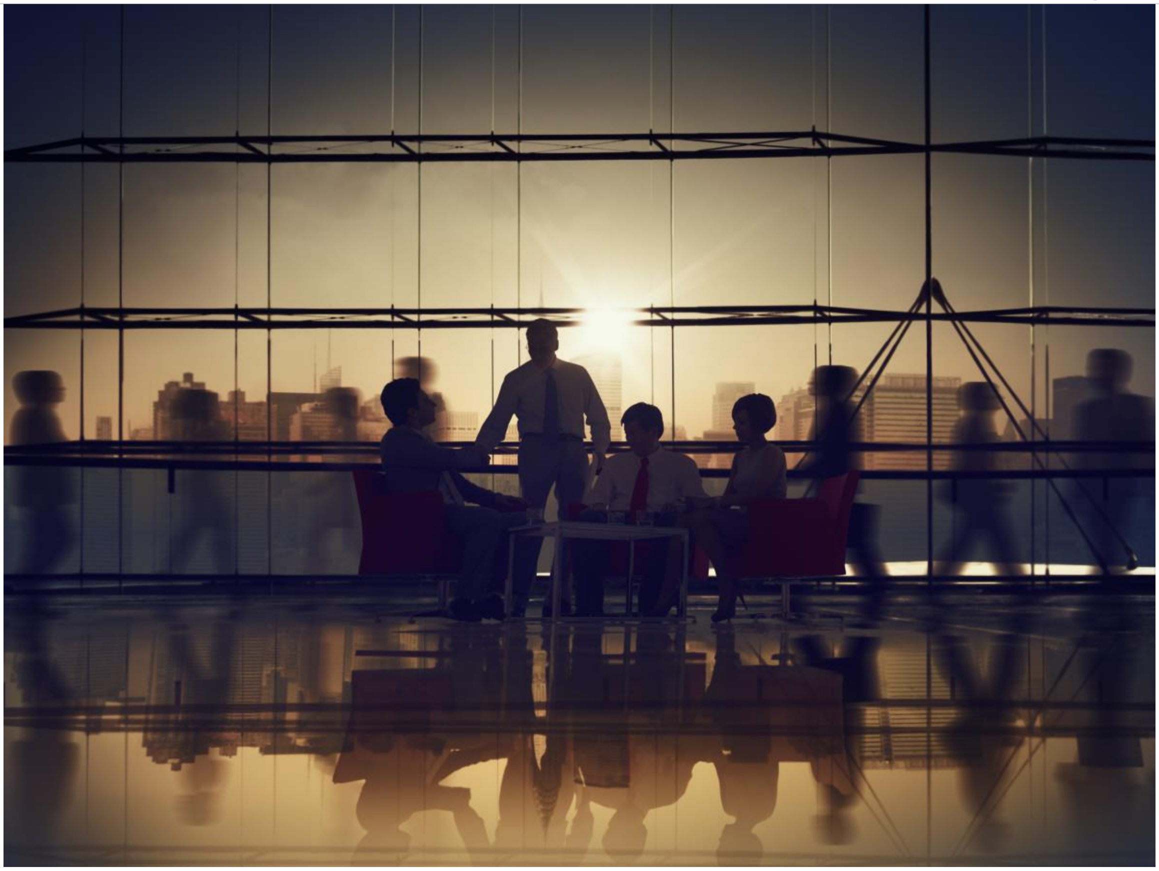


News for the Board of Directors, January 2024

We will start with an interesting presentation from Ben Broadbent, Deputy Governor for Monetary Policy of the Bank of England, at the London Business School, with title: “Signal versus noise”.

We are all aware that the future is unpredictable. When it comes to gauging the economy, however, it's not just the future that's uncertain: so is the present. For all the time and effort put into its forecasts the MPC also spends a great deal of it getting to understand the here and now.

This isn't straightforward. For one thing, it's not always possible to determine precisely what's causing what – to trace the economy we observe back to the underlying forces that are driving it.

Is output growth being moved around by demand or supply? Ditto employment? To take an example of particular relevance right now, has strong wage growth been the result of exceptional tightness of the labour market, especially last year; or is it the "second-round effect" of very high spot inflation in late 2022 and earlier this year?

These things aren't mutually exclusive: almost certainly, both have played a part. But the balance of the two matters. As the direct effects of the pandemic and the war dissipate, wholesale prices of energy and other traded goods have been declining.

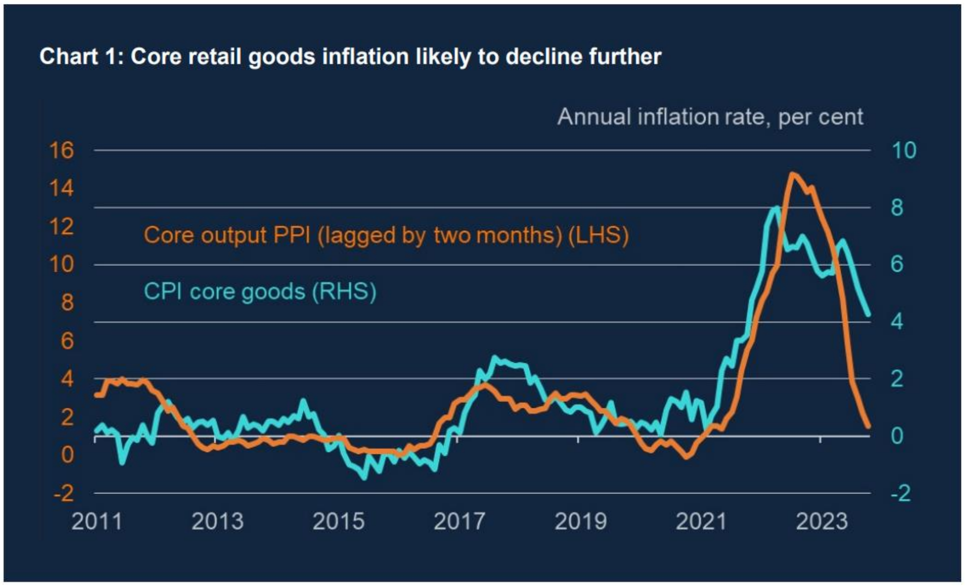


Chart 1: Core retail goods inflation likely to decline further

Sources: ONS and Bank calculations. Core output PPI is for manufactured products excluding non-core items. Core output PPI annual inflation is advanced by two months, which maximises correlation with CPI core goods inflation.

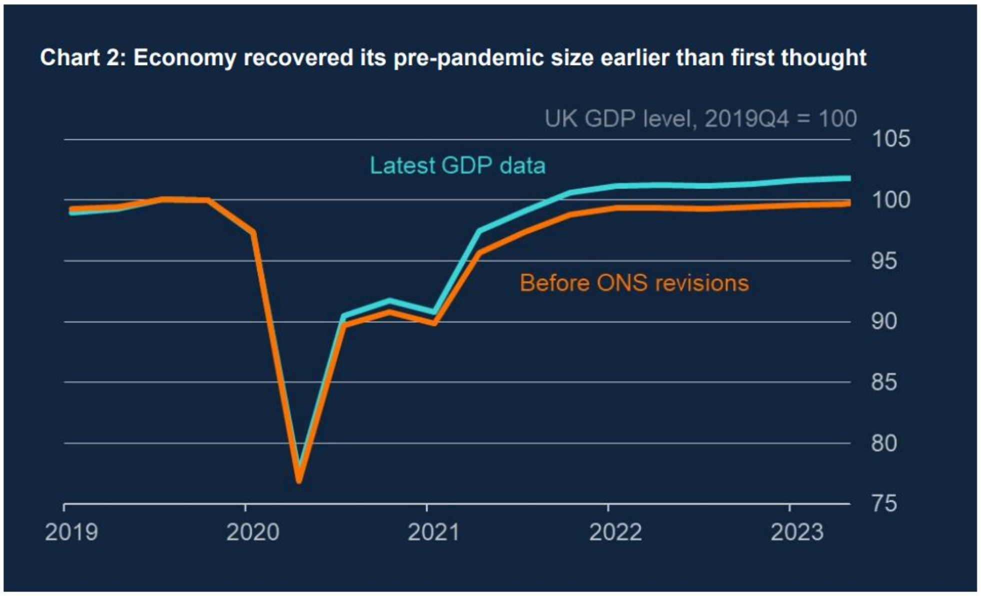


Chart 2: Economy recovered its pre-pandemic size earlier than first thought

Sources: ONS and Bank calculations. ONS 2023 Blue Book revisions. See Box C in the **November Monetary Policy Report** for more details.

