



# **SWIFT's Comments on the Financial Stability Board's draft Cyber Lexicon**

**SWIFT**

**20 August 2018**

**Confidentiality: Public**

SWIFT thanks the Financial Stability Board (FSB) for the opportunity to provide comments on the draft *Cyber Lexicon*.

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](http://www.swift.com)

### SWIFT comments on the draft FSB Cyber Lexicon

We welcome the FSB’s efforts to develop a lexicon of terms related to cyber security and resilience. It is vitally important that there is a common understanding of the terms we use and it is clear that the industry will benefit from having common definitions of similar terms, rather than multiple and diverse reference points.

The alignment of the FSB’s draft lexicon with that of other groups working on comparable frameworks is a practical step towards a safer and more robust financial system.

The global adoption of common definitions could remove any potential conflicts and overlaps between international and local frameworks, thereby helping to reduce the cost of compliance. In this respect, the FSB’s draft lexicon is a welcome step towards reducing regulatory fragmentation.

**Please find below our comments on the proposed lexicon.**

**Question 3:** *In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon? If any particular terms should be added, please suggest a definition, along with any source material for the definition and reasons in support of inclusion of the term and its definition.*

SWIFT believes it would be useful to add the following terms with their definitions:

Term	Definition
<b>Information Sharing and Analysis Centre or (ISAC)</b>	An organisation that provides a central resource for gathering information on cyber threats and providing two-way information sharing capabilities among members
<b>Crown Jewels</b>	Information assets that are most critical to the accomplishment of an organisation’s mission <i>Source: MITRE</i>
<b>One-time password or pin (OTP)</b>	A password that is valid for only one session or transaction <i>Source: NIST</i>

**Question 4:** *Should any of the proposed definitions for terms in the draft lexicon be modified? If so, please suggest specific modifications, along with any source material for the suggested modifications and reasons in support thereof.*

We believe that, based on common language and best market practices, in the definition of the term “Cyber Risk”, the word “impact” should replace “consequences”, and the word “likelihood” should replace “probability”.

Term	Current Definition	Proposed Definition
<b>Cyber Risk</b>	The combination of the probability of cyber events occurring and their consequences.	The combination of the <b>likelihood</b> of cyber events occurring and their <b>impact</b> .
<b>Reasoning:</b> the definition of the term “cyber risk” should cover its two parts – cyber and risk. The concept of “risk” should cover two elements – likelihood and impact.		

**Question 5:** *Going forward and following the publication of the final lexicon, how should the lexicon be maintained to ensure it remains up to date and a helpful tool?*

In order to be as useful as possible in supporting the work that the FSB, standard setting bodies, authorities and private sector participants are undertaking to address cyber security and cyber resilience in the financial sector, the proposed lexicon should be maintained by the FSB and kept up-to-date on an annual basis. The full alignment with the industry’s needs would be achieved if the lexicon is updated only after a community consultation run for a suitable time period.

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