International Association of Potential, New and Sitting Members
of the Board of Directors (IAMBD)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750 Web: www.iambd.org

News for the Board of Directors, September 2023

Dear members and friends,

The FSB is finalising its global regulatory framework for crypto-asset activities to promote the comprehensiveness and international consistency of regulatory and supervisory approaches.

It consists of two distinct sets of recommendations:

(i) High-level recommendations for the regulation, supervision and oversight of cryptoasset activities and markets (CA recommendations);
(ii) Revised high-level recommendations for the regulation, supervision, and oversight of "global stablecoin" arrangements (GSC recommendations).

The framework is based on the principle of "same activity, same risk, same regulation" and provides a strong basis for ensuring that crypto-asset

activities and so-called stablecoins are subject to consistent and comprehensive regulation, commensurate to the risks they pose, while supporting responsible innovations potentially brought by the technological change.

The recommendations focus on addressing risks to financial stability, and they do not comprehensively cover all specific risk categories related to crypto-asset activities.

It takes account of lessons from recent events in crypto-asset markets. Central Bank Digital Currencies (CBDCs), envisaged as digitalised central bank liabilities, are not subject to these recommendations.

The events of the past year have highlighted the intrinsic volatility and structural vulnerabilities of crypto-assets and related players. They have also illustrated that the failure of a key service provider in the crypto-asset ecosystem can quickly transmit risks to other parts of that ecosystem.

As recent events have illustrated, if linkages to traditional finance were to grow further, spillovers from crypto-asset markets into the broader financial system could increase.

The G20 has asked the FSB to coordinate the delivery of an effective regulatory, supervisory and oversight framework for crypto-assets, including finalising the FSB's high-level recommendations for the supervision and regulation of crypto-asset activities, and of so-called global stablecoins (GSCs), by July 2023.

In addition, these recommendations, constituting a regulatory and supervisory framework for crypto-assets and stablecoins, will provide input to a joint paper with the International Monetary Fund (IMF) to be delivered to the G20 in September 2023, which will support a coordinated and comprehensive policy approach to crypto-assets by synthesising the policy findings from IMF work on macroeconomic and monetary issues and FSB work on supervisory and regulatory issues.

The FSB and the sectoral standard-setting bodies (SSBs) have developed a shared workplan for 2023 and beyond, through which they will continue to coordinate work under their respective mandates to promote the development of a comprehensive and coherent global regulatory framework commensurate to the risks crypto-asset markets activities may pose to jurisdictions worldwide, including through the provision of more granular guidance by SSBs, monitoring and public reporting.

To read more: https://www.fsb.org/wp-content/uploads/P170723-1.pdf

Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, find that countries of concern are engaged in comprehensive, long-term strategies that direct, facilitate, or otherwise support advancements in sensitive technologies and products that are critical to such countries' military, intelligence, surveillance, or cyber-enabled capabilities.

Moreover, these countries eliminate barriers between civilian and commercial sectors and military and defense industrial sectors, not just through research and development, but also by acquiring and diverting the world's cutting-edge technologies, for the purposes of achieving military dominance.

Rapid advancement in semiconductors and microelectronics, quantum information technologies, and artificial intelligence capabilities by these countries significantly enhances their ability to conduct activities that threaten the national security of the United States.

Advancements in sensitive technologies and products in these sectors will accelerate the development of advanced computational capabilities that will enable new applications that pose significant national security risks, such as the development of more sophisticated weapons systems, breaking of cryptographic codes, and other applications that could provide these countries with military advantages.

As part of this strategy of advancing the development of these sensitive technologies and products, countries of concern are exploiting or have the ability to exploit certain United States outbound investments, including certain intangible benefits that often accompany United States investments and that help companies succeed, such as enhanced standing and prominence, managerial assistance, investment and talent networks, market access, and enhanced access to additional financing.

The commitment of the United States to open investment is a cornerstone of our economic policy and provides the United States with substantial

benefits. Open global capital flows create valuable economic opportunities and promote competitiveness, innovation, and productivity, and the United States supports cross-border investment, where not inconsistent with the protection of United States national security interests. However, certain United States investments may accelerate and increase the success of the development of sensitive technologies and products in countries that develop them to counter United States and allied capabilities.

I therefore find that advancement by countries of concern in sensitive technologies and products critical for the military, intelligence, surveillance, or cyber-enabled capabilities of such countries constitutes an unusual and extraordinary threat to the national security of the United States, which has its source in whole or substantial part outside the United States, and that certain United States investments risk exacerbating this threat. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. Notifiable and Prohibited Transactions. (a) To assist in addressing the national emergency declared in this order, the Secretary of the Treasury (Secretary), in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant executive departments and agencies (agencies), shall issue, subject to public notice and comment, regulations that require United States persons to provide notification of information relative to certain transactions involving covered foreign persons (notifiable transactions) and that prohibit United States persons from engaging in certain other transactions involving covered foreign persons (prohibited transactions).

(b) The regulations issued under this section shall identify categories of notifiable transactions that involve covered national security technologies and products that the Secretary, in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant agencies, determines may contribute to the threat to the national security of the United States identified in this order. The regulations shall require United States persons to notify the Department of the Treasury of each such transaction and include relevant information on the transaction in each such notification.

(c) The regulations issued under this section shall identify categories of prohibited transactions that involve covered national security technologies and products that the Secretary, in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant agencies, determines pose a particularly acute national security threat because of their potential to significantly advance the military, intelligence, surveillance, or cyber-enabled capabilities of countries of concern. The

regulations shall prohibit United States persons from engaging, directly or indirectly, in such transactions.

Sec. 2. Duties of the Secretary. In carrying out this order, the Secretary shall, as appropriate:

(a) communicate with the Congress and the public with respect to the implementation of this order;

(b) consult with the Secretary of Commerce on industry engagement and analysis of notified transactions;

(c) consult with the Secretary of State, the Secretary of Defense, the Secretary of Commerce, the Secretary of Energy, and the Director of National Intelligence on the implications for military, intelligence, surveillance, or cyber-enabled capabilities of covered national security technologies and products and potential covered national security technologies and products;

(d) engage, together with the Secretary of State and the Secretary of Commerce, with allies and partners regarding the national security risks posed by countries of concern advancing covered national security technologies and products;

(e) consult with the Secretary of State on foreign policy considerations related to the implementation of this order, including but not limited to the issuance and amendment of regulations; and

(f) investigate, in consultation with the heads of relevant agencies, as appropriate, violations of this order or the regulations issued under this order and pursue available civil penalties for such violations.

