fi Could Help Identify When You're Struggling to Breathe

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Wi-Fi routers continuously broadcast radio frequencies that your phones, tablets and computers pick up and use to get you online. As the invisible frequencies travel, they bounce off or pass through everything around them — the walls, the furniture and even you. Your movements, even breathing, slightly alter the signal's path from the router to your device.

Those interactions don't interrupt your internet connection, but they could signal when someone is in trouble. NIST has developed a deep learning algorithm, called BreatheSmart, that can analyze those minuscule changes to help determine whether someone in the room is struggling to breathe. And it can do so with already available Wi-Fi routers and devices. This work was recently published in IEEE Access.

In 2020 NIST scientists wanted to help doctors fight the COVID-19 pandemic. Patients were isolated; ventilators were scarce. Previous research had explored using Wi-Fi signals to sense people or movement, but these setups often required custom sensing devices, and data from these studies were very limited.

"As everybody's world was turned upside down, several of us at NIST were thinking about what we could do to help out," says Jason Coder, who leads NIST's research in shared spectrum metrology. "We didn't have time to develop a new device, so how can we use what we already have?"

Working with colleagues at the Office of Science and Engineering Labs (OSEL) in the FDA's Center for Devices and Radiological Health, Coder and research associate Susanna Mosleh advanced a new way to use existing Wi-Fi routers to measure the breathing rate of a person in the room.

In Wi-Fi, the "channel state information," or CSI, is a set of signals sent from the client (such as a cellphone or laptop) to the access point (such as the router).

The CSI signal sent by the client device is always the same, and the access point receiving the CSI signals knows what it should look like. But as the CSI signals travel through the environment, they get distorted as they bounce off things or lose strength. The access point analyzes the amount of distortion to adjust and optimize the link.

These CSI streams are small, less than a kilobyte, so it doesn't interfere with the flow of data over the channel. The team modified the firmware on the router to ask for these CSI streams more frequently, up to 10 times per

second, to get a detailed picture of how the signal was changing. They set up a manikin used to train medical professionals in an anechoic chamber with a commercial off-the-shelf Wi-Fi router and receiver.

This manikin is designed to replicate several breathing conditions, from normal respiration to abnormally slow breathing (called bradypnea), abnormally rapid breathing (tachypnea), asthma, pneumonia and chronic obstructive pulmonary diseases, or COPD. What alters the Wi-Fi signal is the way the body moves as we breathe. Think of how your chest moves differently when you are wheezing or coughing, compared with breathing normally.

As the manikin "breathed," the movement of its chest altered the path traveled by the Wi-Fi signal. The team members recorded the data provided by the CSI streams. Although they collected a wealth of data, they still needed help to make sense of what they had gathered.

"This is where we can leverage deep learning," Coder said.

Deep learning is a subset of artificial intelligence, a type of machine learning that mimics humans' ability to learn from their past actions and improves the machine's ability to recognize patterns and analyze new data.

Mosleh worked on a deep learning algorithm to comb through the CSI data, understand it, and recognize patterns that indicated different breathing problems. The algorithm, which they named BreatheSmart, successfully classified a variety of respiratory patterns simulated with the manikin 99.54% of the time.

"Most of the work that's been done before was working with very limited data," Mosleh says. "We were able to collect data with a lot of simulated respiratory scenarios, which contributes to the diversity of the training set that was available to the algorithm."

There has been a lot of interest in using Wi-Fi signals for sensing applications, Coder says. He and Mosleh hope that app and software developers can use the process presented in the work as a framework to create programs to remotely monitor breathing.

"All the ways we're gathering the data is done on software on the access point (in this case, the router), which could be done by an app on a phone," Coder says. "This work tries to lay out how somebody can develop and test their own algorithm. This is a framework to help them get relevant information."

To read more: https://www.nist.gov/news-events/news/2022/12/wi-fi-could-help-identify-when-youre-struggling-breathe

