Solvency ii Association
1200 G Street NW Suite 800 Washington DC 20005-6705 USA
Tel: 202-449-9750 Web: www.solvency-ii-association.com

Solvency 2 News, June 2023

Dear members and friends,

The International Organization of Securities Commissions (IOSCO) has published a Consultation Report with the aim of finalizing IOSCO's policy recommendations to address market integrity and investor protection issues in crypto-asset markets in early-Q4 2023.

IOSCO Sets the Standard for Global Crypto Regulation

In line with IOSCO's established approach for securities regulation, the Crypto and Digital Asset Recommendations (CDA Recommendations) are addressed to relevant authorities and look to support jurisdictions seeking to establish compliant markets for the trading of crypto or 'digital' or 'virtual' assets (hereafter "crypto-assets" and read to include all relevant tokens) in the most effective way possible.

This consultation report proposes 18 policy recommendations that IOSCO plans to finalize in early Q4 this year to support greater consistency with respect to regulatory frameworks and oversight in its member

jurisdictions, to address concerns related to market integrity and investor protection arising from crypto-asset activities.

The recommendations have been developed under the stewardship of the IOSCO Board's Fintech Task Force (FTF) in accordance with IOSCO's CryptoAsset Roadmap published in June 2022.

The proposed recommendations are principles-based and outcomes-focused and are aimed at the activities performed by crypto-asset service providers (CASPs).

They apply IOSCO's widely accepted global standards for securities markets regulation to address key issues and risks identified in cryptoasset markets.

The proposed recommendations are activities-based and follow a 'lifecycle' approach in addressing the key risks identified in this report.

They cover the range of activities in crypto-asset markets that involve CASPs from offering, admission to trading, ongoing trading, settlement, market surveillance and custody as well as marketing and distribution (covering advised and non-advised sales) to retail investors.

The proposed recommendations do not cover activities, products or services provided in the so-called "decentralized finance" or "DeFi" area.

Policy Recommendations for Crypto and Digital Asset Markets

Consultation Report

The FTF DeFi workstream is considering issues in relation to DeFi and will publish a consultation report with proposed recommendations later this summer.

One of IOSCO's goals is to promote greater consistency with respect to how IOSCO members approach the regulation and oversight of crypto-asset activities, given the cross-border nature of the markets, the risks of

regulatory arbitrage and the significant risk of harm to which retail investors continue to be exposed.

IOSCO is also seeking to encourage optimal consistency in the way cryptoasset markets and securities markets are regulated within individual IOSCO jurisdictions, in accordance with the principle of 'same activities, same risks, same regulatory outcomes'.

The proposed recommendations also cover the need for enhanced cooperation among regulators.

They aim to provide a critical benchmark for IOSCO members to cooperate, coordinate and respond to cross-border challenges in enforcement and supervision, including regulatory arbitrage concerns, that arise from global crypto-asset activities conducted by CASPs that offer their services, often remotely, into multiple jurisdictions.

While the proposed recommendations are not directly addressed to markets participants, CASPs and all participants in crypto-asset markets are strongly encouraged to carefully consider the expectations and outcomes articulated through the proposed recommendations and the respective supporting guidance in the conduct of registered/licensed, and cross-border activities.

Money Laundering / Fraud / Scams

As with other crypto-assets, stablecoins may appeal to money launderers and criminals who do not wish to subject the proceeds of crime to traditional financial system oversight. Stablecoins are also likely to be perceived as more stable than other crypto-assets, so are more attractive to money launderers and criminals who do not wish to be as exposed to crypto-asset market volatility.

In light of the price instability of crypto-assets, because of their relatively more stable nature scammers have turned to stablecoins, and are soliciting stablecoins from their victims.

To read more:
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD734.pdf

EBA publishes Report on holdings of eligible liabilities issued by G-SIIs and O-SIIs

The European Banking Authority (EBA) published a report on the holdings by EU banks of minimum requirement for own funds and eligible liabilities (MREL) instruments issued by the most systemic European banks.

