EUROPEAN CENTRAL BANK

EUROSYSTEM

DIRECTORATE GENERAL
MARKET INFRASTRUCTURE AND PAYMENTS

ECB-PUBLIC

10 April 2018

TEMPLATE: COMMENTS ON THE DRAFT "CYBER RESILIENCE OVERSIGHT EXPECTATIONS FOR FINANCIAL MARKET INFRASTRUCTURES"

Contact details (will not be published)	Ms.	Andrea M. Flournoy
	Andrea.flournoy@fssc.org	
	N/A	
☐	The comments provided should NOT be published	

The table below shall serve as a template for collecting comments in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**.
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on (i.e. one row for each issue).
- If needed for the provision of further comments, please replicate page 3.

The assessment form consists of the four items which are suggested to be filled as follows:

- **Originator:** Name of the originator and ISO code of the country of the originator (i.e. NAME (AT/BE/BG/...))
- **Issue** (states the topic concerned): General comment, Specific comment on an Expectation, Request for definition and Request for clarification of

issue or terminology

- **Comment:** Suggestion for amendment, clarification or deletion
- **Reasoning:** Short statement why the comment should be taken on board

Please send your comments to ECB-Oversight-consultations@ecb.europa.eu by 05 June 2018.

Originator:

Name of the originator (i.e. name of the company or association)	Financial Services Sector Coordinating Council	ISO code of the country of the originator	US

Comments on the draft Cyber Resilience Oversight Expectations for Financial Market Infrastructures

Issue	Comment	Reasoning
General Comment	Amendment	***1.1 Background*** *Therefore, FMIs should continuously work to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to both the FMI itself and its overall ecosystem.* While FMIs strive to limit the impact of all cybersecurity risks, the FSSCC suggests that this language be enhanced to include limiting risks **to financial stability** as a principle and not general cyber threats that pose risk.
Specific Comment	Clarification	***1.2 Purpose*** *…overseers must simultaneously develop an oversight approach to assess their FMIs against the Guidance.* Clarification should be provided to provide assurance that overseers will develop approaches in a coordinated manner to avoid further regulatory fragmentation which could exacerbate operational risks to FMIs and therefore inadvertently lead to more risk and financial instability to the ecosystem.
Specific Comment	Amendment	***1.2 Purpose*** *…whilst developing the CROE, the Eurosystem oversight function also considered existing international guidance documents and frameworks...Although FMIs may use maturity models from other international standards and frameworks for their internal purposes, the maturity models set out in the CROE provide the benchmark* The FSSCC agrees that a maturity model would continue the work between FMIs and supervisory agencies to bring regulatory harmonization. In continuation of these efforts, it is recommended that key regulators, especially Financial Stability Board (FSB) members, coordinate on a common framework, preferably created in conjunction with the FMIs. The Financial Services Roundtable has begun work with regulators and a cross section of FMIs to develop a Financial Sector Profile that may serve as a starting point for this harmonization.

General Comment	Clarification	***1.3 Addresses*** In addition to the points made in this section it is also important to stress the importance of a harmonized and coordinated guidance and frameworks and to highlight that fragmentation could inadvertently lead to, at a minimum, increased operational risks and financial instability. The Institute of International Finance (IIF) white paper, ***Addressing Regulatory Fragmentation to support a Cyber-resilient Global Financial Service Industry***, provides examples of how the lack of harmonization may cause these consequences.
General Comment	Clarification	***1.4 Requirements by type of FMI*** *The three levels of maturity (**Baseline, Intermediate** and **Advanced)*** The FSSCC believes that the framework could bring further consideration regarding how a maturity level is determined. Developing a maturity model would enable the FMI and regulatory authorities to work together to develop benchmarking opportunities which could provide a consistent means for FMIs to measure and review their preparedness.
General Comment	Amendment	***Governance; Cyber Resilience Strategy; Baseline, Number 2g*** *Which assets will be used to manage cyber resilience and how performance of these assets can be optimised;* A cybersecurity risk management strategy provides sufficient information to provide the high-level direction of the program. It identifies, at a minimum, the threats and threat actors that face the FMI, the risks that these threats and threat actors pose to the FMI operations, the programs/services that are in place to manage these risks and the new programs or program enhancements needed to further manage risks to be within the FMIs risk appetite. This information should be sufficient to provide oversight and drive board discussion on the cybersecurity risk management program. FMIs use a substantial number of technology appliances, software and systems combined with business process controls to implement an effective strategy. Therefore creating a plan at the asset level may not be effective to implementing a cyber resilient strategy. In addition, plans at this level, in general, are not included in a strategy document but are used by those responsible for the daily operational management or implementation of a system. Given that the Board is an oversight function, this level of detail may distract from the conversation of the strategic direction of the cybersecurity risk management program. We recommend that consideration is given to those artifacts needed by the Board to complete its oversight function and bifurcate that which is required for the operational management of the cybersecurity risk management program of the FMI.