Preparing the economy and financial system for hybrid war - Finland's experience

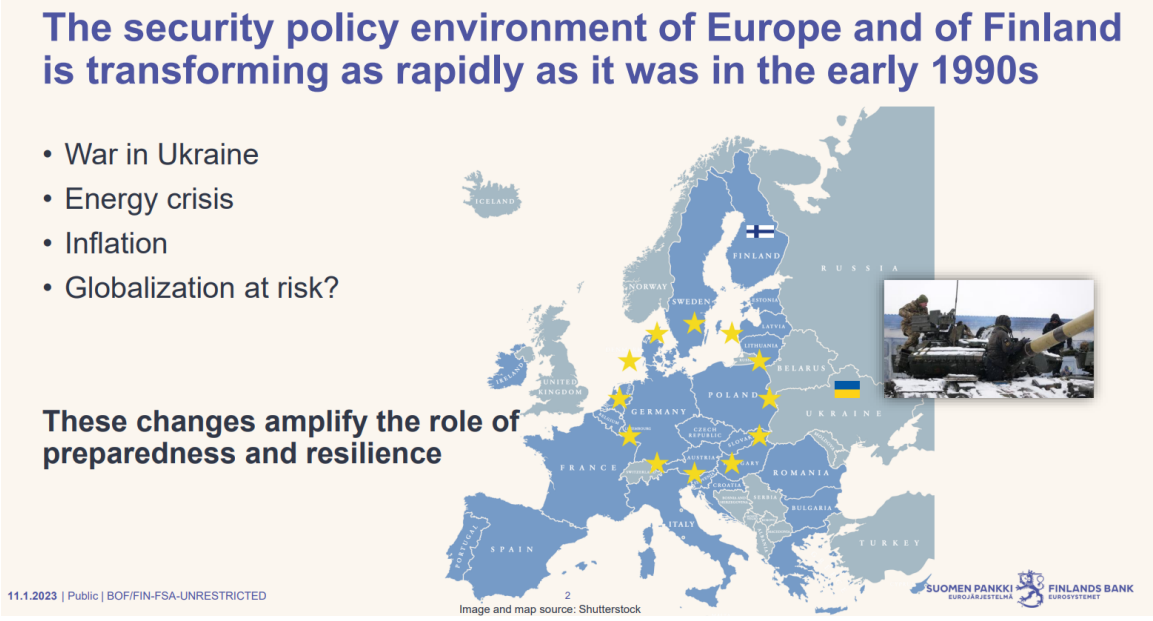
Olli Rehn, Governor of the Bank of Finland, at the Peterson Institute for International Economics (PIIE) Financial Statements web event series

Ladies and Gentlemen,

Greetings from a snowy Helsinki – and thank you very much for this opportunity to exchange views with you at this event today. The topic of my talk is Finland's experience in building up resilience and preparing the economy and financial system to cope with hybrid warfare.

Around a year ago, a rapid recovery from the COVID-19 pandemic was well under way in Europe. Those positive prospects were crushed last February by Russia's illegal and brutal attack against Ukraine.

The horrific bombardment of critical Ukrainian infrastructure has left millions of Ukrainians at the mercy of winter conditions, and no end to the war is in sight.



We need to be prepared for a long confrontation between Putin's Russia and the liberal West, or more broadly between authoritarian governments and liberal democracies.

Russia's war has been a litmus test of European unity. Supporting Ukraine in its fight for freedom remains a policy priority. For Finns, this is really close to our hearts, also by our own experience.

After all, we ourselves were attacked by the Soviet Union in the Second World War, and we still have Europe's longest border with Russia: 832 miles, or 1340 kilometres.

To read more: https://www.suomenpankki.fi/en/media-and-publications/speeches-and-interviews/2023/governor-olli-rehn-preparing-the-economy-and-financial-system-for-hybrid-war-finlands-experience/

CISA Releases Four Industrial Control Systems Advisories

There are 4 very important Industrial Control Systems (ICS) advisories from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) for security flaws affecting products from Siemens, GE Digital, and Contec.

1. Vendor: GE Digital.
Equipment: Proficy Historian.
Exploitable remotely/low attack complexity.
Vulnerabilities: Authentication Bypass using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, Improper Access Control, Weak Encoding for Password.

2. Vendor: Mitsubishi Electric.
Equipment: MELSEC iQ-F and iQ-R Series products.
Exploitable remotely.
Vulnerability: Predictable Seed in Pseudo-Random Number Generator (PRNG).

3. Vendor: Siemens.
Equipment: SINEC INS.
Exploitable remotely/low attack complexity.
Vulnerabilities: OS Command Injection, Inadequate Encryption Strength, Out-of-bounds Write, HTTP Request Smuggling, Inadequate Encryption Strength, Use of Insufficiently Random Values, Authentication Bypass by Spoofing, Path Traversal, Command Injection

4. Vendor: Contec
Equipment: CONPROSYS HMI System (CHS)
Exploitable remotely/low attack complexity.
Vulnerability: OS Command Injection, Use of Default Credentials, Use of Password Hash Instead of Password for Authentication, Cross-site Scripting, Improper Access Control.

