FSB FINANCIAL STABILITY BOARD

Cyber Lexicon

12 November 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

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.[1] 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.[2] Recognising the risks from cyber incidents, authorities 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 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.[3] 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

[1] 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.

[2] 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/.

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.

[3] 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.

with respect to cyber security in the financial sector to the Finance Ministers and Central Bank Governors meeting in Washington, DC. [4] 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.[5] After public consultation, the FSB has developed and is publishing a final lexicon of terms related to cyber security and cyber resilience.[6]

[4] 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/.

[5] 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.

[6] See FSB, *Cyber Lexicon Consultative Document*, 2 July 2018, http://www.fsb.org/2018/07/cyber-lexicon-consultative-document/.

1. 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.

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 is not mandatory.

2. Development of the lexicon

2.1 Process for developing the lexicon

In developing a 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).[7] 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. Thereafter, the draft lexicon was published for consultation, and the final lexicon reflects consideration by the FSB of the comments submitted by respondents in the consultation. Simultaneously with the publication of this final lexicon, the FSB is publishing a report that summarises public comments and explains how they were resolved.[8]

2.2 Selection of terms included in the lexicon

The following criteria have been applied 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 is on terms that are relevant to the financial sector and useful to support work

[7] 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.

[8] See FSB, *Cyber Lexicon Overview of Responses to the Public Consultation*, http://www.fsb.org/2018/11/cyber-lexicon-overview-of-responses-to-the-public-consultation/.

undertaken by the FSB and SSBs, as well as financial sector regulators, supervisors and private sector participants. While all of the terms included in the lexicon are relevant to the financial sector, terms were not excluded on the basis that they might also be relevant to other sectors.

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 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. That said, the line between technical terms and other terms is not always clear, and some ICT-related terms, such as *Denial of Service*, have been included in cases where the FSB concluded that they were likely to be useful in meeting the objectives of the lexicon.

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*, *Risk*, *Risk Assessment*, *Risk Appetite* and *Risk Management*. The lexicon does contain some 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. One example of such a term is *Confidentiality*.

2.3 Criteria used in developing definitions for terms in the lexicon

The working group applied the following criteria in developing definitions for terms in the 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,[9] the work of the G-7 Cyber

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

Expert Group,[10] the work of NIST in its glossary of key information security terms[11] and the work of ISO.[12] 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 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. Whenever possible, the lexicon should not use highly technical language designed to facilitate communications among ICT professionals.

[10] 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.

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

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

Annex: Cyber Lexicon[1]

Notes:

- ***Source citations below are abbreviated. Full source citations appear at the end of the Annex.***
- ***Terms defined in the lexicon are italicised when used in definitions within the lexicon.***
- ***When used in the lexicon, "entity" includes a natural person where the context requires.***

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
Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity. Source: ISO/IEC 2382:2015
Advanced Persistent Threat (APT)	A *threat actor* that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple *threat vectors*. The *advanced persistent threat*: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to execute its objectives. 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
Authenticity	Property that an entity is what it claims to be. Source: ISO/IEC 27000:2018
Availability	Property of being accessible and usable on demand by an authorised entity. Source: ISO/IEC 27000:2018

[1] The terms and definitions in the lexicon were developed only for use with respect 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
Campaign	A grouping of coordinated adversarial behaviours that describes a set of malicious activities that occur over a period of time against one or more specific targets. Source: Adapted from STIX
Compromise	Violation of the security of an *information system*. Source: Adapted from ISO 21188:2018
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. Source: Adapted from ISO/IEC 27000:2018
Course of Action (CoA)	An action or actions taken to either prevent or respond to a *cyber incident*. It may describe technical, automatable responses but can also describe other actions such as employee training or policy changes. 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 Advisory	Notification of new trends or developments regarding a *cyber 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
Cyber Alert	Notification that a specific *cyber incident* has occurred or a *cyber threat* has been directed at an organisation's *information systems*. Source: Adapted from NIST
Cyber Event	Any observable occurrence in an *information system*. *Cyber events* sometimes provide indication that a *cyber incident* is occurring. Source: Adapted from NIST (definition of "Event")

