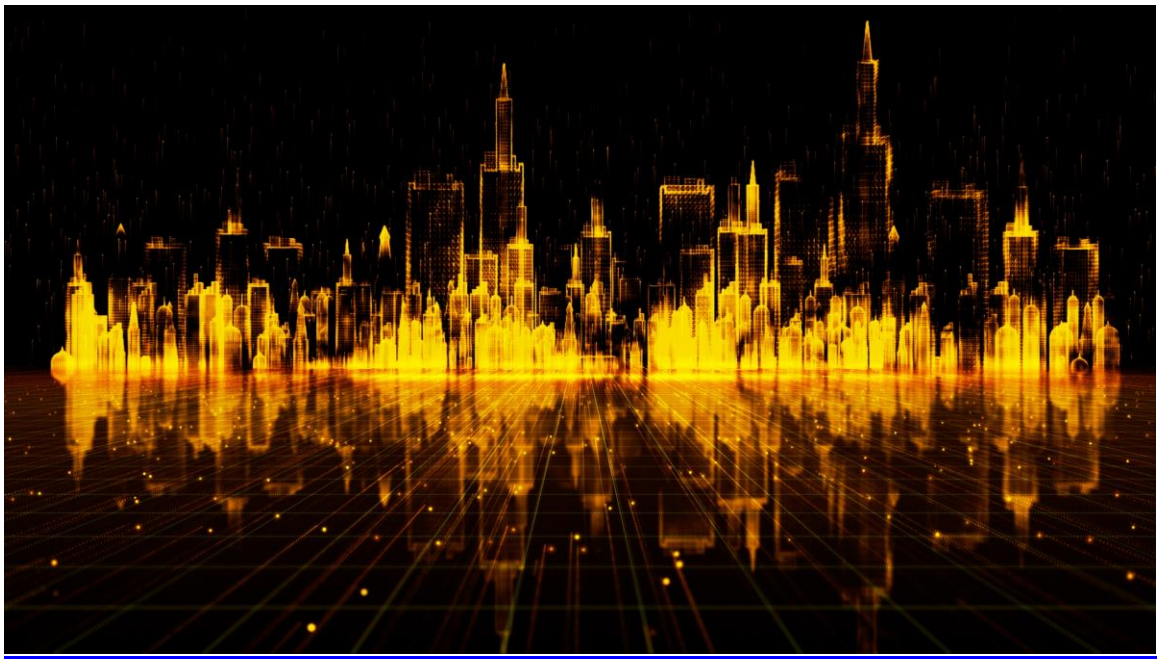
Basel iii Compliance Professionals Association (BiiiCPA)
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.basel-iii-association.com



Basel iii News, February 2022

Dear members and friends,

Neil Esho is the new Secretary General of the Basel Committee on Banking Supervision. His term starts in February 2022 for three years. Mr Esho previously served as Deputy Secretary General of the Basel Committee.

He succeeds Carolyn Rogers, who had served as Secretary General since 2019, and left the Committee in November to become Senior Deputy Governor of the Bank of Canada.

I am delighted to announce Neil's appointment as Secretary General. His extensive supervisory and regulatory background, and the instrumental role he has played in supporting the development of standards such as the Basel III framework, place him in an ideal position to lead the Secretariat in the next phase of the Committee's work as it focuses on implementation as well as on new challenges around cryptocurrencies, climate-related financial risks and the accelerating digitalisation of finance.

I would also like to once again thank Carolyn Rogers for her dynamic leadership, particularly her able steering of the Basel Committee through the Covid-19 pandemic and its many challenges. She has put it on a sound footing to face the changing international banking landscape.

Pablo Hernández de Cos, Chair of the Basel Committee and Governor of the Bank of Spain

Mr Esho has been Deputy Secretary General since July 2014. He joined the Basel Committee Secretariat in April 2006. Prior to that, he was Head of Research at the Australian Prudential Regulation Authority (APRA).

Before joining APRA in 2001, he was a Senior Lecturer at the School of Banking and Finance at the University of New South Wales.

He holds a PhD in finance from the University of New South Wales.

Neil's deep understanding of the Basel Committee's work and the key role he has played in implementing its agenda over the past 15 years will be invaluable as he takes the lead of the Secretariat at this crucial time.

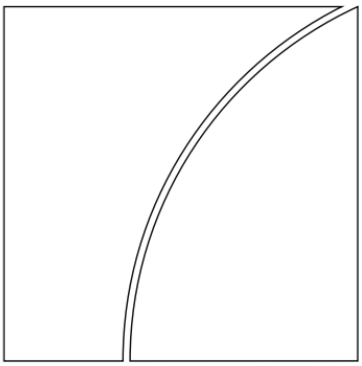
I would also like to express my appreciation for the efforts of his predecessor, Carolyn Rogers, for so strongly setting out the case for the full, consistent and timely implementation of the Basel III standards, and look forward to further progress with Neil's support.

François Villeroy de Galhau, Chairman of the Basel Committee's oversight body, the Group of Central Bank Governors and Heads of Supervision (GHOS), and Governor of the Bank of France

BIS Working Papers No 1000

Dollar beta and stock returns

Valentina Bruno, Ilhyock Shim and Hyun Song Shin - Monetary and Economic Department



BIS Working Papers

No 1000

Dollar beta and stock returns

by Valentina Bruno, Ilhyock Shim and Hyun Song Shin

Monetary and Economic Department

February 2022

Abstract

The financial channel of exchange rates operates through changes in risk-taking by investors and is reflected in the response of financial conditions to exchange rate movements.

We show that stock returns also reflect the financial channel of exchange rates, with higher local currency stock returns associated with a weaker dollar.

The broad dollar index emerges as a global factor, consistent with the financial channel operating through swings in risk-taking by global investors.

We introduce the *dollar beta* as the sensitivity of stock returns to swings in the broad dollar index, and show that emerging market stock indices that have a higher dollar beta tend to have higher average returns, implying that the dollar beta is a cross-section risk factor that is priced.

Introduction

Exchange rates affect the economy through both real and financial channels. Deeper global integration of banking and capital market activity has meant that the financial channel of exchange rates has taken on an increasingly important role in recent decades.

The financial channel of exchange rates operates through changes in the risk capacity of market participants and is reflected in the response of financial conditions to exchange rate movements.

There is an active and accumulating series of studies (to be reviewed below) that show how capital flows and market conditions fluctuate with swings in exchange rates, where an appreciating local currency is associated with more accommodative local financial conditions.

To read more: https://www.bis.org/publ/work1000.pdf

Federal Reserve Board invites public comment on proposed guidance to implement a framework for the supervision of certain insurance organizations overseen by the Board

The Federal Reserve Board invited public comment on proposed guidance to implement a framework for the supervision of certain **insurance** organizations overseen by the Board.

The proposed supervisory framework—for depository institution holding companies significantly engaged in insurance activities—would apply guidance and allocate supervisory resources based on the risk of a firm.

It would also formalize a supervisory rating system for these companies and describe how examiners work with state insurance regulators.

The proposed guidance would apply to any depository institution holding company that is an insurance underwriting company or that has over 25 percent of its consolidated assets held by insurance underwriting subsidiaries.

Comments will be accepted for 60 days after publication in the Federal Register.

Summary

The Board is seeking comment on a new supervisory framework for depository institution holding companies significantly engaged in insurance activities, or supervised insurance organizations.

The proposed framework would provide a supervisory approach that is designed specifically to reflect the differences between banking and insurance.

Within the framework, the application of supervisory guidance and the assignment of supervisory resources would be based explicitly on a supervised insurance organization's complexity and individual risk profile.

The proposed framework would formalize the ratings applicable to these firms with rating definitions that reflect specific supervisory requirements and expectations.

It would also emphasize the Board's policy to rely to the fullest extent possible on work done by other relevant supervisors, describing, in particular, the way it will rely more fully on reports and other supervisory information provided by state insurance regulators to minimize the burden associated with supervisory duplication.

To read more:
https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220128a.htm

https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20220128a2.pdf

Data Protection Engineering

The evolution of technology has brought forward new techniques to share, process and store data. This has generated new models of data (including personal data) processing, but also introduced new threats and challenges.

Some of the evolving privacy and data protection challenges associated with emerging technologies and applications include: lack of control and transparency, possible reusability of data, data inference and re-identification, profiling and automated decision making.

The implementation of the GDPR data protection principles in such contexts is challenging as they cannot be implemented in the traditional, “intuitive” way.

Processing operations must be rethought, sometimes radically (similar to how radical the threats are), possibly with the definition of new actors and responsibilities, and with a prominent role for technology as an element of guarantee.

Safeguards must be integrated into the processing with technical and organisational measures.

From the technical side, the challenge is to translate these principles into tangible requirements and specifications by requirements by selecting, implementing and configuring appropriate technical and organizational measures and techniques.

Data Protection Engineering can be perceived as part of data protection by Design and by Default. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles.

Undeniably it depends on the measure, the context and the application and eventually it contributes to the protection of data subjects’ rights and freedoms.

The current report took a broader look into data protection engineering with a view to support practitioners and organizations with practical implementation of technical aspects of data protection by design and by default.

