HONG KONG, LONDON and WASHINGTON, 5 JUNE 2018 – The Global Financial Markets Association (GFMA) welcomes the European Central Bank (ECB) initiative to implement the CPMI-IOSCO guidance to develop Cyber Resilience Oversight Expectations for Financial Market Infrastructure (FMIs) in Europe.

GFMA believes cyber security is a shared responsibility and therefore welcomes this ECB initiative to set a cyber security framework for FMIs based on internationally recognised standards. The importance placed on cyber resilience for maintaining financial market stability continues to increase. All participants within financial markets must reach a sufficient level of cyber maturity and adhere to clearly specified requirements to effectively deter threats from a broad range of actors.

GFMA welcomes the ECB's approach to develop an EU-wide framework that is:

- **Based on internationally recognised standards;**
- **Recognises different maturity levels that can quantity and measure cyber resilience;**
- **Sets a high minimum standard on cyber resilience; and**
- **Is applicable to different actors involved in the financial sector.**

However, GFMA believes that the six points below need to be addressed to further support the successful adoption of this important framework and increase cyber resilience in financial services:

1. **The requirements should be principles based.**
   - A principle-based framework would provide additional flexibility that is required due to the continually evolving nature of cyber threats and would avoid prescriptive and detailed requirements that may become obsolete over time. This would increase the consistency and alignment with the CPMI IOSCO guidance. Where more detailed guidance is provided the ECB should consider separating these out as examples or use cases, which would provide examples of how the requirements could apply or interpret.

2. **The requirements should map and remain consistent with internationally recognised standards to reduce the risk of fragmentation.**
   - Further alignment with existing cyber security framework standards - such as the NIST Cybersecurity Framework, ISO 27000, and the G7 Fundamental Elements of Cybersecurity (e.g. BAIT, IT SIG, COBIT5) - should be adopted or acknowledged through mutual recognition. Reduced alignment with existing recognised standards increases regulatory complexity and requires resources to be diverted from other cyber activities. This inhibits firms to focus their efforts on the identification and protection against cyber threats (for example, some firms have reported that 40% of corporate cybersecurity activities are compliance oriented rather than security oriented[1]);

3. **The requirements should avoid reference to a two-hour recovery time objective (RTO) for cyber events.**

[1] https://www.nist.gov/sites/default/files/documents/2017/02/14/20160219_financial_services_sector_coordinating_council.pdf

- We request that the ECB CROE framework avoids reference to specific technological resumption of service. The ECB requirement of an RTO of two hours for sector-critical systems may not be technically feasible in all cases and might have the unintended consequence of restoring a system to operation before the nature of the threat or the effects of the event have been fully understood and remediated. The requirements should instead focus on operational resilience and the resumption of service, rather than a specific technology.

4. **The requirements should remain focused on cyber resilience.**
   - The ECB should consider identifying requirements in the framework that are not directly related to cyber resilience, such as references to change management (see the table below - *Section 2.2. Identification* - for references to change management), and potentially removing them. This would ensure that the framework is only focused on cyber resilience as intended and avoids any inconsistent requirements.

5. **The requirements should consider practical implementation challenges and their impact on other financial service actors.**
   - The ECB should consider including a standard or template for FMI's to facilitate outreach to other financial service actors for implementation of the framework. FMIs should be encouraged to collaborate with other financial service actors to ensure compliance with CROE standards. However, while this is prudent given the broad range of entry points through which an FMI may become compromised, there is a risk of disparate engagement from individual FMIs and the impact on a financial institution's own efforts to enhance cyber-resilience. Diverse approaches[2] by FMIs would increase the complexity and burden of this activity on the industry and have the effect of diverting resources away from a firm's own cybersecurity programmes.

6. **The requirements should support industry benchmarking.**
   - Firms should benchmark themselves against the wider industry and develop partnerships with industry associations and cybersecurity practitioners to increase the overall preparedness and awareness of the industry. However, this should be completed with consistent and quantifiable means that can be compared across other industries and internationally recognised benchmarks.

The GFMA[1] welcomes further discussion with the ECB on this response and working together on implementing a supervisory cybersecurity regime that complements existing requirements and standards.