This is now feeding through to inflation rates for retail goods prices and the aggregate CPI itself (Chart 1 plots core goods inflation against its wholesale counterpart; there have been similar trends in food and energy markets).

As this happens, one might expect these second-round effects on wage growth and broader domestic inflation to weaken as well, quite independently of the stance of monetary policy.

To the extent the tight labour market is the cause of strong domestic inflation, however, then the economy would need a longer period of below-trend growth – possibly with corresponding consequences for monetary policy – to bring it back into a more sustainable position.

At any rate, the more general point is that it's not always easy to infer the deeper, unobserved causes of economic fluctuations from the directly observable information.

Second, even what we do get to observe – GDP, employment, wages and the like – may not be perfectly measured.

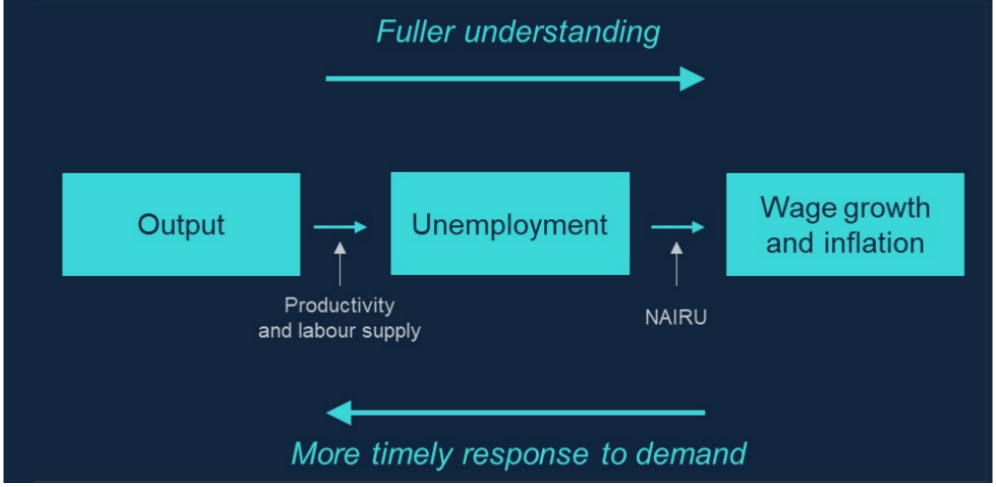
For some things (notably GDP) the relevant information comes in only over time and, as a result, the data are subject to revision.

These changes can be sizeable. Recently, for example, estimated growth during 2020 and 2021 was revised up by almost two percentage points (Chart 2).

As a result the economy is now thought to have reached its pre-pandemic size nearly two years earlier than was previously thought.

To read more:
https://www.bankofengland.co.uk/speech/2023/december/ben-broadbent-speech-at-london-business-school#:~:text=In%20this%20speech%20Ben%20talks,the%20economy%20and%20incoming%20data.

Chart 8: Lags in the inflation process mean that, when the policymaker is uncertain about supply, there's a trade-off between a better understanding of the economy and the timeliness of the policy response


Fuller understanding
Output
Unemployment
Wage growth and inflation
Productivity and labour supply
NAIRU
More timely response to demand

CISA and ENISA enhance their Cooperation

Geopolitics have shaped the cyber threat landscape, bringing like-minded partners closer together in the wake of common cyber challenges and advances in digital technologies.

At the EU-US Cyber Dialogue, ENISA and CISA announced the signing of their Working Arrangement as an important milestone in the overall cooperation between the United States and the European Union in the field of cybersecurity, also following the Joint Statement of European Commissioner Thierry Breton and U.S. Secretary for Homeland Security Alejandro Mayorkas of January 2023.

CISA AND ENISA TO ENHANCE THEIR COOPERATION
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

ENISA's International Strategy directs the Agency to be selective in engaging with international partners and to limit its overall approach in international cooperation to those areas and activities that will have high and measurable added value in achieving the Agency's strategic objectives.

CISA is a key partner to ENISA in achieving these objectives and by extension the EU in achieving a higher common level of cybersecurity.

The Working Arrangement is both a consolidation of present areas of cooperation, as well as opening the door to new ones.

Current examples are the organisation and promotion of the International Cybersecurity Challenge (ICC), exchanging best practices in the area of incident reporting or ad hoc information exchanges on basic cyber threats.

This arrangement is broad in nature and covers both short-term structured cooperation actions, as well as paving the way for longer-term cooperation in cybersecurity policies and implementation approaches.
Cooperation will be sought in the areas of:

1. Cyber Awareness & Capacity Building to enhance cyber resilience: including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings and the sharing and promotion of cyber awareness tools and programmes.

2. Best practice exchange in the implementation of cyber legislation; including on key cyber legislation implementation such as the NIS Directive, incident reporting, vulnerabilities management and the approach to sectors such as telecommunications and energy.

3. Knowledge and information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities and in full respect of data protection requirements.

A work plan will operationalise the Working Arrangement and regular reporting at the EU-US Cyber Dialogues is foreseen.

To read more: https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation

A new era for corporate taxation in the EU enters into force

European Commission

1 January 2024 – Ground-breaking new EU rules come into effect, introducing a minimum rate of effective taxation of 15% for multinational companies active in EU Member States.

The framework will bring greater fairness and stability to the tax landscape in the EU and globally, while making it more modern and better adapted to today's globalised, digital world.

The entry into force of the minimum effective taxation rules, unanimously agreed by Member States in 2022, formalises the EU's implementation of the so-called ‘Pillar 2' rules agreed as part of the global deal on international tax reform in 2021.

While almost 140 jurisdictions worldwide have now signed up to those rules, the EU has been a front-runner in translating them into hard law.

By lowering the incentive for businesses to shift profits to low-tax jurisdictions, Pillar 2 curbs the so-called "race to the bottom"—the battle between countries to lower their corporate income tax rates in order to attract investment.

It is already delivering results, with a number of zero tax jurisdictions around the world having announced the introduction of a corporate income tax for the companies in scope.

In detail

The rules will apply to multinational enterprise groups and large-scale domestic groups in the EU, with combined financial revenues of more than €750 million a year.

They will apply to any large group, both domestic and international, with a parent company or a subsidiary situated in an EU Member State.

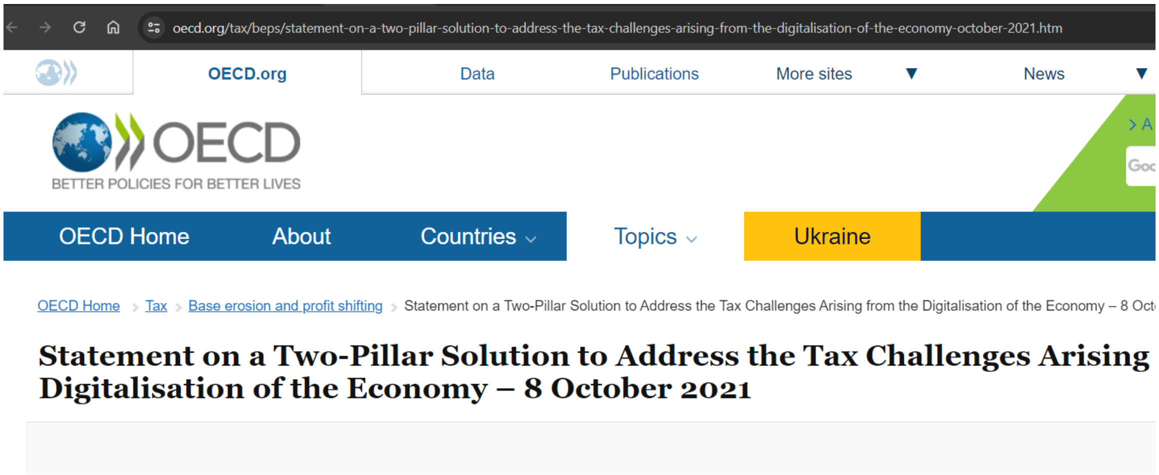
The Directive includes a common set of rules on how to calculate and apply a 'top-up tax' due in a particular country should the effective tax rate be below 15%.