Towards this direction this report presents existing (security) technologies and techniques and discusses possible strengths and applicability in relation to meeting data protection principles as set out in Article 5 GDPR.

Based on the analysis provided in the report, the following conclusions and recommendations for relevant stakeholders are provided below:

1. Regulators (e.g. Data Protection Authorities and the European Data Protection Board) should discuss and promote good practices across the EU in relation to state-of-the-art solutions of relevant technologies and techniques. EU Institutions could promote such good practices by relevant publicly available documents.

2. The research community should continue exploring the deployment of (security) techniques and technologies that can support the practical implementation of data protection principles, with the support of the EU institutions in terms of policy guidance and research funding.

3. Regulators (e.g. Data Protection Authorities and the European Data Protection Board) and the European Commission should promote the establishment of relevant certification schemes, under Article 42 GDPR, to ensure proper engineering of data protection.

To read more:
https://www.enisa.europa.eu/publications/data-protection-engineering

Statement on Pay versus Performance

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

The Commission is reopening the comment period for a proposed rule for corporate disclosure of "pay versus performance." I support this proposed rule because, if adopted, it would strengthen the transparency and quality of executive compensation disclosure.

The rule proposal would fulfill a mandate from Congress under the Dodd-Frank Act of 2010, passed after the 2008 financial crisis.

"Pay versus performance" disclosures describe the relationship between the executive compensation an issuer actually paid and the financial performance of that issuer. Such disclosures would make it easier for shareholders to assess the company's decision-making with respect to its executive compensation policies.

The Commission has long recognized the value of information on executive compensation to investors. The first requirements to make disclosures about executive compensation originated in the 1933 Act. Since then, from time to time the Commission has continued to update compensation disclosure requirements.

In 2015, the Commission proposed rules to implement the Dodd-Frank Act's "pay versus performance" requirement. These proposed rules relied upon total shareholder return as the sole measure of financial performance. Some commenters expressed concerns that total shareholder return would provide an incomplete picture of performance.

In this reopening release, we are considering whether additional performance metrics would better reflect Congress's intention in the Dodd-Frank Act and would provide shareholders with information they need to evaluate a company's executive compensation policies.

I'm pleased to support today's reopening release and look forward to the public's feedback. I'd like to extend my gratitude to the members of the SEC staff who worked on this item, including:

- Renee Jones, Erik Gerding, Connor Raso, Lindsay McCord, Jennifer Zepralka, Anne Krauskopf, Angie Kim, and Jeb Byrne in the Division of Corporation Finance;

- Bryant Morris, Dorothy McCuaig, and Ken Alcé in the Office of the General Counsel;

- Jessica Wachter, Vlad Ivanov, Tara Bhandari, Mike Willis, Julie Marlowe, PJ Hamidi, Robert Miller, and Lauren Moore in the Division of Economic and Risk Analysis;

- Brian Johnson, Amanda Wagner, and Amy Miller in the Division of Investment Management; and

- Kristin Pauley, Marc Johnson, and Laura Metcalfe in the Division of Enforcement;

- Jonathan Wiggins, Omid Harraf, Larry Yusuf, and Mark Jacoby in the Office of Chief Accountant.

On returning inflation back to target

Catherine L. Mann, External Member of the Monetary Policy Committee, Bank of England

Introduction and summary

As an international economist, I have always studied domestic economic conditions through the lens of global influences.

This year the UK offers an excellent laboratory. Global factors have been at the forefront of the inflation surge in the UK, and their effects will persist into early 2022. However, expectations for wages and prices for this year, if realized, could keep UK inflation strong for longer, which might then generate a reinforcing cost-price dynamic.

To return inflation to target, the Monetary Policy Committee's first line of defence is to dampen expectations of future price increases. Achieving an inflection in these expectations along with tailwinds from global factors could mean that a shallower path of future rate rises is needed to bring inflation back to target.

In the last half of 2021, UK CPI inflation surged, more than doubling from 2% in July to 5.4% in December.

Previously, average earnings had rebounded strongly from their trough in 2020 leading to headline wage inflation rates as high as 9% in the summer.

While some of these increases are due to base and compositional effects, demand and supply imbalances both in goods and labour markets built very quickly over the second half of the year.

Residual strength in both wages and prices likely will continue for a time into 2022 as the domestic and global mismatch of supply and demand slowly resolve, as firms try to recover margins eroded in 2021, and as labour markets stay tight.

Indeed, firms in the latest DMP panel (from December) expect to raise their prices by 5% in 2022 – a bit more than the 4% in 2021.
Meanwhile, firms expect continued upward pressure on pay growth in 2022 on the top of the 2-3.5% increases of 2021.

These expectations for prices and wages, if realized, are ingredients for headline inflationary pressures that could stay strong for longer, well into 2023. The question for monetary policy then becomes whether the real factors on the one hand and expectations on the other could together create a reinforcing cost-price dynamic.

Certainly, there are headwinds facing these price and wage expectations. Most importantly, will domestic and global demand in 2022 be strong enough for firms to pass through wage and cost increases into their prices? In the end, it is the collective outturns of business pricing that translates into inflation.

Monetary policy has a role to play in managing expectations as well as ensuring that the economic and financial conditions facing firms and workers are consistent with the 2% target.

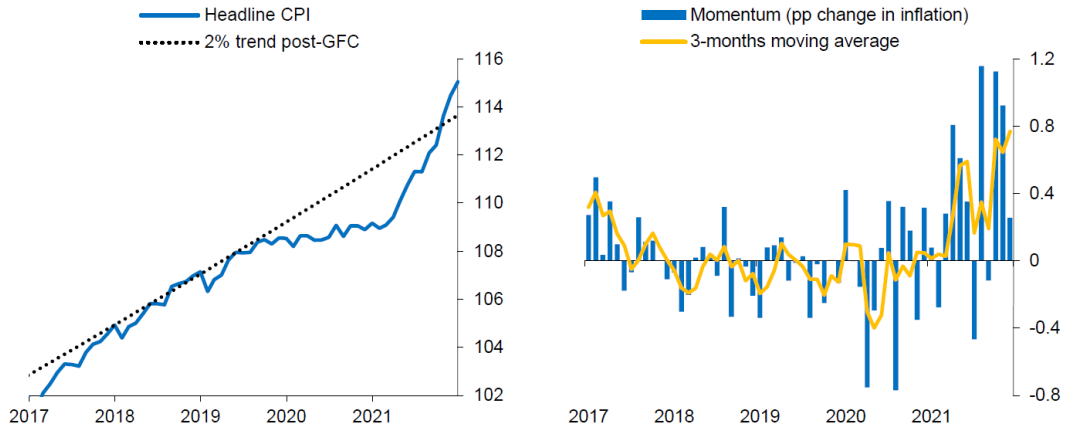
Initial conditions and the 2021 surge

Before we can assess the prospects for returning inflation to the 2% target, we need to recall initial conditions and review sources of the 2021 inflation surge.

Going into the pandemic, the UK CPI price level was roughly trending along its 2% inflation path, unlike in the US or the euro area which had seen persistently lower inflation than intended.

In the first year of the pandemic with lockdowns disrupting a wide range of activities, some firms did cut prices in the UK (and some markets simply did not exist, so there were no prices at all) and the aggregate price level flat-lined.

Chart 1: CPI level (index, LHS) and momentum (percentage points, RHS)

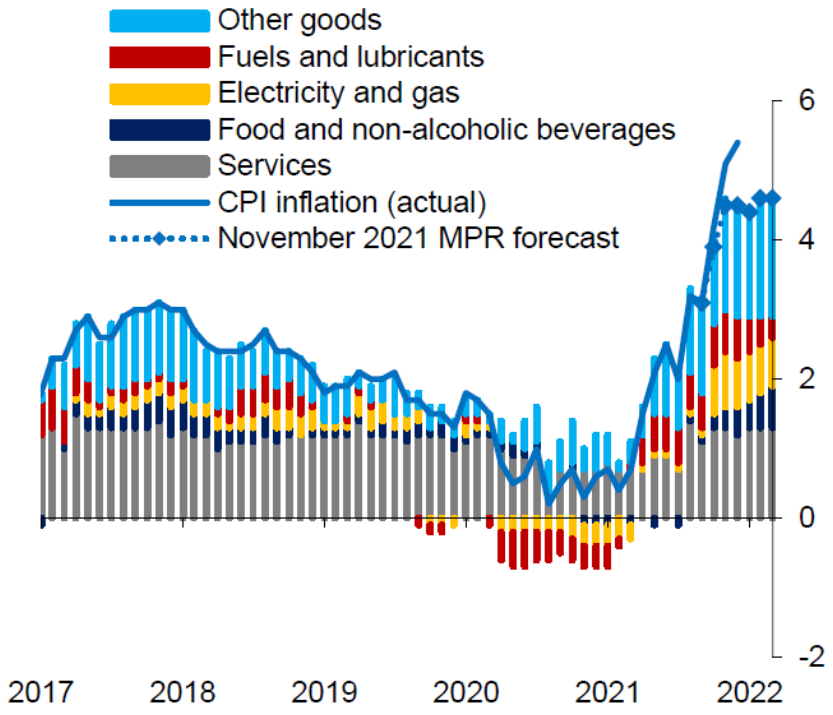


Sources: ONS and Bank calculations. Notes: Trend on LHS shows the level of prices if CPI had grown at 2% annualised rates in every month since December 2010. RHS shows momentum of CPI, i.e. the month-to-month percentage point change of year-on-year inflation. Thus, positive momentum means rising inflation (accelerating prices) and negative momentum falling inflation (decelerating prices). Latest observation: December 2021.

