SWIFT's Comments on the European Central Bank's draft Cyber Resilience Oversight Expectations (CROE) for Financial Market Infrastructures (FMIs)

SWIFT

05 June 2018

Confidentiality: Public

SWIFT thanks the European Central Bank (ECB) for the opportunity to provide comments on the draft "Cyber resilience oversight expectations for financial market infrastructures".

SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholders, comprising more than 2,000 financial institutions. We connect more than 11,000 institutions in more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Natasha de Terán
SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467
www.swift.com

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

SWIFT thanks the European Central Bank (ECB) for the opportunity to provide comments on the draft "Cyber resilience oversight expectations for financial market infrastructures".

We applaud the ECB's efforts to enhance the cyber resilience of FMIs, and believe that the alignment with the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (FMIs) shows continuity in ensuring the safe and efficient operation of FMIs, whose operational resilience plays a crucial role in the overall robustness of the financial system.

The alignment of standards and their global adoption continues to be of paramount importance. It is clear that the industry would benefit more from global standards and consolidation than from having to reconcile multiple and diverse frameworks. The global adoption of the standards could lead to further consolidation, remove the potential conflicts and overlaps between international and local frameworks, and help reduce the cost of compliance.

Whilst it is encouraging that the expectations have been organised as a guidance to allow for operational flexibility, it has to be noted that their scope remains somewhat undefined; we encourage the ECB to ensure that the expectations address all relevant issues in a clear and concise way. It is not always clear whether the expectations refer to the FMI itself or if they also refer to the FMI's participants. While FMI participants create additional entry points which can increase the risk of compromise for both the FMI and its participants, the FMI itself cannot be responsible for its participants' security. The provisions outlined in this guidance must only apply to the FMIs themselves, unless clearly specified otherwise. The CPMI Guidelines for endpoint security within payment systems adequately address participants' security risks; these could potentially be adapted to apply to other FMIs.

Issue	Comment	Reasoning
Governance *(Section 2.1.2.2 par. 36):* The Guidance requires to draft an specific Cyber Code of Conduct	Amendment	Instead of producing a separate Cyber Code of Conduct, we suggest that FMIs should have to lay out requirements and guidance for the expected cyber behaviour of their employees. This may be embedded in the FMI's existing code of conduct or other security-related policies.

2.3. Protection *(Network & Infrastructure Management, Section 2.3.2.1.2, par. 28)* The FMI's infrastructure should be engineered to block or at least limit the effects of a cyber attack on production environments. It should implement automated controls based on the risk scores of its infrastructure assets, and it should be able to automatically disconnect or isolate affected assets in the case of an adverse event.	Clarification	The introduction of automated controls is part of any multi-layered defence. However, if not considered and applied carefully, it could be argued that automation could create more damage in case of false positive or be used as DoS against self. For this reason, there must be additional controls available and a robust control management system in place, as well as discretion. The criteria to automatically disconnect should be clearly defined and should take into account the impact of an unwanted disconnect coming from a false positive alert.
2.3. Protection *(Network & Infrastructure Management, Section 2.3.2.1.2, par. 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.	Deletion	The deception capabilities and controls are also mentioned in a similar context in control 2.4.2., paragraph 29. We recommend that the two controls should either be clarified or merged.

2.3. Protection *(Logical & Physical security management, Section 2.3.2.1.3, par. 43)* The FMI should employ automated mechanisms that allow a continuous audit and monitoring of account creation, modification, enabling, disabling and removal actions, in order to notify appropriate personnel when potential malicious behaviour or damage is detected. The FMI should implement adaptive access controls to prevent potential malicious behaviour or damage.	Clarification	We suggest that the term "adaptive access controls" be further clarified to avoid any misinterpretations.
2.3. Protection *(Logical & Physical security management, Section 2.3.2.1.3, par. 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	Clarification	The term "users" in this control is unclear. There could be many different types "users" involved – users that are internal to the FMI; the FMI's "users" or "participants"; "users" working within "participants"; service providers, and so forth. We feel it is important that the definition be more specific and the control language further clarified.
2.5. Response and recovery – (*Communication and collaboration – Contagion, Section 2.5.2.3.1, par. 34)* The FMI should implement real-time monitoring of external connections, coupled with interactive diagram(s) that shows real-time changes to the network connection infrastructure, volume fluctuation and alerts when risks arise.	Clarification	We believe that this control is rather too specific in nature, and would be more useful if it focussed on what an FMI should monitor as opposed to the method by which it monitors. In addition, we would point out that advanced attacks are very often invisible in volume fluctuation monitoring.

2.5. Response and recovery *(Forensic readiness, Section 2.5.2.4., par. 51)* The FMI should establish procedures to assemble and collate the digital evidence for the purposes of supporting a forensic investigation or legal case, taking into account the requirements of the local jurisdiction. These procedures should describe how investigative staff should produce step-by-step documentation of all activities performed on digital evidence and their impact.	Clarification	The FMI should establish procedures to assemble and collate the digital evidence for the purposes of supporting a forensic investigation or legal case, taking into account the requirements of the local jurisdiction **in which the FMI is based**. It should be left to the FMI's discretion as to whether in any given instance it collects and uses such evidence.
2.6. Testing *(Section 2.6.1, paragraph 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.	Amendment	Although the sharing of test results can be helpful for the financial community, we do not think that FMIs should be forced to share all findings. Test rules may contain proprietary and/or sensitive information regarding an organisation's vulnerabilities which in itself could create additional risks. While we support FMIs collaborating to build a more resilient ecosystem, we suggest modifying the focus to state that FMIs "…share the relevant parts of the test results which may provide valuable information to stakeholders to help improve their cyber security posture."

---------- END OF DOCUMENT ----------