As of 31 December 2021, these holdings appear small and potential direct contagion risks are, therefore, limited.

In particular, more than half of the resolution banks in the sample have exposures to eligible liabilities issued by global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs) below 2% of MREL and 0.6% of the total risk exposure amount (TREA).

In addition, the report finds that, overall, the largest EU banks do not rely on other banks to place their MREL instruments. As of December 2021, G-SIIs and O-SIIs had placed a limited 3.7% of their eligible liabilities with banks in the sample, with seven banks out of 72 placing more than 20%.

As a consequence of these limited exposures, direct spill over effects from a possible bail-in appear limited.

The Report considered systemic crisis under two scenarios:

(i) the failure of G-SIIs and O-SIIs rated below investment grade and

(ii) the failure of the largest issuers of the sample. Under both scenarios, the contagion via direct exposures would not lead to a failure of any of the holders.

None of the banks would breach their Pillar 2 Requirement (P2R) under any of the two scenarios.

Yet, it should be noted that the Report does identify some outliers with higher-than-average exposure.

In particular, twenty-five banks report exposures above 8% of their MREL and six institutions report exposures above 20% of their MREL. Furthermore, the Report neither captures issuances by non-systemic banks nor considers the impact on banks with balance sheets below EUR 5bn – which limits its conclusions.

To read more: https://www.eba.europa.eu/eba-publishes-report-holdings-eligible-liabilities-issued-g-siis-and-o-siis

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1055437/Report%20on%20holdings%20of%20eligible%20liabilities%20%28Art.%20504a%20CRR%20II%29_final.pdf

EU-US Trade and Technology Council enhances cooperation in emerging technologies, sustainable trade and economic security

The European Union and the United States have held the fourth ministerial meeting of the EU-US Trade and Technology Council (TTC) in Luleå, Sweden.

It was co-chaired by European Commission Executive Vice-President Margrethe Vestager, European Commission Executive Vice-President Valdis Dombrovskis, United States Secretary of State Antony Blinken, United States Secretary of Commerce Gina Raimondo, and United States Trade Representative Katherine Tai, joined by European Commissioner Thierry Breton, and hosted by the Swedish Presidency of the Council of the European Union.

The EU and the US remain key geopolitical and trading partners. The EU-US bilateral trade is at historical highs, with over €1.55 trillion in 2022, including over €100 billion of digital trade.

On the occasion of the ministerial meeting, the EU and the US agreed on a list of key outcomes to advance transatlantic cooperation on emerging technologies, sustainable trade, economic security and prosperity, secure connectivity and human rights in the digital environment. Both parties also reaffirmed their unwavering commitment to support Ukraine.

Key outcomes of the 4th TTC ministerial meeting

Transatlantic cooperation on emerging technologies, connectivity and digital infrastructure

The EU and the US share the common understanding that Artificial Intelligence (AI) technologies hold great opportunities but can also present risks for our societies.

They showcased the first results in the implementation of the TTC Joint Roadmap for Trustworthy AI and risk management through dedicated experts' groups, working notably on the identification of standards and tools for trustworthy AI. Going forward, this work will include a focus on generative AI systems.

You may visit: https://digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management

digital-strategy.ec.europa.eu/en/library/ttc-joint-roadmap-trustworthy-ai-and-risk-management

POLICY AND LEGISLATION | Publication 01 December 2022

TTC Joint Roadmap for Trustworthy AI and Risk Management

The EU-US TTC Joint Roadmap aims to advance shared terminologies and taxonomies, but also to inform our approaches to AI risk management and trustworthy AI on both sides of the Atlantic.

The roadmap will help to build (as a next step) a common repository of metrics for measuring AI trustworthiness and risk management methods. It also holds the potential to inform and advance collaborative approaches in international standards bodies related to Artificial Intelligence.

Related topics

International relations

Artificial intelligence

Downloads

TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management — Download

The EU and the US have advanced work on semiconductors, implementing agreements on supply chain early warning and subsidies transparency.

