

Editors of the Cyber Lexicon
Financial Stability Board
fsb@fsb.org

20 August 2018

Cyber Lexicon – Consultative Document (2 July 2018)

Dear Editors

Ernst & Young Global Limited (EY), the central coordinating entity of the Ernst & Young organization, welcomes the opportunity to offer the Financial Stability Board (FSB) its views on the 2 July *Cyber Lexicon* Consultative Document.

EY supports the efforts of the FSB to establish a common lexicon and agrees that it would facilitate the assessment of cyber risk and information sharing as well as support the work of the FSB and standard setting bodies (SSBs) in preparing cyber security and cyber resilience guidance. Consistent definitions of terms by SSBs and regulators improves the quality of information provided by firms with multiple regulators and reduces the cost to provide that information by avoiding minor discrepancies due to the interpretation of terms.

For 20 years now, EY has conducted its Global Information Security Survey (GISS) across all sectors to investigate the most important cybersecurity issues facing organizations today.¹ The EY GISS captures the responses of nearly 1,200 participants in 60 countries across more than 20 sectors. Some of the key findings in this year's survey results reflect several of the challenges businesses throughout the economy are struggling to resolve, including with respect to investment, talent and organizational structure. For example:

- 89% of respondents say their cybersecurity function does not fully meet their organization's need
- 75% of respondents rate the maturity of their program to identify new vulnerabilities affecting their technologies as very low to moderate
- 35% describe their data protection policies as ad hoc or nonexistent
- 12% have no breach detection program in place
- 43% of respondents do not have an agreed upon communications strategy or plan in place in the event of a significant attack
- 57% do not have, or only have, an informal program for gathering intelligence on new threats that could impact the company
- Only 4% of organizations are confident that they have fully considered the information security implications of their current strategy and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks

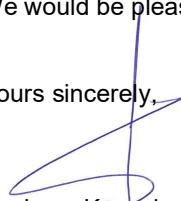
Understanding the nature of cyber risk is the first step in developing more effective solutions. Every organization, public or private, faces this challenge and is exposed to the threat. A common global lexicon would assist these efforts as we all work to better cyber risk management and promote a common understanding of cyber challenges and vulnerabilities. Policymakers and the financial sector must work together to improve cyber information sharing and develop collaborative, flexible and harmonized policy solutions that help organizations better respond to the dynamic nature of the challenge, and a common lexicon would support this work.

¹ The 20th EY Global Information Security Survey captures the responses of nearly 1,200 C-suite leaders and information security and IT executives/managers, representing many of the world's largest and most recognized global organizations across 60 countries. The research was conducted between June-September 2017.

In the attached we respond to each of the FSB's questions in the Consultative Document. We acknowledge that these comments may be published on the FSB website and look forward to your delivery of the lexicon to the G20 summit in Buenos Aires in November 2018.

We would be pleased to discuss our comments with the FSB staff at your convenience.

Yours sincerely,



Paul van Kessel
Global Advisory cybersecurity leader

Attachment: FSB Consultative Questions: EY Detailed Response

Attachment

Ernst & Young Global Limited is pleased to provide comments to the Financial Stability Board on its 2 July *Cyber Lexicon* Consultative Document. We have provided comments against the five questions you have posed as follows:

FSB Consultative Question	EY Response
<p>1. <i>Are the criteria used by the FSB in selecting terms to include in the draft lexicon appropriate?</i></p>	<p>We have no suggested revisions to the criteria as proposed.</p>
<p>2. <i>Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon? Should any additional criteria be used?</i></p>	<p>We support the criteria as proposed, noting that in selecting definitions from multiple source documents there is a risk that the cohesiveness between related terms may be weakened. We suggest including in the criteria “Reliance on existing sources” a preference for ISO 27000 series publications in the first instance.</p>
<p>3. <i>In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon?</i></p>	<p>We suggest deleting the term “Cyber Hygiene” because the definition proposed is not yet comprehensive and therefore should be excluded in accordance with the criteria used in developing definitions for terms in the draft lexicon.</p> <p>The definition proposed was: “A set of practices for managing the most common and pervasive cyber risks faced by organisations.”</p> <p>The application of this definition is limited without also defining or identifying the “set of practices” or “most common and pervasive risks.”</p> <p>We also believe that the term is not required for the objectives of the lexicon to be met, and therefore does not meet the criteria for inclusion of a term within the lexicon. Regulators propose controls for financial services entities to address a set of risks broader than just the “most common and pervasive”.</p> <p>We suggest deleting two terms: Recovery Point Objective (RPO); and Recover Time Objective (RTO) because both are “general business and regulatory terms” and therefore should be excluded in accordance with the criteria used in selecting terms to be included in the lexicon.</p> <p>The definitions proposed for both of these terms were drawn from ISO 22300:2018. We suggest that these terms are typically well defined and that their exclusion is consistent with other terms (such as “business continuity plan”) already excluded for this reason.</p>

<p><i>4. Should any of the proposed definitions for terms in the draft lexicon be modified?</i></p>	<p>We suggest simplifying the definition of Cyber Security by removal of the “Note” OR by defining the additional terms used within the “Note” using existing ISO definitions.</p> <p>The definition proposed was: <i>“Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.”</i></p> <p>While we prefer to simplify the definition by removing the note, if the note is retained, supporting definitions for the terms, <i>“authenticity”, “accountability”, “non-repudiation”</i> and <i>“reliability”</i> should be brought through from ISO sources for completeness.</p>
<p><i>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?</i></p>	<p>We suggest that the update cycle for the lexicon be triggered when one of the “Source” documents is updated and are willing to assist with this review. At the macro level, we suggest trying to limit the requirement for the lexicon through ongoing contribution to a consistent set of ISO definitions.</p>