Sec. 3. Program Development. Within 1 year of the effective date of the regulations issued under section 1 of this order, the Secretary, in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant agencies, shall assess whether to amend the regulations, including whether to adjust the definition of "covered national security technologies and products" to add or remove technologies and products in the semiconductors and microelectronics, quantum information technologies, and artificial intelligence sectors. The Secretary, in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant agencies, shall periodically review the effectiveness of the regulations thereafter.

Sec. 4. Reports to the President. Within 1 year of the effective date of the regulations issued under section 1 of this order and, as appropriate but no less than annually thereafter, the Secretary, in coordination with the

Secretary of Commerce and in consultation with the heads of other relevant agencies and the Director of the Office of Management and Budget, as appropriate, shall provide the President, through the Assistant to the President for National Security Affairs:

(a) to the extent practicable, an assessment of the effectiveness of the measures imposed under this order in addressing threats to the national security of the United States described in this order; advancements by the countries of concern in covered national security technologies and products critical for such countries' military, intelligence, surveillance, or cyber-enabled capabilities; aggregate sector trends evident in notifiable transactions and related capital flows in covered national security technologies and products, drawing on analysis provided by the Secretary of Commerce, the Director of National Intelligence, and the heads of other relevant agencies, as appropriate; and other relevant information obtained through the implementation of this order; and

(b) recommendations, as appropriate, regarding:

(i) modifications to this order, including the addition or removal of identified sectors or countries of concern, and any other modifications to avoid circumvention of this order and enhance its effectiveness; and

(ii) the establishment or expansion of other Federal programs relevant to the covered national security technologies and products, including with respect to whether any existing legal authorities should be used or new action should be taken to address the threat to the national security of the United States identified in this order.

Sec. 5. Reports to the Congress. The Secretary is authorized to submit recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 6. Official United States Government Business. Nothing in this order or the regulations issued under this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof.

Sec. 7. Confidentiality. The regulations issued by the Secretary under this order shall address the confidentiality of information or documentary material submitted pursuant to this order, consistent with applicable law.

Sec. 8. Additional Notifications and Prohibitions. (a) Any conspiracy formed to violate any regulation issued under this order is prohibited.

(b) Subject to the regulations issued under this order, any action that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order or any regulation issued under this order is prohibited.

(c) In the regulations issued under this order, the Secretary may prohibit United States persons from knowingly directing transactions if such transactions would be prohibited transactions pursuant to this order if engaged in by a United States person.

(d) In the regulations issued under this order, the Secretary may require United States persons to:

(i) provide notification to the Department of the Treasury of any transaction by a foreign entity controlled by such United States person that would be a notifiable transaction if engaged in by a United States person; and

(ii) take all reasonable steps to prohibit and prevent any transaction by a foreign entity controlled by such United States person that would be a prohibited transaction if engaged in by a United States person.

Sec. 9. Definitions. For purposes of this order:

(a) the term "country of concern" means a country or territory listed in the Annex to this order that the President has identified to be engaging in a comprehensive, long-term strategy that directs, facilitates, or otherwise supports advancements in sensitive technologies and products that are critical to such country's military, intelligence, surveillance, or cyber-enabled capabilities to counter United States capabilities in a way that threatens the national security of the United States;

(b) the term "covered foreign person" means a person of a country of concern who or that is engaged in activities, as identified in the regulations issued under this order, involving one or more covered national security technologies and products;

(c) the term "covered national security technologies and products" means sensitive technologies and products in the semiconductors and microelectronics, quantum information technologies, and artificial intelligence sectors that are critical for the military, intelligence, surveillance, or cyber-enabled capabilities of a country of concern, as determined by the Secretary in consultation with the Secretary of Commerce and, as appropriate, the heads of other relevant agencies. Where applicable, "covered national security technologies and products" may be limited by reference to certain end-uses of those technologies or products;

(d) the term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(e) the term "person of a country of concern" means:

(i) any individual that is not a United States person and is a citizen or permanent resident of a country of concern;

(ii) any entity organized under the laws of a country of concern or with a principal place of business in a country of concern;

(iii) the government of each country of concern, including any political subdivision, political party, agency, or instrumentality thereof, or any person owned, controlled, or directed by, or acting for or on behalf of the government of such country of concern; or

(iv) any entity owned by a person identified in subsections (e)(i) through (e)(iii) of this section;

(f) the term "person" means an individual or entity;

(g) the term "relevant agencies" includes the Departments of State, Defense, Justice, Commerce, Energy, and Homeland Security, the Office of the United States Trade Representative, the Office of Science and Technology Policy, the Office of the Director of National Intelligence, the Office of the National Cyber Director, and any other department, agency, or office the Secretary determines appropriate; and

(h) the term "United States person" means any United States citizen, lawful permanent resident, entity organized under the laws of the United States or any jurisdiction within the United States, including any foreign branches of any such entity, and any person in the United States.

Sec. 10. General Provisions. (a) The Secretary is authorized to take such actions and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order, including to:

(i) promulgate rules and regulations, including elaborating upon the definitions contained in section 9 of this order for purposes of the regulations issued under this order and further prescribing definitions of other terms as necessary to implement this order;

(ii) investigate and make requests for information relative to notifiable or prohibited transactions from parties to such transactions or other relevant persons at any time, including through the use of civil administrative subpoenas as appropriate;

(iii) nullify, void, or otherwise compel the divestment of any prohibited transaction entered into after the effective date of the regulations issued under this order; and

(iv) refer potential criminal violations of this order or the regulations issued under this order to the Attorney General.

(b) Notwithstanding any other provision of this order, the Secretary is authorized to exempt from applicable prohibitions or notification requirements any transaction or transactions determined by the Secretary, in consultation with the heads of relevant agencies, as appropriate, to be in the national interest of the United States.

(c) To the extent consistent with applicable law, the Secretary may redelegate any functions authorized hereunder within the Department of the Treasury. All agencies of the United States Government shall take all appropriate measures within their authority to carry out the provisions of this order.

(d) If any provision of this order, or the application of any provision of this order to any person or circumstance, is held to be invalid, the remainder of this order and its application to any other person or circumstance shall not be affected thereby.

