FSB FINANCIAL STABILITY BOARD

Cyber Lexicon

Consultative Document

2 July 2018

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board
Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Cyber Lexicon

Introduction

The Communiqué issued at the March 2017 meeting of the G20 Finance Ministers and Central Bank Governors in Baden-Baden noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.[1] With the aim of enhancing cross-border cooperation, the Financial Stability Board (FSB) was asked, as a first step, to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices. In October 2017, the FSB delivered the requested stocktake report regarding existing publicly available regulations and supervisory practices with respect to cyber security in the financial sector to the Finance Ministers and Central Bank Governors meeting in Washington, DC.[2] The Ministers and Governors welcomed the FSB stocktake report, asked the FSB to continue its work to protect financial stability against the malicious use of ICT and noted that this work could be supported by the creation of a common lexicon of terms that are important in the work being pursued.[3]

The FSB has now developed a draft lexicon of terms related to cyber security and cyber resilience, and is publishing the draft lexicon for public consultation. After considering the responses to this consultation, the FSB intends to finalise the lexicon for delivery to the G20 Summit in Buenos Aires in November of this year. The FSB welcomes comments on this document. Comments should be submitted by 20 August 2018 by email to fsb@fsb.org. All comments will be published on the FSB website unless a commenter specifically requests confidential treatment.

[1] See G20, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 March 2017*, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

[2] See FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, 13 October 2017, http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.

[3] See G20, *Chair's Summary: G20 Finance Ministers and Central Bank Governors Meeting, Washington, D.C., USA, 12-13 October 2017*, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/2017-11-03-g20-chairs-summary.pdf;jsessionid=B6890DCD16EB588B45663F2C579BF598?__blob=publicationFile&v=2.

Questions for public consultation (Please provide supporting reasons for your views.)

The FSB invites comments on the draft lexicon and the following specific questions:

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?

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?

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.

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.

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?

1. Background

Cyber incidents are a threat to the entire financial system, a fact that is underscored by recent reports of significant and damaging incidents both inside and outside the financial sector. The 2016 attack on the Bangladesh Bank resulted in the theft of $81 million, the WannaCry ransomware attack in 2017 infected more than 250,000 computer systems in 150 countries, and the Equifax hack in 2017 resulted in the compromise of personal information of over 146 million individuals.[4] Cyber risk to financial institutions is driven by several factors, including evolving technology, which can lead to new or increased vulnerabilities; interconnections among financial institutions and between financial institutions and external parties, e.g. through cloud computing and FinTech providers who in some cases may not be subject to regulation by financial sector authorities; determined efforts by cyber criminals to find new methods to compromise ICT systems; and the attractiveness of financial institutions as targets for cyber criminals seeking illicit financial gain.[5] Recognising the risks from cyber incidents, authorities

[4] See "How cyber criminals targeted almost $1bn in Bangladesh Bank heist", *Financial Times*, 18 March 2016, https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8; "Ransomware cyber-attack threat escalating – Europol", *BBC*, 14 May 2017, http://www.bbc.com/news/technology-39913630; and Form 8-K of Equifax Inc. (filed 7 May 2018), https://www.sec.gov/Archives/edgar/data/33185/000119312518154706/0001193125-18-154706-index.htm.

[5] For a discussion of cyber risk in the context of FinTech (i.e. technology-enabled innovation in financial services), see FSB, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*, 27 June 2017, http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/.

For an example of the evolution of attack methods, see B. Krebs, "Source Code for IoT Botnet 'Mirai' Released", 1 October 2016, https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

across the globe have taken regulatory and supervisory steps designed to facilitate both the mitigation of cyber risk by financial institutions, and their effective response to, and recovery from, cyber incidents.

The Communiqué issued at the March 2017 meeting of the G20 Finance Ministers and Central Bank Governors in Baden-Baden noted that the malicious use of ICT could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.[6] The Ministers and Governors further noted that they would promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20. With the aim of enhancing cross-border cooperation, the FSB was asked, as a first step, to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices. The FSB prepared a stocktake report (Stocktake Report) and summary report (Summary Report), which were informed by survey responses from FSB members and a public-private sector workshop in September 2017.[7]

