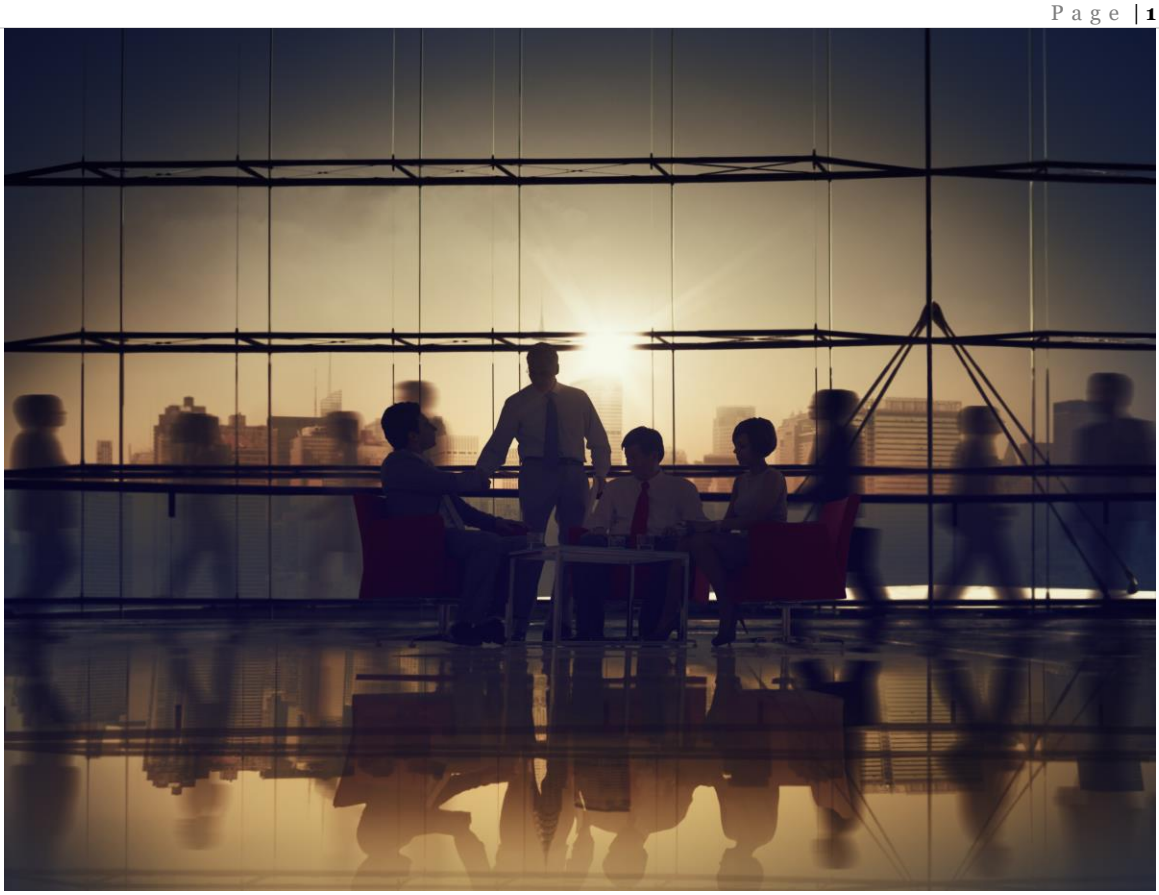


News for the Board of Directors, February 2024

Governor Michelle W. Bowman gave a great presentation (Protect Main Street sponsored by the Center for Capital Markets at the U.S. Chamber of Commerce, Washington, D.C.). We will start with it.

The Path Forward for Bank Capital Reform

"More is better." This axiom often holds true in many respects, but experience also teaches us that there are limits. Today, I'm happy to join you here at the U.S. Chamber of Commerce to talk about proposed changes to bank capital rules in the United States and to probe the limits of the notion that "more is better" when regulators seek to apply it to bank capital requirements.

In July 2023, the federal banking agencies proposed changes to implement the Basel III "endgame" capital reforms.

The published capital rulemaking proposal incorporated an expansive scope and a notable shift in approach by pushing down new Basel capital requirements to all banks with over $100 billion in assets, regardless of their international activities.

The proposal would substantially increase regulatory capital buffer and minimum capital requirements for the covered firms. The comment period closed yesterday, January 16th.

We've seen a robust response from commenters, with a large number of comments submitted during the latter part of the comment period.

As a policymaker, I am pleased to see the careful attention stakeholders have paid to this proposal and the thoughtful feedback that has been provided during the comment period. Public input should help to improve the efficiency and effectiveness of the proposal.

From my perspective, given the significant response from a number of industries and perspectives, as a bank regulatory policymaker, the agencies are obligated to think carefully about the best path forward for this proposal.

This should include making substantive changes to address known deficiencies with the proposal and giving the public an opportunity to comment on any reformulated proposal, to ensure the best possible outcome for the Basel capital reforms.

That path should ensure that sufficient consideration is given to the wide-reaching consequences of capital reform to the U.S. banking industry, the U.S. economy, and, importantly, U.S. businesses.

We should consider tradeoffs in addressing scope, calibration, and tailoring. And we should appropriately adjust the excessive calibrations and eliminate regulatory overreach in the proposed rule.

Today, I'd like to briefly discuss what I see as the consequences of miscalibration of capital reforms—and testing the "more is better" principle—through a discussion of the impacts of finalizing the proposed capital reforms without significant revisions.

I will then outline ideas for a path forward and highlight what I see as the two most pressing problems in the proposal, issues that we must address before finalizing these and other pending rules.

And finally, at the risk of lulling those to sleep who do not eat, drink, and breathe bank capital rules 24/7, I will identify a few important technical issues for resolution because they lead into the two overarching problems that I referenced a moment ago.