To read more: https://www.cisa.gov/uscert/ncas/current-activity/2023/01/17/cisa-releases-four-industrial-control-systems-advisories

NIST Risk Management Framework Aims to Improve Trustworthiness of Artificial Intelligence

New guidance seeks to cultivate trust in AI technologies and promote AI innovation while mitigating risk.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has released its Artificial Intelligence Risk Management Framework (AI RMF 1.0), a guidance document for voluntary use by organizations designing, developing, deploying or using AI systems to help manage the many risks of AI technologies.

> The AI RMF refers to an *AI system* as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy (Adapted from: OECD Recommendation on AI:2019; ISO/IEC 22989:2022).

The AI RMF follows a direction from Congress for NIST to develop the framework and was produced in close collaboration with the private and public sectors. It is intended to adapt to the AI landscape as technologies continue to develop, and to be used by organizations in varying degrees and capacities so that society can benefit from AI technologies while also being protected from its potential harms.

"This voluntary framework will help develop and deploy AI technologies in ways that enable the United States, other nations and organizations to enhance AI trustworthiness while managing risks based on our democratic values," said Deputy Commerce Secretary Don Graves. "It should accelerate AI innovation and growth while advancing — rather than restricting or damaging — civil rights, civil liberties and equity for all."

Compared with traditional software, AI poses a number of different risks. AI systems are trained on data that can change over time, sometimes significantly and unexpectedly, affecting the systems in ways that can be difficult to understand.

These systems are also "socio-technical" in nature, meaning they are influenced by societal dynamics and human behavior. AI risks can emerge from the complex interplay of these technical and societal factors, affecting people's lives in situations ranging from their experiences with online chatbots to the results of job and loan applications.

The framework equips organizations to think about AI and risk differently. It promotes a change in institutional culture, encouraging organizations to approach AI with a new perspective — including how to think about, communicate, measure and monitor AI risks and its potential positive and negative impacts.

The AI RMF provides a flexible, structured and measurable process that will enable organizations to address AI risks. Following this process for managing AI risks can maximize the benefits of AI technologies while reducing the likelihood of negative impacts to individuals, groups, communities, organizations and society.

The framework is part of NIST's larger effort to cultivate trust in AI technologies — necessary if the technology is to be accepted widely by society, according to Under Secretary for Standards and Technology and NIST Director Laurie E. Locascio.

"The AI Risk Management Framework can help companies and other organizations in any sector and any size to jump-start or enhance their AI risk management approaches," Locascio said. "It offers a new way to integrate responsible practices and actionable guidance to operationalize trustworthy and responsible AI. We expect the AI RMF to help drive development of best practices and standards."

The AI RMF is divided into two parts. The first part discusses how organizations can frame the risks related to AI and outlines the characteristics of trustworthy AI systems. The second part, the core of the framework, describes four specific functions — govern, map, measure and manage — to help organizations address the risks of AI systems in practice.

These functions can be applied in context-specific use cases and at any stages of the AI life cycle.

Working closely with the private and public sectors, NIST has been developing the AI RMF for 18 months. The document reflects about 400 sets of formal comments NIST received from more than 240 different organizations on draft versions of the framework. NIST today released statements from some of the organizations that have already committed to use or promote the framework.

The agency also today released a companion voluntary AI RMF Playbook, which suggests ways to navigate and use the framework.

NIST plans to work with the AI community to update the framework periodically and welcomes suggestions for additions and improvements to the playbook at any time. Comments received by the end of February 2023 will be included in an updated version of the playbook to be released in spring 2023.

To read more: https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

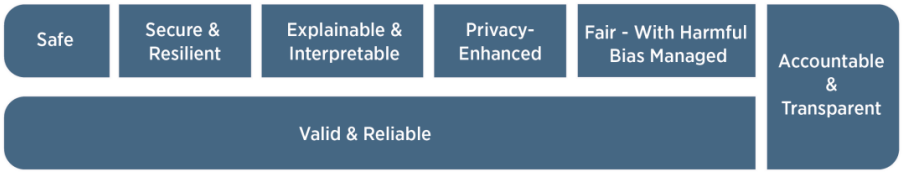


Fig. 4. Characteristics of trustworthy AI systems. Valid & Reliable is a necessary condition of trustworthiness and is shown as the base for other trustworthiness characteristics. Accountable & Transparent is shown as a vertical box because it relates to all other characteristics.

VIDEO: A New Generation of AI Assistants

Perceptually-enabled Task Guidance prototypes demonstrated ability to help people complete recipes as a proxy to unfamiliar tasks

DARPA DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

In this video, DARPA program manager Dr. Bruce Draper describes the technology he thinks could usher in the next "do-it-yourself" revolution.

The Perceptually-enabled Task Guidance (PTG) program aims to develop virtual "task guidance" assistants that can work with different sensor platforms to help military personnel perform complex physical tasks and expand their skillsets.