The Stocktake Report explores existing publicly released regulations, supervisory practices and guidance in the area of cyber security across the financial sector, including whether gaps exist and the degree of uniformity across the financial sector and FSB member jurisdictions. The conclusions from the stocktake include the following. FSB member jurisdictions have been active in addressing cyber security for the financial sector, with all 25 member jurisdictions reporting that they have publicly released regulations or guidance that address cyber security for at least a part of the financial sector.[8] All or nearly all jurisdictions have addressed banks and financial market infrastructures, and a majority have addressed trading venues, insurance companies, broker-dealers and asset managers. All FSB member jurisdictions reported drawing upon a small body of previously developed national or international guidance or standards of public authorities or private bodies in developing their cyber security regulatory and supervisory schemes for the financial sector, which suggests some degree of international convergence. Indeed, a number of content elements were commonly covered, e.g. governance; risk assessment; prevention, detection and reduction of vulnerability; training; and regulatory reporting. Though similar, regulations and guidance are certainly not identical across jurisdictions, e.g. while some schemes were characterised as addressing operational risk generally, others were more targeted to cyber security and/or ICT risk.

For an outline of the high yield of recent attacks targeting the financial sector, see C. Wueest, Symantec, “Financial Threats Review 2017, Targeted financial heists”, May 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.

[6] See G20, *Communiqué: G20 Finance Ministers and Central Bank Governors Meeting, Baden-Baden, Germany, 17-18 March 2017*, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/g20-communique.pdf?__blob=publicationFile&v=3.

[7] See FSB, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices*, 13 October 2017, http://www.fsb.org/wp-content/uploads/P131017-2.pdf; and FSB, *Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices*, 13 October 2017, http://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/.

[8] The FSB member jurisdictions are Argentina, Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom, United States and the European Union.

In addition to summaries of the conclusions from the FSB's stocktake survey, the Summary Report includes key themes raised in the discussion at the September workshop.[9] Private sector participants acknowledged the importance of responding to the legitimate and growing needs of financial regulators and supervisors globally in the area of cyber security and expressed support for principles-based, risk-based and proportional regulation. They expressed concerns about conflicting requirements; multiple similar, but not identical, requirements; and multiple examinations. Both FSB member representatives and private sector participants in the workshop were of the view that information sharing is important in the area of cyber security. Participants generally expressed interest in enhanced cyber security information sharing, although they did not discuss in detail who should share information, e.g. private firms among themselves, regulators among themselves and/or regulators and industry, or what information should be shared, e.g. threat intelligence, effective cyber security industry or regulatory practices, and/or information about specific incidents. Both private and public sector participants noted that cyber security is an inherently cross-border issue, but acknowledged that setting up a cross-border architecture for information sharing presents a significant challenge.

At its October 2017 meeting in Berlin, the FSB Plenary reviewed the results of the stocktake and discussed the key themes raised in the public-private sector workshop.[10] The Plenary agreed that a lexicon of cyber security terms, including on topics related to information sharing, would be developed for use by relevant authorities and international bodies to facilitate consistent use of terminology. In October 2017, the FSB delivered the Stocktake Report and Summary Report to the G20.

At their October 2017 meeting in Washington, DC, the Finance Ministers and Central Bank Governors welcomed the FSB Stocktake Report and agreed that further action is needed to strengthen the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT. The Finance Ministers and Central Bank Governors asked the FSB to continue its work to protect financial stability against the malicious use of ICT in line with the Baden-Baden agreement and noted that this work could be supported by the creation of a common lexicon of terms that are important in the work being pursued.[11]

Accordingly, the FSB has now developed a draft lexicon of terms related to cyber security and cyber resilience, and is publishing the draft lexicon for public consultation. After considering the responses to this consultation, the FSB intends to finalise the lexicon for delivery to the G20 Summit in Buenos Aires in November of this year. The FSB welcomes comments on this document. Comments should be submitted by 20 August 2018 as described in greater detail in the Introduction.

[9] The key themes do not necessarily represent the views of authorities nor consensus views expressed by private sector participants at the workshop.

[10] See FSB, "FSB discusses 2018 workplan and next steps on evaluations of effects of reforms", 6 October 2017, http://www.fsb.org/2017/10/fsb-discusses-2018-workplan-and-next-steps-on-evaluations-of-effects-of-reforms/.

[11] See G20, *Chair's Summary: G20 Finance Ministers and Central Bank Governors Meeting, Washington, D.C., USA, 12-13 October 2017*, http://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Featured/G20/2017-11-03-g20-chairs-summary.pdf;jsessionid=B6890DCD16EB588B45663F2C579BF598?__blob=publicationFile&v=2.