They have put in place a mechanism to prevent subsidy races, deepened cooperation on their respective Chips Acts and will join forces in research to replace PFAS in semiconductor supply chains.

The EU and the US are advancing their work in the area of e-mobility.

They agreed on a common international standard on megawatt charging systems for the recharging of electric heavy-duty vehicles.

This will facilitate transatlantic trade and investment by reducing the manufacturing and deployment costs.

They also developed recommendations for the government-funded implementation of e-vehicle charging infrastructure.

The recommendations: https://joint-research-centre.ec.europa.eu/system/files/2023-05/Transatlantic_Technical_Recommendations_for_Government_Funded_Implementation_of_Electric_Vehicle_Charging_Infrastructure_0.pdf

May 2023

Transatlantic Technical Recommendations for Government Funded Implementation of Electric Vehicle Charging Infrastructure

EU-U.S. Trade and Technology Council

Working Group 2 - Climate and Clean Tech

Workstream: **Electro-mobility and Interoperability with Smart Grids**
Co-Chairs: Maria Cristina Russo, European Commission, and Julie Cerqueira, U.S. Department of Energy

Authors: **Keith Hardy,** U.S. Department of Energy, Argonne National Laboratory
Harald Scholz, European Commission, Joint Research Centre

Both parties have accelerated their cooperation towards a common vision and industry roadmap on 6G wireless communication systems and issued a 6G outlook, which sets out guiding principles and next steps to develop this critical technology.

The EU and US are continuing their efforts to accelerate the roll-out of secure and resilient connectivity projects in third countries and announced today new initiatives in Costa Rica and the Philippines.

Human rights and values in a changing geopolitical digital environment

The EU and US consider that online platforms should exercise greater responsibility in protecting and empowering minors.

Data access for researchers is key to help understand risks on online platforms and to advance understanding of the online ecosystem.

The EU and the US developed a list of high-level principles on the protection and empowerment of minors and data access for researchers, which are in line with the EU's Digital Services Act.

Both parties are also deeply concerned about Russia's strategic use of disinformation narratives, and foreign information manipulation and interference (FIMI) actions in third countries.

The EU and the US have issued a joint statement setting out actions to combat foreign information manipulation and interference in third countries, including a standard for structured threat intelligence and capacity building, particularly in Africa and Latin-America.

You may visit: https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en

TTC Ministerial

Foreign information manipulation and interference in third countries

Foreign information manipulation and interference (FIMI) and disinformation is an ever-changing security and foreign policy issue, with a fast-evolving and complex threat situation. Russia's strategic and coordinated use of such activity in the preparation and execution of its war of aggression against Ukraine has increased global attention to the ways in which aggressors manipulate the information environment, amidst global conflict. Intentional manipulation by malign actors of the information environment and public debate threatens the functioning of democracies and the well-being of societies around the world. We are increasingly faced with hostile campaigns manipulating global, regional, and local audiences by spreading chaos and confusion, aiming to undercut trust in well-established/proven facts, global partnerships and alliances, universal values and international human rights, and democratic norms and processes. We also see attempts to corrode the international, rules-based order and fora such as the UN Security Council through manipulative behaviour that undermines democratic institutions and values.

The European Union and the United States are mutually concerned about foreign information manipulation and interference and disinformation; the long-standing cooperation on this issue between us has contributed to a mutual understanding of the threat and close exchanges on effective responses which respect human rights. The Trade and Technology Council proved to be a crucial forum to add another, even more strategic layer to existing and operational cooperation. Against this background, and next to other ongoing work in various different fora, the European Union and the United States have taken a number of actions to increase transatlantic cooperation to proactively address foreign information manipulation and interference and disinformation, while upholding human rights and fundamental freedoms.

Transatlantic cooperation for easier, greener and safer trade

The EU and US are working to grow their €1.5 trillion worth of bilateral trade further by making it easier to trade and they have today taken steps to facilitate trade in key sectors.

They have extended mutual recognition for pharmaceutical goods to include veterinary medicines and updated the existing EU-US marine equipment mutual recognition rules.