Specific Comment	Amendment	***Governance; Cyber Resilience Strategy and Framework; Intermediate; Number 13*** *The FMI should use relevant metrics and maturity models to assess and measure the adequacy and effectiveness of and adherence to its cyber resilience framework through independent compliance programmes and audits carried out by qualified individuals, on a regular basis.* FSSCC agrees that the oversight of the cyber resilience program should be independent from the individuals responsible for the implementation of the cyber resilient program. We believe that independence may be achieved either by FMI internal resources or an independent third party. Given that FMIs have developed qualified teams to implement cyber resilient programs, further clarity may be needed to state that the use of internal or external audits may satisfy this requirement.
Specific Comment	Amendment	**Governance; Role Of Board and Senior Management; Baseline; Number 19** *In order to discharge the aforementioned responsibilities, the FMI's Board should ensure that it collectively possesses the appropriate balance of skills, knowledge, and experience to understand and assess cyber risks facing the FMI, and is sufficiently informed and capable of posing credible challenge to the recommendations and decisions of designated senior management.* We request that the ECB consider clarifying that the Board requires adequate access to cybersecurity expertise. While we believe that it is important that Boards have access to internal, external, and independent experts to ensure that the Board adequately understands cyber risks and the protections in place to protect from these risks, the composition of a Board would be driven not by a specific skillset but by the overall experience of each member and the combination of experiences across the Board.
Specific Comment	Amendment	***Governance; Culture; Baseline; Number 27*** *Senior management should ensure that situational awareness materials are made available to employees when prompted by highly visible cyber incidents or by regulatory alerts.* While highly visible cyber incidents and regulatory alerts could be part of the cybersecurity awareness strategy, the threat landscape and the impacts of those threats to the FMI should drive the Awareness program. We recommend that the ECB consider that FMIs should have a cybersecurity awareness strategy that aligns with the threat landscape of the FMI and the specific risks that may impact the FMIs operations. The strategy may be influenced by highly visible cyber incidents or regulatory alerts.

Issue	Comment	Reasoning
Request for Clarification	Clarification	***Governance; Skills and Accountability; Baseline; Number 28*** *….This training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security) and emerging issues.* Board members must understand the threats, threat actors, vulnerabilities, and risks that face an FMI in order to execute their oversight responsibilities. Through the other sections of the CROE, the Board is informed of the threats, threat actors, vulnerabilities and risks associated with the business operations and the cyber resilience programs designed to address those risks. It is not clear if the activities completed through the CROE are sufficient to address this requirement or if there is an additional expectation of cybersecurity awareness training.
Request For Clarification	Clarification	***Governance; Culture; Intermediate; Number 36*** *Senior management should produce a formal Cyber Code of Conduct and ensure that all employees comply with it.* Most organizations have a Code Of Conduct to outline the appropriate and expected behaviours and is distributed to employees and contractors of the organization. We request that clarity is provided in the use of the FMI's current Code Of Conduct to be enhanced with the expectations for cybersecurity.
Specific Comment	Amendment	***Governance; Board and Management Responsibilities; Advanced; Number 42*** *The FMI should institute a dedicated cyber expert within the Board.* The subject of Board composition has been reviewed extensively by the financial industry. The Board should consist of directors with a diverse set of functional experience, industry experiences, educational qualifications, etc. to be equipped to deal with a wide range of issues facing the FMI and provide executives with advice and consultation from multiple perspectives. We request that the ECB consider clarifying that the Board requires adequate access to cybersecurity expertise. While we believe that it is important that Boards have access to internal, external, and independent experts to ensure that the Board adequately understands cyber risks and the protections in place to protect from these risks, the composition of a Board would be driven not by a specific skillset but by the overall experience of each member and the combination of experiences across the Board.