Unlike today's AI assistants, PTG technology would be able to see what the user sees and hears what they hear by integrating with a microphone, a head-mounted camera, and displays like augmented reality (AR) headsets, to deliver accurate instructions.

The video: https://www.youtube.com/watch?v=pEM8gcRkA7M

PTG performers* recently demonstrated early successes of their prototypes by using the task of cooking recipes as a proxy for unfamiliar, more complex tasks, such as battlefield medical procedures, military equipment sustainment, and co-piloting aircraft.

*PTG Performers: Kitware (Columbia University; University of California, Berkeley; University of Texas at Austin); PARC (University of California, Santa Barbara; University of Rostock); Northeastern University (University

of California, Santa Barbara; Stony Brook University); New York University; University of Texas at Dallas (University of California, Irvine; University of Florida); Stevens Institute of Technology (Purdue University; University of Michigan; University of Rochester); University of Florida (Northeastern University; Topos Institute; Texas A&M University; University of Arizona); Raytheon Technologies (Valkyries Austere Medical Solutions); Northrop Grumman (University of Central Florida); Red Shred (Third Insight); MIT Lincoln Laboratory

“Today the commercial sector is pursuing new, useful ways to present data to the user but it doesn’t go far enough,” said Draper. “The gamechanger with PTG would be having perceptually-driven AI interfaces that can make sense of the real world, react to whatever the user is doing and provide advice. I'm really impressed at how quickly performing teams are making progress toward the goals.”

To read more: https://www.darpa.mil/news-events/2023-01-25

Implementation of G20 Non-Bank Financial Intermediation Reforms, Progress report

FSB FINANCIAL STABILITY BOARD

This report describes progress in implementing reforms that had been agreed by the G20 following the 2008 global financial crisis to strengthen the oversight and regulation of non-bank financial intermediation (NBFI). The implementation status in various NBFI areas is as follows:

1. Jurisdictions have made progress in implementing Basel III reforms to mitigate spillovers between banks and non-bank financial entities, but implementation is not yet complete.

Four jurisdictions have yet to implement applicable risk-based capital requirements for banks' investments in the equity of funds or the supervisory framework for measuring and controlling banks' large exposures.

2. Adoption of the 2012 IOSCO recommendations to reduce the run risk of money market funds (MMFs) is most advanced in the largest MMF markets.

All FSB members adopted the fair value approach for valuation of MMF portfolios, though one jurisdiction does not have in place requirements for use of the amortised cost method only in limited circumstances.

Progress in liquidity management is less advanced. An IOSCO review found that the policy measures in nine jurisdictions representing about 95% of global net MMF assets are generally in line with the IOSCO recommendations.

3. Adoption of the IOSCO recommendations on incentive alignment approaches for securitisation and of the BCBS standard on revised securitisation framework is ongoing.

About one-third of FSB jurisdictions (for the IOSCO recommendations) and one-sixth of FSB jurisdictions (for the BCBS standard) have yet to implement them.

4. Implementation of FSB recommendations for dampening procyclicality and other financial stability risks associated with securities financing transactions (SFTs) is incomplete and continues to face significant delays in most jurisdictions. On global SFT data collection and aggregation, a few FSB jurisdictions are submitting data to the BIS.

5. Implementation of most FSB recommendations to assess and mitigate systemic risks posed by other non-bank financial entities and activities is ongoing.

The FSB and IOSCO assessed the implementation and effectiveness of their respective recommendations to address liquidity mismatch in open-ended funds (OEFs).

The FSB found that authorities have made meaningful progress in implementing the 2017 FSB Recommendations, but that lessons learnt since then have produced new insights into liquidity management challenges in segments of the OEF sector.

While the assessment suggests that the FSB Recommendations remain broadly appropriate, enhancing clarity and specificity on the policy outcomes the FSB Recommendations seek to achieve would make them more effective from a financial stability perspective.

IOSCO's review of its 2018 Recommendations shows a high degree of implementation of regulatory requirements consistent with the Recommendations' objectives, but some areas may warrant further attention.

In addition to these reforms, the FSB is carrying out further analytical and policy work to enhance the resilience of the NBFI sector, building on the lessons from the March 2020 market turmoil.

To read more: https://www.fsb.org/wp-content/uploads/P180123.pdf

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

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 (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- 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.

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.

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.

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.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.

You may visit: https://www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Visit the Reading Room of the SOXCPA at: https://www.sarbanes-oxley-association.com/Reading_Room.htm

3. Training and Certification - You may visit: https://www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

https://www.sarbanes-oxley-association.com/CJSOXE_Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We tailor all programs to meet specific requirements.