Work will continue to facilitate conformity assessment in certain key sectors, such as machinery.

As part of their commitment to greener and fairer trade, the EU and US have agreed on a work programme for the Transatlantic Initiative on Sustainable Trade.

This will lead to closer cooperation on jointly advancing the green transition.

The newly-launched Clean Energy Incentives Dialogue will help ensure that EU and US incentive programs for a clean economy are mutually reinforcing.

The second principal-level session of the Trade and Labour Dialogue deepened the discussion on the eradication of forced labour from global supply chains, based on joint recommendations from social partners.

The EU and US continue their work on challenges impacting their security.

This includes aligning their respective regulations related to export restrictions on sensitive items to Russia and Belarus.

They continue to coordinate adjustments to control lists, discuss emerging technologies, and cooperate to ensure the non-proliferation of weapons of mass destruction.

The TTC reiterated the importance of robust foreign investment screening to address specific national security risks, and of coordination to diversify our supply chains, to address non-market policies and practices as well as economic coercion.

The EU and US continue to advocate for digital solutions to make trade easier and to promote the digital trade principles agreed in G7.

Background

The European Union and the United States launched the EU-US Trade and Technology Council (TTC) at their ministerial in Brussels on 15 June 2021.

The TTC serves as a forum for the EU and the US to coordinate approaches to address key trade and technology issues, and to deepen transatlantic cooperation in this realm based on shared democratic values.

The inaugural meeting of the TTC took place in Pittsburgh on 29 September 2021.

Following this meeting, 10 working groups were set up covering issues such as technology standards, artificial intelligence, semiconductors, export controls and global trade challenges.

This was followed by a second ministerial in Paris on 16 May 2022 and a third ministerial in College Park, Maryland, in December 2022.

The next meeting of the TTC is planned towards the end of the year hosted by the US.

To read more:
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2922

ESAs launch discussion on criteria for critical ICT third-party service providers and oversight fees

The European Supervisory Authorities (EBA, EIOPA and ESMA - ESAs) published a joint Discussion Paper seeking stakeholders' input on aspects of the Digital Operational Resilience Act (DORA).

This Discussion Paper follows the European Commission's request for technical advice on the criteria for critical ICT third-party providers (CTPPs) and the oversight fees to be levied on them.

Interested stakeholders are invited to provide their input by 23 June 2023.

The Discussion Paper is separated into two parts:

- Proposals covering the criteria to be considered by the ESAs when assessing the critical nature of ICT third-party service providers, in particular, a number of relevant quantitative and qualitative indicators for each of the criticality criteria, along with the necessary information to construct such indicators.

- Proposals in relation to the amount of the fees levied on CTPPs and the way in which they are to be paid, in particular the types of expenditure that shall be covered by fees as well as the appropriate method, basis and information for determining the applicable turnover of the CTPPs, which will form the basis of fee calculation. The ESAs are also seeking input on the fee calculation method and other practical issues regarding the payment of fees.

In light of the two delegated acts envisaged in the Regulation on Digital Operational Resilience for the Financial Sector ("DORA"), the European Commission has requested ('CfA') the ESAs' technical advice to further

specify the criteria for critical ICT third-party service providers (CTPPs) and determine the fees levied on such providers.

The ESAs shall deliver their technical advice by 30 September 2023.

The purpose of this discussion paper is to consult market participants, in an open and transparent manner, on the ESAs' proposals towards the specific issues listed in the CfA.

The provided answers during this consultation will be taken into account in the ESAs' advice.

The first part of this discussion paper presents proposals in relation to the elements needed to specify further the criteria referred to in Article 31(2) of the DORA to be considered by the ESAs when assessing the critical nature of ICT third-party service providers.

In particular, a number of relevant quantitative and qualitative indicators are proposed for each of the criticality criteria, along with the necessary information to build up and interpret such indicators.

Moreover, a number of minimum relevance thresholds are proposed for the quantitative indicators, where possible and applicable.