Specific Comment	Amendment	***Governance; Skills and Accountability; Advanced; Number 48*** *Senior management should actively foster partnerships with industry associations and cybersecurity practitioners to develop solutions for future cyber resilience needs, which will be useful to the FMI and the ecosystem as a whole.* The FSSCC recommends that this statement apply to the Baseline and Intermediate levels in addition to the Advanced.
Specific Comment	Amendment	***Identification; Expectations; Advanced; Number 14*** *The FMI should identify emerging risks in real time, and use automated feeds from above (i.e. AIM and IAM), in order to continuously update its risk assessments and take the necessary mitigating actions, in a timely manner and in line with the FMI's risk tolerance.* A risk assessment is a point-in-time review used to identify gaps in the minimum control standards set forth by the FMI. The risk assessment service is normally updated upon (a) new or changes to existing control standards (b) new or changes to regulatory obligations or (c) changes in the threat landscape that necessitate different or more streamlined minimum control requirements. These programs are not updated in a real time manner through automated feeds. We recommend that the ECB consider structuring this requirement to ensure that FMIs evaluate and update their risk assessment programs based on the aforementioned instances. In addition, it appears that the controls listed in this section are more prescriptive than what can be found in the IOSCO guidance. This may lead to controls that are obsolete over time. We request that the ECB consider using more of a principles-based structure for these requirements.
General Comment	Clarification	***Protection; Control Implementation and Design; Intermediate; Number 6*** *The FMI should develop and implement a bespoke information security management system (ISMS) based on well-recognised international standards (e.g. ISO 27001, ISO 20000-1, etc.), in order to establish, implement, operate, continuously monitor, review, maintain and improve a comprehensive information security control framework.* We recommend the addition of ISO 27103.

General Comment	Clarification	***Protection; Control Implementation and Design; Advanced; Number 8*** *The FMI should seek certification of its ISMS, which is based on well-recognised international standards.* While we agree that the cybersecurity program should be reviewed by either an internal or external, qualified and independent individual, there is a difference between certification and conducting a third party audit. A certification implies compliance to a specific standard that is further validated by a standards body (e.g., ISO 27001, CSA STARS). A third party audit review may be conducted by an independent party that is conducted in a manner consistent with an agreed best practice (e.g., SOC 1/2). Given that many FMIs utilize multiple standards to implements its control environment specific to the needs of the FMI and its risk appetite, it is recommended that a third party audit review is considered in place of a certification requirement. In addition, it appears that the controls listed in this section are more prescriptive than what can be found in the IOSCO guidance. This may lead to controls that are obsolete over time. We request that the ECB consider using more of a principles-based structure for these requirements.
Specific Comment	Amendment	***Protection; Network & Infrastructure Management; Baseline; Number 11*** *The FMI should establish a secure boundary that protects its network infrastructure, using network perimeter defence tools such as router, firewall, IPS/IDS, proxies, VPN, DMZ, etc. The boundary should identify trusted and untrusted zones according to the risk profile and criticality of assets contained within each zone, and appropriate access requirements should be implemented within and between each security zone according to the principle of least privilege.* While routers, firewalls, IPS/IDS and other technologies create secure zones within the networking environment in today's world, the rapid evolution of technology has already begun to combine the functionality of some of these products into single devices. We recommend that the ECB consider replacing this statement with a more general control statement that accomplishes the protection goal. For example, The FMI should establish secure boundaries designed to protect its network infrastructure to ensure that each zone that is created (e.g., trusted, untrusted) has adequate and effective controls to ensure that risks to the network environment can be monitored and alerted and that these zones are accessed through the principle of least privilege

