FSB FINANCIAL STABILITY BOARD

Cyber Lexicon

Updated in 2023

13 April 2023

The Financial Stability Board (FSB) coordinates 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.

Contact 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

Introduction

In 2018, the Financial Stability Board (FSB) developed the Cyber Lexicon to support the work of the FSB, the standard-setting bodies (SSBs) and other international organisations to address cyber security and cyber resilience in the financial sector. Following its initial publication in 2018, the Cyber Lexicon was updated in 2023 to ensure it remained current with the evolving cyber landscape and development of information technology.[1] The same criteria for inclusion and exclusion used in the creation of the lexicon in 2018 (see Section 2) were applied to ensure continued consistency in content. In updating the lexicon, the FSB reviewed over 80 terms proposed by the private sector and national authorities for inclusion, and also considered feedback from a public consultation and via engagement with the private sector.[2]

After considering recent developments in the cyber threat landscape, the terms: 'cyber attack', 'insider threat', 'phishing', 'ransomware' and 'zero-day vulnerability' were deemed to be significant enough for inclusion. Further, the term 'security operations centre' was considered as an essential function of many FIs, which play an integral role in detecting and managing cyber incidents and would benefit from inclusion to further advance the work on enhancing cyber resilience. It was also deemed important to revise the following definitions: 'cyber alert', 'cyber incident', 'cyber incident response plan', 'information system', 'penetration testing' and 'vulnerability assessment'.[3] On the definition of 'cyber incident', there were mixed views over whether it should be kept broad to encompass incidents arising from both malicious and non-malicious activities, or to confine it to focus only on malicious activities. Given that most financial authorities have been using the term more broadly in their policies, regulations and guidance, the FSB decided that the broader definition should be adopted to promote convergence. See Annex B for a detailed explanation on the core concepts underpinning the FSB's definition of cyber incident.

1. Objectives of the lexicon

The objective of FSB work to develop a cyber lexicon is to support the work of the FSB; 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,

---

1 The exercise to update the Cyber Lexicon was conducted as part of the FSB's work to achieve greater convergence in cyber incident reporting.

2 FSB (2023), *Achieving Greater Convergence in Cyber Incident Reporting: Overview of responses to consultative document*, April.

3 Annex A shows how the definitions to these terms were revised.

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 sector participants, could help to enhance cyber security and cyber resilience throughout the financial 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 encouraged. In particular, the FSB's outreach work indicated that greater adoption of the Cyber Lexicon by public authorities, including within legislation and regulatory guidance, would especially motivate its uptake by the private sector.

2. Criteria applied in the development of the lexicon

2.1. Criteria for inclusion 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

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*.

2.2. Criteria used in developing definitions for terms in the lexicon

The following criteria were applied 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,[4] the work of the G-7 Cyber Expert Group,[5] the work of NIST in its glossary of key information security terms[6] and the work of ISO.[7] 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.

3. Cyber Lexicon[8]

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

4 CPMI-IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, June.

5 G-7 (2017), *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector*, October.

6 NIST (2013), *Glossary of Key Information Security Terms*, May.

7 See, for example, ISO (2018), *ISO/IEC 27000:2018*, February.

8 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
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
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

Term	Definition
Cyber Alert	1. 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 2. Announcement of an abnormal situation or condition (from one or more *cyber events*) requiring attention. Source: Adapted from ISO 8468 2007
Cyber Attack	Malicious attempt(s) to exploit *vulnerabilities* through the *cyber* medium to damage, disrupt or gain unauthorized access to *assets.* Source: Adapted from ISO 27100:2020
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")
Cyber Incident	A *cyber event* that adversely affects the *cyber security* of an *information system* or the information the system processes, stores or transmits 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 guide the response 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

Term	Definition
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
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 and networks. Source: Adapted from ISO/IEC 27000:2018
Insider Threat	A trusted entity with potential to use their access or knowledge to adversely affect an organisation's *assets.* Source: Adapted from NIST and CISA
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 an individual is or is able to do". Source: Adapted from ISO/IEC 27040:2015
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 typically working under specific constraints, attempt to circumvent or defeat the security features of an *information system*. Source: NIST
Phishing	A digital form of *social engineering* that attempts to acquire private or confidential information by pretending to be a trustworthy entity in an electronic communication. Source: Adapted from ISO/IEC 27032:2012 and NICCS
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
Ransomware	*Malware* that is used to commit extortion by impairing the use of an *information system* or its information until a ransom demand is satisfied. Source: Adapted from ISACA Full Glossary and SANS
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
Security Operations Centre (SOC)	A formally recognised function or service responsible for protecting *information systems*, as well as monitoring, detecting, assessing and remediating *cyber threats* and *cyber incidents* Source: Adapted from CPMI-IOSCO and ISACA Full Glossary
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

Term	Definition
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
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 Cyber Expert Group
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
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* 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
Zero-day Vulnerability	A previously unknown *vulnerability* within an *information system*. Source: Adapted from the NIST Glossary