These are thresholds below which the degree to which the factor is in play would not be considered sufficiently relevant to trigger the indicator for inclusion in any criticality assessment methodology.

It is important to note that these proposals relate to the identification of indicators relevant to assessing criticality and not to the methodology for that assessment, including the materiality and interaction of the different criteria.

The expected type and total number of CTPPs, the details of the designation procedure as well as the related methodology, are explicitly excluded from this discussion paper and shall be defined at a later stage in the context of the implementation of the oversight framework.

The second part of this discussion paper presents proposals in relation to the amount of the fees levied on CTPPs and the way in which they are to be paid. In particular, proposals are made on the necessary types of expenditure that shall be covered by fees, the appropriate method, basis and available information for determining the applicable turnover of the CTPPs (which will form the basis of fee calculation) as well as the method of fee calculation and other practical issues regarding the payment of fees.

In addition, a proposed financial contribution for voluntary opt-in requests is included in the paper.

Market participants are invited to provide their feedback on the proposals in this discussion paper, which will be considered by the ESAs in finalising the joint technical advice to the European Commission. Responses should be provided through a form available on the ESAs' websites by 23 June 2023 at the latest.

To read more: https://www.eiopa.europa.eu/esas-launch-discussion-criteria-critical-ict-third-party-service-providers-and-oversight-fees-2023-05-26_en

Central bank digital currencies: ongoing policy perspectives

Bank of Canada	Swiss National Bank
European Central Bank	Bank of England
Bank of Japan	Board of Governors Federal Reserve System
Sveriges Riskbank	Bank for International Settlements

A group of central banks, together with the Bank for International Settlements, are working together to explore central bank digital currencies (CBDCs) for the public ("general purpose" or "retail" CBDC).

Since publishing:

(i) a report in October 2020 setting out the common foundational principles and core features of a CBDC; and

(ii) an executive summary and three detailed reports on system design and interoperability, user needs and adoption and financial stability implications in September 2021, the group has continued to share ideas and perspectives on similar themes, which are summarised in this note.

Background/motivation

Most central banks are now exploring CBDCs, and more than a quarter of them are developing or running concrete pilots (Kosse and Mattei (2022)).

Many of our jurisdictions are examining whether there is a need to ensure ongoing retail access to central bank money at a time of profound, ongoing changes across finance, technology and society.

The motivation for introducing a retail CBDC may rest primarily on the role of central bank money as a public good.

At the same time, the introduction of a CBDC could be an innovative opportunity for the monetary system.

It is in this context that the central banks contributing to this group have continued their collaboration to deepen the practical policy and technical analysis of CBDC.

Annex 1 draws out some elements of the discussion in 2022. Some of the members of this group are approaching a point where they may decide on whether or not to move to the next stage of their CBDC work.

This may include deeper investment in design decisions relating to technology, end user preferences and business models, while leaving open the decision on whether to issue CBDC.

To date, none of our jurisdictions have yet decided to proceed with the issuance of a retail CBDC. CBDC issuance and design are sovereign decisions for relevant authorities based on their assessments and a jurisdiction's circumstances. However, there has been value in working collectively on common issues.

To read more: https://www.bis.org/publ/othp65.pdf

After the crypto-winter, the spring of crypto-assets regulation and supervision

Denis Beau, First Deputy Governor of the Bank of France, at the World Bank Global Payments Week 2023 "The Future of Payments", Marrakesh.

Dear colleagues from the World Bank, Ladies and Gentlemen,

According to some commentators, in a context of cascading bankruptcies (i.e. Terra /Luna, Celsius, Three Arrows, Genesis, BlockFi, FTX), the crypto ecosystem may have entered a so-called **"crypto-winter".**

I don't know if this winter is going to last but I believe that it should be seen as **"spring time"** by regulators and supervisors, whose initiatives should be burgeoning.

Recently, many countries have indeed sped up their regulatory work within their jurisdiction.