2. Objective of the lexicon

The objective of FSB work to develop a cyber lexicon is to support the work of the FSB; standard-setting bodies (SSBs), including the Basel Committee on Banking Supervision (BCBS), Committee on Payments and Market Infrastructures (CPMI), International Association of Insurance Supervisors (IAIS) and International Organization of Securities Commissions (IOSCO); authorities; and private sector participants, e.g. financial institutions and international standards organisations, to address cyber security and cyber resilience in the financial sector. The lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract. A lexicon could be useful to support work in the following areas.

Cross-sector common understanding of relevant cyber security and cyber resilience terminology. A lexicon could be useful to foster a common understanding of relevant cyber security and cyber resilience terminology across the financial sector, including banking, financial market infrastructures, insurance and capital markets, and with other industry sectors. A common understanding across the financial sector, including among authorities and private participants, could help to enhance cyber security and cyber resilience throughout the sector. More broadly, a common lexicon could foster a common understanding with other industry sectors and facilitate appropriate cooperation to enhance cyber security and cyber resilience.

Work to assess and monitor financial stability risks of cyber risk scenarios. As the FSB and its members work to assess and monitor financial stability risks associated with cyber incidents, the work could be supported by a lexicon that promotes a common understanding concerning the terminology related to cyber risks. For instance, as part of its regular assessment of vulnerabilities in the global financial system, the FSB from time to time considers the potential for operational risks, including cyber risks, to result in shocks that could be transmitted across the financial system.

Information sharing as appropriate. A lexicon that facilitates a common understanding across the financial sector, including public and private participants, and also across jurisdictions, could be useful in efforts to enhance appropriate information sharing. At the FSB's workshop last September, both FSB member representatives and private sector participants were of the view that information sharing is important in the area of cyber security, but they also noted considerable associated challenges.

Work by the FSB and/or SSBs to provide guidance related to cyber security and cyber resilience, including identifying effective practices. A lexicon could be useful in work by the FSB and/or SSBs to provide guidance related to cyber security and cyber resilience, including identifying effective practices. It could, for example, foster effective regulatory approaches while reducing the risk of duplicative and potentially conflicting regulatory requirements.

The FSB expects that the use of common terminology will facilitate work in the areas outlined above. While the lexicon is intended to support work that the FSB, SSBs, authorities and private sector participants determine to undertake in those areas, it is designed as a helpful tool and its use would not be mandatory.

3. Development of the draft lexicon

3.1 Process for developing the draft lexicon

In developing a draft lexicon which could effectively serve the objective outlined above, the FSB actively sought to incorporate a diversity of views. In order to develop the lexicon, the FSB formed a working group of experts, chaired by the U.S. Federal Reserve Board. The group members were selected for their expertise in cyber security and cyber resilience regulation and supervision and for their representation of a broad range of FSB member jurisdictions and financial sectors (banks, financial market infrastructures, securities and insurance). The working group included representatives of each of the SSBs, namely, BCBS, CPMI, IAIS and IOSCO.

The working group developed an initial draft lexicon. This was followed by a period of engagement in order to enlist expertise outside the working group and the financial sector. Initially, working group members consulted with other public officials in their home jurisdictions, and with members of the SSBs, in order to draw on a broader perspective and facilitate the creation of a lexicon that would be useful both across the financial sector, and in communications between the financial sector and other industry sectors. Thereafter, the working group met with representatives of organisations that have been active in the establishment of, and/or training with respect to, cyber security standards, in order to solicit their feedback. These organisations include the International Organization for Standardization (ISO), ISACA (previously known as the Information Systems Audit and Control Association), the SANS Institute and the U.S. National Institute of Standards and Technology (NIST).[12] In addition, the FSB's Standing Committee on Supervisory and Regulatory Cooperation and the full membership of the FSB had opportunities to contribute to the draft lexicon, which is being published today for consultation.

3.2 Selection of terms included in the draft lexicon

The working group applied the following criteria in selecting terms included in the lexicon.

Meeting the objective of the lexicon. The lexicon should be focused on supporting other work of the FSB, SSBs, authorities and private sector participants related to financial sector cyber security and cyber resilience, including in the four areas enumerated in the Objective section of this document. These areas are: cross-sector common understanding of relevant cyber security and cyber resilience terminology; work to assess and monitor financial stability risks of cyber risk scenarios; information sharing as appropriate; and work by the FSB and/or SSBs to provide guidance related to cyber security and cyber resilience, including identifying effective practices. The focus was on terms that are relevant to the financial sector and useful to support work undertaken by the FSB and SSBs, as well as financial sector regulators, supervisors and private sector participants.

