HONG KONG, LONDON and WASHINGTON, 21 AUGUST 2018 – The Global Financial Markets Association (GFMA) welcomes the Financial Stability Board (FSB) Consultative Document on a Cyber Lexicon.

GFMA welcomes this global initiative by the Financial Stability Board (FSB) to publish a Cyber Lexicon. GFMA believes that cybersecurity is a global threat to financial stability that the coordination between different actors, across sectors and geographies, is becoming increasingly important to prepare and respond in the face to the growing threat of cyber-attacks.

GFMA welcomes the FSB's approach to develop an internationally recognised Cyber Lexicon that,

- **Is applicable cross-sector to enable a common understanding of relevant cyber security and cyber resilience terminology;**
- **Works to assess and monitor cyber risk scenarios for financial stability;**
- **Fosters information sharing as appropriate; and**
- **Complements work by the FSB and/or standard-setting bodies (SSBs) to provide guidance related to cyber security and cyber resilience, including identifying effective practices.**

However, for the Cyber Lexicon to remain relevant, the GFMA recommends the FSB to,

- **Remove technical terms and include additional terms related to cyber resilience;**
- **Explicitly define the profile of the intended user of the Cyber Lexicon; and**
- **Indicate how the Cyber Lexicon is over-arching and interfaces with other areas of cybersecurity.**

The GFMA[1] welcomes further discussion with the FSB on this response and working together on completing a Cyber Lexicon that complements existing requirements and standards.

Notes:

1. The Global Financial Markets Association (GFMA) brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, visit http://www.gfma.org.

Q1. Are the criteria used by the FSB in selecting terms to include in the draft lexicon appropriate in light of the objective of the lexicon? (See Section 2 for the objective, Section 3.2 for the criteria and the Annex for the lexicon.) Should additional criteria be used?

GFMA believes the criteria used by the FSB in selecting terms to include in the draft Cyber Lexicon are appropriate in light of the FSB objectives, but should be enhanced.

The GFMA agrees the FSB Cyber Lexicon should exclude terms deemed either "technical" or "general business and regulatory", to align with the FSB objectives, but go further in identifying those terms that are "core" to cyber security or resiliency, upon which more technical terms relevant to cyber are built. By doing so, the FSB will be able to more fully achieve its objective in advancing common understanding across various jurisdictions and stakeholders involved. Therefore, we have made recommendations to include additional terms in our response to question 3.

Finally, the GFMA believes the FSB should consider articulating how the Cyber Lexicon is over-arching and interfaces with other, more specific, Lexicons such as for example for cyber security frameworks[1], resilience[2], penetration testing[3] or treatment of incidents[4].

Q2. Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon? (See Section 3.3 for the criteria.) Should any additional criteria be used?

GFMA believes the criteria used by the FSB in defining terms in the draft Cyber Lexicon are appropriate in light of the FSB objectives: 1) Reliance on existing sources, 2) Comprehensive definitions and 3) Plain Language.

However, there are instances where the FSB has opted for a more cyber nuanced definition for an otherwise general term. GFMA recommends that definitions retained should be the more general, commonly understood definitions. To the extent that the FSB wishes to use definitions with cyber or information security terms or phrases, the FSB should consider replacing the general term with a more cyber specific term. As an example, the term "Alert" is a widely used and understood term which has broader definition and application than in the cyber context, and thus, the term "Cyber Alert" should be retained, if the FSB would like to define that term in a cyber context.

Finally, where references are made to existing international recognized standards (e.g. NIST, ISO, SANS, ISACA) the FSB Cyber Lexicon should make explicit those references, to facilitate traceability of where these terms are taken from or adapted.

Q3. 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.

GFMA supports the addition of a number of terms for which an agreed upon definition would help to achieve common understanding and drive better cyber security and resiliency outcomes:

[1] NIST "Framework for Improving Critical Infrastructure Cybersecurity" v1.1, p.45-47, (link)
[2] Bank of England and FCA Discussion Paper "Building the UK financial sector's operational resilience", p.38-39 (link)
[3] GFMA "A framework for Regulatory use of Penetration testing in the Financial Services Industry", p.26 (link)
[4] ENISA "Reference Incident Classification Taxonomy" (link)