Both demand recovery and supply limitations in 2021 have now yielded robust inflation momentum, which if price expectations are realized, is poised to continue into 2022 moving the price level further away from the 2% trend. (Chart 1).

Reviewing key sources of the 2021 inflation surge – energy and core goods – both are importantly driven by sources external to the UK economy. (Chart 2).

Chart 2: Decomposition of CPI inflation in the November 2021 MPR forecast (% year-on-year)



Source: November 2021 Monetary Policy Report. Latest observation: December 2021 (actual), March 2022 (forecast).

Global goods prices have been elevated by the rotation away from consumer-facing services towards goods purchases.

The dominant driver of global goods price dynamics is the interplay of three successive US fiscal stimuli combined with geographical mismatches of containers and production stoppages in key economies and for key materials. But, a domestic equivalent to the global supply-demand imbalance has also been apparent in the UK, with production constraints and shortages of HGV drivers.

To read more:
https://www.bankofengland.co.uk/speech/2022/january/catherine-l-mann-speech-on-the-economy-and-monetary-policy-at-omfif

Connecting the digital islands - next steps in trade finance

Eddie Yue, Chief Executive of the Hong Kong Monetary Authority, at the roundtable on "The Future of Trade Finance: Opportunities for Hong Kong, Asia and the World", co-organised by the University of Hong Kong (HKU) Asia Global Institute & International Chamber of Commerce, Hong Kong

Good afternoon everyone. Thank you, Dr Fung, for inviting me to speak, and the HKMA is very pleased to support today's event. It would have been a pleasure to meet you all in person, but I am thankful that this event could go ahead as planned.

Today's topic is the future of trade finance, and I believe we all agree that, to elevate global trade finance to the next level, the recurring pain points of the existing trade finance system need to be fixed.

The issues-including a paper-based system that is inefficient, prone to fraud and human error-have been discussed many times; so I believe by now, we all have a basic understanding of the problems. Indeed, various stakeholders, including the HKMA, have been attempting to solve the pain points by using emerging technologies.

For example, in 2018, the HKMA facilitated the launch of eTradeConnect, which is a blockchain-based platform that aims to digitise paper-based documents and automate the trade finance process. The platform was subsequently connected to a similar platform built by the People's Bank of China to facilitate cross-boundary trade finance processes.

Similar platforms have proliferated around the world, but the trade finance gulf continues to widen. According to the Asian Development Bank, about 10% of global trade suffer from the trade financing gap.

To put this into perspective, the value of the gap amounted to USD $1.7 trillion in 2020, marking a 15% increase from just two years before. SMEs, in particular, accounted for an alarming 40% of rejected trade finance requests. These figures illustrated that global efforts are nowhere near enough, and we should all rethink why the gap is continuing to widen, and how to make our efforts as effective as possible.

A recent report published with the support of Fung Business Intelligence suggested a possible reason: the various digital trade finance platforms

mostly work independently and do not synergise with each other, resulting in what we call digital islands.

It is as if we are all putting our heads down and concentrating on developing our own platforms, forgetting that it is equally important for the platforms to communicate and work with each other. As suggested in the report, interoperation between the platforms could help to further modernise the global trade finance ecosystem and close the gap.

The Commercial Data Interchange, also known as CDI, which the HKMA is building, is precisely designed with enhancing interoperability in mind. By way of introduction, CDI aims to enhance the sharing of commercial data. Currently, every time a bank wants to connect to a data provider, it has to set up a new, separate connection.

With CDI, each bank and data provider will only need a single connection to the CDI platform, allowing banks to quickly access the business data of corporates. Banks will also be able to conveniently and swiftly set up connections with new data providers because CDI uses standardised APIs and data models, and adopts existing mainstream industry standards such as the Legal Entity Identifier.

I mentioned that CDI is designed with improving interoperability in mind. Because the platform can link up scattered digital islands and smoothen data sharing, it has great potential to enhance trade financing process and improve SMEs' access to financing. Let me show you how this could be achieved with the aid of a story.

Mr Chu runs a small business called Chu Kee with the help of his wife and parents. Chu Kee imports chilled chicken from Guangdong and sells them to supermarkets all around Hong Kong. The delicious taste of the chilled chicken and the Chus' impeccable service quickly earned Chu Kee a big group of loyal customers.

A few years ago, when Mr Chu was trying to apply for loans from banks to expand the business, he was unable to produce the financial statements required because he had never properly prepared one before. The loan approval process ended up taking almost six months, and the experience left Mr Chu rather upset, unfortunately.

Last year, Mr Chu was ready to further expand Chu Kee, and decided to give CDI a try. This time, the banks, instead of asking for financial statements, obtained alternative data from various data providers through CDI. For instance, from integrated online shopping platforms, banks learnt the amount of chilled chicken Chu Kee supplied to different supermarkets, and their value.

With the data, the banks understood Chu Kee's latest operating conditions better and made credit decisions speedily. Needless to say, before the data was used and shared, prior consent from Chu Kee was obtained. In the end, Mr Chu secured a substantial loan at a competitive interest rate, and was very pleased with the hassle-free experience.

Now, what if I tell you that the above is based on a true story? Yes, during the technical exploration stage, CDI has already, in real life, helped SMEs in Hong Kong take more control of their own digital footprint, and use their own data to improve their access to financial services.

Importers of chilled food and sneakers, and manufacturers of phone accessories have already enjoyed the benefits of CDI firsthand. As more and more banks and data providers join CDI, we expect that an increasing number of SMEs will benefit from the platform.

For CDI to reach its full potential and successfully connect the digital islands, your active participation is crucial. CDI is definitely a team sport, and we all have a role to play as members of Team Hong Kong.

The HKMA, as a regulator, will facilitate a conducive environment, and we are doing that by building the infrastructure and offering guidance. To banks, we urge you to embrace fintech, and join the CDI platform. To data providers, we invite you to contribute meaningful data, such as logistics data and procurement data between buyers and suppliers, to enrich the types of data available. To SME owners, we encourage you to contact your bank and understand more about CDI. Together, we can take Hong Kong's data ecosystem to new heights, and ultimately contribute to bridging the global trade financing gap.

The benefits of a more digitally integrated trade finance system are plentiful, that much is certain; and the HKMA strives to help bring about an enhanced system in collaboration with different stakeholders. We look forward to working with the International Chamber of Commerce (ICC) and the Fung Group in this regard so that the needs of the underserved segments can be better catered for.

Before I close, I'd like to take this opportunity to offer you a glimpse of the HKMA's vision of digitalising cross-border trade. For those of you who have been following our CBDC developments closely, you will know that we are working on a project called mBridge.
We have already developed a trial CBDC platform, and it has proven ability to speed up cross-border payments from multiple days to near real-time.

We are now exploring the feasibility of connecting eTradeConnect, CDI, and mBridge to strengthen the synergy between the three and further digitalise the cross-border trade process.

First, eTradeConnect will provide the infrastructure for digitalising trade finance, as well as support cross-boundary trade between Hong Kong and Mainland China.

Second, CDI will link up various digital islands to form a seamless data ecosystem. And finally, mBridge will expedite cross-border payments while reducing costs.

We believe that the combined power of the three infrastructure would pave the way for digitalising cross-border trade in the trade corridor between Hong Kong, Mainland China, and other APAC regions. I hope to share further updates with you in the not-so-distant future, and in the meantime, I welcome your feedback and suggestions.

Thank you, and an early Happy Chinese New Year to you all. Wishing you all health, happiness, and good fortune in the Year of the Tiger.

ESRB recommends establishing a systemic cyber incident coordination framework

The European Systemic Risk Board (ESRB) has published a *Recommendation for the establishment of a pan-European systemic cyber incident coordination framework (EU-SCICF)*. You may visit: https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf?f2ec57c21993067e9ac1d73ce93a0772

EN ECB-PUBLIC

RECOMMENDATION OF THE EUROPEAN SYSTEMIC RISK BOARD

of 2 December 2021

on a pan-European systemic cyber incident coordination framework for relevant authorities

(ESRB/2021/17)

The financial sector relies on resilient information and communications technology systems and is highly dependent on the confidentiality, integrity and availability of the data and systems it uses.

Major cyber incidents have the potential to corrupt information and destroy confidence in the financial system, and they may therefore pose a systemic risk. This calls for a high level of preparedness and coordination among financial authorities in order to respond effectively to such major cyber incidents.

The EU-SCICF would aim to strengthen this coordination among financial authorities in the European Union, as well as with other authorities in the Union and key actors at international level. It would complement the existing EU cyber incident response frameworks by addressing the risks to financial stability stemming from cyber incidents.