Notes:

1. The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.

[2] E.g. specific/non-harmonised control frameworks, self-attestations, questionnaires, joint exercises, certifications, etc…

Supporting Information

Section	Comment	Reasoning
Section: 1.1. Background	**General comment:** • **Clarification** • **Amendment**	• **P5. "**Therefore, FMIs should…FMI itself and its overall ecosystem." **Comment:** GFMA recommends the ECB to amend the term "cyber resilience capabilities" to "operational resilience capabilities", as cyber resilience is one element impacting the overall operational resilience of an organisation.
Section: 1.2. Purpose	**General comment:** • **Clarification**	• **P6. "**The CROE are predicated on the… FMIs against the Guidance." **Comment:** While the guidance states that FMIs can use maturity models from international standards for internal purposes, the ECB's CROE is considered the baseline. To avoid different regions developing their own baseline version, it's the GFMA's view that the ECB and other key regulators from other jurisdictions should agree and standardise on a common framework or benchmark rather than create a different one. This would reduce the fragmentation of regulatory requirements and the burden of additional cost on firms. For instance, the GFMA is supporting work on a Financial Sector Profile which aims to provide overall harmonisation of cyber security frameworks for the financial sector, globally. Additionally, the GFMA welcomes the ECB to further clarify the meaning of "compliance" in the statement "FMIs are required to comply with the Guidance immediately" and later "The CROE should, however, not be considered as a checklist of measures FMIs need to strictly comply with, but instead as a set of practices that can contribute to FMIs' compliance with the Guidance".
Section: 1.4. Requirements by type of FMI	**General comment:** • **Clarification**	• **P7. "**Three levels of maturity: Baseline, Intermediate and Advanced." **Comment:** GFMA believes the framework could bring further consideration regarding how a maturity level is achieved. For instance, if an FMI meets a requirement in the baseline section but achieving all other recommendations at the Advanced section, would it be considered at Advanced, or Baseline, or not meeting any? In addition, a three-level maturity model would support enabling benchmarking opportunities, which GFMA views as a support mechanism to increase sector operational resilience. • **P8. "**Although the CROE have been…and judgement is very important." **Comment:** GFMA welcomes efforts from the ECB to design a framework that can allow flexibility in its implementation. However, to ensure consistency in how supervisors will interpret and implement controls at each level the ECB should consider providing additional tools, such as specific definitions and examples, to assure attestation across jurisdictions is measured equally throughout all FMIs.
Section: 2.1. Governance	**General comment:** • **Clarification** • **Amendment**	• **P13. "**2.g. Which assets will be used to manage cyber resilience and how performance of these assets can be optimised." **Comment:**

		GFMA believes further clarity should be provided on the requirement's intent and scope of the term "assets" (e.g. intrusion detection, firewalls, etc). GFMA believes the term should encompass all assets impacting operational resilience of an organisation, not just cyber security assets. Furthermore, Firms may use various types of means and technologies to achieve a cyber (operational) resilience strategy and its objectives, however these are not usually described in detail in a strategy document, which would be shared with a firm's board. This level of detail may be more appropriate to a firm's management which typically has this responsibility. • **P16. "**19. In order to…of designated senior management." **Comment:** GFMA recommends the ECB consider that a firm's board should have adequate access to expertise in cybersecurity or to maintain access to resources or staff with such expertise (internal, external and independent experts). A firm's Board composition shouldn't be driven by a specific skill set but by the overall experience of each member and the combination of experience across the firm. • **P17. "**27. Senior management should ensure…on its intranet site." **Comment:** GFMA recommends amending the term "all employees" to "relevant employees". • **P17.** "28. The annual cyber resilience…and emerging issues." **Comment:** GFMA supports this point and views awareness as key to tackle phishing and the resulting cyber incidents. • **P18.** "36. Senior management should produce…all employees comply with it." **Comment:** GFMA recommends the ECB to amend the sentence to capture that firms "should modify existing Code of Conducts to ensure it captures relevant elements of cyber risk".
Section: 2.2. Identification	**General comment:** • **Clarification** • **Amendment**	• **P21.** "3. The FMI should maintain a…review of its inventory." **Comment:** GFMA believes the ECB's CROE references to change management in this section, and other relevant sections, are more appropriate to technology and production rather than cyber resilience. • **P21.** "5. The FMI should create and maintain…identity links with the outside world." **Comment:** GFMA believes this recommendation is overly prescriptive and detailed, and at odds with the overall objective of the CROE framework which is to remain principle based as is the CPMI IOSCO guidance. • **P22.** "8. The FMI should use automated…in the FMI's inventory." **Comment:** GFMA believes recommendation to automation in this section and other relevant sections of the framework is overly prescriptive, and