Specific Comment	Amendment	***Protection; Network & Infrastructure Management; Baseline; 19*** *The FMI should implement controls that prevent non-controlled devices to connect to its internal network (e.g. personal devices, rogue access point, etc.) and endpoints (e.g. removable media), from inside the premises or outside (e.g. remote connections). The FMI's infrastructure should be regularly scanned to detect rogue devices and access points.* Todays computing environment continues to evolve. FMIs are evolving with the changing access needs of their employees. During this evolution, FMIs are permitting Bring Your Own Device (BYOD), guest wireless access, and other strategies to allow secured access to its network and data while providing protections for its sue. These technology strategies allow for devices which are not in the control of the FMI to access its systems. While these endpoints are not controlled by the FMI, the FMI should institute controls to limit the access of these devices to its production computing environment. We recommend to the ECB a statement that may read similar to the following, 'The FMI should implement controls that manage or prevent non-controlled devices to connect to its network from inside or outside of the premises to ensure that activities in these zones are logged and monitored for inappropriate use or attempts to access business systems. The FMI infrastructure should be regularly scanned to detect rogue devices and access points.
Specific Comment	Amendment	***Protection; Network and Infrastructure Management; Intermediate; Number 26*** *The FMI should implement technical measures to prevent the execution of unauthorised code on institution-owned or managed devices, network infrastructure and system components. The FMI should consider implementing technical measures such as Network Access Control (NAC) solutions in order to prevent the successful connection of unauthorised devices.* While we agree that about the importance of managing the introduction of unauthorized code and access control NAC), these are two (2) separate categories that may need to be split into their own statements. The current statement here are prescriptive and should be more principles-based to align with the IOSCO guidance.

Issue	Comment	Reasoning
Specific Comment	Amendment	***Protection; Network & Infrastructure Management; Intermediate; Number 29*** *In the context of a defence-in-depth strategy, the FMI should seek to implement cyber deception capabilities and techniques that enable it to lure the attacker and trap it to a controlled environment where all activities can be contained and analysed, allowing the FMI to gain vital threat intelligence that will help to improve its protection controls.* This statement defines 'Honeypot' technology which is the deployment of fake systems designed to lure potential attackers into a computing environment where their activities may be tracked and monitored in order to understand the tactics, techniques, and procedures used by the attacker to infiltrate or otherwise impact the network environment. While this technology is one of many tools that may be used by an organization to identify, track and learn adversarial tactics, we believe that the prescriptive nature of this control should be altered to be more principles-based in line with the IOSCO guidance.
Specific Comment	Amendment	***Protection; Logical and Physical Security Management; Intermediate; Number 38*** *The FMI should implement technical controls that trigger automated notification to appropriate personnel whenever user access permissions change. Controls should be in place to prevent unauthorised escalation of user privileges.* We agree the importance of managing user access to applications and business systems. The lack of effective user access control has led to some of the more significant cybersecurity breaches (e.g., rogue trading activities). FMIs employ multiple strategies to protect access throughout the user access lifecycle (i.e., account creation, user transfers, user certification, and account termination). The control as written could ultimately lead to hundreds or thousands of alerts which may lead to an ineffective monitoring control. The processes of new user creation, user transfers and leavers would all generate alerts that would require an administrator to review and investigate.
Specific Comment	Amendment	***Protection; Human Resources Security; Baseline; Number 58b*** *…And on a more general level, the FMI should ensure that there is a process for carrying out recurrent background checks for all employees on a periodic basis, in line with local laws and regulations.* FMIs conduct background checks on its employees and contractors in line with local laws and regulations. While this control provides some assurance on the integrity of a FMIs workforce, we recommend that the ECB consider scoping the continuous background checking requirement (e.g., employees/contractors that provide critical functions, employees/contractors that may transfer securities or payments) as described in this baseline control statement.

General Comment	Amendment	***Detection; Expectations; Intermediate; Number 12*** *The FMI should develop and implement a Security Information and Event Management system (SIEM), which provides automated mechanisms to correlate, across its business units, all the network and system alerts and any other anomalous activity in order to detect and prevent multifaceted attacks (e.g. simultaneous account takeover and DDOS attack).* We believe that the controls listed in this section are more prescriptive than what can be found in the IOSCO guidance. This may lead to controls that are obsolete over time. We request that the ECB consider using more of a principles-based structure for these requirements.
Specific Comment	Amendment	***Response and Recovery; Cyber Resilience Incident Management; Baseline; Number 7*** *The FMI should regularly test its cyber contingency, response, resumption and recovery plans, against a range of different plausible scenarios, and ensure that the plans are approved by the Board.* While the Board should ensure that FMIs have documented recovery plans and engage in the regular testing of these contingency plans, it may not have sufficient knowledge of the daily business operations to approve the adequacy and effectiveness of those plans. This level of understanding best lies with the senior management of the FMI which is accountable for understanding the business operations and the cyber resilient strategies that provide a continuity of service.