However, we have also seen variances in combining three regulatory approaches:

- banning crypto-asset activities;
- containing and isolating them from traditional finance and the real economy, which implies banning certain specific aspects and practices (e.g. advertising);
- regulating the crypto-asset market, either by assimilating crypto-assets to traditional financial assets and applying the corresponding existing regulatory regime, or by adopting a dedicated regulation (e.g. on stablecoins).

With the exception of China, the world's major economies and currency zones have developed or are in the process of adopting a combination of the last two approaches, based on the principle of "same activities, same risks, same rules". As a blunt banning of crypto-asset activities is not seen as an option for most, for a number of reasons, starting for instance with the belief in France that it would most likely lead to regulatory arbitrages

between jurisdictions, most of the attention at national and international level has been put on "what?" (what activities and what risks) and "how?" (by which means) to regulate.

In my short introductory remarks today, I would like to share with you my perspective, as the organisers of this Global Payments Week Conference have kindly suggested, speaking from the standpoint of a central bank in charge of ensuring financial stability, on the types of risks associated with crypto-activities that particularly need to be considered for regulation and supervision, and the importance of a convergent and coordinated regulatory approach on crypto-assets at the international level.

To read more:
https://acpr.banque-france.fr/sites/default/files/medias/documents/20230518_gpw2023_keynote_speech_dbeau_en.pdf

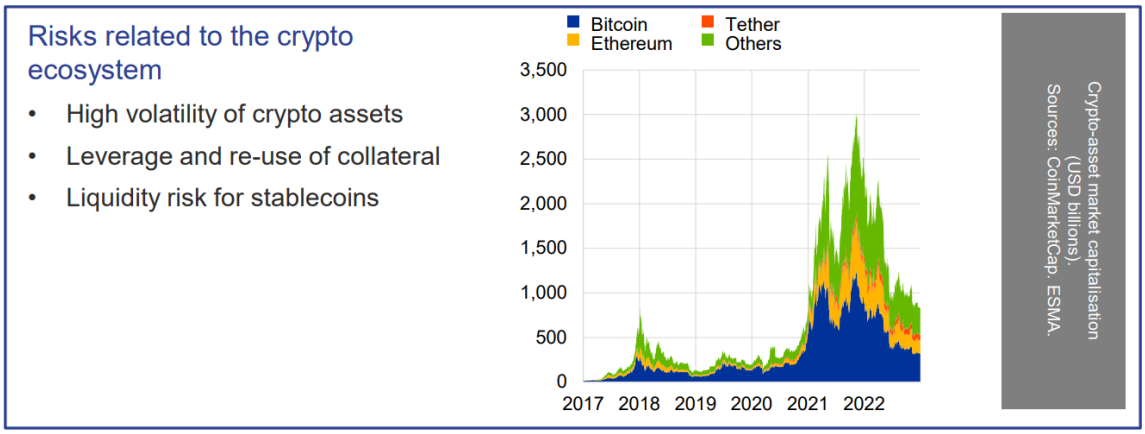
ESRB publishes EU Non-bank Financial Intermediation Risk Monitor 2023

ESRB
European Systemic Risk Board
European System of Financial Supervision

The European Systemic Risk Board (ESRB) has today published the EU Non-bank Financial Intermediation Risk Monitor 2023 (NBFI Monitor).

This is the eighth edition in an annual series monitoring systemic risks and vulnerabilities associated with investment funds and other financial institutions.

For the first time, this edition extends the monitoring universe to crypto-assets and associated intermediaries (namely stablecoins, centralised finance platforms and decentralised finance protocols) as they provide financial intermediation and can be exposed to the same vulnerabilities and financial risks as the traditional financial sector.



Source: ESRB.

Financial stability risks increased overall in 2022, owing to rising geopolitical tensions, higher-than-expected inflation and tightening financial conditions. Against this backdrop, the NBFI Monitor highlights three main risks and vulnerabilities.

An economic slowdown and tightening financial conditions could increase credit risk. This is particularly relevant for investment funds exposed to low-rated bonds and loans, financial vehicle corporations engaged in securitisation and financial corporations engaged in lending.

If credit risk were to materialise it could lead to losses, which in the case of investment funds could result in large outflows and liquidity strains.