(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

To read more: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/

DOD Announces Establishment of Generative AI Task Force

U.S. Department of Defense

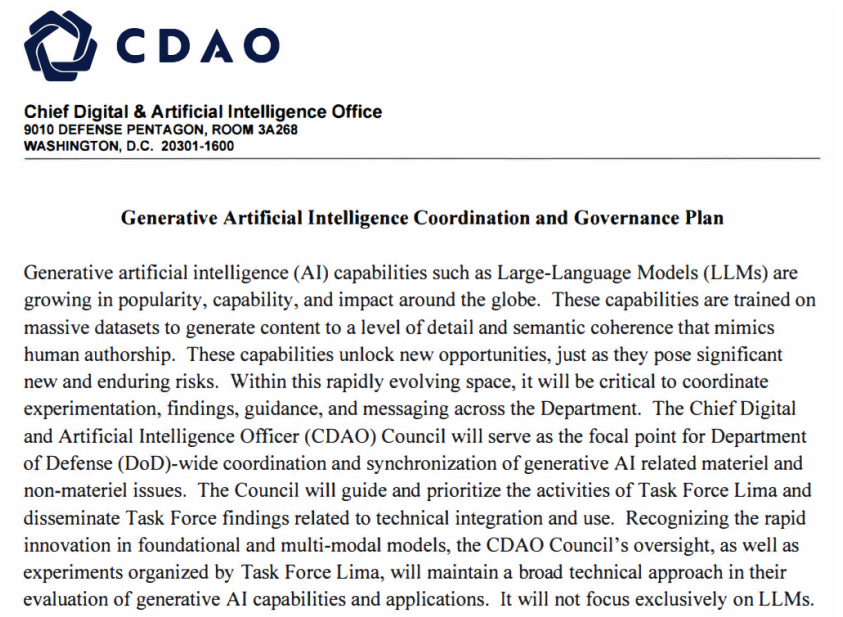
The Department of Defense (DoD) announced the establishment of a generative artificial intelligence (AI) task force, an initiative that reflects the DoD's commitment to harnessing the power of artificial intelligence in a responsible and strategic manner.

Deputy Secretary of Defense Dr. Kathleen Hicks directed the organization of Task Force Lima; it will play a pivotal role in analyzing and integrating generative AI tools, such as large language models (LLMs), across the DoD.

"The establishment of Task Force Lima underlines the Department of Defense's unwavering commitment to leading the charge in AI innovation," Hicks said.

"As we navigate the transformative power of generative AI, our focus remains steadfast on ensuring national security, minimizing risks, and responsibly integrating these technologies. The future of defense is not just about adopting cutting-edge technologies, but doing so with foresight, responsibility, and a deep understanding of the broader implications for our nation."

Led by the Chief Digital and Artificial Intelligence Office (CDAO), Task Force Lima will assess, synchronize, and employ generative AI capabilities across the DoD, ensuring the Department remains at the forefront of cutting-edge technologies while safeguarding national security.



CDAO

Chief Digital & Artificial Intelligence Office
9010 DEFENSE PENTAGON, ROOM 3A268
WASHINGTON, D.C. 20301-1600

Generative Artificial Intelligence Coordination and Governance Plan

Generative artificial intelligence (AI) capabilities such as Large-Language Models (LLMs) are growing in popularity, capability, and impact around the globe. These capabilities are trained on massive datasets to generate content to a level of detail and semantic coherence that mimics human authorship. These capabilities unlock new opportunities, just as they pose significant new and enduring risks. Within this rapidly evolving space, it will be critical to coordinate experimentation, findings, guidance, and messaging across the Department. The Chief Digital and Artificial Intelligence Officer (CDAO) Council will serve as the focal point for Department of Defense (DoD)-wide coordination and synchronization of generative AI related materiel and non-materiel issues. The Council will guide and prioritize the activities of Task Force Lima and disseminate Task Force findings related to technical integration and use. Recognizing the rapid innovation in foundational and multi-modal models, the CDAO Council's oversight, as well as experiments organized by Task Force Lima, will maintain a broad technical approach in their evaluation of generative AI capabilities and applications. It will not focus exclusively on LLMs.

"The DoD has an imperative to responsibly pursue the adoption of generative AI models while identifying proper protective measures and

mitigating national security risks that may result from issues such as poorly managed training data," said Dr. Craig Martell, the DoD Chief Digital and Artificial Intelligence Officer.

"We must also consider the extent to which our adversaries will employ this technology and seek to disrupt our own use of AI-based solutions."

Leveraging partnerships across the Department, Intelligence Community and other government agencies, the task force will help minimize risk and redundancy while pursuing generative AI initiatives across the Department.

Artificial intelligence has emerged as a transformative technology with the potential to revolutionize various sectors, including defense. By leveraging generative AI models, which can use vast datasets to train algorithms and generate products efficiently, the Department aims to enhance its operations in areas such as warfighting, business affairs, health, readiness, and policy.

"The adoption of artificial intelligence in defense is not solely about innovative technology but also about enhancing national security," said U.S. Navy Capt. M. Xavier Lugo, Task Force Lima mission commander and member of the CDAO's Algorithmic Warfare Directorate.

"The DoD recognizes the potential of generative AI to significantly improve intelligence, operational planning, and administrative and business processes. However, responsible implementation is key to managing associated risks effectively."

The CDAO became operational in June 2022 and is dedicated to integrating and optimizing artificial intelligence capabilities across the DoD.

The office is responsible for accelerating the DoD's adoption of data, analytics, and AI, enabling the Department's digital infrastructure and policy adoption to deliver scalable AI-driven solutions for enterprise and joint use cases, safeguarding the nation against current and emerging threats.

For more information about Task Force Lima, please visit the CDAO website at ai.mil. You can also connect with the CDAO on LinkedIn (@ DoD Chief Digital and Artificial Intelligence Office) and Twitter (@dodcdao). Additional updates and news can be found on the CDAO Unit Page on DVIDS.

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

AUG 10 2023

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Establishment of Chief Digital and Artificial Intelligence Officer Generative Artificial Intelligence and Large Language Models Task Force, Task Force Lima