If a subsidiary company is not subject to the minimum effective rate in a foreign country where it is located, the Member State of the parent company will also apply a top-up tax on the latter.

In addition, the Directive ensures effective taxation in situations where the parent company is situated outside the EU in a low-tax country which does not apply equivalent rules.

Background

With this historic law, the EU's pledge to be among the first to implement the OECD tax reform, has come to fruition. Ensuring a global minimum level of taxation for Minimum corporate taxation is one of the two work streams of the global OECD agreement (Pillar 2) - the other is the partial re-allocation of taxing rights (known as Pillar 1).


oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm
OECD.org
Data
Publications
More sites ▼
News ▼
OECD
BETTER POLICIES FOR BETTER LIVES
OECD Home
About
Countries ⌄
Topics ⌄
Ukraine

OECD Home > Tax > Base erosion and profit shifting > Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy – 8 Oct

Statement on a Two-Pillar Solution to Address the Tax Challenges Arising Digitalisation of the Economy – 8 October 2021

You may visit: https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm

The latter will adapt the international rules on how the taxation of corporate profits of the largest and most profitable multinationals is shared amongst countries, to reflect the changing nature of business models and the ability of companies to do business without a physical presence.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6712

PCAOB Staff Outline 2024 Inspection Priorities with Focus on Driving Improvements in Audit Quality

The staff report includes key risks and considerations auditors should focus on, along with questions for audit committees and more.

Public Company Accounting Oversight Board (PCAOB) inspectors outlined their priorities for 2024 inspections in a PCAOB staff report. The report highlights key risks, like high interest rates, and other considerations, like audit areas with recurring deficiencies, that auditors should be focused on when planning and performing audit procedures. It notes that the PCAOB will continue to prioritize inspections of financial-services sector audits, digital assets, and more.

The report also includes suggested questions for audit committees to hold firms accountable to high standards when hiring and overseeing the audit process.

“Our inspection priorities Spotlight provides firms with important insights to help them plan and perform high-quality audits investors deserve,” said PCAOB Chair Erica Y. Williams. “We encourage firms and audit committees to make use of this important tool to help improve audit quality.”

The report also reiterates the inspection staff’s commitment to enhancements to our inspection program, such as increasing the number of engagements reviewed and improving the timeliness of inspection reports.

Among the PCAOB’s inspection enhancements in 2024 will be the creation of a PCAOB team that will evaluate culture across the largest domestic audit firms. This initiative will include interviewing firm personnel and evaluating other documentation, with the aim of using this information to enhance the PCAOB’s understanding of how audit firm cultures may be affecting audit quality.

Overall Business Risk Considerations:

Our 2024 inspection program will consider overall business risks present in the audits inspected. A few of these business risks include:

1. Persistent high interest rates, tightening of credit availability, and/or inflationary challenges.

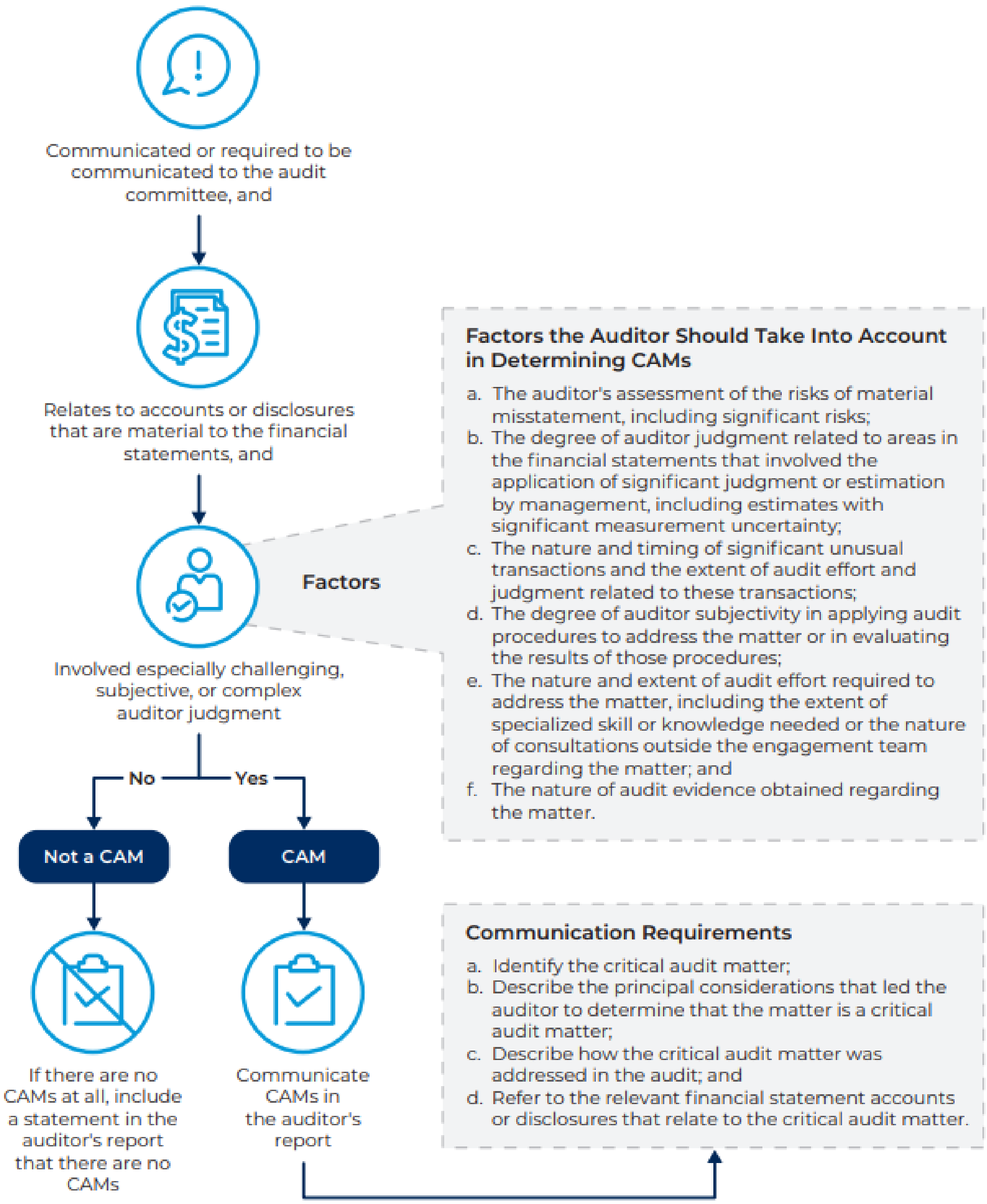
2. Disruptions in the supply chain and rising costs.

3. Business models that are significantly impacted by rapidly changing technology.

4. Geopolitical conflicts.

5. Financial statements that include areas with a higher inherent risk of fraud, estimates involving complex models or processes, and/or presentation and disclosures that may be impacted by complexities in the public company's activities.