Market liquidity risk could put further pressure on non-bank financial intermediaries engaged in liquidity transformation. Several indicators show that liquidity conditions in EU bond markets deteriorated in 2022.

Alongside cyclical liquidity risk, the monitor also identifies persistent challenges related to structural changes in liquidity provision and demand. These structural changes are linked, for instance, to open-ended funds offering daily redemptions.

Excessive use of leverage could amplify liquidity and market risks, lead to contagion and magnify shocks to financial stability. This vulnerability affects the traditional non-bank entities discussed in the report as well as crypto intermediaries, since both use leverage and rely on collateral.
To help identify risk, the NBFI Monitor 2023 includes two special features.

The special feature on stress related to liability-driven investment (LDI) strategies provides insights into how risks associated with liquidity and leverage materialise. It investigates the extent to which EU-domiciled LDI funds were prepared for margin and collateral calls related to the rise in interest rates.

The second special feature focuses on vulnerabilities affecting crypto-assets and associated intermediaries that are similar to those among traditional non-bank financial intermediaries. It considers how the crypto ecosystem uses leverage and engages in credit intermediation, and liquidity and maturity transformation. It also examines its interconnectedness.

Crypto trading platforms offer a very high level of leverage to clients although actual use has been trending downward. Leverage amount offered by selected crypto trading platforms

Trading platform	Maximum leverage offered	Products used in leverage
BitMEX	100x	Perpetual swaps
Kraken	5x	Crypto-assets
FTX	20x	Futures, leveraged tokens
eToro	2x	Contracts for differences
Bitlevex	100x	Options
Bybit	100x	Perpetual swaps and futures
Binance	125x	Leveraged tokens

*Sources: Decrypting financial stability risks in crypto-asset markets, L. Hermans et al., **ECB Financial Stability Review**, May 2022.*

To read more:
https://www.esrb.europa.eu/pub/pdf/reports/nbfi_monitor/esrb.nbfi202306~58b19c8627.en.pdf

Joint European Supervisory Authority Discussion paper on DORA

In light of the two delegated acts envisaged in the Regulation on Digital Operational Resilience for the Financial Sector ("DORA"), the European Commission has requested ('CfA') the ESAs' technical advice to further specify the criteria for critical ICT third-party service providers (CTPPs) and determine the fees levied on such providers.

The ESAs shall deliver their technical advice by 30 September 2023.

The purpose of this discussion paper is to consult market participants, in an open and transparent manner, on the ESAs' proposals towards the specific issues listed in the CfA. The provided answers during this consultation will be taken into account in the ESAs' advice.

The first part of this discussion paper presents proposals in relation to the elements needed to specify further the criteria referred to in Article 31(2) of the DORA to be considered by the ESAs when assessing the critical nature of ICT third-party service providers.

In particular, a number of relevant quantitative and qualitative indicators are proposed for each of the criticality criteria, along with the necessary information to build up and interpret such indicators. Moreover, a number of minimum relevance thresholds are proposed for the quantitative indicators, where possible and applicable.

These are thresholds below which the degree to which the factor is in play would not be considered sufficiently relevant to trigger the indicator for inclusion in any criticality assessment methodology.

It is important to note that these proposals relate to the identification of indicators relevant to assessing criticality and not to the methodology for that assessment, including the materiality and interaction of the different criteria.

The expected type and total number of CTPPs, the details of the designation procedure as well as the related methodology, are explicitly excluded from this discussion paper and shall be defined at a later stage in the context of the implementation of the oversight framework.

The second part of this discussion paper presents proposals in relation to the amount of the fees levied on CTPPs and the way in which they are to be paid. In particular, proposals are made on the necessary types of

expenditure that shall be covered by fees, the appropriate method, basis and available information for determining the applicable turnover of the CTPPs (which will form the basis of fee calculation) as well as the method of fee calculation and other practical issues regarding the payment of fees.