Considerations in Capital Policy

Capital plays a critical role in the U.S. banking system, promoting the safe and sound operation of banks and supporting confidence in the broader banking system. Capital helps banks provide financial products and services, including credit, that support American businesses.

I think we can all agree that higher levels of capital enhance financial resilience—up to a point. At the time of a bank's failure, capital—especially common equity capital, as the first type of funding to absorb losses—protects depositors and other creditors.

Capital allows banks to continue providing products and services, promoting a well-functioning financial system, even during times of stress.

But capital is not costless. Capital does not come into existence only at the point of failure—capital is an ongoing requirement, and an ongoing cost, for all banks.

The cost of capital— both the required minimum amount of capital and buffers and the market price of capital—influences every aspect of the business of banking, including the business lines a bank pursues, the products and services it offers, and the cost and availability of those products and services.

Banks are not obligated to offer the same financial products or services over time. Banks also are not obligated to maintain the same costs of products and services. Indeed, it would be irresponsible for a bank to ignore the cost of capital in managing its business, just as it would be irresponsible for a bank to ignore market preferences and forces when choosing its lines of business.

Increases to the cost of capital do not simply evaporate on a bank's balance sheet, they are passed through to customers in various ways, including in the form of higher costs for financial services or in reduced availability of services available in the market.

The cost of bank capital also influences where activities occur, either within the regulatory perimeter of the banking system or in non-bank entities and the broader shadow-banking system.

When the cost of a bank engaging in an activity exceeds the cost of performing the same activity in a non-bank, that cost differential creates pressure that over time leads to a shift in these activities to non-bank providers.

Where does that leave us? Achieving good policy requires acknowledging and balancing the benefits and costs of capital requirements, since it is one of the most important inputs policymakers can use to enhance the safety and efficiency of the banking system. Relying simply on the "more is better" approach downplays or ignores these critically important tradeoffs.

When policymakers consider changes to the capital framework, particularly increases of the magnitude contemplated in the proposal, we must carefully weigh the benefit of increased safety from higher capital levels, with the direct costs to banks, and the downstream effects on consumers, businesses, and the broader economy.

We must also consider the broader regulatory landscape and how changes to capital regulations may complement, overlap, or conflict with other regulatory requirements. And importantly, we must consider the broader implications for the structure of the U.S. financial system and for financial stability.

While these considerations may caution us against capital increases of the magnitude contemplated in the proposal, I do see a potential path forward for capital reform.

The Path Forward

As I consider next steps, I am cautiously optimistic that policymakers can work toward a reasonable compromise, one that addresses two of the most critical shortcomings of the proposal: over-calibration and the lack of regulatory tailoring.

Public feedback has also assisted in identifying the aspects of the proposal that result in the most severe unintended consequences. In my mind, it will be necessary for policymakers to modify the proposal to mitigate these issues and concerns as we move forward.

Calibration

First, I would like to address calibration. The costs of this proposal, if implemented in its current form, would be substantial.

As the proposal describes, Federal Reserve staff estimates these changes to result in an aggregate 20 percent increase in total risk-weighted assets across bank holding companies subject to the rule, although some commenters have projected much greater effects on some firms.

While the actual impact on binding capital requirements will vary by firm, it is apparent even with the incomplete information available today that this will represent a large increase in capital requirements.

In October of 2023, the Federal Reserve launched a data collection to gather more information from the banks affected by the Basel III capital proposal.

The purpose of this quantitative impact study was to help better understand the estimated effects of the proposal. My understanding is that the Federal Reserve will release its analysis of those findings and some aggregated information for comment.

And just as for the initial proposal, stakeholder feedback on this quantitative impact study and staff analysis will be very instructive as we seek to analyze and understand the expected impacts of the proposed capital reforms.

Based on the information available, increasing capital requirements as initially proposed could result in significant harm to the U.S. economy through the impact on U.S. businesses, while failing to achieve the intended goals of improving safety and soundness and promoting financial stability.

Much of the public feedback and concern focused on the calibration of the proposal and the corresponding impact across a number of industries. Farmers, ranchers, and agricultural producers that use derivatives to hedge price risks in agricultural supply chains have noted that the increased costs of providing these services from the proposal could lead banks to limit their availability in the marketplace.

Small-business owners (including builders, manufacturers, restaurant owners, and others) have indicated that the proposal could "make borrowing costs unaffordable and capital inaccessible."

These real-world examples only scratch the surface of the harmful effects of this proposal as described by a broad range of stakeholders noting the impact on a wide array of businesses. My initial observation is that, in the aggregate, the comments reflect a spectrum of concerns that are largely driven by calibration.

These well-founded concerns and the risks they highlight are not surprising in light of the scale of the proposed capital increase.

In addition, this direct independent feedback provides a new lens through which to view the proposal, enabling us to specifically identify and confront the predictable effects: higher costs of capital for banks and services for customers, less availability and narrower selection of services, and increased concentration in the providers of financial products and services.

These consequences could disproportionately harm underserved markets, businesses, and communities, as bank customers will bear the cost of these increased capital requirements.

In addition to the direct impacts of excessive calibration, policymakers must also consider international comparability and competitive disadvantages. A key element of the Basel capital rules is to promote greater international comparability, a goal that is frustrated when U.S. regulators over-calibrate requirements, at a level in excess of international peers and not supported by proportionate levels of risk.

Significant banking activities occur in the international and cross-border context, and we know that financial stability risks can spread throughout global financial markets. One approach to mitigate the spread of financial stability risks is to promote minimum standards across jurisdictions that not only improve competitive equity in banking markets but that also make the financial system safer.

The capital proposal reflects elements of the agreed upon Basel standards, but it far exceeds those agreed standards. Adjusting the calibration of the Basel capital reform proposal would have the important secondary benefit of enhancing this international consistency.

