London Stock Exchange Group Response to the CPMI-IOSCO consultative report on Guidance on cyber resilience for financial market infrastructures

London Stock Exchange Group (LSEG) welcomes the opportunity to comment on the Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (CPMI-IOSCO) Consultative report on Guidance on cyber resilience for financial market infrastructures (the Consultative Report). We recognise the ongoing commitment of CPMI-IOSCO to support financial stability and economic growth by providing further guidance to the Principles for Financial Markets Infrastructures (the "Principles").

As one of the largest operators of safe, efficient and diversified international market infrastructures, London Stock Exchange Group has been undertaking prudent risk management across all operational risk areas including cyber resiliency. We recognise that operational resilience can be a determining factor in the overall resilience of the financial system and broader economy. Due to the interconnectedness of financial market infrastructures (FMIs), cyber attacks in the financial sector have the potential to create widespread financial instability. For this reason, we fully support the industry's ongoing efforts to enhance FMIs' cyber resiliency. In particular, we welcome CPMI-IOSCO's international effort to harmonise the cyber resilience standards across jurisdictions. In our view it is crucial to ensure that an **internationally consistent approach** is taken in order **to mitigate against any regulatory arbitrage**. Further, we believe that such an approach is especially **important in view of the upcoming international framework for CCPs' Recovery and Resolution** of which we consider that non-default losses will be a key component.

Executive Summary

Outline and relationship with the Principles

- LSEG is pleased that the Consultative Report complements and further clarifies the Principles and does not seek to establish additional standards. We agree that the guidance should help FMIs to achieve robust cyber resilience according to their own operational framework and size. In particular, they should be **goal-orientated** so that they can be **implemented in a proportionate manner** and avoid being overly prescriptive, particularly by requiring additional formal documents and seeking to establish very specific conditions and timeframes.

Broad relevance and collaboration

- In relation to the **broad relevance** of the guidance and CPMI-IOSCO's encouragement for FMIs to collaborate with their stakeholders, we wish to stress that in certain sensitive areas (for example, data sharing) the recommended collaboration may not be appropriate as it may lead to **additional risk exposures**.
- Further, LSEG notes that there are limits to what assurances FMIs can give in relation to the **compliance and conduct of various stakeholders or other third party participants** in relation to their cyber security procedures.

Governance

- While we support the proposed guidance relating to the skill set of the board and senior management of the FMI, it is important to note that, due to the **current shortage of cyber skills in people of board and/or senior management level experience**, complying with this

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com

may require significant training and time. We would encourage CPMI-IOSCO to take such factors into account when devising the skill set requirements of those with cyber responsibility at board level.

Response and Recovery

- Regarding the proposed **response and recovery procedures,** it is important to note that requiring FMI's to have procedures in place to ensure the **resumption of critical operations within two hours** of the cyber disruption and to enable the relevant FMI to **complete settlement by the end of the day of such disruption** may have unintended consequences. Indeed, a hard deadline could force FMIs to restore operations sooner than they would otherwise consider it safe to do so. This may **exacerbate the situation** because if the system's integrity is compromised then successful recovery within 2 hours may not necessarily mean that the restored system is "fit for purpose" (for example, the operational system may be recovered but the data may still be corrupted). We would therefore encourage the guidance to require the restoration of the system to an approved operational state 'without delay'.

LSEG would like to ask for further clarifications and suggest alternatives in the following areas:

1 Introduction

The Consultative report correctly recognises that certain cyber attacks can **render some risk management and business continuity arrangements ineffective** (*Cyber risks are unique, 1.1.3c).* We would encourage CPMI-IOSCO to consider this principal further when considering the timeframe in which an FMI can restore its operations. In this regard, please see our response to section 6 below.