Scope of the lexicon. The lexicon should be limited in scope and focused on the core terms necessary to support the objective of the lexicon. The lexicon is not intended to be a

[12] In the FSB's stocktake survey, FSB members frequently reported relying on the work of ISO, ISACA and NIST. See FSB, *Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices* (Figure 2 and accompanying text), 13 October 2017, http://www.fsb.org/wp-content/uploads/P131017-2.pdf.

comprehensive lexicon of all cyber security- and cyber resilience-related terms. Considerable high quality work has already been completed by a number of organisations to develop cyber security, cyber resilience and ICT definitions, including the work of ISO, ISACA, the SANS Institute and NIST. The goal of FSB lexicon development was not to replicate this work, but rather to develop and propose common definitions of a core set of terms relevant to financial sector participants in both the public and private sectors.

Exclusion of technical terms. In view of the lexicon's focus on core terms for the financial sector, technical ICT terms should generally be excluded from the lexicon. First, they are not core terms necessary to support the objective of the lexicon. Second, defining these terms is generally outside the expertise of the financial sector authorities who comprise the FSB's membership and is more appropriately left to standard setters whose expertise lies in ICT and related areas. Third, the FSB is not well-placed to define technical terms that may become obsolete rapidly as a result of technological and other changes.

Exclusion of general business and regulatory terms. The lexicon should generally not include terms that are used by financial sector participants in areas extending beyond cyber security and cyber resilience. These terms, while they may be important in addressing cyber security and cyber resilience, are typically well defined and well understood and, in any event, are not unique to cyber security and cyber resilience. Examples of terms excluded on this basis are Business Continuity Plan, Criticality and Enterprise Risk Management. The draft lexicon contains certain terms that may have broader or multiple meanings in different supervisory contexts. In such cases, the definitions in the draft lexicon relate only to the context of cyber security and cyber resilience. Examples of such terms include Confidentiality and Continuous Monitoring.

3.3 Criteria used in developing definitions for terms in the draft lexicon

The working group applied the following criteria in developing definitions for terms in the draft lexicon.

Reliance on existing sources. Development of the lexicon should draw on the extensive work that has previously been done or is underway by other groups in developing lexicons and glossaries related to cyber security and cyber resilience, such as the work of CPMI-IOSCO in its guidance on cyber resilience for financial market infrastructures,[13] the work of the G7 Cyber Expert Group,[14] the work of NIST in its glossary of key information security terms[15] and the work of ISO.[16] The FSB's work should build upon prior efforts, draw from those efforts materials that are relevant for the FSB's purposes and make modifications only as needed and appropriate to the FSB's purposes.

Comprehensive definitions. Definitions included in the lexicon should be comprehensive. Definitions selected for the terms in the lexicon should cover all the key elements necessary to

[13] See CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, June 2016, www.bis.org/cpmi/publ/d146.pdf.

[14] See G-7, *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, October 2017, http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf.

[15] See NIST, *Glossary of Key Information Security Terms*, May 2013, nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[16] See, for example, ISO, "ISO/IEC 27000:2018", February 2018, https://www.iso.org/standard/73906.html.

a definition of the term. Modifications to definitions in existing sources would be appropriate where a gap was identified in an existing definition selected for inclusion in the lexicon.

Plain Language. Definitions used in the lexicon should be concise and use clear, plain language and avoid technical terms and complex grammatical constructions.

4. Request for comment

The FSB draft lexicon appears in the Annex. As described in greater detail in the Introduction, the FSB invites comments on the draft lexicon and, specifically, on the questions set forth in the Introduction.

Annex: Draft Cyber Lexicon[1]

Note: Source citations below are abbreviated. Full source citations appear at the end of the Annex.

Term	Definition
Access Control	Means to ensure that access to assets is authorised and restricted based on business and security requirements. Source: ISO/IEC 27000:2018
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
Alert	Notification that a specific attack or threat has been directed at an organisation's information systems. Source: Adapted from NIST
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. Source: ISACA Fundamentals
Authentication	Provision of assurance that a claimed characteristic of an entity is correct. Source: ISO 27000:2018
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018
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

[1] The terms and definitions in the lexicon apply only to the financial services sector and the financial institutions therein. The lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract.