Determining and Communicating Critical Audit Matters (CAMs)


Communicated or required to be communicated to the audit committee, and
Relates to accounts or disclosures that are material to the financial statements, and
Factors
Involved especially challenging, subjective, or complex auditor judgment
No
Yes
Not a CAM
CAM
If there are no CAMs at all, include a statement in the auditor's report that there are no CAMs
Communicate CAMs in the auditor's report

Factors the Auditor Should Take Into Account in Determining CAMs

a. The auditor's assessment of the risks of material misstatement, including significant risks;
b. The degree of auditor judgment related to areas in the financial statements that involved the application of significant judgment or estimation by management, including estimates with significant measurement uncertainty;
c. The nature and timing of significant unusual transactions and the extent of audit effort and judgment related to these transactions;
d. The degree of auditor subjectivity in applying audit procedures to address the matter or in evaluating the results of those procedures;
e. The nature and extent of audit effort required to address the matter, including the extent of specialized skill or knowledge needed or the nature of consultations outside the engagement team regarding the matter; and
f. The nature of audit evidence obtained regarding the matter.

Communication Requirements

a. Identify the critical audit matter;
b. Describe the principal considerations that led the auditor to determine that the matter is a critical audit matter;
c. Describe how the critical audit matter was addressed in the audit; and
d. Refer to the relevant financial statement accounts or disclosures that relate to the critical audit matter.

Prioritized Sectors/Industries:

In 2024, in addition to continuing to select some engagements for review based on risk and some randomly, we will do the following:

1. Continue our emphasis on selecting audits of companies engaging in merger and acquisition activities or business combinations.

2. Continue our emphasis on selecting audits of broker-dealers that file compliance reports and others that provide customers with various investment opportunities, such as introducing brokers.

3. Continue to select non-traditional audit areas to inspect.

PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

SPOTLIGHT

Staff Priorities for 2024 Inspections and Interactions With Audit Committees

Inspections Considerations:

The report also discusses a range of considerations that should be important for auditors when planning and performing risk assessments and audit procedures.

These considerations include:

1. Challenges and Recurring Deficiencies We Have Observed in Our Inspections of Auditors of Broker-Dealers

2. Recurring Deficiencies

3. Evaluating Audit Evidence

4. Understanding the Company and Its Environment

5. Use of Other Auditors

6. Going Concern
7. Critical Audit Matters (CAMs)
8. Digital Assets
9. Cybersecurity
10. Use of Data and Technology

To read more: https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/2024-priorities-spotlight.pdf?sfvrsn=7c595fae_2

EU banks' liquidity coverage ratio declined but remains well above the minimum requirement

eba European Banking Authority

The European Banking Authority (EBA) published its report on liquidity measures, which monitors and evaluates the liquidity coverage requirements currently in place in the EU.

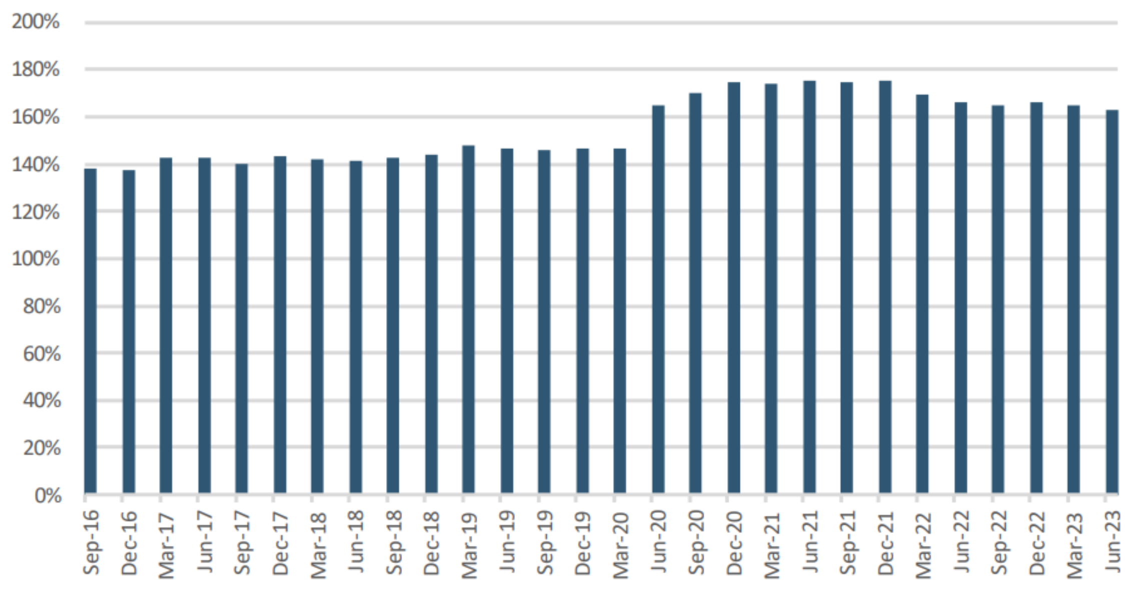
Between June 2022 and June 2023, the EU banks' liquidity coverage ratio (LCR) declined but remained comfortably above the minimum requirement.

However, within this review period there were important fluctuations in the components of the ratio, driven mostly by changes in the banks' allocation of funding deposits and the ongoing reduction of central bank liquidity.

Unlike the LCR in domestic currency, EU banks' LCR in foreign currencies remained below 100%.

EU banks' LCR buffers remain meaningfully higher than the minimum requirement. However, during the review period from June 2022 to June 2023, EU banks' LCR showed a decline of 3 percentage points and ended up at a level of 163%, as of June 2023.

Figure 1: LCR evolution (weighted average)



Source: Supervisory reporting and EBA calculations.

This relatively moderate decline on a year-on-year basis masks some important developments in the underlying components of the ratio.

In the fall of 2022, there was a marked decline in the net outflows (the denominator of the LCR) that was only partly offset by a decline in High-Quality Liquid Assets (HQLAs), the nominator of the LCR.

This decline in net outflows is mostly explained by banks shifting retail deposits to categories that are exempted from the calculation of the outflows, while the decline in HQLAs mostly reflected the gradual reduction in excess liquidity by several EU central banks.

In the first half of 2023 the HQLAs continued to decline with a temporary acceleration in March following the turmoil in the global banking markets, while the net outflows remained stable.

Within the sample of institutions, large banks saw their LCR declining while small and medium-sized banks increased their ratios.

The ongoing reduction of central bank liquidity has a negative impact on EU banks' LCRs. In addition to the impact that resulted from the gradual unwinding of the asset purchase programmes by the ECB and the Swedish Riksbank, banks in the euro area repaid EUR 337bn of the targeted longer-term refinancing operations (TLTRO) loans in June 2023.

These repayments resulted in a drop in the LCR by -3.55 percentage points for the affected banks on average.

The decline in liquid assets for banks with TLTRO funds was two times higher than for the banks with no such liabilities. At the end of June 2023, euro area banks reported EUR 438bn of remaining TLTRO balances.

As has been the case in previous years, EU banks continue to hold lower liquidity buffers in foreign currencies.