We support CPMI-IOSCO's efforts to ensure that FMIs continue to adapt, evolve and improve their cyber resilience capabilities and to ensure relevant third party stakeholders are aware of the FMI's cyber reliance objectives and support their implementation (1.3.3 *Stakeholder considerations* and 1.3.5 *Ongoing efforts to improve FMIs' cyber resilience*). However, to ensure that the guidance can be realistically implemented by FMIs, it should recognise the **limitations on a FMI's ability to fully control certain events,** for example, with regard to operations of interconnected entities after an incident, where FMIs should "ensure that such entities can resume operations as soon as it is safe and practicable to do so" (Contagion, 6.4.2) and FMI's should "ensure that its service providers meet the same high level of cyber resilience they would need to meet if their services were provided by the FMI itself" (4.3.1 Risks from interconnections)

We believe that these provisions should be applied in a proportionate manner and that this may be achieved by amending the CPMI-IOSCO guidance to be **goal-oriented, as opposed to only principle-oriented** (*1.2.2 Principle based*). Where appropriate, the guidance should allow for sufficient flexibility for FMIs to determine how to achieve the goals in proportion to the level of risk generated by the nature of their activity and their size. In monitoring compliance with the guidance, we believe that national competent authorities (NCAs) will have an important role to play in setting appropriate timelines *(1.3.6 Guidance and implementation in the context of relevant legal framework.)*

Currently, there are several work streams dealing with cyber resilience. In the European Union, the Network and Information Security (NIS) directive will soon enter into force. In the United States, the Commodity Futures Trading Commission (CFTC) is consulting on some aspects of cyber resilience. In France, the "Loi de Programmation Militaire" (article 22), which is a new framework of security requirements for all French critical operators, will soon enter into force. It is crucial that CPMI-IOSCO

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com

uses its unique global position to ensure that the guidance proposed is consistent with such rules and does not prescribe an over-extension of such rules.

2 Governance

We believe that in order to simplify the governance requirements and to ensure that stakeholders can access the correct information at all times, **one simplified document addressing both the cyber resilience framework and the cyber resilience strategy of an FMI would be appropriate** in many cases. (*2.2.1 Cyber resilience strategy & 2.2.2 Cyber resilience framework*). We would encourage CPMI-IOSCO to consider removing the requirement to have separate documents addressing the cyber resilience framework and the cyber resilience strategy of an FMI in the final guidance. If CPMI-IOSCO considers that maintaining a separate cyber resilience framework and cyber resilience strategy is necessary, we would recommend that the guidance set out the reasons for such separation.

We support a **harmonised, industry-based risk assessment methodology** (including metrics and maturity models) to assess the adequacy of, and the levels of adherence to, an FMI's cyber resilience framework. However, we would encourage CPMI-IOSCO to clarify in the guidance that, depending on the size and risk profile of the relevant FMI, such FMI should **assess whether it may be appropriate to conduct compliance programmes and audits for each entity**, against each participant, vendor, partner, service provider and vendor product. Further, **the frequency of such compliance programmes and audits should depend on the FMI's assessment of applicable risks**. (*2.2.8 Audits and compliance*).

Whilst we agree with the guidance proposed for the **knowledge and skill set of the board and senior management** of the FMI, it is important to note that, due to the **current shortage of cyber skills in people of board and/or senior management level experience**, complying with this may require significant training and time. We would encourage CPMI-IOSCO to recognise in the guidance that appropriate governance arrangements for particular FMIs should vary **depending on the level of risk generated by the nature of their activity and their size**. For example, it may be more appropriate for certain members of the board and senior management to obtain specific industry certifications to demonstrate that they have the "appropriate skills and knowledge to understand and manage the risks posed by cyber threats" and to appoint specific posts such as Chief Information Security Officer (CISO) for larger FMIs than smaller ones.(*2.3.3 Skills*)

The level of **independence required from the senior executive** responsible and accountable overall for the cyber resilience framework **should also be clarified**, and we would welcome further best practice recommendations from CPMI-IOSCO on how such independence should be reflected in an FMI's budget allocation, remuneration and reporting line structures, and whether an external (consultant) or an internal hire may be suitable for such role. (*2.3.4 Accountability)*.

