SWIFT Response to European Commission Consultation on the Digital Operational Resilience Act

SWIFT

19 March 2020

Confidentiality: Public

SWIFT thanks the European Commission for the opportunity to provide comments on the call for input on the Digital Operational Resilience Act.

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 2,400 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.

Please do not hesitate to contact us should you want to discuss our response.

Kind regards,
Dario La Nasa

Global Deputy Head of Public Affairs
Tel: + 32 2 655 32 36
Mob: + 32 476 07 30 62
EU Transparency Register number: 011095511691-05
www.swift.com

-BEGIN-

Question 28. Is your organisation currently subject to any ICT and security testing requirements?

- [✓ Yes]
- No
- Don't know
- no opinion
- not relevant

Question 28.1 Do you face any issues with overlapping or diverging obligations?

- [✓ Yes]
- No
- Don't know
- no opinion
- not relevant

Question 28.2 Do you practice ICT and security testing on a voluntary basis?

- [✓ Yes]
- No
- Don't know
- no opinion
- not relevant

Question 28.3 To the extent you deem it necessary, please explain your reasoning for your answers to question 28 (and possible sub-questions):

Additional comments to 28.1

The existence of different cyber security and resilience regulations causes unnecessary duplication. Even small differences between national regulations introduce confusion and risk, barriers to business, increase cost and the compliance burden, without adding value. SWIFT is in favour of greater harmonisation and international cooperation, in line with best international security practice.

Additional comments to 28.2

Security is our number one priority and that is why we established and maintain a comprehensive testing programme as an integral part of our cyber resilience framework. The testing programme consists of a broad spectrum of methodologies, practices, exercises and tools for monitoring, assessing and evaluating effectiveness. We execute these tests in compliance with industry standards, such as ISO27001/2, PCI-DSS, and eIDAS. We also have specific security testing in our ISAE3000 controls, and are ISAE3000 certified.

Question 29. Should all financial entities be required to perform a baseline testing/assessment of their ICT systems and tools? What could its different elements be?

- Gap analyses?
- Compliance reviews?
- Vulnerability scans?
- Physical security reviews?
- Source code reviews?

SWIFT answer: No opinion to all elements of testing

Question 29.1 Is there any other element of a baseline testing/assessment framework that all financial entities should be required to perform? Please specify which one(s) and explain your reasoning:

Financial institutions are already subject to numerous testing regimes in different jurisdictions. We encourage international harmonisation of cyber security provisions and the removal of duplication to help simplify the assessment framework, whilst maintaining a high baseline. *For example, it is an industry-wide practice to carry out red team testing, but against different baselines and benchmarks.*

Question 29.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 29:

Harmonisation of security testing would benefit the industry by ensuring an internationally common baseline of requirements and provisions, which would facilitate the industry's planning and execution of such testing while having to conduct normal daily operations. While this is the case for most "checklist-based" testing procedures, red team testing should continue to be conducted without constraints, as its effectiveness comes from the "freedom" to look for different routes to reach its objective. The result of a red team test may in fact result in an update of checklists and/or a discovery of previously unknown vulnerabilities.

Question 30. For the purpose of being subject to more advanced testing (e.g. threat led penetration testing, TLPT), should financial entities be identified at EU level (or should they be

designated by competent authorities) as "significant" on the basis of a combination of criteria such as:

- Proportionality–related factors (i.e. size, type, profile, business model)?
- Impact – related factor (criticality of services provided)?
- Financial stability concerns (Systemic importance for the EU)?

SWIFT answer: No opinion to all of the options.

Question 30.1 Are there any other appropriate qualitative or quantitative criteria and thresholds? Please specify which one(s) and explain your reasoning:

There are varying criteria and thresholds in different jurisdictions.

Question 30.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 30:

Not applicable

Question 31. In case of more advanced testing (e.g. TLPT), should the following apply?

- Should it be run on all functions? No
- Should it be focused on live production systems? No
- To deal with the issue of concentration of expertise in case of testing experts, should financial entities employ their own (internal) experts that are operationally independent in respect of the tested functions? No opinion
- Should testers be certified, based on recognised international standards? Yes
- Should tests run outside the Union be recognised as equivalent if using the same parameters (and thus be held valid for EU regulatory purposes)? Yes
- Should there be one testing framework applicable across the Union? Would TIBER-EU be a good model? No opinion
- Should the ESAs be directly involved in developing a harmonised testing framework (e.g. by issuing guidelines, ensuring coordination)? No opinion
- Do you see a role for other EU bodies such as the ECB/SSM, ENISA or ESRB? Should more advanced testing (e.g. threat led penetration testing) be compulsory? No opinion

Question 31.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 31:

There are functions where testing is less critical, especially advanced forms of testing. As for testing live production systems: this should be risk based. Some production systems are so critical that the potential risk of a test interrupting it, could cause greater damage than the added value of the test.

Also, for services offered remotely by a same provider to multiple customers (for instance cloud or outsourced services), customers should not be required to perform security testing on the provider's infrastructure since security testing on the provider's infrastructure could impact all provider's customers. Instead, alternative mechanisms should be proposed to provide assurance on the security of such services (such as security certifications or regular reports).

Question 32. What would be the most efficient frequency of running such more advanced testing given their time and resource implications?

- Every six months

- Every year
- Once every three years
- Other

Question 32.1 What other frequency of running such more advanced testing given their time and resource implications would be the most efficient?

Frequency should be risk-based: testing should be more frequent on higher-risk environments.

Question 32.1 To the extent you deem it necessary, please explain your reasoning for your answer to question 32:

No further comments.

Question 33. The updates that financial entities make based on the results of the digital operational testing can act as a catalyst for more cyber resilience and thus contribute to overall financial stability. Which of the following elements could have a prudential impact?

- The baseline testing/assessment tools (see question 29)?
- More advanced testing (e.g. TLPT)?

SWIFT answer: No opinion to both

Question 33.1 Is there any other element that could have a prudential impact? Please specify which one(s) and explain your reasoning:

None.

Question 33.2 To the extent you deem it necessary, please explain your reasoning for your answers to question 33:

No further comments.