Dr. Craig Martell
Chief Digital and Artificial Intelligence Officer

Ms. Margie Palmieri
Deputy Chief Digital and Artificial Intelligence Officer

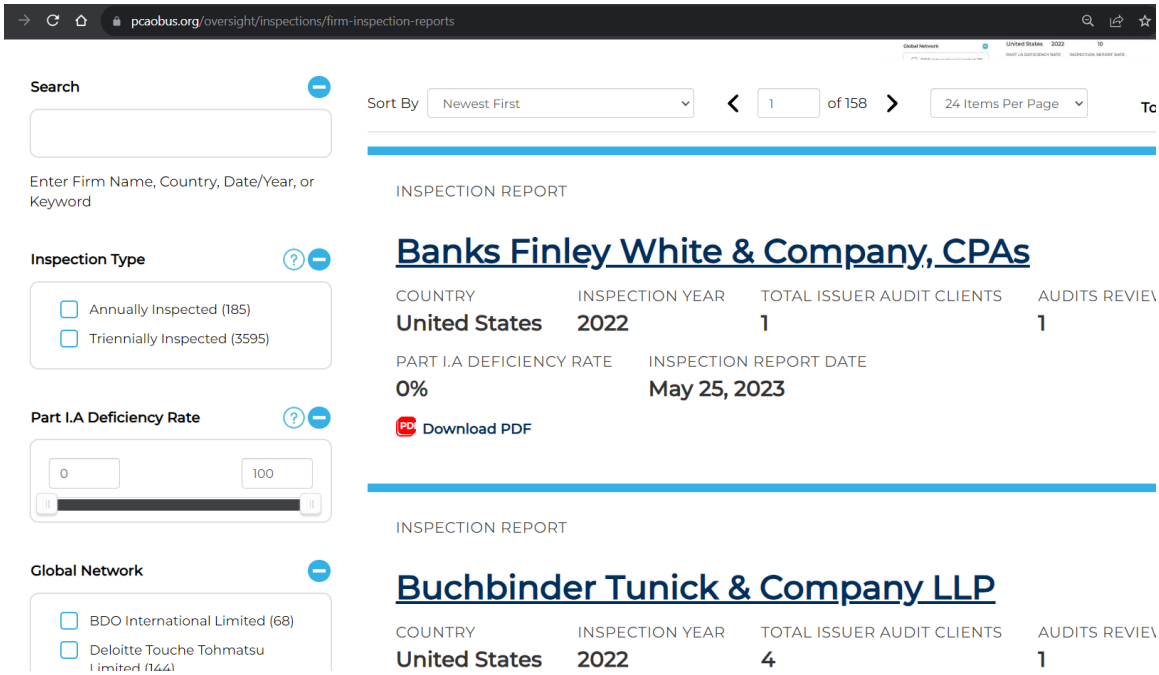
To read more: https://media.defense.gov/2023/Aug/10/2003279040/-1/-1/1/ESTABLISHMENT_OF_CDAO_GENERATIVE_AI_AND_LARGE_LANGUAGE_MODELS_TASK_FORCE_TASK_FORCE_LIMA_OSD006491-23_RES_FINAL.PDF

PCAOB Launches New Online Tools to Help Users Find and Compare Inspection Report Data

Visitors to the PCAOB website can now easily filter over 3,700 inspection reports by deficiency rate and more

The Public Company Accounting Oversight Board (PCAOB) unveiled an array of website transparency enhancements that allow investors, audit committee members, and other stakeholders to better access and understand data from PCAOB inspection reports.

Six new search filters, including Part I.A deficiency rate, are now live on the PCAOB's Firm Inspection Reports page to help users analyze and compare more than 3,700 inspection reports. You may visit: https://pcaobus.org/oversight/inspections/firm-inspection-reports



"PCAOB inspection reports provide investors, audit committees, and potential clients with important information they can use to make informed decisions. By making that information easier to find and compare, these new tools will empower users to hold firms accountable for producing high-quality audits," said PCAOB Chair Erica Y. Williams.

Previously, visitors to the PCAOB website could only search inspection reports by four filters: firm name, country/geography, year when a report was published (i.e., approved by the Board), and whether a report includes public quality control criticisms.

The enhancements released today add six new filters that can be applied to PCAOB inspection reports. The filters are:

1. **Inspection type:** Users can filter according to whether a firm inspection report falls into the 'annual' or 'triennial' inspection frequency category for the inspection year.

2. **Total issuer audit clients:** Users can now get a better and more immediate sense of the size of triennially inspected audit firms by sorting inspection reports according to the number of audit clients that firms had, as determined at the outset of the inspection.

3. **Part I.A deficiency rate:** Users can now sort inspection reports according to the percentage of audits with Part I.A deficiencies. Part I.A of inspection reports discusses deficiencies, if any, that were of such significance that PCAOB staff believed the audit firm, at the time it issued its audit report(s), had not obtained sufficient appropriate audit evidence to support its opinion on the public company's financial statements and/or internal control over financial reporting.

4. **Specific global network:** Users can now refine search results so they include only firms that belong to a specific global audit firm network.

5. **Inspection year:** Users can now filter inspection reports according to the year that the PCAOB's inspectors completed the inspection, not just the year when the report was published.

6. **Audits reviewed:** Users can search inspection reports by number of issuer audits that the PCAOB reviewed as part of its inspection. Additionally, users can now download the entire data set into three formats: CSV, XML, and JSON. These three formats maximize the ability of users to integrate PCAOB data into third-party applications for further analysis.

"Each year, the hard work of the PCAOB's inspection staff yields an extraordinary amount of useful information for investors and others," said George R. Botic, Director of the PCAOB's Division of Registration and Inspections. "We are strongly committed to making more of this information more accessible and insightful for PCAOB stakeholders, and we are pleased that today's website enhancements further that commitment."

Today's website enhancements build on the transparency enhancements for inspection reports announced in May 2023. The PCAOB continues to work on projects this year that will further increase transparency for all external stakeholders.

For more on PCAOB inspection reports and the inspection process, visit PCAOB's Inspections page.

To read more: https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-launches-new-online-tools-to-help-users-find-and-compare-inspection-report-data

Macro risks top insurers' worry list according to EIOPA's Insurance Risk Dashboard

1. Risk levels for the European insurance sector remain broadly constant, with all risk categories pointing to medium risks with the exception of macro risk.

Macro-related risks remain among the most relevant for the insurance sector.

Forecasted GDP growth at global level further increased to 0.74%. CPI forecasts slightly decreased to 3.22%, yet remaining at high level.

Credit risks is at medium level. The CDS spreads increased for financial secured bonds in the second quarter of 2023, while CDS spreads for other fixed income market segments receded slightly.

Market risks decreased from high to medium level as volatility in equity market decreased and duration mismatch narrowed compared to the previous assessment.

2. Liquidity and funding risks show an increase in cash holdings and a drop in the liquid assets ratio in the first quarter of 2023.

Profitability and solvency risks show a drop in the investment return for life insurers in 2022 mainly due to the large increase of unrealized losses following the increase of interest rates.

The distribution of the SCR ratio for insurance groups decreased. Similarly, life insurers reported a slight decline in the median SCR ratio.

On the other hand, assets over liabilities increased due to the higher interest rates.

Interlinkages and imbalances risks remain at medium level while insurance risks decreased in Q1-2023, with the median year-on-year premium growth for non-life insurance decreasing to end 2021 levels.