To address this issue of calibration, policymakers must develop and work toward a target, a top-line aggregate capital level that would best promote safety and soundness and one that has a broad consensus among policymakers.

Earlier efforts on the Basel proposal would have resulted in something closer to "capital neutrality"—with essentially minimal top-line change in aggregate capital requirements across the U.S. banking system.

I would note that the U.K. approach contemplates an average increase in the low single digits.

I look forward to learning more about stakeholder views on calibration from the comments we have received.

To read more:
https://www.federalreserve.gov/newsevents/speech/bowman20240117a.htm

Strategy

EMPOWERING COMMUNITIES

Cybersecurity is a shared responsibility. Europe strives for a cross sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in MSs and the EU institutions and agencies.

It strives to ensure the complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

CYBERSECURITY POLICY

Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives.

Cybersecurity must not be restricted to a specialist community of technical cybersecurity experts. Cybersecurity must therefore be embedded across all domains of EU policies. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

OPERATIONAL COOPERATION

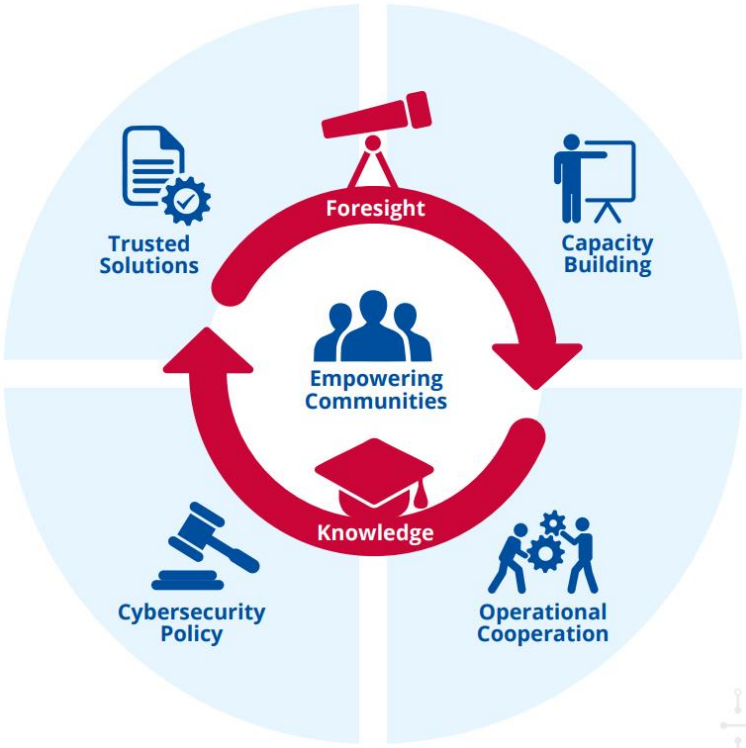
The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyberattacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large-scale and cross-border) cyber-attacks and cyber crisis.

Cross-border interdependencies have highlighted the need for effective cooperation between MSs and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

CAPACITY BUILDING

The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of information and communications technology (ICT) infrastructures and technologies by individuals, organisations and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply.

The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the MSs but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.



TRUSTED SOLUTIONS

Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating the security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust in digital solutions and the wider digital environment.

FORESIGHT

Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policymakers would be able to define early mitigation strategies that improve the EU's resilience to cybersecurity threats and find solutions to address emerging challenges.

KNOWLEDGE

The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling objectives, to work in a constantly moving environment – in terms of digital developments as well as

with regard to actors – to face the challenges of our time, a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge is clearly needed. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

NIS2	Adopted	The European Parliament and the Council of the European Union approved legislation that sets clearer rules for entities in a wider range of sectors. NIS2 reinforces and extends the existing approach under the NIS1 directive, strengthening and streamlining the cybersecurity risk management and incident reporting provisions, and extending the scope by adding additional sectors, such as space or telecom (important for securing satellite communications, a vital infrastructure in remote rural areas, but also as a fail over in times of a natural disaster or military conflict). NIS2 underlines the special role of telecoms as a highly mature sector, a conduit for cyberattacks, and a possible filter, protecting less mature and harder to protect sectors such as health care. In addition, the NIS2 ambitions need to be supported, for instance to improve incident reporting, to create a better situational picture, of vulnerability disclosure policies and an EU vulnerability database, of supply chain security and other coordinated EU-wide cybersecurity risk assessments, including expanding the scope in terms of sectors covered, and of creating the right culture and environment for essential and important entities to share cybersecurity-relevant information such as cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. MSs have 21 months to transpose NIS2 into national law and to implement it. In parallel, ENISA is developing its service and expertise for this with the introduction of service catalogue based on existing NIS1 expertise that is reflected in this single programming document (SPD). ENISA is already invested in activities linked to the development and implementation of NIS2, with its resilience, cooperation and capacity-building work, and will be building up its own capacities to support the implementation of the directive in the coming years, using existing resources and building on these wherever necessary.
The EU Cybersecurity Act	Amendment	On 18 April 2023, the Commission proposed a targeted amendment to the EU CSA (ENISA's founding regulation). The proposed targeted amendment aims to enable, by means of Commission implementing acts, the adoption of European cybersecurity certification schemes for 'managed security services'. This is in addition to ICT products, services and processes, which are already covered under the CSA. Such security services play an increasingly important role in the prevention and mitigation of cybersecurity incidents.