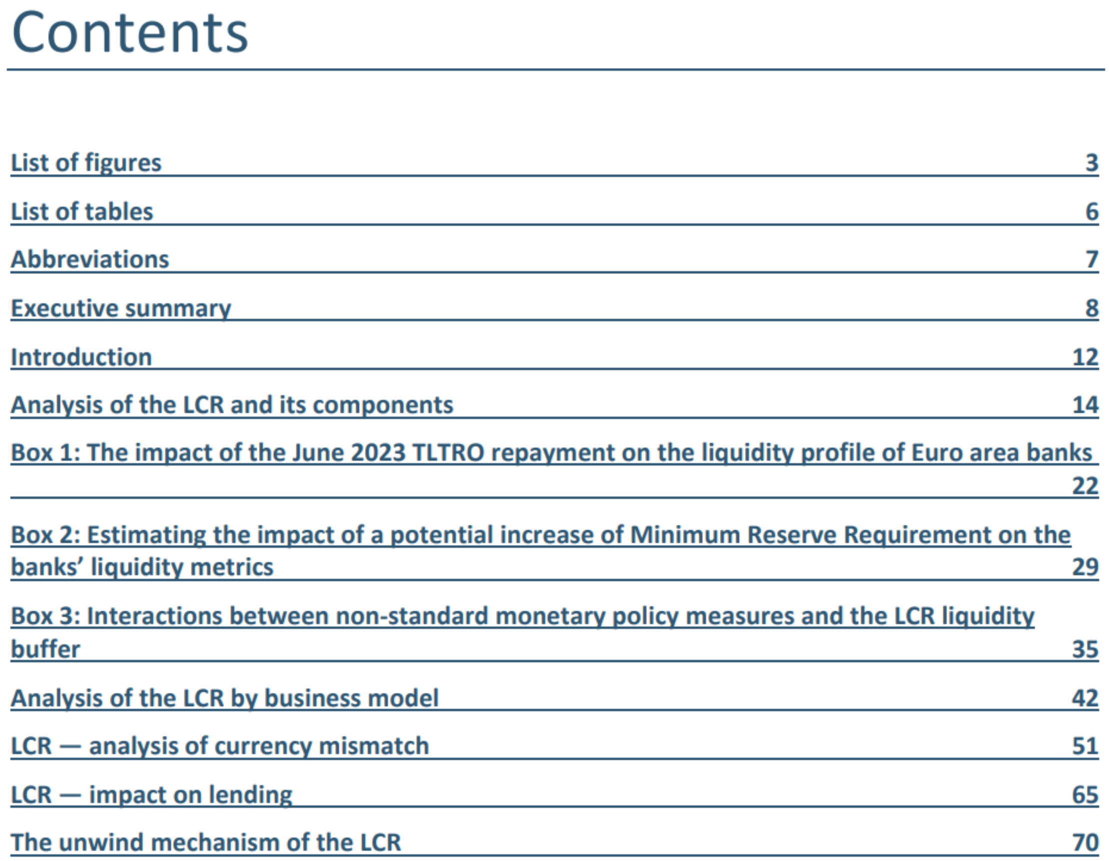
The LCR in US dollar slightly improved during the period of review from June 2022 to June 2023 but remained below 100%. Over the same period the LCR in GBP deteriorated.

The ability of banks to access the market for currency swaps may become constrained during periods of stress.

This was also evidenced by the widening of the cross-currency basis swaps during the March 2023 turmoil in the global banking markets.

Banks and competent authorities need to pay attention to any unjustified shortfalls in foreign currency LCRs to avoid risks crystallising in volatile market conditions.

Finally, the present Report also contains an assessment of the impact of the LCR on the banks' lending activities. It also includes detailed analysis of the effect of the ongoing reduction of central bank liquidity on the LCR.



Contents

To read more: https://www.eba.europa.eu/publications-and-media/press-releases/eu-banks-liquidity-coverage-ratio-declined-remains-well-above

https://www.eba.europa.eu/sites/default/files/2023-12/82ad9abc-826d-478e-bd80-29813f6ed94a/Report%20on%20Liquidity%20Measures%20under%20Article%20509%281%29%20of%20the%20CRR.pdf

ESMA presents methodology for climate risk stress testing and analysis of the financial impact of greenwashing controversies

The European Securities and Markets Authority (ESMA), the EU’s financial markets regulator and supervisor, published two articles, one outlining an approach to modelling the impact of asset price shocks from adverse scenarios involving climate-related risks, the other exploring the use of ESG controversies for the purpose of monitoring greenwashing risk.

Risk article: Dynamic modelling of climate-related shocks in the fund sector

The article presents a methodological approach to modelling climate-related shocks in the fund sector, which includes dynamic impacts, such as inflows and outflows from investors and portfolio rebalancing by managers. The analysis focuses on the overall direction of these effects, finding that investor outflows can worsen falls in fund values following an initial shock.

ESMA European Securities and Markets Authority

19 December 2023
ESMA50-524821-3073

ESMA TRV Risk Analysis Sustainable Finance

Dynamic modelling of climate-related shocks in the fund sector

The article: https://www.esma.europa.eu/sites/default/files/2023-12/ESMA50-524821-3073_TRV_Article_Dynamic_modelling_climate_shocks_fund_sector.pdf

Dynamic modelling of climate-related shocks in the fund sector is part of ESMA’s work in relation to its mandates in the area of climate stress testing.

To anticipate the impact of climate-related shocks on the financial system, the European Commission has mandated the ESAs to perform regular climate change stress tests or scenario analyses and to develop methods, parameters and scenarios for supervisors to use in their own climate stress testing.

In addition, the ESAs have a mandate to conduct a coordinated one-off climate change stress test across the financial sector in coordination with the European Central Bank (ECB) and the European Systemic Risk Board (ESRB), reporting results by 1Q25.

Risk article: Financial impact of greenwashing controversies

The article highlights how data on ESG controversies can be useful to monitor potential reputational risks around greenwashing. It also outlines the challenges involved in using such data. The number of greenwashing controversies involving large European firms increased between 2020 and 2021 and tended to be concentrated within a few firms belonging to three main sectors, including the financial sector. Growing public scrutiny highlights the importance of clear policy guidance by regulators and efforts by supervisors to ensure the credibility of sustainability-related claims.

You may visit: https://www.esma.europa.eu/sites/default/files/2023-12/ESMA50-524821-3072_TRV_Article_The_financial_impact_of_greenwashing_controversies.pdf

The analysis on the financial impact of greenwashing controversies is important since the transition to a low-carbon economy requires trust in the commitment and ability of corporates companies to adapt their business operations to help deliver climate-related objectives. However, greenwashing risks undermine this trust by sapping consumer and investor confidence, underlining the importance of monitoring and tackling the problem.

To read more: https://www.esma.europa.eu/press-news/esma-news/esma-presents-methodology-climate-risk-stress-testing-and-analysis-financial

BIS Working Papers, No 1158 - Financial development and the effectiveness of macroprudential and capital flow management measures, Monetary and Economic Department, January 2024

Yusuf Soner Başkaya, Ilhyock Shim, Philip Turner

After the Global Financial Crisis (GFC) in 2007–09, a large number of central banks and financial regulators in both advanced economies (AEs) and emerging market economies (EMEs) acknowledged the importance of macroprudential policy (MaPP) in securing both domestic financial stability and external stability.

In particular, the role of the macroprudential policy has been characterised as increasing the financial system's resilience by identifying the sources of systemic risk and taking appropriate policy actions. In addition, many central banks and other financial authorities in EMEs paid attention to capital flow management measures (CFMs) to mitigate the adverse effects of excessive capital flow or exchange rate volatility and secure external stability, as recognised at the G20 meeting of Finance Ministers and Central Bank Governors held in October 2010. Since then, significant progress has been made in designing and implementing MaPP by both AEs and EMEs.

Some EMEs continued to use various types of CFM to reduce the volatility of capital flows or exchange rates.

The increased use of MaPP measures and CFMs since the GFC naturally brought in the question of whether such policy measures were effective in taming excessive growth in credit, asset prices and capital inflows. However, we think that there are still important gaps in research on this question for several reasons.

First, many countries implement MaPP measures, in addition to CFMs, which aim at taming excessive capital flows as well as at excessive growth in credit and asset prices.

In contrast, the general approach in the literature is to estimate the effectiveness of MaPP measures on financial stability-related outcomes such as credit growth and asset prices without considering the potential effects of CFMs.

This, however, potentially generates omitted variable bias for the effects of MaPP measures. Second, despite the acknowledgement of the potential implications of excessive capital flows for financial instability and the potential use of MaPP to mitigate such financial instability risks, the number of studies assessing the effectiveness of MaPP measures is limited.

More importantly, such studies usually do not account for different types of CFM, which potentially provides a limited view on the potential effects of such policies. In this paper, using a very detailed cross-country dataset on MaPP measures and

CFMs at quarterly frequency, we analyse the effectiveness of such policies on capital inflows and the volume of credit.

