CPMI-IOSCO Consultative Paper: *Guidance on Cyber Resilience for Financial Market Infrastructures*

ASX RESPONSE TO CPMI-IOSCO FEBRUARY 2016

ASX

Contacts

For general enquiries, please contact:

Anna Campbell – General Manager,
Regulatory Assurance
T +61 (0)2 8298 8072
E anna.campbell@asx.com.au

Daryn Wedd – General Manager,
Technology Governance
T +61 (0)2 9227 0978
E daryn.wedd@asx.com.au

CONTENTS

Introduction

ASX Group (ASX) would like to thank CPMI and IOSCO for the opportunity to respond to Consultative Paper: Guidance on cyber resilience for financial market infrastructures (November 2015), (the "Cyber Guidance").

ASX recognises the critical role financial market infrastructures (FMIs) play in promoting financial stability and the importance of appropriate cyber resilience capabilities in order to manage cyber risks effectively.

ASX understands that cyber resilience is of significant importance to all stakeholders within the financial services industry and supports the enhancement of the Principles for Financial Market Infrastructures to ensure a coordinated regulatory approach to cyber security on a global level.

Overview

CPMI-IOSCO has identified a range of requirements which ASX believes are appropriate. The tables under "ASX response to consultation recommendations" provide our views on the recommendations provided in the Cyber Guidance, section by section.

We highlight a number of areas of particular importance to ASX below:

Ultimate responsibility

ASX has four FMIs in its corporate group. We believe that the most practical approach for an organisation with multiple FMIs is for the group's parent entity or Board (or Board Committee) to have ultimate responsibility for cyber resilience matters. Clearly documented governance arrangements could set out the arrangements for responsibility of cyber resilience matters for the entire group. ASX further believes that duplication of individual cyber resilience strategies and/or frameworks for each FMI under a group arrangement would be inefficient and thus supports a combined approach.

Interconnections

ASX understands the need to take an encompassing view of cyber threats facing an FMI's ecosystem. In doing so, ASX recognises that there are limitations to the extent that an FMI can control or influence the cyber risks borne by other participants in that ecosystem and therefore believes that an FMI's responsibility should amount to management of their own risks, while communicating with other stakeholders in the ecosystem, as appropriate.

Resuming Operations

ASX recognises that resumption of critical operations, as rapidly as possible in the event of a disruption, is crucial in promoting financial stability. ASX notes that many cyber-related investigations may take a significant amount of time to establish the root cause of a disruption and believe that a requirement to resume operations within two hours may not always be possible. ASX considers that it is important to resume the operation of critical systems as soon as it is both safe and reasonably practicable.

Disclosure

While we support, in principle, an approach to information-sharing and continuous improvement, ASX considers that it is fundamentally important that FMIs are not required to make any prescribed disclosure wherever it could lead to the release of commercially sensitive information. Such disclosure would only elevate the risk of cyber threat by exposing potential vulnerabilities in the processes and systems which constitute the cyber resilience infrastructure of an FMI.

Implementation

ASX notes that the Cyber Guidance does not contain a date, or period, for implementation. If CPMI-IOSCO intends to establish an implementation date, ASX requests a transitional period of at least 6 months for FMIs to comply with the new requirements. Where recommendations require a technology build or deployment of additional services, the transitional period required may be longer.

ASX response to consultation recommendations

Governance

Cyber Guidance Reference	Comment
2.2.1 Cyber resilience strategy	ASX believes that the best approach to managing cyber risk involves a whole-of-organisation response. ASX has four FMIs in its corporate group. Requiring each FMI board to individually approve a cyber resilience strategy/ framework creates duplication and is inefficient. A practical approach for corporate groups with multiple FMIs, such as ASX, is for the group's parent entity (which may not be an FMI) Board or Board Committee to have responsibility for cyber matters. Clearly documented governance arrangements could set out this body's responsibility for cyber resilience matters for the entire group, and how the boards of the FMIs are consulted on and kept informed of relevant matters. ASX recommends that the Cyber Guidance be amended to explicitly recognise this approach for FMIs that are part of corporate groups.
2.2.1 Cyber resilience strategy *&* *2.3.1 Ultimate responsibility*	ASX recognises the importance of appropriate Board-level oversight of cyber resilience matters. The Cyber Guidance implies that FMIs should have two separate documents, a cyber resilience strategy (ratified by the Board) and a cyber resilience framework (endorsed by the Board). The difference between ratification and endorsement is not clear. Separating strategy and framework documents may not be practical for all FMIs. Some may see the two as inextricably connected. Different FMIs will take different approaches to overseeing their organisation's response to cyber resilience. ASX recommends that the Cyber Guidance be amended to clarify whether there is any difference in the expectation of Board-level ratification and endorsement, and explicitly provide FMIs with the flexibility to create these documents in the form that best suits their individual requirements. For example, an FMI may choose to have a single document that covers both the FMI's strategic objectives and cyber resilience framework, or to develop a strategy that is underpinned by a set of approved policies and procedures that make up the framework elements described in the Cyber Guidance.