Regulation on digital operational resilience for the financial sector (DORA)	Adopted	In parallel with NIS2, in December 2022 the Parliament and the Council adopted DORA (Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector). The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. The regulation aims to ensure that all participants in the financial system are subject to a common set of standards to mitigate ICT risks for their operations and have the necessary safeguards in place to mitigate cyberattacks and other risks. DORA requires financial entities to ensure that they can withstand all types of ICT-related disruptions and threats. ENISA is actively supporting the mapping of cyber legislation initiatives in the finance sector and works closely with the Commission and relevant EU bodies on cybersecurity aspects of DORA including crisis management, incident reporting and information sharing.
Cyber diplomacy toolbox	Adopted	In addition, to support MS and European institutions, bodies and agencies (EUIBAs) in deterring and responding to cyberattacks from non-EU countries, the EU adopted a framework for a joint EU diplomatic response to malicious cyber activities, in the Council conclusions of 19 June 2017 ([2]). The European External Action Service (EEAS) recently published updated implementation guidelines for the cyber diplomacy toolbox detailing specific steps MSs could take ([3]). The guidelines underline the importance of measures taken by MSs under the NISD to improve resilience, the role of ENISA in establishing information-sharing channels with industry to gain situational awareness, and the importance of cooperation between the Cyber Crisis Liaison Organisation Network (EU-Cyclone), the Computer Security Incidence Response Team (CSIRT) network, ENISA, the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU) and the European Union Agency for Law Enforcement Cooperation, and EEAS Single Intelligence Analysis Capacity, to ensure that internal and external EU initiatives are coherent.

To read more: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2024-2024

The first set of final draft technical standards under the Digital Operational Resilience Act (DORA).

The three European Supervisory Authorities (EBA, EIOPA and ESMA – the ESAs) published the first set of final draft technical standards under the Digital Operational Resilience Act (DORA) aimed at enhancing the digital operational resilience of the EU financial sector by strengthening financial entities' Information and Communication Technology (ICT) and third-party risk management and incident reporting frameworks. The joint final draft technical standards include:

1. Final report, Draft Regulatory Technical Standards to further harmonise ICT risk management tools, methods, processes and policies as mandated under Articles 15 and 16(3) of Regulation (EU) 2022/2554

Contents

2. Final report on Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554.

Contents

3. Final report on Draft Regulatory Technical Standards specifying the criteria for

the classification of ICT related incidents, materiality thresholds for major incidents and significant cyber threats under Regulation (EU) 2022/2554.

Contents

4. Final Report On Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554

Contents

To read more: https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party

We carefully monitor the developments at: https://www.digital-operational-resilience-act.com
This website belongs to Cyber Risk GmbH, a sister entity of the association.

The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 solves an important problem in the EU financial regulation.

Before DORA, financial institutions managed the main categories of operational risk mainly with the allocation of capital, but they did not manage all components of operational resilience.

After DORA, they must also follow rules for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents.

DORA explicitly refers to ICT risk and sets rules on ICT risk-management, incident reporting, operational resilience testing and ICT third-party risk monitoring.

This Regulation acknowledges that ICT incidents and a lack of operational resilience have the possibility to jeopardise the soundness of the entire financial system, even if there is "adequate" capital for the traditional risk categories.

Artificial intelligence in central banking

Douglas Araujo, Sebastian Doerr, Leonardo Gambacorta, Bruno Tissot

BIS

Key takeaways

1. Central banks have been early adopters of machine learning techniques for statistics, macro analysis, payment systems oversight and supervision, with considerable success.

2. Artificial intelligence brings many opportunities in support of central bank mandates, but also challenges – some general and others specific to central banks.

3. Central bank collaboration, for instance through knowledge-sharing and pooling of expertise, holds great promise in keeping central banks at the vanguard of developments in artificial intelligence.

Long before artificial intelligence (AI) became a focal point of popular commentary and widespread fascination, central banks were early adopters of machine learning methods to obtain valuable insights for statistics, research and policy (Doerr et al (2021), Araujo et al (2022, 2023)).

The greater capabilities and performance of the new generation of machine learning techniques open up further opportunities. Yet harnessing these requires central banks to build up the necessary infrastructure and expertise.

Central banks also need to address concerns about data quality and privacy as well as risks emanating from dependence on a few providers.

This Bulletin first provides a brief summary of concepts in the machine learning and AI space. It then discusses central bank use cases in four areas:

(i) information collection and the compilation of official statistics;

(ii) macroeconomic and financial analysis to support monetary policy;

(iii) oversight of payment systems; and (iv) supervision and financial stability.

The Bulletin also summarises the lessons learned and the opportunities and challenges arising from the use of machine learning and AI.

It concludes by discussing how central bank cooperation can play a key role going forward.

Overview of machine learning methods and AI

Broadly speaking, machine learning comprises the set of techniques designed to extract information from data, especially with a view to making predictions.

Machine learning can be seen as an outgrowth of traditional statistical and econometric techniques, although it does not rely on a pre-specified model or on statistical assumptions such as linearity or normality.

The process of fitting a machine learning model to data is called training.

The criterion for successful training is the ability to predict outcomes on previously unseen ("out-of-sample") data, irrespective of how the models predict them.

This section describes some of the most common techniques used in central banks, based on the regular stocktaking exercises organised in the central banking community under the umbrella of the BIS Irving Fisher Committee on Central Bank Statistics (IFC).

To read more: https://www.bis.org/publl/bisbull84.pdf

SEC Adopts Rules to Enhance Investor Protections Relating to SPACs, Shell Companies, and Projections

The Securities and Exchange Commission adopted new rules and amendments to enhance disclosures and provide additional investor protection in initial public offerings (IPOs) by special purpose acquisition companies (SPACs) and in subsequent business combination transactions between SPACs and target companies (de-SPAC transactions).

SPAC IPOs and de-SPAC transactions can be used as a means for private companies to enter the public markets.

Given the complexity of these transactions, the Commission seeks to enhance investor protection in SPAC IPOs and de-SPAC transactions with respect to the adequacy of disclosure and the responsible use of projections.