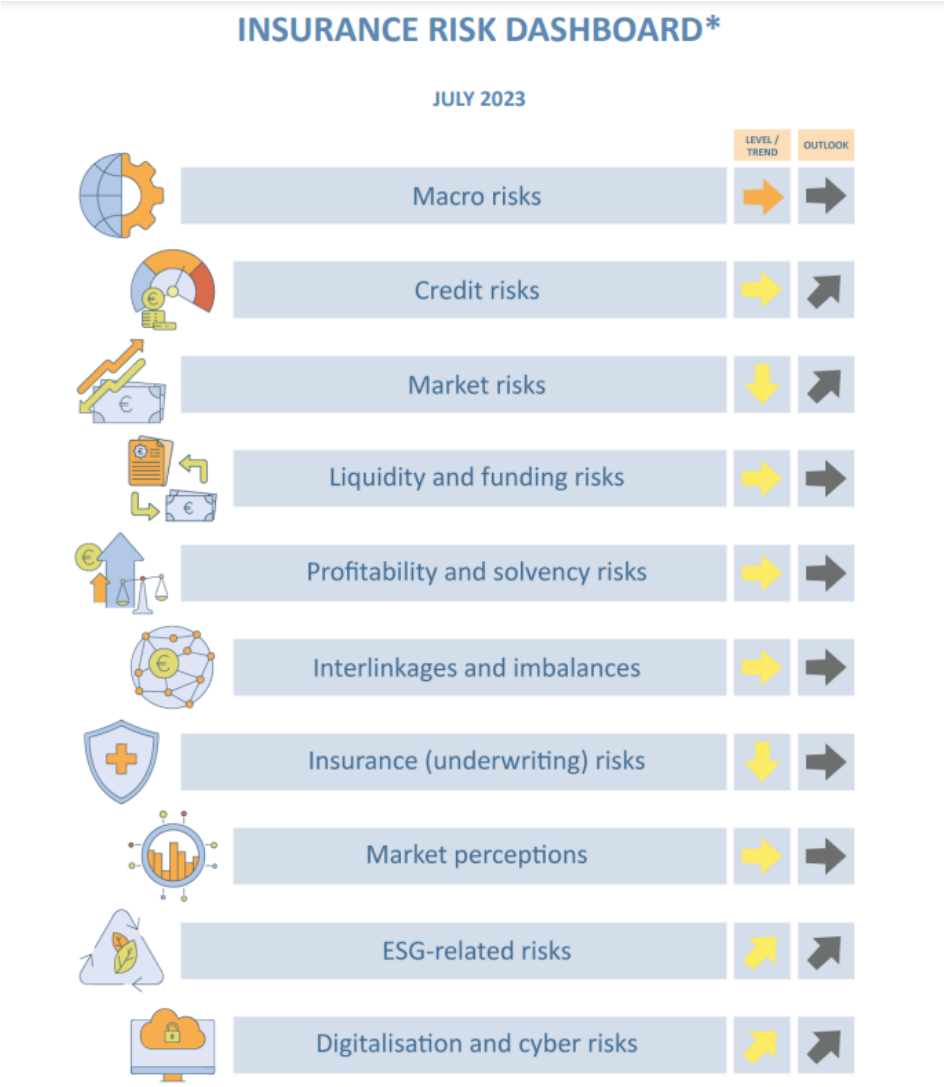
3. Market perceptions show positive returns for insurance stocks, albeit an underperformance of life insurance stocks when compared to the market for the second quarter of 2023.

4. ESG related risks display an increasing trend with the median exposure towards climate relevant assets slightly increased to 3.3% of total assets. Moreover, the catastrophe loss ratio also deteriorated.

On the other hand, the share of insurers' investments in green bonds over total green bonds outstanding is stable compared to the previous quarter.

5. Digitalization and cyber risks also display an increasing trend with the materiality of these risks for insurance as assessed by supervisors increasing in the first half of 2023.

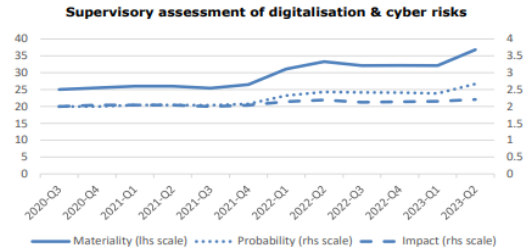
The frequency of cyber incidents impacting all sectors of activity, as measured by publicly available data, increased since the same quarter of last year. The indicator cyber negative sentiment indicates a decreasing concern in the second quarter of 2023.



DIGITALISATION & CYBER RISKS

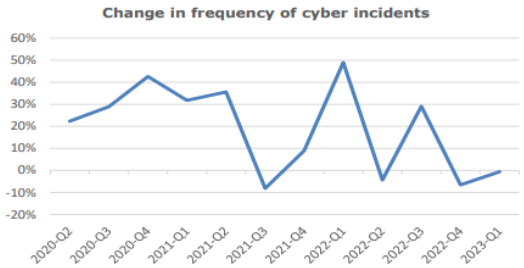
Digitalization and cyber risks remain at medium level, but increasing. The materiality of these risks for insurance as assessed by supervisors increased for the first half 2023. The frequency of cyber incidents impacting all sectors of activity, as measured by publicly available data, increased since the same quarter of last year. Cyber negative sentiment indicates a decreasing concern in the second quarter of 2023.

The supervisory assessment of digitalisation and cyber risks increased in the first half of 2023. Cyber-attacks are on a growing trend and concerns of a hybrid geopolitical conflict remain.



Note: Scores compiled based on the assessment of probability and impact (rhs: scale from 1 to 4) of digitalisation & cyber risks from National Competent Authorities. The country averages for each answer is then normalised (lhs: scale 0-100). Source: EIOPA's Insurance Bottom-up Survey

The y-o-y change in frequency of cyber incidents has increased in the first quarter of 2023, with the number of cyber incidents affecting all sectors of activity in line with the long term average.