Specific Comment	Amendment	***Response and Recovery; Cyber Resilience Incident Management; Baseline; Number 14*** *The FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Notwithstanding this capability to resume critical operations within two hours, FMIs should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate, while taking into account the fact that completion of settlement by the end of day is crucial.* FMIs understand and strive to develop cyber resilient systems that allow for the quick recovery of critical operational functions. The ability to recover these functions are key to establishing confidence in the efficient movement of financial markets. The original two (2) hour recovery objective in the Principles for Financial Market Infrastructures (PFMI) 17 of Business Continuity Management was related to physical disruptions (e.g., loss of a data center). To mitigate the effects of these physical disruptions, the Operational Risk discussion in Principle 17 directs FMIs to incorporate use of secondary sites with IT systems designed to enable resumption of operations within 2 hours following disruptive events. Cybersecurity attacks pose unique challenges that are distinct from physical disruptions. ➢ Physical events have a known starting point When a physical event occurs, there is an easily predictable and dimensional impact as well as a standard path for failing over to alternate sites and staffing. Given the nature of cyber-attacks, the time of the initial attack may be unknown and the extent to which the attack has promulgated through the network is unknown. Additionally back-up systems, designed to mitigate a physical event within 2 hours, may be affected by a cyber event as information is copied from the primary to the secondary site occurs on a frequent basis. ➢ The attack-type of a cyber event is unknown When a physical disruption occurs, the type of disruption may be quickly determined so that actions may be taken to address the issue (i.e., failover to a secondary location). A cyber event requires time to reverse engineer the malware to determine at a minimum (a) the promulgation method of the malware (b) the malware properties (e.g., destructive, command and control) and (c) the method of remediation (i.e., how to remove the malware). In the event of a material systems compromise, the information from these steps will be required to provide other FMIs and financial industry participants with sufficient information to allow the stricken FMI to be reinserted into the financial ecosystem and to limit the contagion risk that may be realized if the malware is not properly remediated. The Bank Of International Settlements (BIS) white paper, *Regulatory Approaches to Enhance Banks' Cybersecurity Frameworks*, uses specific recovery time objectives as an example where care should be taken due to the risks that meeting these objectives could cause. It is recommended that a dialogue be opened with FMIs to evaluate an appropriate approach to addressing recovery objectives.

Specific Comment	Amendment	***Response and Recovery; Crisis Communication and Responsible Disclosure; Baseline; Number 43*** *The FMI should develop mechanisms to provide instantaneous notification of cyber incidents to its senior management, relevant employees and relevant stakeholders (including oversight and regulatory authorities) through multiple communication channels with tracking and verification of receipt. Such mechanisms should be based on predefined criteria and informed by scenario-based planning and analysis, as well as prior experience.* Alerts are generated based on predefined criteria that is set by the administrator. A single alert or group of alerts must be investigated by an analyst to determine what, if anything, malicious is occurring within the network environment. The immediate notification of stakeholders and supervisory/regulatory authorities may not only lead to thousands of alerts but may also be de minimus events, misconfigurations, or other daily technology break/fix challenges within the network. Security events should be properly investigated so a determination can be made as to who is notified and sufficient background on the occurrence. The control as written may lead to an administrative burden on the supervisor/regulator and the FMI.
General Comment	Clarification	***Testing; Penetration Tests; Baseline; Number 19*** *The FMI should conduct penetration tests on their external-facing services and the internal systems and networks to identify vulnerabilities in the adopted technology, organisation and operations regularly, or at least on an annual basis. Penetration tests should be conducted whenever systems are updated or deployed.* Penetration testing is a common control that should be conducted on a periodic basis to identify potential application weaknesses that may result from coding or configuration errors. Given the frequency of patching and configuration changes, we ask the ECB to clarify that penetration testing is not required when a system is patched or for minor configuration changes.