FSB Cyber Lexicon : GFMA Comments for adding terms

Term	Definition selected	Definition source	Rationale
Acceptable Risk	Risk that is understood and tolerated by a user, operator, owner, or accreditor.	The IETF's "RFC 4949 - Internet Security Glossary, Version 2" definition: Risk that is understood and tolerated by a system's user, operator, owner, or accreditor, usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss. Link: here	"Acceptable risk" is a distinct term to "Risk Acceptance". GFMA suggests the RFC definition with a modification to remove language following "accreditor" as it implies a level of quantification may not be available or otherwise attainable.
Critical Infrastructure	System and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.	NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition: System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e)] Link: here	"Critical infrastructure" is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. GFMA suggest the NIST definition but modified to be generalized for applicability in any jurisdiction.
Information and Communication Technology (ICT)	Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information.	NIST SP 800-161 Definition: Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information.	"Information and Communication Technology (ICT)" is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. GFMA suggest the ISACA's definition, as is, the most accurate and concise.
Risk	The combination of the probability of an event and its consequence.	ISACA's "Cybersecurity Fundamentals Glossary" Definition: The combination of the probability of an event and its consequence. Link: here	"Risk" would serve as a root definition to other "risk" based terms. GFMA suggest the ISACA's definition, as is, as the most accurate and concise.

Risk Acceptance	Explicit or implicit decision to take a particular risk.	DHS Cyber Lexicon definition: Explicit or implicit decision not to take an action that would affect all or part of a particular risk. Link: here ISO Guide 73:2009 - Risk acceptance definition, with modification: Informed decision to take a particular risk. Link: here	"Risk Acceptance" refers to the implicit or explicit level of risk that a firm will accept, which is relevant to any risk environment, including cyber security. GFMA suggest a combination of: 1) The DHS definition, and 2) The ISO's definition.
Risk Analysis (or Risk Assessment)	A process used to identify and evaluate risk and its potential effects.	ISACA's "Cybersecurity Fundamentals Glossary" Definition: A process used to identify and evaluate risk and its potential effects. Link: here	"Risk Analysis" or "Risk Assessment" are synonymous terms. GFMA suggest the ISACA's definition, as is, the most accurate and concise.
Risk Appetite	A broad-based description of the desired level of risk that an entity will take in pursuit of its mission.	The COSO's "Strengthening Enterprise Risk Management for Strategic Advantage" definition: A broad-based description of the desired level of risk that an entity will take in pursuit of its mission. Link: here	"Risk appetite" is core to a firm's strategy, strategic thinking, and the initiatives it undertakes. GFMA suggest the COSO definition, as is, as it is the clearest articulation of the difference between "risk appetite" and "risk tolerance".
Risk Assessment (or Risk Analysis)	A process used to identify and evaluate risk and its potential effects.	ISACA's "Cybersecurity Fundamentals Glossary" Definition: A process used to identify and evaluate risk and its potential effects. Link: here	"Risk Analysis" or "Risk Assessment" are synonymous terms. GFMA suggest the ISACA's definition, as is, as the most accurate and concise.
Risk Management	Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or mitigating it to an acceptable level	DHS Cyber Lexicon Definition: Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.	"Risk Management" is a widely used term, for which definition is inconsistent and not commonly well understood. GFMA suggest the DHS Cyber Lexicon definition, modifying the term "controlling" with "mitigating."

		Link: here	
Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise.	"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition: A structured approach used to oversee and manage risk for an enterprise. Link: here	"Risk Management Framework" is a widely used term, for which definition is inconsistent and not commonly well understood. GFMA suggest the NIST IR Lexicon definition, as is, as it is the most concise and applicable to the enterprise space.
Risk Management Plan (or Risk Management Strategy)	Course of action or actions to be taken in order to manage risks.	DHS Cyber Lexicon definition for Risk Management Strategy, no modification: Course of action or actions to be taken in order to manage risks. Link: here	"Risk Management Plan" and "Risk Management Strategy" are synonymous and widely used terms. GFMA suggest the DHS definition, as is, as it is the most concise and applicable.
Risk Management Policy	Statement of the overall intentions and direction of an organization related to risk management.	ISO Guide 73: 2009 "Risk management - Vocabulary" Definition, no modification: Statement of the overall intentions and direction of an organization related to risk management. Link: here	"Risk Management Policy" is a widely used term for which a universally accepted definition is needed given it ubiquity in risk management programs. GFMA suggest the ISO definition, as is, as it is the most concise and applicable.
Risk Management Process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.	ISO Guide 73: 2009 "Risk management - Vocabulary" Definition: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk. Link: here	"Risk Management Process" is a widely used term for which a universally accepted definition is needed given it ubiquity in risk management programs. GFMA suggest the ISO definition, as is, as it is the most concise and applicable.
Risk Management Strategy (or Risk Management Plan)	Course of action or actions to be taken in order to manage risks.	DHS Cyber Lexicon definition for Risk Management Strategy: Course of action or actions to be taken in order to manage risks. Link: here	"Risk Management Plan" and "Risk Management Strategy" are synonymous and widely used terms. GFMA suggest the DHS definition, as is, as it is the most concise and applicable.