In particular, we consider how domestic credit variables (such as total credit to the private non-financial sector, domestic bank credit, total corporate credit, household loans, housing loans and consumer loans) and capital flow variables (such as cross-border bank inflows, bond inflows and offshore issuance of debt securities) respond to MaPP measures and CFMs.

This contrasts with the general practice in the literature which focuses on the policy impact on either the dynamics of domestic credit or those of capital flows.

Our approach differs from the rest of the literature in that our empirical model simultaneously accounts for the effect of MaPP measures and CFMs on credit dynamics and capital inflows, which is guided by the policy practice, especially in many EMEs.

In particular, there are the following few merits of identifying the effect of MaPP measures and CFMs on credit growth and capital flows in model that controls for both types of policies.

First, both MaPP measures and CFMs affect total credit, defined as the sum of credit extended by domestic financial intermediaries in the form of loans and bonds and cross-border borrowing also in the form of loans and debt securities, as well as the domestic financial conditions of an economy, often measured by the cost of credit such as loan rates or long-term bond yields.

To read more: https://www.bis.org/publ/work1158.pdf

NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI Systems

1. AI systems can malfunction when exposed to untrustworthy data, and attackers are exploiting this issue.

2. New guidance documents the types of these attacks, along with mitigation approaches.

3. No foolproof method exists as yet for protecting AI from misdirection, and AI developers and users should be wary of any who claim otherwise.

Adversaries can deliberately confuse or even "poison" artificial intelligence (AI) systems to make them malfunction — and there's no foolproof defense that their developers can employ. Computer scientists from the National Institute of Standards and Technology (NIST) and their collaborators identify these and other vulnerabilities of AI and machine learning (ML) in a new publication.

Their work, titled Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations (NIST.AI.100-2), is part of NIST's broader effort to support the development of trustworthy AI, and it can help put NIST's AI Risk Management Framework into practice. The publication, a collaboration among government, academia and industry, is intended to help AI developers and users get a handle on the types of attacks they might expect along with approaches to mitigate them — with the understanding that there is no silver bullet.

"We are providing an overview of attack techniques and methodologies that consider all types of AI systems," said NIST computer scientist Apostol Vassilev, one of the publication's authors. "We also describe current mitigation strategies reported in the literature, but these available defenses currently lack robust assurances that they fully mitigate the risks. We are encouraging the community to come up with better defenses."

AI systems have permeated modern society, working in capacities ranging from driving vehicles to helping doctors diagnose illnesses to interacting with customers as online chatbots. To learn to perform these tasks, they are trained on vast quantities of data: An autonomous vehicle might be shown images of highways and streets with road signs, for example, while a chatbot based on a large language model (LLM) might be exposed to records of online conversations. This data helps the AI predict how to respond in a given situation.

One major issue is that the data itself may not be trustworthy. Its sources may be websites and interactions with the public. There are many opportunities for bad actors to corrupt this data — both during an AI system's training period and afterward, while the AI continues to refine its behaviors by interacting with the physical world. This can cause the AI to perform in an undesirable manner. Chatbots, for example, might learn to respond with abusive or racist language when their guardrails get circumvented by carefully crafted malicious prompts.

"For the most part, software developers need more people to use their product so it can get better with exposure," Vassilev said. "But there is no guarantee the exposure will be good. A chatbot can spew out bad or toxic information when prompted with carefully designed language."

In part because the datasets used to train an AI are far too large for people to successfully monitor and filter, there is no foolproof way as yet to protect AI from misdirection. To assist the developer community, the new report offers an overview of the sorts of attacks its AI products might suffer and corresponding approaches to reduce the damage.

The report considers the four major types of attacks: evasion, poisoning, privacy and abuse attacks. It also classifies them according to multiple criteria such as the attacker's goals and objectives, capabilities, and knowledge.

Evasion attacks, which occur after an AI system is deployed, attempt to alter an input to change how the system responds to it. Examples would include adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs or creating confusing lane markings to make the vehicle veer off the road.

Poisoning attacks occur in the training phase by introducing corrupted data. An example would be slipping numerous instances of inappropriate language into conversation records, so that a chatbot interprets these instances as common enough parlance to use in its own customer interactions.

Privacy attacks, which occur during deployment, are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. An adversary can ask a chatbot numerous legitimate questions, and then use the answers to reverse engineer the model so as to find its weak spots — or guess at its sources. Adding undesired examples to those online sources could make the AI behave inappropriately, and making the AI unlearn those specific undesired examples after the fact can be difficult.

Abuse attacks involve the insertion of incorrect information into a source, such as a webpage or online document, that an AI then absorbs. Unlike the aforementioned poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

"Most of these attacks are fairly easy to mount and require minimum knowledge of the AI system and limited adversarial capabilities," said co-author Alina Oprea, a professor at Northeastern University. "Poisoning attacks, for example, can be mounted by controlling a few dozen training samples, which would be a very small percentage of the entire training set."

The authors — who also included Robust Intelligence Inc. researchers Alie Fordyce and Hyrum Anderson — break down each of these classes of attacks into subcategories and add approaches for mitigating them, though the publication acknowledges that the defenses AI experts have devised for adversarial attacks thus far are incomplete at best. Awareness of these limitations is important for developers and organizations looking to deploy and use AI technology, Vassilev said.

“Despite the significant progress AI and machine learning have made, these technologies are vulnerable to attacks that can cause spectacular failures with dire consequences,” he said. “There are theoretical problems with securing AI algorithms that simply haven’t been solved yet. If anyone says differently, they are selling snake oil.”

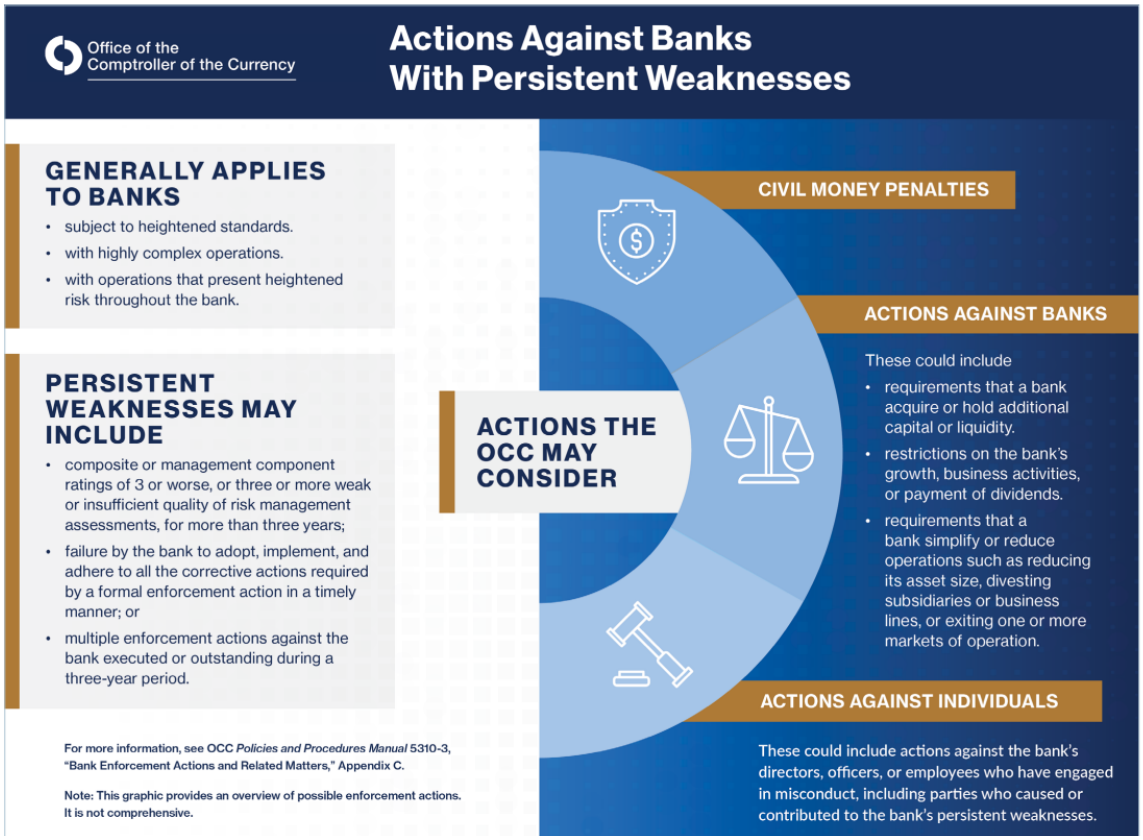
To read more: https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

Annual Report

Office of the Comptroller of the Currency

The OCC Annual Report provides Congress with an overview of the condition of the federal banking system. The annual report discusses the OCC's strategic priorities and details agency regulatory and policy initiatives. Additionally, the report discusses the agency's financial management and condition, including its audited financial statements.