Specific Comment	Amendment	***Testing; Red-Teaming Tests; Intermediate; Number 32*** *The FMI should outsource the conduct of red-teaming exercises to external, third-party providers. Simultaneously, the FMI should build its internal processes and capabilities to undertake the externally outsourced exercise (e.g. establishing an internal White Team, developing incident escalation procedures, following appropriate methodologies and establishing robust risk management controls), as set out in the TIBER-EU framework.* While in some cases, we understand that the outsourcing of red team exercises is necessary. We believe that for organizations for which the competent capability exists; these FMIs should be allowed to lead their own red team. This is consistent with the CPMI-IOSCO guidance, ***Guidance On Cyber Resilience For Financial Market Infrastructures***, which reads '*A red team may consist of an FMI's own employees and/or outside experts, who are in either case independent of the function being tested*.'
Specific Comment	Amendment	***Testing; General; Advanced; Number 38*** *The FMI should share the test results with relevant stakeholders to boost the cyber resilience of its ecosystem and the financial sector as a whole, as far as possible and under specific information sharing arrangements.* While it is agreed that FMIs should confirm that testing has been completed and provide high-level information regarding the test, detailed test results may contain proprietary and sensitive information regarding the FMIs vulnerabilities. By sharing this information across hundreds of third parties, a breach of one (1) FMI or third party could lead to the exposure of a FMIs sensitive information not involved in the breach.

Issue	Comment	Reasoning
Specific Comment	Amendment	***Testing; Vulnerability Assessments; Advanced; Number 39*** *The FMI should consider developing a Bug Bounty programme as part of its vulnerability management process, and have appropriate safeguards in place to manage the programme.* While a Bug Bounty programme may be part of the overall management of a systems security service, there are many other controls (e.g., static code testing, application penetration testing, code reviews) that may also be used by an FMI to protect its information systems. We request that the ECB consider using more of a principles-based structure for these requirements.
Specific Comment	Amendment	***Testing; Red-Teaming Tests; Advanced; Number 42*** *In addition to periodic independent, external red-team exercises, the FMI should develop an internal red-team capability, with the appropriate methodologies, sophisticated tools and appropriately skilled personnel. The internal red-team test should regularly conduct red-team exercises and engage with the internal blue team, to transmit its findings and make improvements to the FMI's cyber resilience posture.* There are some FMIs that have developed the competency to conduct internal red team exercises. This is consistent with the CPMI-IOSCO guidance, ***Guidance On Cyber Resilience For Financial Market Infrastructures***, which reads '*A red team may consist of an FMI's own employees and/or outside experts, who are in either case independent of the function being tested.*' Therefore, a firm may adhere to the Advanced control while not meeting the Intermediate control #32 in this same section. We request that the ECB consider aligning this requirement with the CPMI-IOSCO Guidance for red team exercises.
General Comment	Clarification	***Annex 1 – Glossary*** For the definitions that will be populated for the CROE, we request that the ECB have definitions consistent with those definitions being developed by the Financial Stability Board (FSB) Cybersecurity Lexicon. This will ensure that terminology used within the CROE remains consistent with new regulations/guidance.

General Comment	Clarification	***Annex 3 – Guidance On The Senior Executive; Number 1*** *The FMI should appoint a Senior Executive, normally a Chief Information Security Officer (CISO), who is responsible for all cyber resilience issues within the FMI and with regard to third parties. The Senior Executive ensures that the cyber resilience objectives and measures defined in the FMI's cyber strategy, cyber resilience policies and guidelines are properly communicated both internally and, when relevant, to third parties, and that compliance with them is reviewed, monitored and ensured.* We request that the ECB clarify that this senior executive may exist at the corporate level as opposed to each legal entity for which a separate supervisory authority may exist in so far as the senior executive has the appropriate authority and competency to execute the role within the legal entity.
General Comment	Clarification	***Annex 3 – Guidance On The Senior Executive; Number 2b/3a*** *2b) The Senior Executive or CISO function has in particular the following tasks:* *Participating in the cyber risk management, as the second line of defence;* *3a) In terms of organisation and processes, the Senior Executive or CISO must be independent to avoid any potential conflicts of interest. Therefore, the following measures, in particular, are expected to be applied:* *Organisational set-up to ensure the Senior Executive or CISO can act independently from the IT/operations department and be able to report to senior management and the Board directly and at any time5; also ensuring that the Senior Executive or CISO is not involved in internal audit activities;* At the highest level, the second line of defence completes the following activities: (1) Defines governance through the development of policies and standards in line with industry best practices; (2) Provides advisory services on the management of risks (e.g., legal, compliance, strategic, operational/cybersecurity); (3) Measures, through risk assessments, the adherence of the organization to its polices and standards; and (4) Reports findings to the appropriate governance committees. Given these activities, Information Technology (IT) is not a line 2 function. Therefore, we ask that the ECB clarify if this statement is designed to move the CISO out of the IT function.