Cyber Guidance Reference	Comment
2.2.5 An FMI's ecosystem	ASX understands the need to take an encompassing view of cyber threats facing an FMI's ecosystem. In doing so, ASX recognises that there are limitations to the extent that an FMI can control or influence the cyber risks borne by other participants in that ecosystem. ASX recommends that the Cyber Guidance be amended to recognise that an FMI's responsibility should amount to management of their own risks, and, although assistance and advice may be provided to those entities that make up the wider ecosystem, an FMI is not responsible for managing the risks borne by other entities.
2.2.6 International and national standards	ASX supports the idea that FMIs should use current industry best approaches to cyber resilience. ASX requests that the Committee consider providing guidance as to the standards and guidelines they consider to be 'leading standards' in order to avoid confusion and ambiguity.
2.2.8 Audits and compliance	ASX's internal audit and regulatory assurance functions provide independent assurance to the boards of ASX's FMIs. Those functions have an understanding of ASX's operating environment and are in most cases best placed to provide that assurance. The General Managers of those functions have a direct reporting line to the board on matters relevant to those boards. ASX recommends that the Cyber Guidance be amended to recognise that the independent compliance programmes and audits can be provided by independent functions within the organisation.
2.3.1 Ultimate responsibility	In many organisations, a board will delegate responsibility for monitoring risk management activities to a Committee such as an Audit and Risk Committee. This approach is consistent with existing PFMI guidance, provided these governance arrangements are clearly and thoroughly documented. ASX recommends that the Cyber Guidance be amended to clarify that the Board can delegate this responsibility to a Committee by including words to the effect of "the Board, or its delegate".

Identification

Cyber Guidance Reference	Comment
3.2.1 Identification of business functions and processes	ASX understands the requirement to identify and protect all processes that may potentially be exposed to cyber threats. In doing so, ASX recognises that there may be some business processes across an FMI that are not directly impacted by cyber risk. The Cyber Guidance appears to look beyond cyber-related business processes and encapsulates all business functions and supporting processes in the suggested risk assessment process. ASX recommends that the Cyber Guidance be amended such that a cyber resilience risk assessment targets only key cyber risk areas.
3.2.2. Identification of information assets and related access	ASX recognises the importance of ensuring clear identification of information assets for the purposes of understanding access rights. ASX believes that, in some cases, it may be more important for an FMI to focus on identifying threat scenarios, rather than information assets, in order to inform the required cyber controls. While the security of information assets is important, it is equally important to ensure the reliability and availability of systems, and to ensure that data is not interfered with. Depending on the nature of the FMI, it could be argued that data theft is a less likely attack scenario than data manipulation or interference (e.g. changing settlement details, margin calculations).
3.3 Interconnections – impact from and on an FMI's ecosystem	ASX understands the need to take an encompassing view of cyber threats facing an FMI's ecosystem. In doing so, ASX recognises that there are limitations to the extent that an FMI can control or influence the cyber risks borne by other participants in that ecosystem. ASX recommends that the Committee consider replacing the term 'coordinate' in the following sentence "… an FMI should identify the cyber risks that it bears from and poses to entities in its ecosystem and *coordinate* with relevant stakeholders…." With '*communicate*' or '*liaise*'. The term 'coordination' implies a level of management that may not be desirable or practical. Although an FMI has a significant role to play in ensuring the strength of the ecosystem, it is not responsible for managing the risks borne by other entities within that ecosystem. In addition, where FMIs compete for business in a particular jurisdiction, there may be trade practices or competition laws that regulate the coordination of certain activities while excluding others in the market (such as competitors).