The ESRB report "Mitigating systemic cyber risk" explains in detail how the EU-SCICF would facilitate an effective response to a major cyber incident. You may visit: https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf?bd2b11e760cff336f84c983133dd23dc

Building on the ESRB report published in 2020, Systemic cyber risk, the report also assesses the ability of the current macroprudential framework to

address the risks and vulnerabilities stemming from systemic cyber risk. It concludes that the macroprudential mandate and toolkits of financial authorities need to be expanded to include cyber resilience.

The report proposes a macroprudential strategy that should contribute to a better mitigation of the risks to financial stability stemming from cyber incidents. A monitoring and analytical framework for systemic cyber risk needs to be implemented to help design and calibrate this new set of macroprudential tools on cyber resilience.

For example, testing the cyber resilience of the financial system through scenario analysis can show how systemic institutions in the financial system would respond to and recover from a severe but plausible cyber incident scenario.

To draw conclusions from such cyber resilience stress tests on financial stability, macroprudential authorities need to set an acceptable level of disruption to operational systems that provide critical economic functions.

It is also important to increase the understanding of systemic cyber risk-related vulnerabilities and contagion channels in the financial system. To this end, systemically important nodes at financial and operational levels should be identified – including third-party providers.

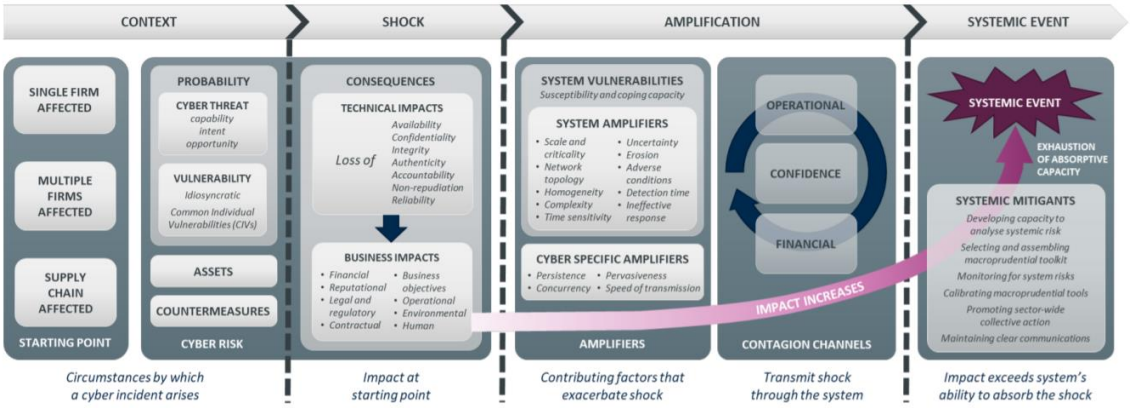
The ESRB and its dedicated European Systemic Cyber Group (ESCG) intend to explore a monitoring and analytical framework for systemic cyber risk and the required tools to address this risk in their future work. This work will focus on testing the cyber resilience of the financial system through scenario analysis and the definition of expectations for acceptable levels of disruption.

To read more:
https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.recommendation220127_on_cyber_incident_coordination~0ebcbf5f69.en.pdf?f2ec57c21993067e9ac1d73ce93a0772

https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf?bd2b11e760cff336f84c983133dd23dc

Figure 1

Systemic cyber risk model



Source: ESRB (2020).

SEC Publishes Annual Staff Report on Nationally Recognized Statistical Rating Organizations

The Securities and Exchange Commission has issued its annual Staff Report on Nationally Recognized Statistical Rating Organizations (NRSROs), providing a summary of the SEC staff's examinations of NRSROs and discussing the state of competition, transparency, and conflicts of interest among NRSROs.

In past years, the SEC's Office of Credit Ratings (OCR) covered these subject areas in two separate annual reports. The combined report includes a variety of substantive and organizational changes to provide greater transparency about NRSROs and their credit ratings businesses, and the market more broadly.

"The oversight of Nationally Recognized Statistical Rating Organizations is critical to the Commission's focus on investor protection," said SEC Chair Gary Gensler. "The Office of Credit Ratings' work contributes to our efforts to promote accuracy in credit ratings and help ensure that credit ratings are not unduly influenced by conflicts of interest."
"OCR's examinations protect investors by scrutinizing NRSRO compliance with applicable laws and rules and identifying instances of non-compliance," said OCR Director Ahmed Abonamah. "The report

provides a comprehensive and integrated overview of OCR's activities, demonstrating the exceptional work of my colleagues in their efforts to protect investors."

The report highlights the risk-based approach of OCR's examination program. As described in the report, in addition to the eight statutorily mandated review areas, OCR staff examined the NRSROs':

- Consideration of ESG factors and products;
- COVID-19 related risk areas;
- Activities related to collateralized loan obligations, commercial real estate, and consumer asset-backed securities;
- Adherence to policies, procedures, and methodologies with respect to rating low-investment grade corporate securities; and
- Controls, policies, and procedures for ratings of municipal securities.

To read more: https://www.sec.gov/news/press-release/2022-15

The report: https://www.sec.gov/files/2022-ocr-staff-report.pdf

Statement before the Financial Stability Oversight Council on Money Market Funds, Open-End Bond Funds, and Hedge Funds

U.S. SECURITIES AND EXCHANGE COMMISSION

Thank you, Secretary Yellen, for focusing the Council's attention on financial resiliency with regard to three key parts of our capital markets — particularly money market funds, open-end bond funds, and hedge funds.

The fund industry gives retail and institutional investors the opportunity to pool their assets, get investment advice, and attain diversification and efficiency.

These pools of assets have become a significant part of our markets. There's $5 trillion in money market funds, nearly $7 trillion in open-end bond funds, and $9 trillion in gross assets under management in hedge funds.

The nature, scale, and interconnectedness of these fund sectors, though, also pose issues for financial stability. This is not just based on financial economic theory, but also upon the practical lessons of the past.

We've seen such risks emanate from these sectors during the 2008 financial crisis, at the start of the COVID crisis in March 2020, and in 1998, when the hedge fund Long-Term Capital Management failed.

Money market funds and open-end bond funds, by their design, have a potential liquidity mismatch — between investors' ability to redeem daily on the one hand, and funds' securities that may have lower liquidity.

While this might not be as significant a concern in normal markets, we've seen that in stress times, these funds' liquidity mismatches can raise systemic issues. Hedge funds can present financial resiliency risks through leverage or derivatives positions.

I think the Securities and Exchange Commission has a responsibility to help protect for financial stability, which maps onto many parts of our statutes, but particularly onto the "orderly" part of our mission. Thus, I've asked SEC staff to make recommendations for the Commission's consideration with regard to bolstering the resiliency of each of these fund sectors.

The Commission recently voted to propose amendments to rules that govern money market funds. I'd like to thank William Birdthistle and Sarah ten Siethoff for their work and today's presentation on the SEC's proposal.

With respect to open-end bond funds, I've asked staff whether there are improvements we can consider regarding the fund liquidity rule or through other reforms to enhance fund liquidity, pricing, and resiliency in possible future stress events.

With respect to hedge funds, in January, the Commission voted to propose amendments to Form PF — a form first adopted after the financial crisis that provides certain private fund information to the SEC and other financial regulators.

Among other things, the proposed amendments would require certain advisers to hedge funds to provide current reporting of events that could be relevant to financial stability.

Looking ahead, I've asked staff to work jointly with staff at the Commodity Futures Trading Commission to consider whether they would recommend amending the joint portions of Form PF related to the periodic reports of hedge funds.

Further, in November, the Commission proposed a rule to require public reporting of large security-based swap positions. Total return swaps, a type of security-based swaps, contributed to the transmission of risk during the failure of Archegos Capital Management last year. We also re-proposed a new rule to prevent fraud, manipulation, and deception in connection with security-based swap transactions.

I support the FSOC Statement on Nonbank Financial Intermediation today and welcome FSOC members' input on the SEC's ongoing consideration on how to best enhance resiliency in these critical fund sectors.

Thank you.

BaFin can inform the public based on indications of possible market manipulation

Katharina Meinhardt, BaFin Legal Division for Securities Supervision and Competence Centre for Constitutional, Administrative and European Law

The courts confirm: if Germany's financial supervisor has indications of possible market manipulation, it may inform the public about this and need not wait until proof of market manipulation has been established.

BaFin regularly publishes notifications on its website informing the public from an early stage about extensive advertising activities for certain shares and advising caution when dealing with buy recommendations of this kind.

Often, the purpose of such buy recommendations is to induce investors to acquire the shares in question so that the share price rises in response to the increased demand.

This enables the senders of the recommendations or others behind such recommendations who purchased the shares beforehand at a lower price to profit from selling the shares at a higher price.

A market participant felt disadvantaged by this practice. He therefore filed a summary proceeding at the Administrative Court (Verwaltungsgericht) of Frankfurt am Main, demanding the deletion of one such notification.

His application was rejected (case ref. 7 L 3357/20.F) and the market participant then appealed to the Higher Administrative Court of Hesse (Hessische Verwaltungsgerichtshof), which confirmed in full the decision passed by the court of first instance (case ref. 6 B 685/21).

"The decisions confirm that BaFin may inform the public of the danger of prohibited market manipulation at the first indication of such dealings," said BaFin's Chief Executive Director Beatrice Freiwald, "thereby strengthening trust in the capital market and ensuring market integrity".