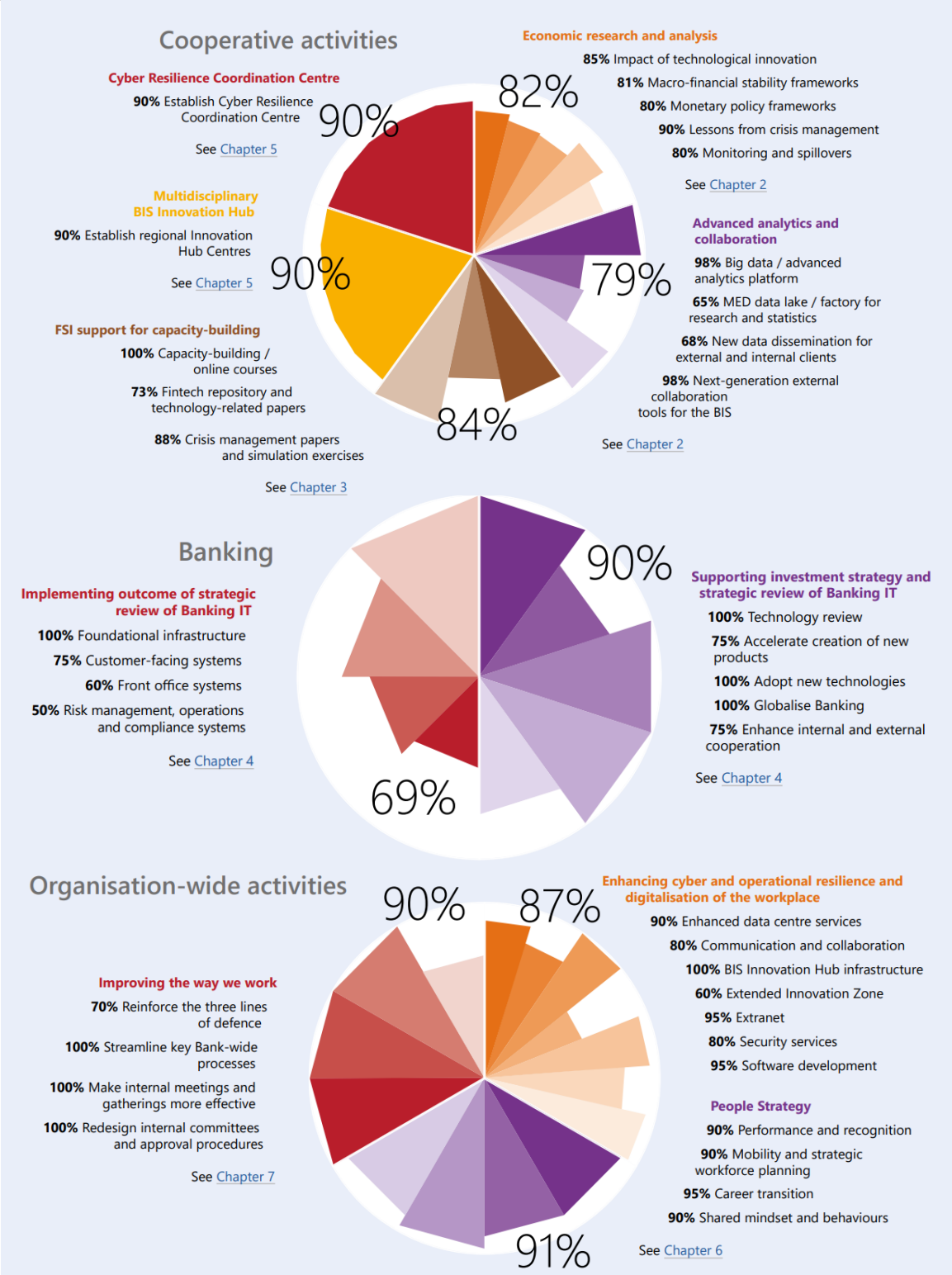
Note: Year-on-year change in frenquency of cyber incidents. Source: HACKMAGEDDON website

To read more: https://www.eiopa.europa.eu/system/files/2023-07/July%202023%20Risk%20Dashboard.pdf

Annual Report 2022/23

BIS

The Annual Report highlights how the BIS has helped central banks to navigate the complex policy landscape, while enabling and supporting its stakeholders during the year.



To read more (249 pages):
https://www.bis.org/about/areport/areport2023.pdf

NIST CSWP 29 (Initial Public Draft)
The NIST Cybersecurity Framework 2.0

Date Published: August 8, 2023
Comments Due: November 5, 2023

This is the public draft of the NIST Cybersecurity Framework (CSF or Framework) 2.0.

The Framework has been used widely to reduce cybersecurity risks since its initial publication in 2014. Many organizations have told NIST that CSF 1.1 remains an effective framework for addressing cybersecurity risks.

There is also widespread agreement that changes are warranted to address current and future cybersecurity challenges and to make it easier for organizations to use the Framework.

NIST is working with the community to ensure that CSF 2.0 is effective for the future while fulfilling the CSF's original goals and objectives.

NIST seeks feedback on whether this draft revision addresses organizations' current and anticipated future cybersecurity challenges, is aligned with leading practices and guidance resources, and reflects comments received so far.

In addition, NIST requests ideas on the best way to present the modifications from CSF 1.1 to CSF 2.0 to support transition.

NIST encourages concrete suggestions for improvements to the draft, including revisions to the narrative and Core.

This draft includes an updated version of the CSF Core, reflecting feedback on the April discussion draft.

This publication does not contain Implementation Examples or Informative References of the CSF 2.0 Core, given the need to frequently update them. Draft, initial Implementation Examples have been released under separate cover for public comment.

NIST seeks feedback on what types of Examples would be most beneficial to Framework users, as well as what existing sources of implementation guidance might be readily adopted as sources of Examples (such as the NICE Framework Tasks, for example). NIST also seeks feedback on how often Implementation Examples should be updated and whether and how to accept Implementation Examples developed by the community.

Table of Contents

As the CSF 2.0 is finalized, the updated Implementation Examples and Informative References will be maintained online on the NIST Cybersecurity Framework website, leveraging the NIST Cybersecurity and Privacy Reference Tool (CPRT).

Resource owners and authors who are interested in mapping their resources to the final CSF 2.0 to create Informative References should reach out to NIST.

To read more: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.ipd.pdf

Data Governance Act: common logos to easily identify trusted EU data intermediaries and data altruism organisations to re-use data

European Commission

The Commission has introduced common logos to easily identify trusted data intermediation service providers and data altruism organisations in the EU, which will connect data holders, both individuals and companies with data users.

EU Recognised Data Intermediary

EU Recognised Data Altruism Organisation

Identifying trusted data intermediation services and data altruism organisations is part of the implementation of the Data Governance Act.

The data intermediation services and data altruism organisations that satisfy the conditions enshrined in the Data Governance Act and opt for the use of the logos, will have to display the logo clearly on every online and offline publication.

The use of these logos at EU level will differentiate the recognised trusted services from other services, contributing to transparency in the data market.

The logo for data altruism organisations recognised in the EU must be accompanied by a QR code with a link to the EU public register of recognised data altruism organisations, which will be available as of 24 September 2023.

The logos have been adopted through an Implementing Regulation and will be registered as trademarks, to protect them from improper use.

Data is a powerful resource that can fuel innovation across Europe's industrial ecosystems.

The Data Governance Act aims to make more data available by increasing trust in data-sharing and tackling technical barriers.