The rules also address investor protection concerns more broadly with respect to shell companies and blank check companies, including SPACs.

“Just because a company uses an alternative method to go public does not mean that its investors are any less deserving of time-tested investor protections,” said SEC Chair Gary Gensler.

“Today’s adoption will help ensure that the rules for SPACs are substantially aligned with those of traditional IPOs, enhancing investor protection through three areas: disclosure, use of projections, and issuer obligations.

Taken together, these steps will help protect investors by addressing information asymmetries, misleading information, and conflicts of interest in SPAC and de-SPAC transactions.”

The new rules and amendments require, among other things, enhanced disclosures about conflicts of interest, SPAC sponsor compensation, dilution, and other information that is important to investors in SPAC IPOs and de-SPAC transactions.

The rules also require registrants to provide additional information about the target company to investors that will help investors make more informed voting and investment decisions in connection with a de-SPAC transaction.

The rules more closely align the required disclosures and legal liabilities that may be incurred in de-SPAC transactions with those in traditional IPOs.

For example, in certain situations, the rules require the target company to sign a registration statement filed by a SPAC (or another shell company) in connection with a de-SPAC transaction.

This would make the target company a "co-registrant" and assume responsibility for disclosures in that registration statement.

In addition, the rules make the Private Securities Litigation Reform Act of 1995 safe harbor from liability for forward-looking statements unavailable to certain blank check companies, including SPACs.

In connection with de-SPAC transactions, the rules include disclosure requirements related to projections, including disclosure of all material bases of the projections and all material assumptions underlying the projections. The rules also update and expand guidance on the use of projections in all SEC filings.

The adopting release is published on SEC.gov and will be published in the Federal Register. You may visit: https://www.sec.gov/files/rules/final/2024/33-11265.pdf

SECURITIES AND EXCHANGE COMMISSION

17 CFR Parts 210, 229, 230, 232, 239, 240, and 249

[Release Nos. 33-11265; 34-99418; IC-35096; File No. S7-13-22]

RIN 3235-AM90

Special Purpose Acquisition Companies, Shell Companies, and Projections

AGENCY: Securities and Exchange Commission.

ACTION: Final rules; guidance.

SUMMARY: The Securities and Exchange Commission ("Commission") is adopting rules intended to enhance investor protections in initial public offerings by special purpose acquisition companies (commonly known as SPACs) and in subsequent business combination transactions between SPACs and private operating companies (commonly known as de-SPAC transactions).

The rules will become effective 125 days after publication in the Federal Register.

Compliance with the structured data requirements, which require tagging of information disclosed pursuant to new subpart 1600 of Regulation S-K in Inline XBRL, will be required 490 days after publication of the rules in the Federal Register.

To read more: https://www.sec.gov/news/press-release/2024-8

The European Supervisory Authorities (ESAs) recommend steps to enhance the monitoring of BigTechs' financial services activities

The European Supervisory Authorities (EBA, EIOPA and ESMA) published a Report setting out the results of a stocktake of BigTech direct financial services provision in the EU.

Table 1: Stocktake results: MAGs as electronic money institutions (EMI), payment institutions (PI), credit institutions (CI), insurance intermediaries/undertakings.

	Group	Subsidiary	Home MS	Host MS
E-Money Institutions	**Alphabet (Google)**	Google Payment Lithuania UAB	LT	12
	Meta Platforms (Facebook)	Facebook Payments International Limited	IE	14
	Amazon	Amazon Payment Europe SCA	LU	16
	Alibaba (Ant Group)	Alipay (Europe) Limited S.A.	LU	4
	Uber	Uber Payments B.V.	NL	10
	NTT Docomo	DOCOMO Digital Payment Services AG	LI*	3
Payment I	**Alphabet (Google)**	Google Payment Ireland Limited	IE	13
	Tencent	Wechat	NL	2
Credit I	**Orange**	Orange Bank	FR	3
	Rakuten	Rakuten Europe Bank S.A.	LU	13
Insurance	**Tesla**	Tesla Insurance ltd (undertaking)	MT	1
	Vodafone	Vodafone Insurance Limited (undertaking)	MT	9
	Amazon	Amazon EU Sarl (intermediary)	LU	2
	Apple	Apple Distribution International (intermediary)	IE	2
	Orange	Orange Slovensko (Intermediary)	SK	/

*LI: until 1 June 2022

The Report identifies the types of financial services currently carried out by BigTechs in the EU pursuant to EU licences and highlights inherent opportunities, risks, regulatory and supervisory challenges.

The ESAs will continue to strengthen the monitoring of the relevance of BigTech in the EU financial services sector, including via the establishment of a new monitoring matrix.

In 2023 the ESAs, via the European Forum for Innovation Facilitators (EFIF), conducted a cross-sectoral stocktake of BigTech subsidiaries providing financial services in the European Union (EU) as a follow-up to the ESAs' 2022 response to the European Commission's Call for Advice on Digital Finance.

The stocktake showed that BigTech subsidiary companies currently licenced to provide financial services pursuant to EU law mainly provide services in the payments, e-money and insurance sectors and, in limited cases, the banking sector. However, the ESAs have yet to observe their presence in the market for securities services.

JC 2024 02

01/02/2024

Report on 2023 stocktaking of BigTech direct financial services provision in the EU

Joint-ESA Report

To further strengthen the cross-sectoral mapping of BigTechs' presence and relevance to the EU's financial sector, the ESAs propose to set-up a data mapping tool within the EFIF.

This tool is intended to provide a framework that supervisors from the National Competent Authorities would be able to use to monitor on an ongoing and dynamic basis the BigTech companies' direct and indirect relevance to the EU financial sector.