3 Identification

We recognise the **interdependent environment** in which FMIs operate and agree that the ability of an FMI to understand its internal situation and external dependencies is key to being able to respond to cyber threats. However, we believe that CPMI-IOSCO should provide clearer guidance on the level of co-ordination required between an FMI and external stakeholders. For example, information-sharing with stakeholders may be inappropriate in certain cases, for example, where this involves the disclosure of confidential or competitively-sensitive information, and may therefore lead to additional risk exposures for the FMI. (*3.3. Interconnection*).

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com

In addition, whilst we agree that it is important for an FMI to understand its interconnected links, it is the **identification and understanding of the types of threat posed and the methods used to disrupt services** that is key to ensuring the stability of the FMI's ecosystem. The guidance should therefore recommend that FMIs focus resources on identifying potential threats and disruption methods so that they can test their systems appropriately and be in a better position to defend an attack.

4 Protection

We would encourage CPMI-IOSCO to consider the abundance of legacy systems in the markets. While the systems used by FMIs themselves are often up to date, the same cannot be guaranteed for every entity within the FMI's ecosystem. Therefore, although **new systems can implement resilience by design, it would prove cumbersome and require substantial redesigning to implement the same level of resilience into legacy systems**. It would be useful to clarify in the guidance what constitutes rigorous testing against standards for these environments and whether undertaking third party assurance testing would suffice for this purpose. (*4.2.2 Resilience by design*)

We agree with CPMI-IOSCO's recommendation that FMIs should maintain a strong ICT control environment. However, we would encourage CPMI-IOSCO to reflect in the guidance that the different FMIs have different degrees of maturity and therefore the level of ICT controls should be handled proportionally. LSEG agrees that the guidance should establish minimum levels of ICT controls requirements for all FMIs, but not be too prescriptive, in order to allow each FMI flexibility in determining appropriate ICT controls to address the relevant cyber risks.

To require **FMIs to ensure that service providers meet the same standards of cyber resilience** as if the FMI provided the service itself, imposes a heavy burden on the FMI, as the FMI may not be able to accurately simulate cyber resilience standards for services that fall outside of its scope and that it therefore outsources. *(4.3.1 Risks from interconnections)* In this regard, we encourage CPMI-IOSCO to clarify that the guidelines impose a proportionate standard on FMIs, for example, that this requirement only applies to those service providers that pose a risk to the FMI's critical services (i.e. "critical services providers"). Further, the guidance should specify the standards that FMIs need to meet to comply with this requirement. CPMI-IOSCO should specify whether obliging FMI's service provider to provide evidence of its own compliance with the cyber resilience guidelines would be sufficient.

5 Detection

LSEG encourages CPMI-IOSCO to specify in the guidance whether FMIs are required to implement specific **minimum standards in their detection capabilities** (*5.2.2 Comprehensive scope of monitoring*), for example, whether FMIs should operate an Intrusions Detection System (IDS) or Security Information & Event Management (SIEM) capability . In addition, it is important to note that smaller and medium-sized firms may have more limited detection capabilities due to a lack of adequate resources or specialist threat intelligence capability. We would therefore encourage CPMI-IOSCO to consider such limitations when proposing any such minimum standards.

6 Response and Recovery

We agree that FMIs should have robust **response and recovery procedures** in place to respond to cyber attacks. However, it is important to note that requiring FMI's to have procedures in place to ensure the **resumption of critical operations within two hours** of the cyber disruption and to

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com

enable the relevant FMI to **complete settlement by the end of the day of such disruption** may have unintended consequences. (*6.2.2 Resumption within two hours*).

It may take some time to perform a thorough investigation following detection of a successful cyber attack and to determine the extent of the damage before any remediation action can be taken. Implementing the two hours requirement in national law could therefore force FMIs to restore operations too quickly. LSEG has demonstrated it can recover critical services within 2 hours and, where requested, has demonstrated such capability to its regulators on an annual basis. However, the primary focus of cyber resilience strategies should be on ensuring the "integrity" of the systems and data before and after recovery as well as confidentiality and availability of such data. If the system's integrity is compromised then successful recovery within 2 hours may not always be long enough to ensure that the recovered system, and the data within it, accurately reflects the system's pre-attacked state. We would therefore encourage the guidance to require the restoration of the system to an approved operational state 'without delay'. LSEG also encourages CPMI-IOSCO to give further guidance on the point at which the two hours would start to run (i.e. from when the attack was discovered or following completion of investigation).