		detailed, and at odds with the overall objective of the CROE framework which is to remain principle based as is the CPMI IOSCO guidance. • **P23.** "14. The FMI should identify…with the FMI's risk tolerance." **Comment:** This recommendation implies design requirements are in place. GFMA recommends the CROE to remain principle based and avoid prescriptive requirements on firm's controls and process designs. For instance, the requirements could be replaced with the following "'the cyber risk assessment program should be evaluated and updated as the FMI (a) makes changes to the networking environment or (b) makes changes to the business/products that the FMI supports to ensure that the risks to the environment from emerging threats is understood and measured."
Section: 2.3. Protection	**General comment:** • **Clarification** • **Amendment**	• **P25.** "8. The FMI should seek certification of its ISMS which is based on well recognised international standards." **Comment:** This recommendation references the certification of an Information Management Security System (ISMS). GFMA believes firms should be able to use a combination of standards to develop their cyber risk and control structures, as this requirement may force firms to choose one standard, leading to reduced flexibility for a firm's cyber risk management programs. • **P26.** "11. The FMI should establish…the principle of least privilege." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on a firm's controls and process designs. For instance, the requirements could be replaced with the following: "The FMI should implement network segmentation in their organization, which meets the principle of least privilege." • **P27.** "19. The FMI should implement controls…and access points." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs. For instance, the requirements could be replaced with the following: "The FMI should implement controls that manage or prevent non-controlled devices to connect to its internal network from inside or outside of the premises to ensure that activities in these zones is logged and monitored for inappropriate use or attempts to access business systems. The FMIs infrastructure should be regularly scanned to detect rogue devices and access points." • **P27.** "35. The FMI should have a dedicated…software and/or services go live." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs.

		For instance, not all applications have a password history and/or password complexity setting. • **P28.** "26. The FMI should implement technical measures…unauthorised devices." **Comment:** GFMA recommends the ECB to separate these two requirements as catering to different risks. • **P30.** "38. The FMI should implement…escalation of user privileges." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs. For instance, implementation of this control could potentially lead to numerous alerts, ultimately leading to ineffective controls due to volume of alerts. • **P33.** "58.B. During employment…in line with local laws and regulations." **Comment:** GFMA recognises the importance of monitoring employees; however, the requirement seems impractical and technically difficult to achieve for firms operating in multiple jurisdictions. Therefor GFMA recommends the ECB to amend this statement and use a risk-based approach for background checks. • **P36.** "77. The FMI should obtain assurance…summary of test reports, SLAs, KPIs etc." **Comment:** GFMA supports this point as this would allow FMIs to recognise a vendor's industry certifications as a key component of third party oversight.
Section: 2.4. Detection	**General comment:** • **Clarification** • **Amendment**	• **P39.** "38. The FMI should develop…in its protective measures." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs. For instance, zero-day exploits take advantage of unknown or unpublished vulnerabilities. Therefore, when an exploit is launched under these circumstances, it is difficult, if not impossible, to detect or protect from these exploits.
Section: 2.5. Response and Recovery	**General comment:** • **Clarification** • **Amendment**	• **P41.** "7. The FMI should regularly test…approved by the Board." **Comment:** GFMA believes the CROE should make clarify expectations of what a firm's board responsibilities and ownership of tasks are versus the board's ability to delegate to adequate senior staff of the organisation. For instance, implementation of this requirement would mean that it is the Board's role to approve a firm's contingency plans. GFMA believes that the Board should be accountable for ensuring these plans are in place, but their adequacy and effectiveness should be the responsibility of Senior Executives.

		Therefore, GFMA recommends the ECB to amend this statement, to describe that a firm's board should be made aware of recovery plans, but the plans can be approved and maintained by the relevant senior executives. • **P42.** "14. The FMI should design and test…settlement by end of day is crucial." **Comment:** GFMA views imposing a sector critical standard, requiring entities to establish an RTO of two hours for their sector critical systems, as impractical, technically infeasible and potentially a risk to financial stability and contagion risk. GFMA fully recognises the importance of resumption of service to an institution's resiliency program, however in the cybersecurity context, by contrast to kinetic disruptions, the technical capability of a firm to restore a system to operations, and the time frame for doing so, varies greatly depending on the nature of the attack and the size and complexity of the system. Moreover, unlike kinetic disruptions (such as a loss of power, loss of location, etc.), which as a technical matter are immediately apparent and are limited to a defined sphere, cybersecurity attacks are often difficult to detect or diagnose and frequently pose a risk of contagion to other systems or the market at large. Additional time is required for investigating the actual cause of the operational impact and then testing and validating systems after the attack to ensure that the systems are ready for safe operation. Given the unique characteristics of a cyber-attack, the ability to recover business operations and ensure that the environment is safe to reconnect to the financial ecosystem within a 2-hour time period may increase the contagion risk of a significant cyber-attack. Furthermore, it would be challenging as a practical matter to define the starting point for measuring the two-hour RTO when the precise beginning point of a cyber event is obscure or recurring, or when the objective of the attack is unclear. Rather than establishing an RTO time limit for specific systems, GFMA recommends a more practical and feasible approach which focuses more broadly on resumption of service, measured by the entity's best efforts to ensure the ability to safely meet contractual and regulatory service obligations. • **P44.** "32. The FMI should develop…practicable to do so." **Comment:** GFMA believes this requirement is a positive step forward for increasing the resilience of financial service sector but is aspirational in nature and may prove complicated to implement and monitor. • **P45.** "34. The FMI should implement real-time monitoring…when risks arise." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs. This requirement while aspirational in nature may prove complicated to design and implement. • **P.45** "38. The FMI establish criteria…criticality of the risk."