Risk Measurement	A process to determine the likelihood of an adverse event or threat occurring and the potential impact.	The Federal Financial Institutions Examination Council's (FFIEC) "IT Examination Handbook Infobase" Definition: A process to determine the likelihood of an adverse event or threat occurring and the potential impact of such an event on the institution. The result of risk measurement leads to the prioritization of potential risks based on severity and likelihood of occurrence. Link: here	"Risk Measurement" is a widely used term, but for which application is inconsistent and for which the definition is not commonly understood. GFMA suggest the FFIEC definition and removing terms either not containing defining language, or terms applicable at enterprise level.
Risk Tolerance	Reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve.	COSO's "Strengthening Enterprise Risk Management for Strategic Advantage" definition: Risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve. Link: here	"Risk Tolerance" is a core term often conflated with risk appetite, for which disparate definitions can be found. GFMA suggest the COSO definition, as is, as it is the clearest articulation of the difference between "risk appetite" and "risk tolerance".
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.	"NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms" Definition(s): 1. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. 2. Any circumstance or event with the potential to adversely impact organizational operations (including	"Threat" is a widely used term, for which disparate definitions can be found. GFMA suggest the NIST definition and removing language associated to "information systems", as it is deemed expansive enough.

		mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Link: here	
Threat Analysis (or Threat Assessment)	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment: Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. Link: here	"Threat Assessment" and "Threat Analyses" synonymous and widely used terms, but for which application is inconsistent. GFMA suggest the NIST definition as is, as it is the most concise and applicable.
Threat Assessment (or Threat Analysis)	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.	NIST 800-30, Rev. 1 (and CNSSI No. 4009) Definition of Threat Assessment: Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. Link: here	"Threat Assessment" and "Threat Analyses" synonymous and widely used terms, but for which application is inconsistent. GFMA suggest the NIST definition as is, as it is the most concise and applicable.
Threat Intelligence	Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event.	CPMI-IOSCO definition: Information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event (may also be referred to as "cyber threat information"). Link: here	"Threat Intelligence" is a widely used term but for which application is inconsistent. GFMA recommends the CPMI-IOSCO definition, and removing the parenthetical content, as source of confusion between two separate term, "Threat Intelligence" and "Cyber Threat Information".

Q4. 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.

Please see our comments further below.

FSB Cyber Lexicon : GFMA Comments for updating or removing terms

Term	Current definition	Propose changes	Reasoning
Access Control	Means to ensure that access to assets is authorised and restricted based on business and security requirements. Source: ISO/IEC 27000:2018	**None**	N/A
Advisory	Notification of new trends or developments regarding a threat to, or vulnerability of, information systems. This notification may include analytical insights into trends, intentions, technologies or tactics used to target information systems. Source: Adapted from NIST	**None**	N/A
Alert	Notification that a specific attack or threat has been directed at an organisation's information systems. Source: Adapted from NIST	**None**	N/A
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals	**None**	N/A
Authentication	Provision of assurance that a claimed characteristic of an entity is correct. Source: ISO 27000:2018	**None**	N/A
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018	**None**	N/A
Campaign	A grouping of adversarial behaviours that describes a set of malicious activities that occur over a period of time against a specific set of targets. Source: Adapted from STIX	**Remove**	
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities or processes. Source: ISO/IEC 27000:2018	**Update** **Suggested definition:** "Property that information is not made available or disclosed to unauthorised individuals, entities or processes or systems".	Suggestion to add "systems" for completeness.