Term	Definition
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities or processes. Source: ISO/IEC 27000:2018
Configuration Management	An activity of managing the configuration of an information system throughout its life cycle. Source: ISO/IEC 10032:2003
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)
Course of Action (CoA)	An action taken to either prevent a cyber incident or respond to a cyber incident. Source: Adapted from STIX
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)
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")
Cyber Hygiene	A set of practices for managing the most common and pervasive cyber risks faced by organisations. Source: Adapted from Carnegie Mellon University
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")
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

Term	Definition
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”)
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
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
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
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
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
Detect	Develop and implement the appropriate activities to identify the occurrence of a cyber event. Source: Adapted from NIST Framework

Term	Definition
Distributed Denial of Service (DDoS)	A denial of service that is delivered using numerous sources simultaneously. Source: Adapted from NICCS
Exploit	Defined way to breach the security of information systems through vulnerability. Source: ISO/IEC 27039:2015
Identify	Develop the organisational understanding to manage cyber risk to systems, assets, data and capabilities. Source: Adapted from NIST Framework
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 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
Indicators of Compromise (IoCs)	Evidence of an intrusion that can be identified in an information system. Source: Adapted from SANS InfoSec Reading Room
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
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
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

Term	Definition
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
Multi-Factor Authentication	Authentication using two or more of the following factors: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; -- biometric factor, "something an individual is or is able to do". Source: ISO/IEC 27040:2015
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
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
Protect	Develop and implement the appropriate safeguards to ensure delivery of services. Source: Adapted from NIST Framework
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
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
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

Term	Definition
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 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
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
Social Engineering	A general term for trying to deceive people into revealing confidential information or performing certain actions. Source: Adapted from FFIEC
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
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent. Source: Adapted from STIX
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
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

Term	Definition
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

Sources

Carnegie Mellon University	Carnegie Mellon University Software Engineering Institute, Cyber Hygiene: A Baseline Set of Practices (2017) https://resources.sei.cmu.edu/asset_files/Presentation/2017_017_001_508771.pdf
CPMI-IOSCO	CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (June 2016) https://www.bis.org/cpmi/publ/d146.pdf
FFIEC	FFIEC (Federal Financial Institutions Examination Council) IT Examination Handbook Infobase, Glossary https://ithandbook.ffiec.gov/glossary.aspx
FIRST	FIRST Traffic Light Protocol (TLP), Version 1.0 https://www.first.org/tlp/docs/tlp-v1.pdf
ISACA Fundamentals	ISACA Cybersecurity Fundamentals Glossary (2016) http://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf
ISACA Full Glossary	ISACA Glossary https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf
ISO/IEC 10032:2003	ISO/IEC TR 10032:2003 https://www.iso.org/standard/38607.html
ISO 22300:2018	ISO 22300:2018 https://www.iso.org/standard/68436.html
ISO/IEC 27000:2018	ISO/IEC 27000:2018 https://www.iso.org/standard/73906.html
ISO/IEC 27032:2012	ISO/IEC 27032:2012 https://www.iso.org/standard/44375.html
ISO/IEC 27033-1:2015	ISO/IEC 27033-1:2015 https://www.iso.org/standard/63461.html
ISO/IEC 27035-1:2016	ISO/IEC 27035-1:2016 https://www.iso.org/standard/60803.html
ISO/IEC 27039:2015	ISO/IEC 27039:2015 https://www.iso.org/standard/56889.html

ISO/IEC 27040:2015	ISO/IEC 27040:2015 https://www.iso.org/standard/44404.html
NICCS	NICCS (National Initiative for Cybersecurity Careers and Studies), Explore Terms: A Glossary of Common Cybersecurity Terminology http://niccs.us-cert.gov/glossary
NIST	NIST, Glossary of Key Information Security Terms, Revision 2 (May 2013) https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
NIST 800-150	NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing (October 2016) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf
NIST Framework	NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (16 April 2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
SANS InfoSec Reading Room	SANS Institute, InfoSec Reading Room: Using IOC (Indicators of Compromise) in Malware Forensics (21 February 2013) https://www.sans.org/reading-room/whitepapers/forensics/ioc-indicators-compromise-malware-forensics-34200
STIX	Structured Threat Information Expression (STIX™) 2 https://oasis-open.github.io/cti-documentation/stix/intro.html