		Comment: GFMA recommends the ECB to consider a materiality threshold for this requirement. • **P46.** "43. The FMI should develop mechanisms… as well as prior experience." **Comment:** GFMA requests the ECB to clarify the need to provide notification from multiple channels, as this may lead to an increase in attack surface and lead to further inefficiencies to complete time critical activities for relevant stakeholders and senior management. • **P.46** "47. Based on 1), 2) and 3) …and their retention period." **Comment:** GFMA recommends the CROE to remain principle based in nature and avoid prescriptive requirements on firm's controls and process designs. For instance, providing a specific name to the policy for "Forensic Readiness Policy" is of no consequence, rather than providing the goals of the said policy that ought to be in place.
Section: 2.6. Testing	**General comment:** • **Clarification** • **Amendment**	• **P48.** "2.6 Testing" **Comment:** Tests defined by the ECB CROE framework are scoped as either vulnerability assessments, scenario-based testing, penetration tests or tests using red teams. GFMA believes the framework should distinguish more clearly between security testing programs and independent assessments and validations; and provide clear definition of terms regarding type tests envisaged (e.g. regulatory penetration testing). • **P.52** "38. The FMI should share the test…sharing arrangements." **Comment:** GFMA recommends the ECB to consider in this requirement how firms can mitigate the risk of sharing testing results which may contain proprietary and/or sensitive information regarding the organization's vulnerabilities; this may end up in the wrong hands. We recommend that firms do not provide the detailed testing results to their clients or peers, rather inform and provide evidence that testing has been completed to levels providing assurance. In this regard, the GFMA has specific comments related to the development and implementation of the TIBER_EU framework, and the use of in-house red teams, and would welcome the opportunity to discuss these specific points with the ECB. • **P.53** "39. The FMI should consider developing a Bug Bounty…to manage the programme." **Comment:** GFMA recommends the ECB to consider in this requirement how firms can ensure their subject matter experts are conducting tests and providing bug information back to vendors, and how this activity could be developed more broadly within the organisation. This would reduce the need for multiple employees to attempt performing these activities which could lead to potential risks or unintended consequences. • **P53.** "42. In addition, FMI to periodic independent…FMI's cyber resilience posture."

		Comment: GFMA recommends the ECB to amend the statement to allow for the use of in-house red teams. FMI's have established independent teams which provide in-house red team service to firms on a regular basis and we strongly urge the ECB to allow the use of such teams for testing.
Section: 2.7. Situational Awareness	**General comment:**	**Comment:** GFMA does not have further comments other than the ones provided above.
Section: 2.8. Learning and Evolving	**General comment:**	**Comment:** GFMA does not have further comments other than the ones provided above.
Section: Annex 3: Guidance on the Senior Executive	**General comment:** • **Clarification** • **Amendment**	• **P.65** "2. The Senior executive or CISO...audit activities" **Comment:** GFMA views further clarity should be considered regarding the expectation and independence of the CISO function and the relationship with other functions within a firm (e.g. Risk, Audit, Legal, Compliance, Operations & Technology). For instance, the CISO function is often aligned to the Operations & Technology department so whilst there may not be a direct management line to the IT/operations department, there may not be a sufficient degree of independence. Similarly, the role of Risk and Audit functions is important as well; for example, in the ECB's TIBER EU penetration testing framework, it requires that "At the end of each test, the board of the entity, the TI provider and the RT provider should sign an attestation confirming that the test was conducted in accordance with the mandatory requirements of the TIBER-EU framework. This will provide the legitimacy for mutual recognition". Understanding in more detail how the board attestation model will work is key, as it is likely that attestation will be driven through other functions for validity and robustness of information.

Contacts

GFMA	Alison Parent	+1 (202) 962-7393	aparent@gfma.org
AFME	Emmanuel Le Marois	+44 (0)20 3828 2674	emmanuel.lemarois@afme.eu
SIFMA	Tom Wagner	+ 1 (212) 313-1161	twagner@sifma.org
ASIFMA	Wayne Arnold	+852 2531 6500	warnold@asifma.org