Figure 1: Potential opportunities arising from intragroup dependencies

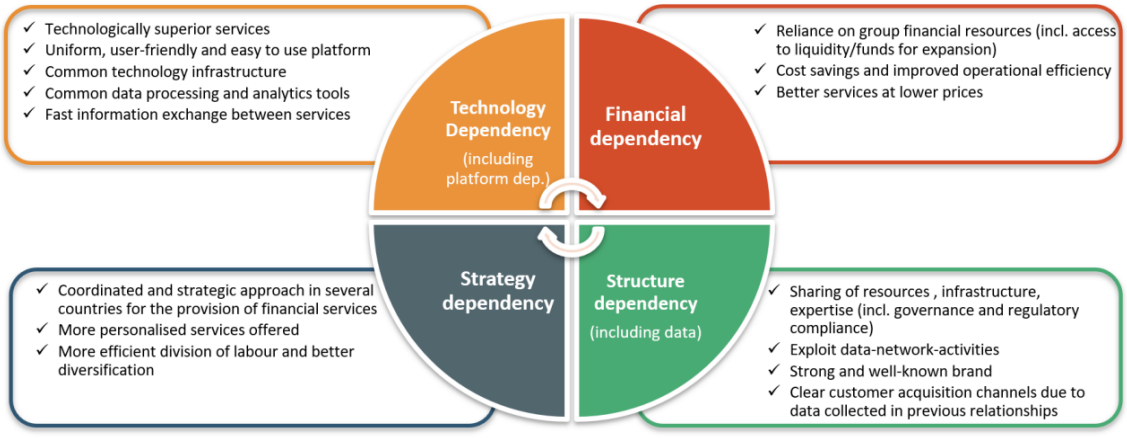
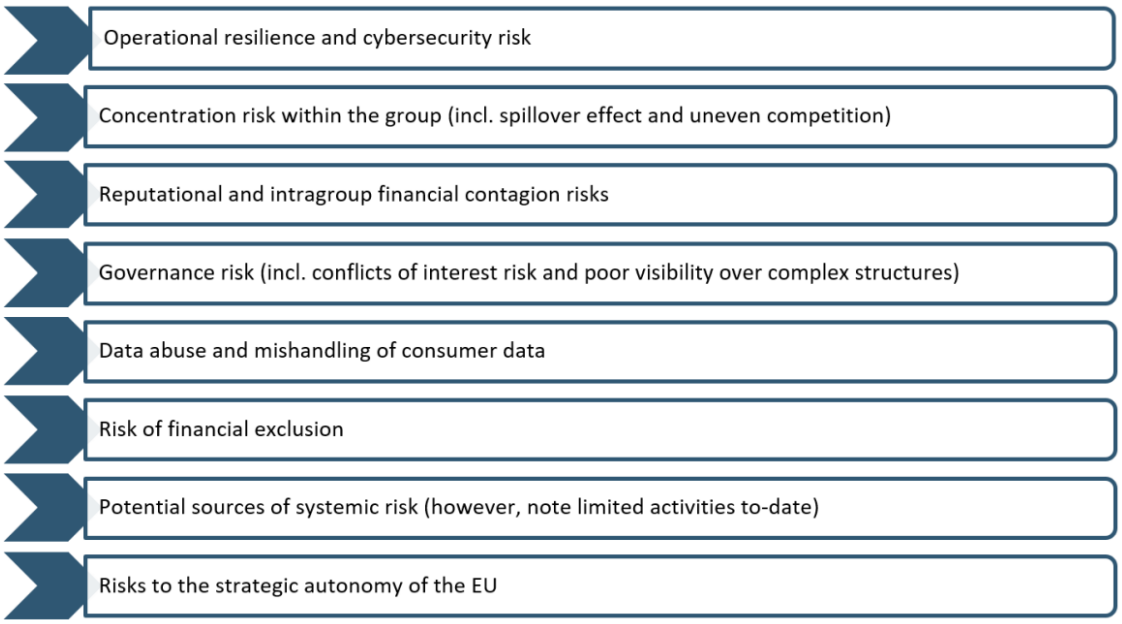


Figure 2: Potential risks arising from intragroup dependencies



The ESA will also continue the cross-disciplinary exchanges in the setting of the EFIF to further foster the exchange of information between EFIF members and other relevant financial and non-financial sector authorities involved in the monitoring of BigTechs' activities (e.g., data protection and consumer protection authorities).

To read more: https://www.eiopa.europa.eu/system/files/2024-02/Joint%20ESAs%20Report%20-%20Stocktaking%20of%20BigTech%20direct%20financial%20services%20provision%20in%202023.pdf

The U.S. AI Safety Institute Consortium (AISIC).

On February 7, 2024 US Secretary of Commerce Gina Raimondo announced key members of the executive leadership team to lead the U.S. AI Safety Institute (USAISI), which will be established at the National Institute of Standards and Technology (NIST).

In support of efforts to create safe and trustworthy artificial intelligence (AI), NIST is establishing the U.S. Artificial Intelligence Safety Institute (USAISI).

To support this Institute, NIST has created the U.S. AI Safety Institute Consortium.

The Consortium brings together more than 200 organizations to develop science-based and empirically backed guidelines and standards for AI measurement and policy, laying the foundation for AI safety across the world.

This will help ready the U.S. to address the capabilities of the next generation of AI models or systems, from frontier models to new applications and approaches, with appropriate risk management strategies.