Configuration Management	An activity of managing the configuration of an information system throughout its life cycle. Source: ISO/IEC 10032:2003	**None**	N/A
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities and threats to support organisational risk management decisions. Source: NIST 800-150, Appendix B (citing NIST 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, Sept. 2011)	**Update** **Suggested definition:** "Maintaining ongoing awareness of systems, processes, technology, operations and threats to support organizational risk management decisions."	Suggestion to make more general because the term "Continuous Monitoring" is a more general term.
Course of Action (CoA)	An action taken to either prevent a cyber incident or respond to a cyber incident. Source: Adapted from STIX	**None**	N/A
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems. Source: Adapted from CPMI-IOSCO (citing NICCS)	**None**	N/A
Cyber Event	Any observable occurrence in an information system. Events sometimes provide indication that a cyber incident is occurring. Source: Adapted from NIST (definition of "Event")	**None**	N/A
Cyber Hygiene	A set of practices for managing the most common and pervasive cyber risks faced by organisations. Source: Adapted from Carnegie Mellon University	**None**	N/A
Cyber Incident	A cyber event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies -- whether resulting from malicious activity or not. Source: Adapted from NIST (definition of "Incident")	**Update** **Suggested definition:** "A cyber event that compromises the confidentiality, integrity or availability of an information system." **Source**: ISO/IEC27000.2018E on definition for "information security incident"	Suggestion to make the definition more succinct and avoid inclusion of "hypothetical" harms.

Cyber Incident Response Plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident. Source: Adapted from NIST (definition of "Incident Response Plan") and NICCS	**None**	N/A
Cyber Resilience	The ability to anticipate and adapt to changes in the environment and withstand, contain and rapidly recover from a cyber incident. Source: Adapted from CPMI-IOSCO and NIST (definition of "Resilience")	**None**	N/A
Cyber Risk	The combination of the probability of cyber events occurring and their consequences. Source: Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of "Risk") and ISACA Full Glossary (definition of "Risk")		
Cyber Security	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. Source: Adapted from ISO/IEC 27032:2012	**None**	N/A
Cyber Threat	A circumstance or cyber event with the potential to intentionally or unintentionally exploit one or more vulnerabilities, resulting in a loss of confidentiality, integrity or availability. Source: Adapted from CPMI-IOSCO	"Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service." Source: "NIST IR 7298 (Rev. 2) — Glossary of Key Information Security Terms," the second	Suggestion to update the definition to relate to the suggested additional term of "Threat".

		definition of the term Threat.	
Data Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored or otherwise processed. Source: ISO/IEC 27040:2015	**None**	N/A
Defence-in-Depth	Information security strategy integrating people, technology and operations capabilities to establish a variety of barriers across multiple layers and dimensions of the organisation. Source: Adapted from NIST and FFIEC	**None**	N/A
Denial of Service (DoS)	Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users. Source: Adapted from ISO/IEC 27033-1:2015	**None**	N/A
Detect	Develop and implement the appropriate activities to identify the occurrence of a cyber event. Source: Adapted from NIST Framework	**Update** "Detect Function"	Suggestion to change the term "Detect" to "Detect Function" and keeping the NIST definition, to avoid confusion between terms and definitions used.
Distributed Denial of Service (DDoS)	A denial of service that is delivered using numerous sources simultaneously. Source: Adapted from NICCS	**None**	N/A
Exploit	Defined way to breach the security of information systems through vulnerability. Source: ISO/IEC 27039:2015	**None**	N/A
Identify	Develop the organisational understanding to manage cyber risk to systems, assets, data and capabilities. Source: Adapted from NIST Framework	**Update** "Identify Function"	Suggestion to change the term "Identify" to "Identify Function" and keeping the NIST definition, to avoid confusion between terms and definitions used.
Identity Access Management (IAM)	Encapsulates people, processes and products to identify and manage the data used in an information system and to authenticate users and grant or deny access rights to data and	**None**	N/A