To learn more:

https://digital-strategy.ec.europa.eu/en/news/data-governance-act-common-logos-easily-identify-trusted-eu-data-intermediaries-and-data-altruism

https://digital-strategy.ec.europa.eu/en/library/data-governance-act-implementing-regulation

The Importance of a Comprehensive Risk Assessment by Auditors and Management

Paul Munter, SEC, chief accountant

Introduction

Managements and auditors risk assessment processes are critical to the decisions regarding financial reporting and the effectiveness of internal control over financial reporting (ICFR).

Accordingly, we are troubled by instances in which management and auditors appear too narrowly focused on information and risks that directly impact financial reporting, while disregarding broader, entity-level issues that may also impact financial reporting and internal controls.

Such a narrow focus is detrimental to investors as it can result in material risks to the business going unaddressed and undisclosed, thereby diminishing the quality of financial information.

Issues that may also impact financial reporting and internal controls often present themselves as isolated incidents across an issuer—for example, a data breach in a system not part of ICFR, a repeat non-financial reporting-related regulatory finding classified as lower risk, a misstatement to the financial statements determined to be a revision restatement (i.e., “little r”), or a counterparty risk limit breach.

Some management and certain auditors may be inadvertently biased toward evaluating each such incident individually or rationalizing away potentially disconfirming evidence, and conclude that these matters do not individually, or in the aggregate, rise to the level of management disclosure or auditor communication requirements.

This statement discusses management’s obligation to

(1) take a holistic approach when assessing information about the business and avoid the potential bias toward evaluating problems as isolated incidents, in order to timely identify risks, including entity-level risks;

(2) design processes and controls that are responsive to identified risks; and

(3) effectively identify information that issuers are required to communicate to investors. We also discuss auditors' responsibilities as gatekeepers to hold management accountable in the public interest.

Risk Assessment

Management Considerations

Changing economic conditions may have a significant and sudden impact on an issuer's business, which could change risks or create new ones.

Therefore, to be effective, risk assessment processes must comprehensively and continually consider issuers' objectives, strategies, and related business risks; evaluate contradictory information; and deploy appropriate management resources to respond to those risks.

For example, management's risk assessment process may consider observations from regulators, analyst reports, and short-seller reports. Management is also required to provide auditors complete information related to certain communications from regulatory agencies.

Management needs to be alert to new or changing business risks to identify changes that could significantly impact its system of internal control, and design and implement responses that support issuers' ability to appropriately disclose information in its periodic filings.

Business risks, such as a company's loss of financing, customer concentrations, or declining conditions affecting the company's industry, could affect issuers' ability to settle their obligations when due, and affect the risks of material misstatements in financial statements not being identified on a timely basis.

Likewise, risks related to changes in technology could impact the effectiveness of controls around processing of transactions.

Auditor Considerations

Risk assessment forms the basis of the audit process.

A lack of professional skepticism, including objective consideration of contradictory information, in this critical process could result in an auditor not identifying or assessing risks appropriately, which could impact the effectiveness of the audit.

When identifying risks of material misstatement and designing appropriate audit responses, auditors should remain alert to potential changes in issuers' objectives, strategies, and business risks.

Auditors should consider the possible impact of an issuer's public statements regarding changes in their strategy, board composition, or other governance matters—and whether such statements contradict management's assessment of its control environment.

Auditors also should assess the consistency of information disclosed by issuers in periodic filings and the judgments made by management throughout the financial reporting process compared with the information obtained throughout the performance of the audit.

If material inconsistencies exist, auditors should determine whether those disclosures indicate a potential new or evolving business risk that could materially affect the financial statements or the effectiveness of ICFR.

Entity-Level Controls

Management should evaluate whether issuers have implemented processes and controls that can timely prevent or detect a material misstatement in financial statements.

While an issuer's financial reporting objective may be separate from its operational or compliance objectives, an issuer's internal control system should be dynamic and expand beyond a singular focus on ICFR.

When evaluating control deficiencies identified outside of an issuer's financial reporting objective, management and auditors should consider the root cause of the deficiency and whether it impacts the issuer's ICFR conclusions.

For example, the root causes behind a regulator's findings related to enterprise-wide governance and controls, while not directly related to financial reporting control activities, could have an impact on management's ICFR conclusions due to their impact on the risk assessment and monitoring components of ICFR.

Rather than a biased defaulting to an assessment of narrowly defined, process-level deficiencies, management and auditors' aggregation analysis should consider the root cause of individual control deficiencies, to determine whether such deficiencies indicate a broader, more pervasive deficiency at the entity-level.

We encourage auditors to avoid potential bias toward rationalizing away disconfirming evidence and instead to apply objective judgment when evaluating whether insufficient deficiency evaluations by management constitute evidence of ineffective monitoring activities.

Further, when assessing the severity of control deficiencies identified as a result of a misstatement, management and auditors should consider not only the actual misstatement, but also the magnitude of potential misstatement (i.e., the so-called "could factor").

The "could factor" evaluation includes assessing the total population of transactions or amounts exposed to the deficiency in the impacted accounts or classes of transactions.

In particular, when the root cause is an inadequate entity-level risk assessment process, the "could factor" can extend to a wider population of potential misstatements beyond the identified misstatement.

Reporting Obligations

Clear and transparent communication for the benefit of investors is critical. Management's financial reporting obligations include disclosures around its annual ICFR evaluations, descriptions of identified material weaknesses, and, on a quarterly basis, changes that have materially affected, or are reasonably likely to materially affect, an issuers' ICFR.

Additionally, management is required to provide a discussion in its filings of material factors that make an investment in the registrant speculative or risky.

Management may identify these factors for disclosure as part of their risk assessment procedures, which includes an evaluation of all information available, including contradictory information.

In some instances, business risks may also impact financial statement disclosures when the risks and uncertainties could significantly affect the amounts reported in the financial statements in the near term.

Auditors protect investors and further the public interest through the preparation of informative, accurate, and independent audit reports. Therefore, the auditor's report is a critical means of communication with investors, and auditors should consider the different mechanisms within the auditor's report to communicate with investors.

In an integrated audit, an auditor's reporting obligation includes expressing an adverse opinion on the issuer's ICFR if there are deficiencies that, individually or in combination, result in one or more material weaknesses, including those resulting from entity-level control deficiencies.

If, through the auditor's risk assessment process, a business risk is determined to represent a risk of material misstatement to the financial

statements that is discussed with the audit committee, these matters may meet the definition of a critical audit matter and require communication to investors within the auditor's report.