Consortium members contributions will support one of the following areas:

- Develop new guidelines, tools, methods, protocols and best practices to facilitate the evolution of industry standards for developing or deploying AI in safe, secure, and trustworthy ways

- Develop guidance and benchmarks for identifying and evaluating AI capabilities, with a focus on capabilities that could potentially cause harm

- Develop approaches to incorporate secure-development practices for generative AI, including special considerations for dual-use foundation models, including:

  - Guidance related to assessing and managing the safety, security, and trustworthiness of models and related to privacy-preserving machine learning;

  - Guidance to ensure the availability of testing environments

- Develop and ensure the availability of testing environments

- Develop guidance, methods, skills and practices for successful red-teaming and privacy-preserving machine learning

- Develop guidance and tools for authenticating digital content

- Develop guidance and criteria for AI workforce skills, including risk identification and management, test, evaluation, validation, and verification (TEVV), and domain-specific expertise

- Explore the complexities at the intersection of society and technology, including the science of how humans make sense of and engage with AI in different contexts

- Develop guidance for understanding and managing the interdependencies between and among AI actors along the lifecycle

NIST received over 600 Letters of Interest from organizations across the AI stakeholder community and the United States. As of February 8, 2024, the consortium includes more than 200 member companies and organizations.

The AI Safety Institute Consortium (AISIC) is pleased to announce its inaugural cohort of members:

A

- Accel AI Institute
- Accenture LLP
- Adobe
- Advanced Micro Devices (AMD)
- AFL-CIO Technology Institute (Provisional Member)
- AI Risk and Vulnerability Alliance
- AIandYou
- Allen Institute for Artificial Intelligence
- Alliance for Artificial Intelligence in Healthcare
- Altana
- Alteryx
- Amazon.com
- American University, Kogod School of Business
- AmpSight
- Anika Systems Incorporated
- Anthropic
- Apollo Research
- Apple
- Ardent Management Consulting
- Aspect Labs
- Atlanta University Center

F

- FAIR Institute
- FAR AI
- Federation of American Scientists
- FISTA
- ForHumanity
- Fortanix, Inc.
- Free Software Foundation
- Frontier Model Forum
- Financial Services Information Sharing and Analysis Center (FS-ISAC)
- Future of Privacy Forum

G

- Gate Way Solutions
- George Mason University
- Georgia Tech Research Institute
- GitHub
- Gladstone AI
- Google
- Gryphon Scientific
- Guidepost Solutions

H

P

- Palantir
- Partnership on AI (PAI)
- Pfizer
- Preamble
- PwC
- Princeton University
- Purdue University, Governance and Responsible AI Lab (GRAIL)

Q

- Qualcomm Incorporated
- Queer in AI

R

- RAND Corporation
- Redwood Research Group
- Regions Bank
- Responsible AI Institute
- Robust Intelligence
- RTI International

S

- SaferAI
- Salesforce
- SAS Institute

- Atlanta University Center Consortium
- Autodesk, Inc.

B

- BABL AI Inc.
- Backpack Healthcare
- Bank of America
- Bank Policy Institute
- Baylor College of Medicine
- Beck's Superior Hybrids
- Benefits Data Trust
- Humane Intelligence
- Booz Allen Hamilton
- Boston Scientific
- BP
- BSA | The Software Alliance
- BSI Group America

C

- Canva
- Capitol Technology University
- Carnegie Mellon University
- Casepoint
- Center for a New American Security
- Center For AI Safety
- Center for Security and Emerging Technologies (Georgetown University)
- Center for Democracy and Technology
- Centers for Medicare & Medicaid Services
- Centre for the Governance of AI
- Cisco Systems
- Citadel AI
- Citigroup
- CivAI
- Civic Hacker LLC
- Cleveland Clinic
- Coalition for Health AI (CHAI) (Provisional Member)
- Cohere
- Common Crawl Foundation
- Cornell University

- Hewlett Packard Enterprise
- Hispanic Tech and Telecommunications Partnership (HTTP)
- Hitachi Vantara Federal
- Hugging Face
- Human Factors and Ergonomics Society
- Humane Intelligence
- Hypergame AI

I

- IBM
- Imbue
- Indiana University
- Inflection AI
- Information Technology Industry Council
- Institute for Defense Analyses
- Institute for Progress
- Institute of Electrical and Electronics Engineers, Incorporated (IEEE)
- Institute of International Finance
- Intel Corporation
- Intertrust Technologies
- Iowa State University, Translational AI Center (TrAC)

- Iowa State University, Translational AI Center (TrAC)

J

- JPMorgan Chase
- Johns Hopkins University

K

- Kaiser Permanente
- Keysight Technologies
- Kitware, Inc.
- Knexus Research
- KPMG

L

- LA Tech4Good
- Leadership Conference Education Fund, Center for Civil Rights and Technology
- Leela AI

- SAS Institute
- SandboxAQ
- Scale AI
- Science Applications International Corporation
- Scripps College
- SecureBio
- Society of Actuaries Research Institute
- Software & Information Industry Association
- SonarSource
- SRI International
- Stability AI (Provisional Member)
- stackArmor
- Stanford Institute for Human-Centered AI, Stanford Center for Research on Foundation Models, Stanford Regulation, Evaluation, and Governance Lab
- State of California, Department of Technology
- State of Kansas, Office of Information Technology Services
- StateRAMP
- Subtextive
- Syracuse University

T

T

- Taraaz
- TensTorrent USA
- Texas A&M University
- Thomson Reuters (Provisional Member)
- Touchstone Evaluations
- Trustible
- TrueLaw
- Trufo

U

- UnidosUS
- UL Research Institutes
- University at Albany, SUNY Research Foundation
- University at Buffalo, Institute for Artificial Intelligence and Data Science

- Cranium AI
- Credo AI
- CrowdStrike
- Cyber Risk Institute

D

- Dark Wolf Solutions
- Data & Society Research Institute
- Databricks
- Dataiku
- DataRobot
- Deere & Company
- Deloitte
- Beckman Coulter
- Digimarc
- DLA Piper
- Drexel University
- Drummond Group
- Duke University
- The Carl G Grefenstette Center for Ethics at Duquesne University