To read more: https://www.ots.treas.gov/publications-and-resources/publications/annual-report/files/2023-annual-report.html



Office of the Comptroller of the Currency

Actions Against Banks With Persistent Weaknesses

GENERALLY APPLIES TO BANKS

- subject to heightened standards.
- with highly complex operations.
- with operations that present heightened risk throughout the bank.

PERSISTENT WEAKNESSES MAY INCLUDE

- composite or management component ratings of 3 or worse, or three or more weak or insufficient quality of risk management assessments, for more than three years;
- failure by the bank to adopt, implement, and adhere to all the corrective actions required by a formal enforcement action in a timely manner; or
- multiple enforcement actions against the bank executed or outstanding during a three-year period.

ACTIONS THE OCC MAY CONSIDER

CIVIL MONEY PENALTIES

ACTIONS AGAINST BANKS

These could include

- requirements that a bank acquire or hold additional capital or liquidity.
- restrictions on the bank's growth, business activities, or payment of dividends.
- requirements that a bank simplify or reduce operations such as reducing its asset size, divesting subsidiaries or business lines, or exiting one or more markets of operation.

ACTIONS AGAINST INDIVIDUALS

These could include actions against the bank's directors, officers, or employees who have engaged in misconduct, including parties who caused or contributed to the bank's persistent weaknesses.

For more information, see OCC *Policies and Procedures Manual* 5310-3, "Bank Enforcement Actions and Related Matters," Appendix C.

Note: This graphic provides an overview of possible enforcement actions. It is not comprehensive.

Statement on the Approval of Spot Bitcoin Exchange-Traded Products

Gary Gensler, Chair of the U.S. Securities and Exchange Commission

Today, the Commission approved the listing and trading of a number of spot bitcoin exchange-traded product (ETP) shares.

I have often said that the Commission acts within the law and how the courts interpret the law. Beginning under Chair Jay Clayton in 2018 and through March 2023, the Commission disapproved more than 20 exchange rule filings for spot bitcoin ETPs. One of those filings, made by Grayscale, contemplated the conversion of the Grayscale Bitcoin Trust into an ETP.

We are now faced with a new set of filings similar to those we have disapproved in the past. Circumstances, however, have changed. The U.S. Court of Appeals for the District of Columbia held that the Commission failed to adequately explain its reasoning in disapproving the listing and trading of Grayscale's proposed ETP (the Grayscale Order).

The court therefore vacated the Grayscale Order and remanded the matter to the Commission. Based on these circumstances and those discussed more fully in the approval order, I feel the most sustainable path forward is to approve the listing and trading of these spot bitcoin ETP shares.

The Commission evaluates any rule filing by a national securities exchange based upon whether it is consistent with the Exchange Act and regulations thereunder, including whether it is designed to protect investors and the public interest.

The Commission is merit neutral and does not take a view on particular companies, investments, or the assets underlying an ETP.

If the issuer of a security and the listing exchange comply with the Securities Act, the Exchange Act, and the Commission's rules, that issuer must be provided the same access to our regulated markets as anyone else.

Importantly, today's Commission action is cabined to ETPs holding one non-security commodity, bitcoin.

It should in no way signal the Commission's willingness to approve listing standards for crypto asset securities. Nor does the approval signal anything about the Commission's views as to the status of other crypto assets under the federal securities laws or about the current state of non-compliance of certain crypto asset market participants with the federal securities laws. As I've said in the past, and without prejudging any one crypto asset, the vast majority of crypto assets are investment contracts and thus subject to the federal securities laws.

Investors today can already buy and sell or otherwise gain exposure to bitcoin at a number of brokerage houses, through mutual funds, on national securities exchanges, through peer-to peer payment apps, on non-compliant crypto trading platforms, and, of course, through the Grayscale Bitcoin Trust. Today's action will include certain protections for investors:

First, sponsors of bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products. Investors in any bitcoin ETP that is listed and traded will benefit from the disclosure included in public registration statements and required periodic filings.

While these disclosures are required, it is important to note that today's action does not endorse the disclosed ETP arrangements, such as custody arrangements.

Second, these products will be listed and traded on registered national securities exchanges. Such regulated exchanges are required to have rules designed to prevent fraud and manipulation, and we will monitor them closely to ensure that they are enforcing those rules.

Furthermore, the Commission will fully investigate any fraud or manipulation in the securities markets, including schemes that use social media platforms.

Such regulated exchanges also have rules designed to address certain conflicts of interest as well as to protect investors and the public interest.

Further, existing rules and standards of conduct will apply to the purchase and sale of the approved ETPs. This includes, for example, Regulation Best Interest when broker-dealers recommend ETPs to retail investors, as well as a fiduciary duty under the Investment Advisers Act for investment advisers.

Today's action does not approve or endorse crypto trading platforms or intermediaries, which, for the most part, are non-compliant with the federal securities laws and often have conflicts of interest.

Third, Commission staff is separately completing the review of registration statements for 10 spot bitcoin ETPs simultaneously, which will help create a level playing field for issuers and promote fairness and competition, benefiting investors and the broader market.

Since 2004, this agency has had experience overseeing spot non-security commodity ETPs, such as those holding certain precious metals. That experience will be valuable in our oversight of spot bitcoin ETP trading.

Though we're merit neutral, I'd note that the underlying assets in the metals ETPs have consumer and industrial uses, while in contrast bitcoin is primarily a speculative, volatile asset that's also used for illicit activity including ransomware, money laundering, sanction evasion, and terrorist financing.

While we approved the listing and trading of certain spot bitcoin ETP shares today, we did not approve or endorse bitcoin. Investors should remain cautious about the myriad risks associated with bitcoin and products whose value is tied to crypto.

To read more: https://www.sec.gov/news/statement/gensler-statement-spot-bitcoin-011023

NIST SP 800-55 Vol. 1 (Initial Public Draft)
Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures

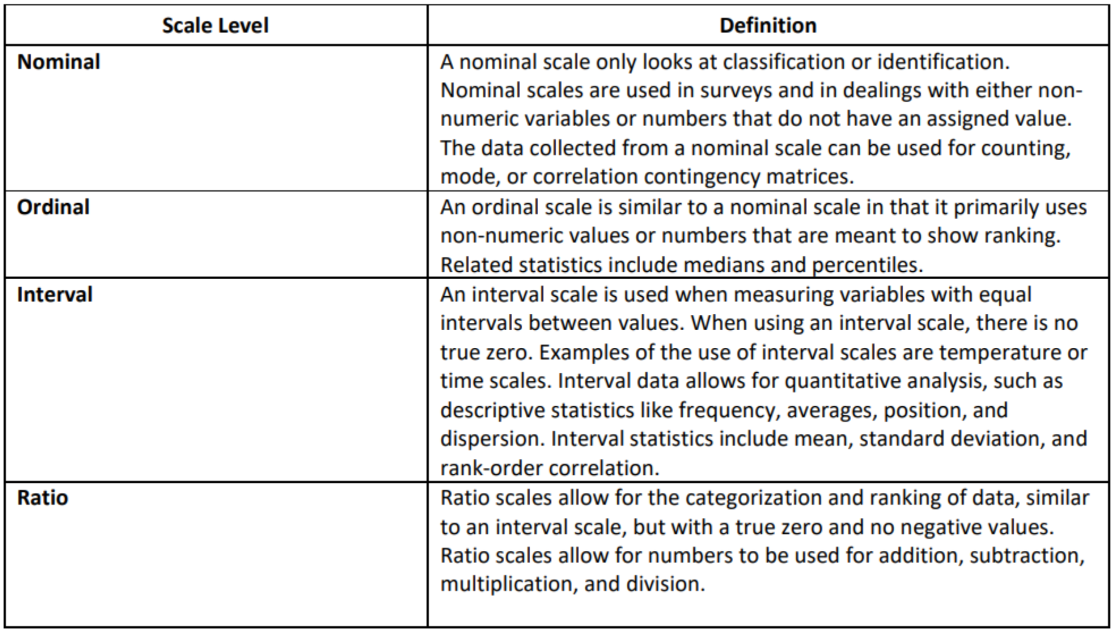
The initial public drafts of NIST Special Publication (SP) 800-55, Measurement Guide for Information Security, Volume 1 – Identifying and Selecting Measures and Volume 2 – Developing an Information Security Measurement Program are available for comment after extensive research, development, and customer engagement.

In response to the feedback from the pre-draft call for comment and initial working draft (annotated outline), NIST continued to refine the publications by organizing the guidance into two volumes and developing more actionable and focused guidance in each.

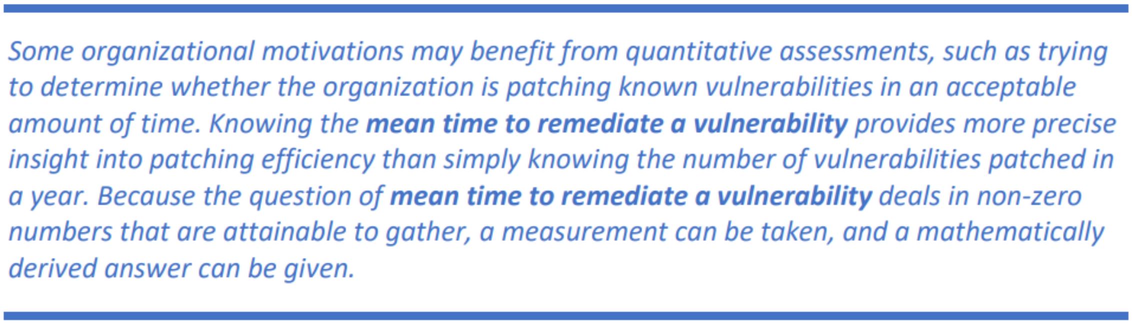
Volume 1 – Identifying and Selecting Measures is a flexible approach to the development, selection, and prioritization of information security measures. This volume explores both quantitative and qualitative assessment and provides basic guidance on data analysis techniques as well as impact and likelihood modeling.

Volume 2 — Developing an Information Security Measurement Program is a methodology for developing and implementing a structure for an information security measurement program.

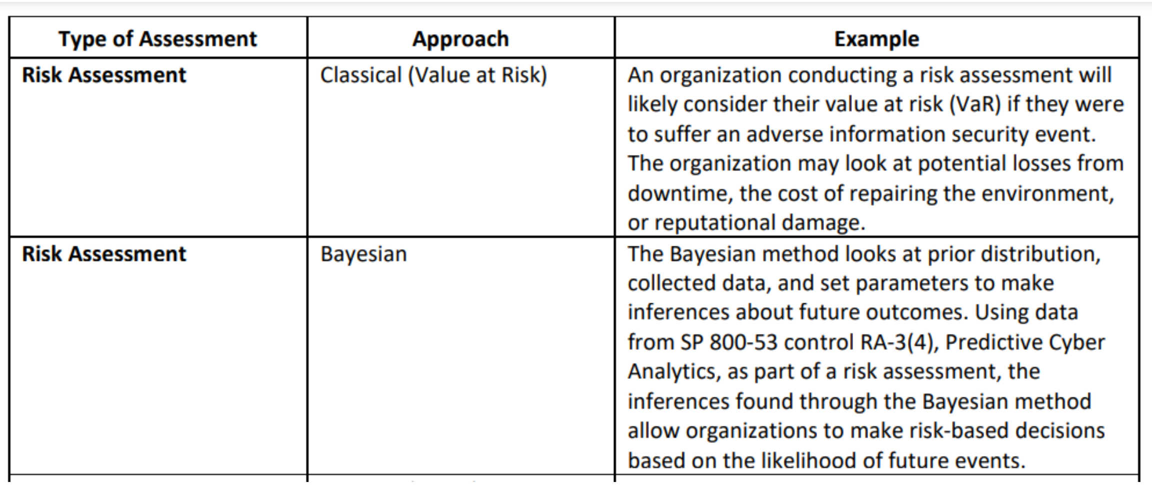
Table 1. Stevens Scale of Measurement



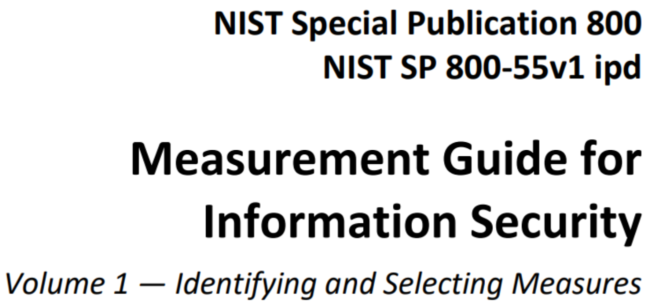
Scale Level	Definition
Nominal	A nominal scale only looks at classification or identification. Nominal scales are used in surveys and in dealings with either non-numeric variables or numbers that do not have an assigned value. The data collected from a nominal scale can be used for counting, mode, or correlation contingency matrices.
Ordinal	An ordinal scale is similar to a nominal scale in that it primarily uses non-numeric values or numbers that are meant to show ranking. Related statistics include medians and percentiles.
Interval	An interval scale is used when measuring variables with equal intervals between values. When using an interval scale, there is no true zero. Examples of the use of interval scales are temperature or time scales. Interval data allows for quantitative analysis, such as descriptive statistics like frequency, averages, position, and dispersion. Interval statistics include mean, standard deviation, and rank-order correlation.
Ratio	Ratio scales allow for the categorization and ranking of data, similar to an interval scale, but with a true zero and no negative values. Ratio scales allow for numbers to be used for addition, subtraction, multiplication, and division.



*Some organizational motivations may benefit from quantitative assessments, such as trying to determine whether the organization is patching known vulnerabilities in an acceptable amount of time. Knowing the **mean time to remediate a vulnerability** provides more precise insight into patching efficiency than simply knowing the number of vulnerabilities patched in a year. Because the question of **mean time to remediate a vulnerability** deals in non-zero numbers that are attainable to gather, a measurement can be taken, and a mathematically derived answer can be given.*



Type of Assessment	Approach	Example
Risk Assessment	Classical (Value at Risk)	An organization conducting a risk assessment will likely consider their value at risk (VaR) if they were to suffer an adverse information security event. The organization may look at potential losses from downtime, the cost of repairing the environment, or reputational damage.
Risk Assessment	Bayesian	The Bayesian method looks at prior distribution, collected data, and set parameters to make inferences about future outcomes. Using data from SP 800-53 control RA-3(4), Predictive Cyber Analytics, as part of a risk assessment, the inferences found through the Bayesian method allow organizations to make risk-based decisions based on the likelihood of future events.



NIST Special Publication 800
NIST SP 800-55v1 ipd

Measurement Guide for Information Security

Volume 1 — Identifying and Selecting Measures

To read more: https://csrc.nist.gov/pubs/sp/800/55/v1/ipd

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