In addition, the guidance should recognise that, in a cyber incident affecting the integrity of the system, **even the "golden copy" of data kept may be corrupted.** (*6.3.2 Data integrity*) We could encourage CPMI-IOSCO to provide further guidance on measures to ensure the golden copy is fit for purpose.

Once a successful cyber attack is identified, FMIs should be able to receive **clean data from relevant third parties or participants, with whom FMIs have set up data sharing agreements** in advance (*6.4.1 Data Sharing Agreements*). LSEG believes that FMIs cannot "ensure" that they will receive such clean data from third parties (i.e. it is out of FMIs' control) and the guidance should be redrafted to reflect this.

LSEG has the capability to divert non-clean traffic in the event of a denial-of-service attack (affecting availability), allowing good traffic to be received. This obligation lies with LSEG in events of this type, not a third party. CPMI-IOSCO should specify the expectations from the data sharing agreements, what is considered a timely manner and the consequences of "unclean" data being received.

The guidance also encourages FMIs to work together with interconnected entities to **ensure they can resume operations** as soon as it is safe and practicable to do so. We would like to reiterate that FMIs have limited ability to "ensure" third party behaviour. (6.4.2 Contagion)

7 Testing

We support the proposal for FMIs to implement a comprehensive testing programme and where applicable, include relevant external stakeholders. (*7.2.1 Testing programme*) However, we believe that the guidance should make it clear that **FMIs are not required to conduct tests in production environments which may adversely impact daily operation** and can test in controlled or replicated mirrored environments such as pre-production.

8 Situational awareness

LSEG encourages CPMI-IOSCO to specify that active **participation in information-sharing groups and collectives in the event of an incident should remain voluntary**. (*8.3.2 Information-sharing groups*) Mandating information-sharing may pose increased risks to the FMI and affect its reputation, especially where such information is confidential or competitively-sensitive.

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com

9 Learning and evolving

We support a **harmonised, industry-based risk assessment methodology** (metrics and maturity models) *(9.3.1 Metrics).* We encourage CPMI-IOSCO to give non-mandatory guidance on a list of appropriate metrics and methodology, allowing sufficient flexibility for FMIs.

**

About London Stock Exchange Group

London Stock Exchange Group (LSE.L) is a diversified international market infrastructure and capital markets business sitting at the heart of the world's financial community. The Group can trace its history back to 1698.

The Group operates a broad range of international equity, bond and derivatives markets, including London Stock Exchange; Borsa Italiana; MTS, Europe's leading fixed income market; and Turquoise, pan-European equities MTF. It is also home to one of the world's leading growth markets for SMEs, AIM. Through its platforms, the Group offers international business and investors unrivalled access to Europe's capital markets.

Post trade and risk management services are a significant part of the Group's business operations. In addition to majority ownership of multi-asset global CCP operator, LCH.Clearnet Group, LSEG operates CC&G, the Italian clearinghouse; Monte Titoli, the T2S-ready European settlement business; and globeSettle, the Group's newly established CSD based in Luxembourg.

The Group is a global leader in indexing and analytic solutions. FTSE Russell offers thousands of indexes that measure and benchmark markets around the world. The Group also provides customers with an extensive range of real time and reference data products, including SEDOL, UnaVista, and RNS.

London Stock Exchange Group is a leading developer of high performance trading platforms and capital markets software for customers around the world. Currently, over 40 organisations and exchanges use

Contact: Beata Sivak: BSivak@lseg.com; Eve Chen: Eve.Chen@lchclearnet.com; Natalie Caldwell: Natalie.Caldwell@lchclearnet.com