E

- EBG Advisors
- EDM Council
- Eightfold AI
- Elder Research
- Electronic Privacy Information Center
- Elicit
- EleutherAI Institute
- Emory University
- Enveil
- EqualAI
- Erika Britt Consulting
- Ernst & Young, LLP
- Exponent
- Linux Foundation, AI & Data
- Lucid Privacy Group
- Lumenova AI

M

- Magnit Global Solutions
- Manatt, Phelps & Phillips
- MarkovML
- Massachusetts Institute of Technology, Lincoln Laboratory
- Mastercard
- Meta
- Microsoft
- MLCommons
- Model Evaluation and Threat Research (METR, formerly ARC Evals)
- Modulate
- MongoDB

N

- National Fair Housing Alliance
- National Retail Federation
- New York Public Library
- New York University
- NewsGuard Techologies
- Northrop Grumman
- NVIDIA

O

- ObjectSecurity LLC
- Ohio State University
- O'Neil Risk Consulting & Algorithmic Auditing, Inc. (ORCAA)
- OpenAI
- OpenPolicy
- OWASP (AI Exchange & Top 10 for LLM Apps)
- University of Oklahoma, Data Institute for Societal Challenges (DISC)
- University of Oklahoma, NSF AI Institute for Research on Trustworthy AI in Weather, Climate, and Coastal Oceanography (AI2ES)
- University at Buffalo, Center for Embodied Autonomy and Robotics
- University of Texas at San Antonio (UTSA)
- University of Maryland, College Park
- University Of Notre Dame Du Lac
- University of Pittsburgh
- University of South Carolina, AI Institute
- University of Southern California
- U.S. Bank National Association

V

- Vanguard
- Vectice
- Visa

W

- Wells Fargo & Company
- Wichita State University, National Institute for Aviation Research
- William Marsh Rice University
- Wintrust Financial Corporation
- Workday

To read more: https://www.nist.gov/artificial-intelligence/artificial-intelligence-safety-institute

Consultation on Guidelines on preventing the abuse of funds and certain crypto-assets transfers for ML/TF (Travel rule Guidelines)

The European Banking Authority (EBA) today launched a public consultation on new Guidelines on preventing the abuse of funds and certain crypto-assets transfers for money laundering and terrorist financing purposes.

These 'travel rule' Guidelines specify the steps that Payment Service Providers (PSPs), Intermediary PSPs (IPSPs), crypto-asset service providers (CASPs) and Intermediary CASPs (ICASPs) should take to detect missing or incomplete information that accompanies a transfer of funds or crypto-assets.

They also detail the procedures all these providers should put in place to manage a transfer of funds or a transfer of crypto-assets that lacks the required information.

These Guidelines aim at forging a common understanding to ensure the consistent application of EU law as well as a stronger anti-money laundering and countering the financing of terrorism (AML/CFT) regime.

The consultation runs until 26 February 2024.

The main objective of these Guidelines is to prevent the abuse of funds and crypto-assets transfers for terrorist financing and other financial crime purposes.

The Guidelines also ensure that relevant authorities can fully trace such transfers where this is necessary to prevent, detect or investigate money laundering and terrorist financing.

To achieve this, the EBA promotes the development of a common understanding by PSPs, IPSPs, CASPs and ICASPs and competent authorities across the EU, of what are the effective procedures to detect and manage the transfer of funds and crypto-assets lacking the required information on the payer/originator and the payee/beneficiary, and how they should be applied.

Consultation process

Comments to the consultation paper can be sent by clicking on the "send your comments" button on the EBA's consultation page. The deadline for the submission of comments is 26 February 2024.

The EBA will hold a virtual public hearing on the consultation paper on 17 January 2024 from 14:00 to 16:00 Paris time. The EBA invites interested stakeholders to register using this link by 3 January 2023 at 16:00 CET. The dial-in details will be communicated to those who have registered for the meeting.

All contributions received will be published following the end of the consultation, unless requested otherwise.

Legal basis, background

In July 2021 the European Commission issued a legislative package with four proposals to reform the EU's legal and institutional AML/CFT framework. It included a proposal for a recast of Regulation (EU) 2015/847, now published in the Official Journal of the European Union since June 2023 as Regulation (EU) 2023/1113.

The recast brings the EU's legal framework in line with the Financial Action Task Force (FATF)'s standards by extending the obligation to include information about the originator and beneficiary to CASPs – the so-called "travel rule".

It also amends Directive (EU) 2015/849 to subject CASPs, which are authorized in accordance with the Regulation (EU) 2023/1114 to the same AML/CFT requirements and AML/CFT supervision as credit and financial institutions.

Article 36 (first and second subparagraphs) of Regulation (EU) 2023/1113 and Article 19a(2) of Directive (EU) 2015/849 mandate the EBA to issue guidelines to competent authorities, PSPs and CASPs on:

(a) the measures those providers should take to comply with certain articles of Regulation (EU) 2023/1113;

(b) the technical aspects of the application of this Regulation to direct debits; and

© the measures, including the criteria and means for identification and verification of the identity of the originator or beneficiary of a transfer made to or from a self-hosted address.

The EBA is proposing to deliver this mandate by repealing the 2017 Joint European supervisory authorities (ESAs)'s Guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information (JC/GL/2017/16) and replace them with new Guidelines.

Responses

Responses to the consultations can be sent to the EBA. All contributions received will be published after the consultation closes, unless requested otherwise.

Deadline for submitting responses: 26/02/2024 at 23:59

To read more: https://www.eba.europa.eu/publications-and-media/events/consultation-guidelines-preventing-abuse-funds-and-certain-crypto

Disclaimer

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

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

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

This information:

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

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

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

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

- is not professional or legal advice;

- is in no way constitutive of interpretative;

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

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

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

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

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

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

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

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

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

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

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

Our training and certification programs

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

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

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

Contact Us

Lyn Spooner
Email: lyn@iambd.org

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