Preventative measures also permitted

Both courts were of the opinion that the criteria for issuing the challenged notification were met under section 6 (2) sentence 1 to 3 of the German Securities Trading Act (Wertpapierhandelsgesetz – WpHG) in conjunction with Article 15 and Article 12 of the European Market Abuse Regulation (MAR).

BaFin is permitted to publish a notification if there is an imminent risk of the prohibitions and requirements of MAR being infringed. Preventative

measures are also permitted under these provisions. It is not necessary that the infringement of the prohibition of market manipulation has actually taken place or been proved.

In the case at issue, there was an imminent danger of market manipulation within the meaning of Article 12 of MAR and, thus, of infringement of the prohibition of market manipulation under Article 15 of MAR.

Both courts established that the constitutional rights of the applicant had not been violated. According to the courts, the notification had been made correctly and had taken account of the legal provisions relating to state disclosure of information. BaFin had acted in accordance with its remit and informed the public in a proper and factually correct manner.

To read more:
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2021/fa_bj_2111_marktmanipulation_en.html;jsessionid=D8B749E4A956A71F925924C5775A8B27.2_cid503

MAS-led Industry Consortium Publishes Assessment Methodologies for Responsible Use of AI by Financial Institutions

The Monetary Authority of Singapore (MAS) announced today the release of five white papers detailing assessment methodologies for the Fairness, Ethics, Accountability and Transparency (FEAT) principles, to guide the responsible use of AI by financial institutions (FIs).

The white papers were published by the Veritas Consortium, comprising 27 industry players. The Consortium also released an open-source toolkit to help FIs adopt the Fairness Assessment Methodology.

The white papers provide:

- a comprehensive FEAT checklist for FIs to adopt during their Artificial Intelligence and Data Analytics (AIDA) software development lifecycles;

- an enhanced Fairness Assessment Methodology to enable FIs to define their AIDA system's fairness objectives, identify personal attributes of individuals and any unintentional bias;

- a new Ethics and Accountability Assessment Methodology, which provides a framework for FIs to carry out quantifiable measurement of ethical practices, in addition to the qualitative practices currently adopted;

- a new Transparency Assessment Methodology which helps FIs determine whether and how much internal/external transparency is needed to explain and interpret the predictions of machine learning models.

To accelerate FIs' adoption of the FEAT methodologies and principles, the Consortium has developed an open-source software toolkit.

The toolkit enables the automation of the fairness metrics assessment and allows for visualisation of the interface for fairness assessment and for the plug-ins to integrate with FI's IT systems.

Four core teams within the Consortium were formed to develop the methodologies, toolkit and business use case studies in the banking and insurance sectors:

- Swiss Re and Accenture refined the Fairness Assessment Methodology and applied it to insurance predictive underwriting;

- United Overseas Bank (UOB), AXA and Accenture developed the Ethics and Accountability Assessment Methodology and applied it to customer marketing and insurance fraud detection;

- Standard Chartered Bank (SCB), HSBC and Truera developed the Transparency Assessment Methodology and applied it to credit risk scoring and customer marketing; and

- Accenture and Bank of China developed Veritas Toolkit version one with the support from BNY Mellon, HSBC, SCB and UOB.

In the next phase, the consortium will develop additional use cases and run pilots with selected FI members to integrate the methodologies with members' existing governance framework.

MAS is also collaborating with the Infocomm Media Development Authority and the Personal Data Protection Commission (PDPC) to include the Toolkit in the PDPC's Trustworthy AI testing framework.

Sopnendu Mohanty, Chief FinTech Officer, MAS, said, "The new open-source software, assessment methodologies and enhanced guidance will further improve the technical capabilities of financial institutions in developing responsible AI for the financial sector.

The Veritas initiative continues to deliver tangible outcomes that demonstrate collaborative public-private partnership to drive trust in the adoption of AI technology, enhance confidence and foster innovation in Singapore's FinTech ecosystem."

Resources

Annex - List of Veritas Consortium Members:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Annex---List-of-Veritas-Consortium-Members.pdf

Veritas Document 3 - FEAT Principles Assessment Methodology:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-3---FEAT-Principles-Assessment-Methodology.pdf

Veritas Document 3A - FEAT Fairness Principles Assessment Methodology:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-3A---FEAT-Fairness-Principles-Assessment-Methodology.pdf

Veritas Document 3B - FEAT Ethics and Accountability Principles Assessment Methodology:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-3B---FEAT-Ethics-and-Accountability-Principles-Assessment-Methodology.pdf

Veritas Document 3C - FEAT Transparency Principles Assessment Methodology:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-3C---FEAT-Transparency-Principles-Assessment-Methodology.pdf

Veritas Document 4 - FEAT Principles Assessment Case Studies:
https://www.mas.gov.sg/-/media/MAS-Media-Library/news/media-releases/2022/Veritas-Document-4---FEAT-Principles-Assessment-Case-Studies.pdf

The European Supervisory Authorities (ESAs) recommend actions to ensure the EU's regulatory and supervisory framework remains fit-for-purpose in the digital age

- The application of innovative technologies is facilitating changes to the structure of the EU financial sector. Value chains are evolving, the use of digital platforms is growing rapidly and new mixed-activity groups are emerging.

- The ESAs recommend a series of actions to the European Commission to strengthen EU financial services regulation and enhance supervisory capabilities in line with these developments.

The three European Supervisory Authorities (EBA, EIOPA and ESMA) published today a joint report in response to the European Commission's February 2021 Call for Advice on Digital Finance.

The proposals that were put forward aim at maintaining a high level of consumer protection and addressing risks arising from the transformation of value chains, platformisation and the emergence of new 'mixed-activity groups' i.e. groups combining financial and non-financial activities.

The ESAs note that the use of innovative technologies in the EU financial sector is facilitating changes to value chains, that dependencies on digital platforms are increasing rapidly, and that new mixed-activity groups are emerging. These trends open up a range of opportunities for both EU consumers and financial institutions, but also pose new risks.

Therefore, the ESAs recommend rapid action to ensure that the EU's financial services regulatory and supervisory framework remains fit-for-purpose in the digital age.

The proposals include:

(i) a holistic approach to the regulation and supervision of the financial services value chain;

(ii) strengthened consumer protection in a digital context, including through enhanced disclosures, complaints handling mechanisms, measures aimed at preventing the mis-selling of tied/bundled products, and improved digital and financial literacy;

(iii) further convergence in the classification of cross-border services;

(iv) further convergence in addressing money laundering/financing of terrorism risks in a digital context;

(v) effective regulation and supervision of 'mixed-activity groups', including a review of prudential consolidation requirements;

(vi) strengthened supervisory resources and cooperation between financial and other relevant authorities, including on a cross-border and multi-disciplinary basis; and

(vii) active monitoring of the use of social media in financial services.

Background

The European Commission's September 2020 Digital Finance Strategy sets out the European Commission's intention to review the existing financial services legislative frameworks in order to protect consumers, safeguard financial stability, protect the integrity of the EU financial sectors and ensure a level playing field.

As part of this review, in February 2021 the European Commission issued a Request to EBA, EIOPA and ESMA for technical advice on digital finance and related issues. In particular, the European Commission called on the ESAs to provide advice on the regulation and supervision of more fragmented or non-integrated value chains (section 3.1), platforms and bundling of various financial services (section 3.2), and groups combining different activities (section 3.3).

In accordance with the Call for Advice, the ESAs have carried out an analysis of market developments as well as the risks and opportunities posed by digitalisation in finance and set out their findings and advice in the report to the European Commission.

Note

According to Article 16a(1) of the Founding Regulations for each of the ESAs, they may, upon a request from the European Parliament, the Council or the European Commission, or on their own initiative, provide opinions to the European Parliament, the Council and the European Commission on all issues related to its area of competence. Article 56 of the Founding Regulations provides that ESAs shall, within the scope of their tasks, "reach joint positions by consensus with, as appropriate, [the other ESAs]". Based on the above-mentioned legal provisions, the ESAs are competent to assess opportunities and risks related to digitalisation of financial services and provide the advice requested by the European Commission.

To read more:
https://www.eba.europa.eu/esas-recommend-actions-ensure-eu%E2%80%99s-regulatory-and-supervisory-framework-remains-fit-purpose-digital

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0591&from=EN

Helping users stay safe: Blocking internet macros by default in Office

Kellie Eickmeyer

It's a challenging time in software security; migration to the modern cloud, the largest number of remote workers ever, and a global pandemic impacting staffing and supply chains all contribute to changes in organizations. Unfortunately, these changes also give bad actors opportunities to exploit organizations:

> *"Cybercriminals are targeting and attacking all sectors of critical infrastructure, including healthcare and public health, information technology (IT), financial services, and energy sectors. Ransomware attacks are increasingly successful, crippling governments and businesses, and the profits from these attacks are soaring."*
>
> - Microsoft Digital Defense Report, Oct 2021

For years Microsoft Office has shipped powerful automation capabilities called active content, the most common kind are macros. While we provided a notification bar to warn users about these macros, users could still decide to enable the macros by clicking a button. Bad actors send macros in Office files to end users who unknowingly enable them, malicious payloads are delivered, and the impact can be severe including malware, compromised identity, data loss, and remote access. See more in this blog post:

> *"A wide range of threat actors continue to target our customers by sending documents and luring them into enabling malicious macro code. Usually, the malicious code is part of a document that originates from the internet (email attachment, link, internet download, etc.). Once enabled, the malicious code gains access to the identity, documents, and network of the person who enabled it."*
>
> - Tom Gallagher, Partner Group Engineering Manager, Office Security

For the protection of our customers, we need to make it more difficult to enable macros in files obtained from the internet.