Term	**Definition**
Cyber Incident	A *cyber event* that: i. jeopardizes the *cyber security* of an *information system* or the information the system processes, stores or transmits; or ii. violates the 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
Cyber Resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to *cyber threat*s and other relevant changes in the environment and by withstanding, containing and rapidly recovering from *cyber incident*s. Source: Adapted from CERT Glossary (definition of "Operational resilience"), CPMI-IOSCO and NIST (definition of "Resilience")
Cyber Risk	The combination of the probability of *cyber incidents* occurring and their impact. 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. 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 with the potential to exploit one or more *vulnerabilities* that adversely affects *cyber security*. 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 data transmitted, stored or otherwise processed. Source: Adapted from ISO/IEC 27040:2015

Term	Definition
Defence-in-Depth	Security strategy integrating people, processes and technology 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 (function)	Develop and implement the appropriate activities to identify the occurrence of a *cyber event*. Source: Adapted from NIST Framework
Distributed Denial of Service (DDoS)	A *denial of service* that is carried out 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 (function)	Develop the organisational understanding to manage *cyber risk* to *assets* and capabilities. Source: Adapted from NIST Framework
Identity and Access Management (IAM)	Encapsulates people, processes and technology to identify and manage the data used in an *information system* to authenticate users and grant or deny access rights to data and system resources. Source: Adapted from ISACA Full Glossary
Incident Response Team (IRT) [also 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)	Identifying signs that a *cyber incident* may have occurred or may be currently occurring. Source: Adapted from NIST (definition of “Indicator”)
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events. Source: Adapted from NICCS

Term	Definition
Information System	Set of applications, services, information technology *assets* or other information-handling components, which includes the operating environment. Source: Adapted from ISO/IEC 27000:2018
Integrity	Property of accuracy and completeness. Source: ISO/IEC 27000:2018
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their *information systems*. Source: Adapted from ISO/IEC 27032:2012
Multi-Factor Authentication	The use of two or more of the following factors to verify a user's identity: -- knowledge factor, "something an individual knows"; -- possession factor, "something an individual has"; -- biometric factor, "something that is a biological and behavioural characteristic of an individual". Source: Adapted from ISO/IEC 27040:2015 and ISO/IEC 2832-37:2017 (definition of "biometric characteristic")
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities. Source: ISO 27000:2018
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	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an *information system*. Source: NIST
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of *cyber incidents*. Source: Adapted from NIST Framework

Term	Definition
Recover (function)	Develop and implement the appropriate activities to maintain plans for *cyber resilience* and to restore any capabilities or services that were impaired due to a *cyber incident*. Source: Adapted from NIST Framework
Reliability	Property of consistent intended behaviour and results. Source: ISO/IEC 27000:2018
Respond (function)	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 *cyber threat intelligence* process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event. Source: CPMI-IOSCO
Social Engineering	A general term for trying to deceive people into revealing 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
Threat Assessment	Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat. Source: Adapted from NIST
Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes. Source: NIST 800-150

Term	Definition
Threat-Led Penetration Testing (TLPT) [also known as Red Team Testing]	A controlled attempt to compromise the *cyber resilience* of an entity by simulating the *tactics, techniques and procedures* of real-life *threat actors*. It is based on targeted *threat intelligence* and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations. Source: G-7 Fundamental Elements
Threat Vector	A path or route used by the *threat actor* to gain access to the target. Source: Adapted from ISACA Fundamentals
Traffic Light Protocol (TLP)	A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established colour code to indicate expected sharing boundaries to be applied by the recipient. Source: Adapted from FIRST
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. Source: ISO/IEC 27042:2015
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
Vulnerability Assessment	Systematic examination of an *information system*, and its controls and processes, 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: Adapted from NIST

Sources

CERT Glossary	Carnegie Mellon Software Engineering Institute, CERT® Resilience Management Model, Version 1.2, Glossary of Terms https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514934.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
G-7 Fundamental Elements	G-7 Fundamental Elements for Threat-Led Penetration Testing https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.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 2832:2015	ISO/IEC 2832:2015 https://www.iso.org/standard/63598.html
ISO/IEC 2832-37:2017	ISO/IEC 2832-37:2017 https://www.iso.org/standard/66693.html
ISO 21188:2018	ISO 21188:2018 https://www.iso.org/standard/63134.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
ISO/IEC 27042:2015	ISO/IEC 27042:2015 https://www.iso.org/standard/44406.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
STIX	Structured Threat Information Expression (STIX™) 2 https://oasis-open.github.io/cti-documentation/stix/intro.html