	system resources. The goal of IAM is to provide appropriate access to organisation resources. Source: Adapted from ISACA Full Glossary		
Incident Response Team (IRT) [commonly known as CERT or CSIRT]	Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle. Source: ISO/IEC 27035-1:2016	**None**	N/A
Indicators of Compromise (IoCs)	Evidence of an intrusion that can be identified in an information system. Source: Adapted from SANS InfoSec Reading Room	**None**	N/A
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage cyber risks or respond to cyber incidents. Source: Adapted from NICCS	**Update** An exchange of data, information and/or knowledge that can be used to manage risks or respond to security incidents.	Suggestion to make more general because the term "Information Sharing" is a more general term.
Information System	Set of applications, services, information technology assets or other information-handling components. Note: This term is used in its broadest sense when referenced within the lexicon, which includes the operating environment. Source: Adapted from ISO/IEC 27000:2018	**None**	N/A
Integrity	The property whereby information, an information system, or a component of a system has not been modified in an unauthorised manner. Source: Adapted from NICCS and CPMI-IOSCO	**None**	N/A
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the organisation and/or the organisation's information system. Source: Adapted from ISO/IEC 27032:2012	**None**	N/A
Multi-Factor Authentication	Authentication using two or more of the following factors: -- knowledge factor, "something an individual knows";	**Update** **Suggested definition:**	Suggest changing the preamble to "Authentication using two or more factors,

	-- possession factor, “something an individual has”; -- biometric factor, “something an individual is or is able to do”. Source: ISO/IEC 27040:2015	"Authentication using two or more factors, including the following factors:"	including the following factors:"
Patch Management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs. Source: NIST	**None**	N/A
Penetration Testing	An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of an information system. Source: Adapted from NICCS	**None**	N/A
Protect	Develop and implement the appropriate safeguards to ensure delivery of services. Source: Adapted from NIST Framework	**Update** “Protect Function”	Suggestion to change the term “Protect” to “Protect Function” and keeping the NIST definition, to avoid confusion between terms and definitions used.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber event. Source: Adapted from NIST Framework	**Update** “Recover Function”	Suggestion to change the term “Recover” to “Recover Function” and keeping the NIST definition, to avoid confusion between terms and definitions used.
Recovery Point Objective (RPO)	Point to which information used by an activity is restored to enable the activity to operate on resumption. Source: ISO 22300:2018	**Update** "Point to which information used by an activity is restored to enable the activity to operate normally on resumption."	Recommendation to include the word "normally." The objective is to not just restore information or systems, but to do so in a way that restores information or system integrity.
Recovery Time Objective (RTO)	Period of time following an incident within which a product or service or an activity is resumed, or resources are recovered. Source: ISO 22300:2018	**None**	N/A
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organisational activities and/or business processes to provide an assessment of the security	**None**	N/A

	capability of the information system and organisation. Source: Adapted from NIST		
Respond	Develop and implement the appropriate activities to take action regarding a detected cyber event. Source: Adapted from NIST Framework	**Update** "Respond Function"	Suggestion to change the term "Respond" to "Respond Function" and keeping the NIST definition, to avoid confusion between terms and definitions used.
Situational Awareness	The ability to identify, process and comprehend the critical elements of information through a process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: Adapted from CPMI-IOSCO	**None**	N/A
Social Engineering	A general term for trying to deceive people into revealing confidential information or performing certain actions. Source: Adapted from FFIEC	**None**	N/A
Tactics, Techniques and Procedures (TTPs)	The behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique. Source: Adapted from NIST 800-150	**None**	N/A
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: Adapted from STIX	**None**	N/A
Traffic Light Protocol (TLP)	A set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipient(s). Source: FIRST	**Update** "A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established color code to indicate expected sharing boundaries to be applied by the recipient."	Recommendation to modify the definition as TLP vary across domains. They do not always consist of four colors for instance.

Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. Source: Adapted from CPMI-IOSCO and ISO/IEC 27000:2018	**None**	N/A
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation. Source: NIST	**Update** "Systematic examination of a system, product, control, or process to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation."	Suggestion to make more general because the term "Information Sharing" is a more general term (as per suggested update above)

Q5. 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?

For the Cyber Lexicon to remain up to date and helpful, GFMA believes the FSB should:

- Define a period for regular review. We believe a yearly review is appropriate;
- Define a procedure for making changes to the Cyber Lexicon outside of the periodic review (e.g. events, triggers for updates);
- Clarify and provide transparency on how feedback and changes are being made; and
- Consider engagement and input form a balanced group of stakeholders (e.g. regulatory and industry) to keep the Cyber Lexicon up to date to current developments.

Contacts

GFMA	Alison Parent	+1 (202) 962-7393	aparent@gfma.org
AFME	Emmanuel Le Marois	+44 (0)20 3828 2674	emmanuel.lemarois@afme.eu
SIFMA	Tom Wagner	+ 1 (212) 313-1161	twagner@sifma.org
ASIFMA	Wayne Arnold	+852 2531 6500	warnold@asifma.org