Changing Default Behavior

We're introducing a default change for five Office apps that run macros:

VBA macros obtained from the internet will now be blocked by default.

For macros in files obtained from the internet, users will no longer be able to enable content with a click of a button. A message bar will appear for users notifying them with a button to learn more. The default is more

secure and is expected to keep more users safe including home users and information workers in managed organizations.

This change only affects Office on devices running Windows and only affects the following applications: Access, Excel, PowerPoint, Visio, and Word. The change will begin rolling out in Version 2203, starting with Current Channel (Preview) in early April 2022. Later, the change will be available in the other update channels, such as Current Channel, Monthly Enterprise Channel, and Semi-Annual Enterprise Channel.

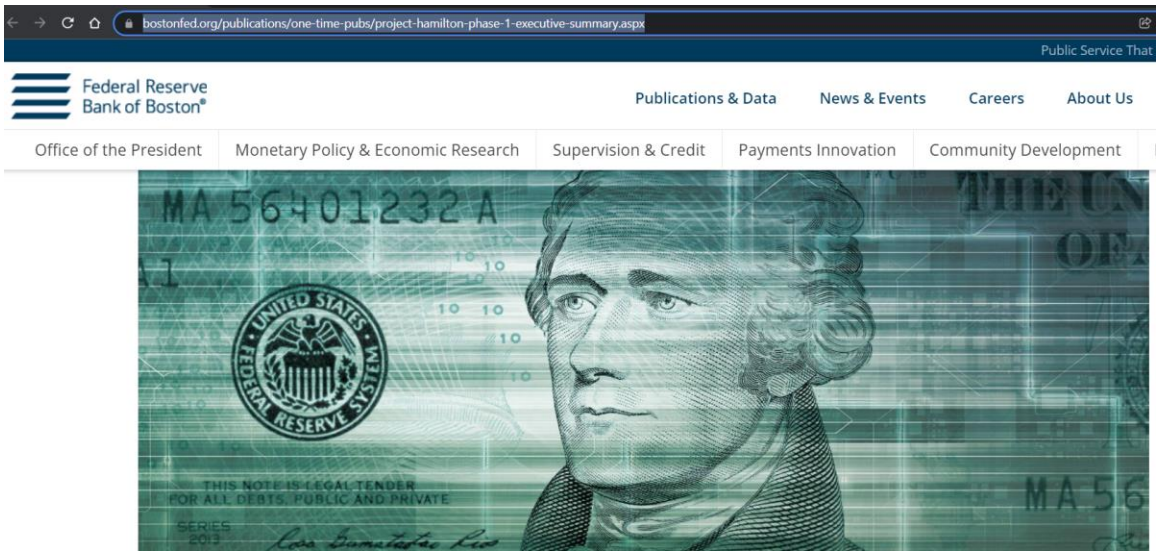
At a future date to be determined, we also plan to make this change to Office LTSC, Office 2021, Office 2019, Office 2016, and Office 2013.

To read more:
https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

The Federal Reserve Bank of Boston and Massachusetts Institute of Technology release technological research on a central bank digital currency

The Federal Reserve Bank of Boston and the Digital Currency Initiative (https://dci.mit.edu/)at the Massachusetts Institute of Technology released the findings of their initial technological research into a central bank digital currency, or CBDC.

The published research describes a theoretical high-performance and resilient transaction processor for a CBDC that was developed using open-source research software, OpenCBDC. You may visit: https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx



This collaborative effort, known as Project Hamilton, focuses on technological experimentation and does not aim to create a usable CBDC for the United States. The research is separate from the Federal Reserve's Board's evaluation of the pros and cons of a CBDC.

"It is critical to understand how emerging technologies could support a CBDC and what challenges remain," said Boston Fed Executive Vice President and Interim Chief Operating Officer Jim Cunha. "This

collaboration between MIT and our technologists has created a scalable CBDC research model that allows us to learn more about these technologies and the choices that should be considered when designing a CBDC."

The whitepaper released today details findings from the first research phase. In this phase, researchers selected concepts from cryptography, distributed systems, and blockchain technology to build and test platforms that would give policymakers substantial flexibility in the potential creation of a CBDC. The paper describes the following findings:

- The team met its goal of creating a core processing engine for a hypothetical general purpose CBDC and explored it in two architectures.

- The work produced one code base capable of handling 1.7 million transactions per second.

- The vast majority of transactions reached settlement finality in under two seconds within architectures that support secure, resilient performance and offer the significant technological flexibility required to adjust to future policy direction.

Researchers with MIT and the Boston Fed released the code for Project Hamilton, OpenCBDC.

"There are still many remaining challenges in determining whether or how to adopt a central bank payment system for the United States," said Neha Narula, director of the Digital Currency Initiative at MIT. "What is clear is that open-source software provides an important way to collaborate, experiment, and implement. In addition to supporting collaboration, monetary systems benefit from transparency and verifiability, which open-source offers."

About Project Hamilton

Project Hamilton is a multi-year collaboration between the Boston Fed and MIT's Digital Currency Initiative that was announced in 2020. The project explores the use of existing and new technologies to build and test a hypothetical digital currency platform.

The project's first phase produced the research and code released today for a high-performance transaction processor. The code is the first contribution to OpenCBDC, a project maintained by MIT which will serve as a platform for further CBDC research. Project Hamilton aims to inform future contributions to the code and inform policy discussions about CBDC.

In the coming years, the second phase of this partnership will allow Project Hamilton to explore alternative technical designs to improve the already robust privacy, resiliency, and functionality of the technology outlined in the first phase.

The Federal Reserve Bank of Boston serves the First Federal Reserve District, which includes all of New England except Fairfield County, Connecticut.

Within the district, the Bank monitors local economic conditions to aid in the formulation of monetary policy; engages in outreach to promote economic growth, community revitalization, and economic and financial education; supervises banks and bank holding companies; and provides financial services to facilitate banking operations.

Romance Scams

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

The criminals who carry out romance scams are experts at what they do and will seem genuine, caring, and believable. Con artists are present on most dating and social media sites.

The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim, and gain trust. Scammers may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money.

Scam artists often say they are in the building and construction industry and are engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they ask for money for a medical emergency or unexpected legal fee.

If someone you meet online needs your bank account information to deposit money, they are most likely using your account to carry out other theft and fraud schemes.

Tips for Avoiding Romance Scams:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.

- Research the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere.

- Go slowly and ask lots of questions.

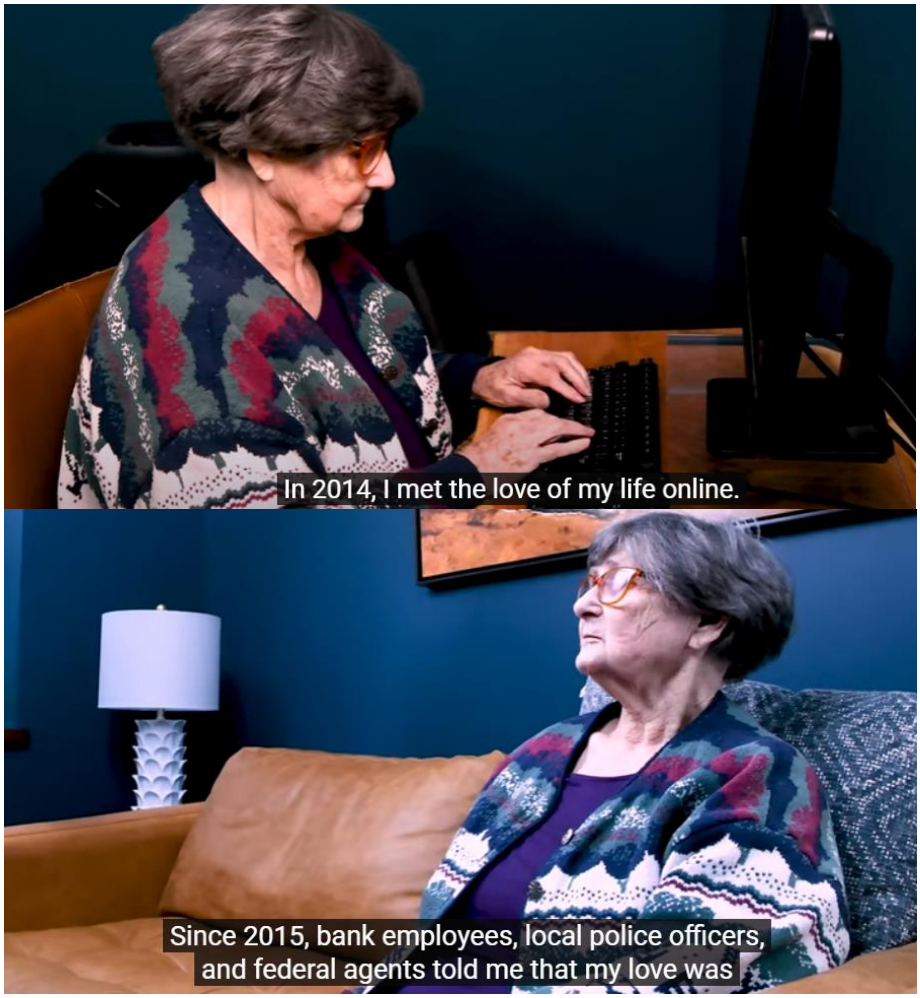
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.

- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.

- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a few months, for whatever reason, you have good reason to be suspicious.

- Never send money to anyone you have only communicated with online or by phone.

To learn more:
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams



https://www.youtube.com/watch?v=vthPmLORVrM

https://youtu.be/108UWM1jsF8
https://youtu.be/BmIvqOYwGGU

https://www.ic3.gov/Media/Y2019/PSA190805

Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules

WHAT IS CONFIDENCE/ROMANCE FRAUD?

Confidence/romance fraud occurs when an actor deceives a victim into believing they have a trust relationship—whether family, friendly, or romantic—and leverages the relationship to persuade the victim to send money, provide personal and financial information, or purchase items of value for the actor. In some cases, the victim is persuaded to launder money on behalf of the actor.

Actors often use online dating sites to pose as U.S. citizens located in a foreign country, U.S. military members deployed overseas, or U.S. business owners seeking assistance with lucrative investments.

Preparing for the Financial System of the Future

Governor Lael Brainard, at the 2022 U.S. Monetary Policy Forum, New York, New York

The financial system is undergoing fast-moving changes associated with digitalization and decentralization. Some of these innovations hold considerable promise to reduce transaction costs and frictions, increase competition, and improve financial inclusion, but there are also potential risks.

With technology driving profound change, it is important we prepare for the financial system of the future and not limit our thinking to the financial system of today.

The Evolving Digitalization and Decentralization of Finance

In recent years, there has been explosive growth in the development and adoption of new digital assets that leverage distributed ledger technologies and cryptography.

The market capitalization of cryptocurrencies grew from less than $100 billion five years ago to a high of almost $3 trillion in November 2021 and is currently around $2 trillion.

In parallel, we have seen rapid growth in the platforms that facilitate the crypto finance ecosystem, including decentralized finance (DeFi) platforms.

These crypto platforms facilitate a variety of activities, including lending, trading, and custodying crypto-assets, in some cases outside the traditional regulatory guardrails for investor and consumer protection, market integrity, and transparency.

The growth in the crypto finance ecosystem is fueling demand for stablecoins—digital assets that are intended to maintain stable value relative to reference assets, such as the U.S. dollar. Stablecoin supply grew nearly sixfold in 2021, from roughly $29 billion in January 2021 to $165 billion in January 2022.

There is a high degree of concentration among a few dollar-pegged stablecoins: As of January 2022, the largest stablecoin by market

capitalization made up almost half of the market, and the four largest stablecoins together made up almost 90 percent.

Today, stablecoins are being used as collateral on DeFi and other crypto platforms, as well as in facilitating trading and monetization of cryptocurrency positions on and between crypto and other platforms.

In the future, some issuers envision that stablecoins will also have an expanded reach in the payment system and be commonly used for everyday transactions, both domestic and cross-border. So it is important to have strong frameworks for the quality and sufficiency of reserves and risk management and governance.

As noted in a recent report on stablecoins by the President's Working Group on Financial Markets, it is important to guard against run risk, whereby the prospect of an issuer not being able to promptly and adequately meet redemption requests for the stablecoin at par could result in a sudden surge in redemption demand.

It is also important to address settlement risk, whereby funds settlement is not certain and final when expected, and systemic risk, whereby the failure or distress of a stablecoin provider could adversely affect the broader financial system.

The prominence of crypto advertisements during the Super Bowl highlighted the growing engagement of retail investors in the crypto ecosystem. In late 2021, Pew Research found that 16 percent of survey respondents reported having personally invested in, traded, or otherwise used a cryptocurrency—up from less than 1 percent of respondents in 2015. There is also rising interest among institutional investors.

So it is perhaps not surprising that established financial intermediaries are undertaking efforts to expand the crypto services and products they offer. If the past year is any guide, the crypto financial system is likely to continue to grow and evolve in ways that increase interconnectedness with the traditional financial system.

As a result, officials in many countries are undertaking efforts to understand and adapt to the transformation of the financial system. Many jurisdictions are making efforts to ensure statutory and regulatory frameworks apply like rules to like risks, and some jurisdictions are issuing or contemplating issuing central bank currency in digital form.

Preparing for the Payment System of the Future

The Federal Reserve needs to be preparing for the payment landscape of the future even as we continue to make improvements to meet today's needs. In

light of the rapid digitalization of the financial system, the Federal Reserve has been thinking critically about whether there is a role for a potential U.S. central bank digital currency (CBDC) in the digital payment landscape of the future and about its potential properties, costs, and benefits.

Our financial and payment system delivers important benefits today and is continuing to improve with developments like real-time payments. Nonetheless, certain challenges remain, such as a lack of access to digital banking and payment services for some Americans and expensive and slow cross-border payments.

Growing interest in the digital financial ecosystem suggests that technology is enabling potential improvements that merit consideration.

In addition, it is important to consider how new forms of crypto-assets and digital money may affect the Federal Reserve's responsibilities to maintain financial stability, a safe and efficient payment system, household and business access to safe central bank money, and maximum employment and price stability.

It is prudent to explore whether there is a role for a CBDC to preserve some of the safe and effective elements of the financial system of the present in a way that is complementary to the private sector innovations transforming the financial landscape of the future.

The public and private sector play important complementary roles within the financial system in the United States. From Fedwire to FedNow, the Federal Reserve has over a century of experience working to improve the infrastructure of the U.S. payment system to provide a resilient and adaptable foundation for dynamic private sector activity.

In parallel, private sector banks and nonbanks have competed to build the best possible products and services on top of that foundation and to meet the dollar-denominated needs of consumers and investors at home and around the world. The result is a resilient payment system that is responsive to the changing needs of businesses, consumers, and investors.

While the official sector provides a stable currency, operates some important payment rails, and undertakes regulation and oversight of financial intermediaries and critical financial market infrastructures, the private sector brings competitive forces encouraging efficiency and new product offerings and driving innovation.

Responsible innovation has the potential to increase financial inclusion and efficiency and to lower costs within guardrails that protect consumers and investors and safeguard financial stability.

As we assess the range of future states of the financial system, it is prudent to consider how to preserve ready public access to government-issued, risk-free currency in the digital financial system—the digital equivalent of the Federal Reserve's issuance of physical currency.

The Board recently issued a discussion paper that outlines the Federal Reserve's current thinking on the potential benefits, risks, and policy considerations of a U.S. CBDC.

The paper does not advance any specific policy outcome and does not signal that the Board will make any imminent decisions about the appropriateness of issuing a U.S. CBDC.

It lays out four CBDC design principles that analysis to date suggests would best serve the needs of the United States if one were created.

Those principles are that a potential CBDC should be privacy-protected, so consumer data and privacy are safeguarded; intermediated, such that financial intermediaries rather than the Federal Reserve interface directly with consumers; widely transferable, so the payment system is not fragmented; and identity-verified, so law enforcement can continue to combat money laundering and funding of terrorism.

Financial Stability

Given the Federal Reserve's mandate to promote financial stability, any consideration of a CBDC must include a robust evaluation of its impact on the stability of the financial system—not only as it exists today but also as it may evolve in the future.

In consideration of the financial system today, it would be important to explore design features that would ensure complementarity with established financial intermediation.

A CBDC—depending on its features—could be attractive as a store of value and means of payment to the extent it is seen as the safest form of money.

This could make it attractive to risk-averse users, perhaps leading to increased demand for the CBDC at the expense of other intermediaries during times of stress. So it is important to undertake research regarding the tools and design features that could be introduced to limit such risks, such as offering a non-interest bearing CBDC and limiting the amount of CBDC an end user could hold or transfer.

As I noted at the start, the digital asset and payment ecosystem is evolving at a rapid pace. Thus, it is also important to contemplate the potential role of a CBDC to promote financial stability in a future financial system in

which a growing range of consumer payment and financial transactions would be conducted via digital currencies such as stablecoins. If current trends continue, the stablecoin market in the future could come to be dominated by just one or two issuers.

Depending on the characteristics of these stablecoins, there could be large shifts in desired holdings between these stablecoins and deposits, leading to large-scale redemptions by risk-averse users at times of stress that could prove disruptive to financial stability.

In such a future state, the coexistence of CBDC alongside stablecoins and commercial bank money could prove complementary, by providing a safe central bank liability in the digital financial ecosystem, much like cash currently coexists with commercial bank money.

It is essential that policymakers, including the Federal Reserve, plan for the future of the payment system and consider the full range of possible options to bring forward the potential benefits of new technologies, while safeguarding stability.