In addition, a proposed financial contribution for voluntary opt-in requests is included in the paper. Market participants are invited to provide their feedback on the proposals in this discussion paper, which will be considered by the ESAs in finalising the joint technical advice to the European Commission.

To read more: https://www.esma.europa.eu/sites/default/files/2023-05/ESAs_Discussion_Paper_CfA_DORA_criticality_criteria_and_OVS_fees.pdf

Joint European Supervisory Authority
Discussion paper on DORA

Discussion paper on the joint ESAs advice to the European Commission on two delegated acts specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers, under Articles 31 and 43 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operation resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

NPSA Changes to Insider Risk Definitions

National Protective Security Authority

Background

Definitions enable us to have a common understanding of a word or subject; they allow us all to be on the same page and facilitate clear lines of communications. Having clear definitions of insider risk terminology is vital to support new and existing NPSA customers, who will have varying levels of knowledge in the subject area.

NPSA (formerly CPNI) has, until now, defined an insider as “a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes”.

This definition was utilised for the purposes of the research underpinning the 2009 and 2013 Insider Data Collection Study.

For the reasons outlined below, we felt it was the right time to refresh how we define our terms in relation to insider risk.

What is changing?

From May 2023 onwards NPSA will be utilising the following definitions through our various advice delivery and communications channels;

1. **Insider -** Any person who has, or previously had, authorised access to or knowledge of the organisation’s resources, including people, processes, information, technology, and facilities.

2. **Insider Risk -** The likelihood of harm or loss to an organisation, and its subsequent impact, because of the action or inaction of an insider.

3. **Insider Threat -** An insider, or group of insiders, that either intends to or is likely to cause harm or loss to the organisation.

4. **Insider Event -** The activity, conducted by an insider (whether intentional or unintentional) that could result in, or has resulted in, harm or loss to the organisation.

Below summarises how the NPSA definition of insider will be communicated:

Rationale for changing
Insider risk comes from everyone 'inside' your organisation

NPSA's key message that we want to convey is that if you have people, you have risk. We therefore want all our customers to be insider risk ready.

Our extensive and ongoing research indicates that harm or loss to an organisation could be as a direct result of unintentional activity from those with legitimate access, as well as from personnel who intend to exploit their access.

Being research led

It's vital as an NTA we keep challenging our existing position. Following a rapid research review of literature, we found that most 'insider' definitions do not include exploitation or malice in the definition.

The definitions usually relate to access rather than exploitation. Close partners (e.g. CERT, US Government) similarly have also made recent changes to their definitions in a way aligns with NPSA's forthcoming changes.

Developing a consistent lexicon

To date, NPSA has only communicated one definition which related to an 'Insider'. This definition, however, failed to separate the community within which insider risk sits within and from those specific individuals that become an insider threat. This has resulted in language being utilised interchangeably and often in the wrong context. We want to change this, so we are all communicating in the same way.

Our next steps

Communications

NPSA Personnel & People Security Research & Development Team will be working alongside our communication colleagues to update existing guidance and products on our website to ensure it is consistent with this new terminology.

Please bear with us whilst these changes are made. This document will be made available on the NPSA Website under the Insider Risk Page. We ask that NPSA customers refer to the revised definitions contained within this update.

Evaluation

It's vital we evaluate whether changes to NPSA's Insider lexicon results in greater clarity for our customers and supports you in understanding and mitigating this risk in a coherent way. We would welcome your feedback either via utilising the contact us form or providing feedback here.

To read more: https://www.npsa.gov.uk/blog/personnel-security/npsa-changes-insider-risk-definitions

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.

Solvency II Association

At every stage of your career, our association provides networking, training, certification, information, updates, alerts, and services you can use. Join us. Stay current. Take advantage of the new opportunities. Read our monthly newsletter. Get certified.

You can explore what we offer to our members:

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

2. Monthly Updates – Visit the Reading Room of the association at: https://www.solvency-ii-association.com/Reading_Room.htm

3. Training and Certification – You may visit: https://www.solvency-ii-association.com/CSiiP_Distance_Learning_Online_Certification_Program.htm

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