Protection

Cyber Guidance Reference	Comment
4.2.3 Strong ICT controls	ASX supports the requirement for a strong information and communications technology control environment. The Cyber Guidance appears to focus on encryption, change management and patching. While ASX agrees that these are important controls, ASX recognises that these are not the only controls that should be considered by an FMI.
4.3.1 Risks from interconnections	ASX understands the need to take an encompassing view of cyber threats facing an FMI's ecosystem. In doing so, ASX recognises that there are limitations to the extent that an FMI can control or influence the cyber risks borne by other participants in that ecosystem. The Cyber Guidance appears to place a significant burden on an FMI if the expectation is that an FMI must "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". This proposed requirement seems to indicate that an FMI is expected to independently audit every service provider and vendor. ASX recommends that the Cyber Guidance be amended to reflect whether an attestation from the service provider, or similar, would be sufficient. In addition, many FMIs will simply not allow service providers to have direct access to sensitive systems and networks. In these instances, it may not be necessary to ensure the service providers conform to the same standards as the FMI.
4.4.1 Security analytics	ASX recognises the importance of ensuring clear identification of insider threats. ASX believes the Cyber Guidance would be enhanced by the removal of the last sentence (reference to data loss identification). Data loss is one of the many risks faced by an FMI and may not be as high a risk as for other financial organisations due to the nature of the information stored.

Response and Recovery

Cyber Guidance Reference	Comment
6.2.1 Incident response planning	ASX understands the importance of effective response planning. The Cyber Guidance is unclear as to whether it would be appropriate for a system or network to be recovered and brought back online when an issue/s has been resolved, or, whether it would be more desirable to wait until an investigation is complete. ASX notes that many cyber investigations take days or weeks before getting to the root cause of a disruption and identifying what, if anything, has been compromised. ASX requests that the Cyber Guidance be amended to clarify.
6.2.2 Resumption within two hours	ASX recognises the critical role FMIs play in promoting financial stability and, consequently, the importance of resuming operations as rapidly as possible in the event of a disruption. The Cyber Guidance proposes the requirement for an FMI to plan to resume critical operations within two hours of a cyber-related disruption. ASX believes that this requirement is unlikely to be feasible and/ or practical in all scenarios. At section 6.2.3, the Cyber Guidance appears to acknowledge that the objective of resuming critical operations within two hours may not always be able to be achieved. ASX recommends that the Cyber Guidance be amended to require the resumption of critical operations within two hours, *where possible*.
6.2.3 Contingency planning	ASX understands the importance of effective contingency planning. ASX recommends that the Cyber Guidance be amended to remove the reference to manual processing. Manual processing is only one of the options available and would typically be the least favoured.
6.4.4 Responsible disclosure policy	ASX understands the concepts of continuous improvement and appropriate information-sharing. In doing so, ASX recognises that there are limitations to the extent of information an FMI would want to share cross-industry. ASX recommends that the Cyber Guidance be amended to clarify what is meant by the 'disclosure of potential vulnerabilities' and to whom, specifically, these disclosures are expected to be made. Vulnerabilities, should they be identified, are likely to be deemed highly sensitive and confidential, such that an FMI would not want to risk potentially advertising ways to exploit a system.

Testing

Cyber Guidance Reference	Comment
7.3.1 Coordination	ASX understands the need to take an encompassing view of cyber threats facing an FMI's ecosystem. While FMIs may organise industry wide disaster recovery testing, such testing is on a different scale to hosting and managing an industry wide cyber resilience test. ASX believes that cyber resilience testing is more effective, and achieves greater participation, when co-ordinated by regulatory or other government bodies and therefore recommends that the Cyber Guidance be amended to require FMIs participate in relevant exercises organised by relevant regulatory authorities, and in such exercises organised by other entities within an FMI's ecosystem *where desirable*.

Situational Awareness

Cyber Guidance Reference	Comment
8.3.1 Planning ahead	ASX understands the concepts of continuous improvement and appropriate information-sharing. ASX believes that the Cyber Guidance should infer an understanding that there will be some information that is commercial in confidence and cannot be shared externally.

Learning & Evolving

Cyber Guidance Reference	Comment
9.3.1 Metrics	ASX supports the idea that FMIs should aim to evolve and continually develop more mature states of cyber resilience. ASX believes that the Cyber Guidance could be enhanced by the inclusion of some examples of the type of metrics expected to be utilised, as an indication of best practice in KPI measurement.