International Considerations

Analysis of the potential future state of the financial system is not limited to the domestic implications. The dollar is important to global financial markets: It is not only the predominant global reserve currency, but the dollar is also the most widely used currency in international payments.

Decisions by other major jurisdictions to issue CBDCs could bring important changes to global financial markets that may prove more or less disruptive and that could influence the potential risks and benefits of a U.S. CBDC.

Thus, it is wise to consider what the future states of global financial markets and transactions would look like both with and without a Federal Reserve-issued CBDC. For example, the People's Bank of China has been piloting the digital yuan, also known as e-CNY, in numerous Chinese cities over the past two years.

The substantial early progress on the digital yuan may have implications for the evolution of cross-border payments and payment systems. And it may influence the development of norms and standards for cross-border digital financial transactions.

It is prudent to consider how the potential absence or issuance of a U.S. CBDC could affect the use of the dollar in payments globally in future states where one or more major foreign currencies are issued in CBDC form.

A U.S. CBDC may be one potential way to ensure that people around the world who use the dollar can continue to rely on the strength and safety of U.S. currency to transact and conduct business in the digital financial system.

More broadly, it is important to consider how the United States can continue to play a lead role in the development of standards governing international digital financial transactions involving CBDCs consistent with norms such as privacy and security.

Given the dollar's important role as a payment instrument across the world, it is essential that the United States be on the frontier of research and policy development regarding CBDC, as international developments related to CBDC can have implications for the global financial system.

Technology Research and Experimentation

Given the range of possible future states with significant digitization of the financial system, it is important that the Federal Reserve is actively engaging with the underlying technologies.

Our work to build 24x7x365 instant payments rails leverages lessons from some of today's most resilient, high-performing, and large-scale technology platforms across the globe.

It is providing important insights on the clearing and settlement models associated with real time payments as well as on fraud, cyber resilience, cloud computing, and related technologies.

In parallel with the Board's public consultation on CBDC, the Federal Reserve Bank of Boston, in collaboration with the Massachusetts Institute of Technology, has developed a theoretical high-performance transaction processor for CBDC.

They recently published the resulting software under an open-source license as a way of engaging with the broader technical community and promoting transparency and verifiability.

Moreover, the Board is studying how innovations, such as distributed ledger technology, could improve the financial system. This work includes experimentation with stablecoin interoperability and testing of retail payments across multiple distributed payment ledger systems. The Federal Reserve Bank of New York recently established an Innovation Center, focused on validating, designing, building, and launching new financial technology products and services for the central bank community.

These technology research and development initiatives are vital to our responsibilities to promote a safe and efficient payment system and financial stability, whatever the future may bring.

Conclusion

The financial system is not standing still, and neither can we. The digital financial ecosystem is evolving rapidly and becoming increasingly connected with the traditional financial system.

It is prudent for the Board to understand the evolving payment landscape, the technological advancements and consumer demands driving this evolution, and the consequent policy choices as it seeks to fulfill its congressionally-mandated role to promote a safe, efficient, and inclusive system for U.S. dollar transactions.

To prepare for the financial system of the future, the Federal Reserve is engaging in research and experimentation with these new technologies and consulting closely with public and private sector partners.

ESRB issues new warnings and recommendations on medium-term residential real estate vulnerabilities

The European Systemic Risk Board (ESRB) has published five warnings and two recommendations on medium-term residential real estate vulnerabilities. It has also published an assessment of compliance with recommendations issued in 2019.

Warnings were sent to the competent ministers of five countries with newly identified vulnerabilities that have not been addressed sufficiently: Bulgaria, Croatia, Hungary, Liechtenstein and Slovakia.

Recommendations were sent to the competent ministers of two countries, Austria and Germany, which had already received ESRB warnings in 2016 and 2019, respectively, and whose vulnerabilities have not been addressed sufficiently.

After these recommendations were issued, the authorities in Austria and Germany announced new measures to address vulnerabilities in the residential real estate sector.

The ESRB assesses vulnerabilities in the residential real estate sector because of its importance for financial and macroeconomic stability. In 2016 and 2019, the ESRB conducted systematic, forward-looking assessments of such vulnerabilities in the European Economic Area (EEA).

Recently, the ESRB concluded another assessment of this sector in the EEA, which formed the basis for the latest set of country-specific warnings and recommendations. The ESRB has a mandate to issue such warnings when significant systemic risks are identified and to make recommendations for remedial action.

The assessment covered all EU Member States, Iceland, Liechtenstein and Norway and analysed the main trends in various real estate indicators as well as the macroprudential policy actions that countries have taken to mitigate the financial stability risks identified.

The outcome of this analysis shows that financial stability risks related to residential real estate have continued to increase in several countries in the context of macroeconomic risks related to the coronavirus (COVID-19) pandemic and continued strong dynamics in housing markets, housing credit and household indebtedness.

The key vulnerabilities highlighted by the ESRB assessment are of a medium-term nature and, depending on the country, relate to rapid house

price growth and possible overvaluation of residential real estate, the level and dynamics of household indebtedness, the growth of housing credit and signs of a loosening of lending standards.

The specific vulnerabilities vary from country to country, and the details can be found in the individual warnings and recommendations.

Beyond macroprudential policy considerations, in a number of countries, some underlying vulnerabilities would be mitigated more efficiently with the help of reforms of housing and tax policies.

In view of the economic uncertainty during the pandemic, any policy action should be carefully assessed to ensure that it contributes to mitigating residential real estate vulnerabilities, while aiming to avoid procyclical effects on the overall performance of the real economy and the financial system.

Residential real estate vulnerabilities have remained elevated in the countries that received ESRB recommendations in 2019.

In a number of these countries, vulnerabilities have persisted in spite of recent measures introduced to address them.

The latter countries are Denmark, Finland, Luxembourg, the Netherlands and Sweden.

In most cases, house prices have continued rising or have grown even faster than before, resulting in unchanged or increased house price overvaluation.

The risk related to household indebtedness has also remained unchanged or increased in several countries, partly as a result of strong mortgage credit growth. In most cases, lending standards for new mortgage loans have not significantly improved or have shown signs of deterioration.

For the remaining EEA countries, either the ESRB has not identified a build-up of material vulnerabilities in the residential real estate sector, or such vulnerabilities have been identified but the current policy stance is assessed as sufficient in addressing them.

Full details of the ESRB's assessment are included in the ESRB report "Vulnerabilities in the residential real estate sectors of the EEA countries", which has been published today alongside the warnings and recommendations. The assessment of vulnerabilities is based on available data and covers developments up to mid-November 2021.

The ESRB has also published a compliance report on the countries that received ESRB recommendations in 2019 concerning medium-term

vulnerabilities in their residential real estate sectors. You may visit: https://www.esrb.europa.eu/pub/pdf/recommendations/esrb.Country-specific_Recommendations202201~816f54bbf7.en.pdf

Compliance report

February 2022

Country-specific Recommendations of the European Systemic Risk Board of 27 June 2019 on medium-term vulnerabilities in the residential real estate sector in Belgium (ESRB/2019/4), Denmark (ESRB/2019/5), Luxembourg (ESRB/2019/6), the Netherlands (ESRB/2019/7), Finland (ESRB/2019/8) and Sweden (ESRB/2019/9), respectively

The report reviews the policy responses aimed at mitigating the vulnerabilities in Belgium, Denmark, Finland, Luxembourg, the Netherlands and Sweden.

The ESRB monitors and assesses compliance with its recommendations via an “act or explain” mechanism.

The ESRB recommendations issued in 2019 have a specific timeline for implementation (ranging from 2020 to 2022).

Overall, the compliance assessment findings are as follows: one addressee is assessed as fully compliant (Luxembourg), three addressees are assessed as largely compliant (Belgium, Denmark and Sweden) and two addressees are assessed as partially compliant (Finland and the Netherlands).

Going forward, the ESRB will continue exercising its mandate of macroprudential oversight of the financial system in the EU Member States, Iceland, Liechtenstein and Norway, including identifying financial stability vulnerabilities related to real estate.

The ESRB will continue to issue warnings if a significant systemic risk to financial stability is identified and, where appropriate, will issue recommendations for remedial action.

To read more:
https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr220211~9393d5e991.en.html

Disclaimer

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

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

This information:

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

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

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

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

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

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

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

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Basel iii Compliance Professionals Association (BiiiCPA)

The Basel iii Compliance Professionals Association (BiiiCPA) is the largest association of Basel iii Professionals in the world. It is a business unit of the Basel ii Compliance Professionals Association (BCPA), the largest association of Basel ii Professionals in the world.

We invite you to connect with the global community of experts working for the implementation of the Basel III framework, to gain insight into the G20 efforts to regulate the global financial system, to explore new career avenues, and most of all, to acquire lifelong skills.

You can explore what we offer to our members:

1. Membership - Become a standard, premium or lifetime member.
You may visit:
https://www.basel-iii-association.com/How_to_become_member.htm

2. Monthly Updates – Visit the Reading Room of the association at:
https://www.basel-iii-association.com/Reading_Room.html

3. Training and Certification – You may visit:
https://www.basel-iii-association.com/Basel_III_Distance_Learning_Online_Certification.html

For instructor-led training, you may contact us. We tailor Basel III presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.