Although not required, we remind auditors that they may use an "emphasis paragraph" to highlight any matter relating to the financial statements and disclosures, which could include matters related to an issuer's objectives, strategies, and related business risks, as discussed above.

Conclusion

As Chair Gary Gensler has noted, "there's a basic bargain in our capital markets: investors get to decide what risks they wish to take" while "[c]ompanies that are raising money from the public have an obligation to share information with investors on a regular basis."

Timely and transparent reporting by management, and informative, accurate, and independent reports by auditors, are critical components of the system that help companies maintain their end of the bargain—their commitment to provide high quality financial information and information about the effectiveness of their ICFR to investors.

When business risks change, a robust, iterative risk assessment process and strong entity and process-level controls are essential to transparent and high-quality financial reporting.

Auditors in their public gatekeeper role serve as an independent check on management's performance of these critical functions and should transparently communicate with investors in accordance with PCAOB standards.

To read more: https://www.sec.gov/news/statement/munter-importance-risk-assessment-082523

Reflections on the 2023 banking turmoil

Pablo Hernández de Cos, Chair of the Basel Committee on Banking Supervision and Governor of the Bank of Spain, at the Eurofi Financial Forum 2023, Santiago de Compostela.

Good evening, and thank you for inviting me to speak at our dinner tonight.

I should start by wishing you all "una gran bienvenida" to Spain. And, in the event that some of you came to Santiago de Compostela by completing the Camino, let me say "felicidades" and "Ultreia et Suseia"!

A common expression in Spain is that "el Camino da más de lo que recibe" – the Camino gives more than it receives. While I cannot claim to offer you any more ecclesiastical insights this evening, I will be reflecting on the recent banking turmoil and the implications for the global banking system and the Basel Committee.

For some of you, the turmoil may seem like a distant memory. Since the frenzied months of March to May, many banks have been reporting bumper financial results on the wave of rising interest rates.

A cursory look at financial markets since that period would also suggest that the worst may be behind us. So why do I plan to look back at what may be regarded as some as a historical event?

Put simply, the banking turmoil that started in March is the most significant system-wide banking stress since the Great Financial Crisis (GFC) in terms of scale and scope.

Over the span of 11 days – from 8 to 19 March 2023 – four banks with total assets of about $900 billion were shut down, put into receivership or rescued. This was followed by the failure of a fifth bank with roughly $230 billion in assets on 1 May 2023.

To give you a sense of the order of magnitude, the total value of these banks' assets is roughly equivalent to Spain's annual GDP (leaving aside the stock versus flow nature of these numbers).
The distress of these individual banks, while having largely distinct causes, triggered an assessment of the resilience of the broader banking system.

In response, large-scale public support measures were deployed by some jurisdictions to mitigate the impact of the stress, including significant central bank liquidity provision to banks, the activation of FX swap lines, government backstops or guarantees, and, in certain cases, an extension of deposit guarantee schemes.

In many respects, today's stabilisation of the banking system is due to a combination of public support measures and the increased resilience provided by post-GFC regulatory reforms, most notably Basel III. We had hoped that we would not need to rely on the former so frequently.

Against that backdrop, the Basel Committee undertook a review of this period and conducted a stocktake of the regulatory and supervisory implications of these developments, with a view to learning lessons.

I am pleased to inform you that, as recently announced by the Group of Governors and Heads of Supervision, good progress has been made with this work.

I will focus my remarks tonight by offering my personal views on some of the main takeaways and identifying some issues that may warrant further reflection.

Risk management and governance

There is perhaps a near universal agreement that one of the main lessons from the turmoil is the importance of banks' risk management practices and governance arrangements as the first and most important source of financial and operational resilience.

The boards and management of banks should be the first port of call in managing and overseeing risks; these functions cannot be outsourced to supervisors.

Jumping straight to discussions about the regulatory and supervisory implications of recent events is akin to forgiving banks for not fulfilling their primary responsibilities and likewise shareholders for not exercising due diligence.

Yet the banking turmoil highlighted a series of weaknesses by some banks in this area, including:

- fundamental shortcomings in (basic) risk management of traditional banking risks (such as interest rate risk and liquidity risk, and various forms of concentration risk);

- a failure to appreciate how various risks that were building up were interrelated and could compound one another;
- inadequate and unsustainable business models, including an excessive focus on growth and short-term profitability (fuelled by remuneration policies), at the expense of appropriate risk management;
- a poor risk culture and ineffective senior management and board oversight; and
- a failure to adequately respond to supervisory feedback and recommendations.

Many of these elements may appear obvious and quite basic in nature. So it is of deep concern to see that, in 2023, some banks' boards and senior management failed in their most elementary responsibilities of overseeing and challenging a bank's strategy and risk tolerance. More is clearly needed to shore up such responsibilities.

Consider the following historical anecdote.4 In 1800, a French chemist by the name of Éleuthère Irénée du Pont set up a gunpowder factory in Delaware. He quickly realised that gunpowder factories have an undesirable property: they tend to explode frequently. In response, du Pont took two initiatives.

First, he required that the director (himself) live inside the factory with his family, putting his life on the line – what you could view as "skin in the game".

Second, he established a rule that every new piece of machinery had to be operated for the first time by the factory's senior management. If the machine blew up, the manager would suffer the consequences. Needless to say, the safety of the plant increased overnight.

I don't think I need to draw out explicitly the comparisons with today's banking system. But it is clear that the turmoil raises some fundamental questions about the current banking system.

Is it simply inevitable that there will always be "outlier" banks with serious governance and risk management shortcomings? Is this a "feature" of a banking model that combines leverage and maturity transformation with a focus on short-term gains? Have we optimised the alignment of incentives between banks' boards and senior management and broader financial stability objectives? I don't have the answers to all of these questions, but I think they certainly merit further reflection.

To read more: https://www.bis.org/speeches/sp230914.htm

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.

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

The IAMBD offers standard, premium and lifetime membership, networking, training, certification programs, a monthly newsletter with alerts and updates, and services we can use.

The association develops and maintains three certification programs and many specialized tailor-made training programs for directors.

Join us. Read our monthly newsletter with news, alerts, challenges and opportunities. Get certified. Provide independent evidence that you are an expert.

You can explore what we offer to our members:

1. Membership - Become a premium or lifetime member.
You may visit:
https://www.iambd.org/HowToBecomeMember.html

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.iambd.org/Reading_Room.htm

3. Training and Certification - Become a Certified Member of the Board of Directors (CMBD), Certified Member of the Risk Committee of the Board of Directors (CMRBD) or Certified Member of the Corporate Sustainability Committee of the Board of Directors (CMCSCBD).

You may visit:
https://www.iambd.org/Distance_Learning_and_Certification.htm

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