Annex A: Revision log

Revision	Changes(s) made	
1.0 Nov 2018	First edition of Cyber Lexicon, containing 50 terms and definitions.	
2.0 Apr 2023	**New terms** ■ Cyber Attack ■ Insider Threat ■ Phishing ■ Ransomware ■ Security Operations Centre (SOC) ■ Zero-day Vulnerability	
	Adjusted definitions of existing terms	
	Cyber Alert	1. 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 2. Announcement of an abnormal situation or condition (from one or more *cyber events*) requiring attention. Source: Adapted from ISO 8468 2007
	Cyber Incident	A *cyber event* that~~:~~ ~~i) jeopardizes~~ adversely affects 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.
	Cyber Incident Response Plan	The documentation of a predetermined set of instructions or procedures to ~~respond~~guide the response to, and limit consequences of, a *cyber incident*.
	Information System	Set of applications, services, information technology *assets* or other information-handling components, which includes the operating environment and networks.
	Penetration Testing	A test methodology in which assessors~~, using all available documentation (e.g. system design, source code, manuals) and~~ typically working under specific constraints, attempt to circumvent or defeat the security features of an *information system*.
	Vulnerability Assessment	Systematic examination of an *information system*~~, and its controls and processes,~~ 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.

Annex B: Background on core concepts

In line with the Cyber Lexicon's objective to promote common understanding, this annex elaborates on core concepts which, based on responses to consultation, would benefit from further explanation. In particular, two subsets of terms attract the greatest level of interest:

- **occurrence** terminology, and the relationship between event, incident and attack; and
- **domain** terminology, and specifically how 'cyber' relates to other domains.

It is important to note that the majority of terms described in this annex fall outside of the scope of the Cyber Lexicon, and are therefore not appropriate for inclusion. Additionally, the definitions provided for excluded terms have not been subject to the same rigour and analysis as included terms, but are presented to provide an indicative view on relationships between terms. It is possible that these terms and definitions (or variants thereof) could become eligible for inclusion in future, if the scope of the Lexicon is broadened.

As well as examining individual terms, suggested definitions, and their source material, an illustration of the interplay between related terms is shown in Figure 1. Note that the relative size or positioning of elements within this diagram are notional, and do not represent precise depictions. This annex also describes how domain and occurrence terms can be combined to form compound terms found within the Cyber Lexicon.

Occurrence

The terms grouped under the concept of occurrence are used to describe 'what happened', irrespective of the domain in which they took place. The following four commonly referenced terms are further explained:

- **event**: '*an observable occurrence or change of a particular set of circumstances*'. Drawing on both ISO[9] and NIST[10] sources, this definition reinforces the principle that an occurrence needs to be observed to be considered as an event.
- **incident**: *'an event, series of events, or situation that leads to a disruption, loss, emergency or crisis'*. This definition is sourced from ISO,[11] but adjustments have been made to remove the concept of potentiality. This adjustment reduces definitional uncertainty by providing a clear and unambiguous transition between an event and an incident, i.e. when adverse effects[12] are observed. The definition here also augments the source material to include circumstances where multiple related events lead to an incident (not just singular events).

---

9 ISO 27005:2022, Definition of 'event': *Occurrence or change of a particular set of circumstances.*

10 NIST SP 800-61, Definition of 'event': *Any observable occurrence in a network or system.*

11 ISO 22361:2022: Definition of 'incident': *Event or situation that can be, or could lead to, a disruption, loss, emergency or crisis.*

12 Adverse effects include observable negative impact or harm.

- **near miss**: *'an event where no harm or impact occurs but has the potential to do so.'* Drawing on ISO definitions related to Health and Safety[13], references to injury and ill health are substituted for more generalised expression of adverse effects (i.e. harm or impact). In addition, the definition is adjusted to be based off of events rather than incidents, so that the removal of potentiality is maintained.

- **attack**: *'malicious attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.'* This definition is sourced primarily from ISO[14], as the wording can be used in context other than cyber security. The definition is augmented to make explicit reference to a malicious act drawing on equivalent NIST references[15]. As shown in Figure 1, the relationship between this term and 'incident' illustrates that an attack can be either successful (and have adverse effects), or unsuccessful.

Domain

The domain concept is used to describe a 'space' or 'medium' whose components share similar characteristics. Although many other domains exist, the following selection are provided for comparative purposes, given their relative proximity to the 'cyber' domain:

- **data**: *'Reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.'* This definition establishes data as a raw representation of facts, drawing on ISO[16] rather than NIST[17] sources which were considered to be more descriptive.

- **information**: *'Knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning.'* Drawing on the same ISO source[18] as 'data', the key differentiator between these two terms is that information puts data in context and conveys meaning.

- **Information Technology (IT)**: *'Development, maintenance, and use of technology to acquire, process, store and distribute digital information.'* The unchanged ISO definition[19] reflects IT as a compound term, describing the use of technology in the context of (digital) information. Figure 1 reflects a partial overlap with data and information to exclude the analogue medium.

---

13 ISO 45001:2018, Definition of 'near miss': *An incident where no injury and ill health occurs but has the potential to do so.*

14 ISO 27000:2018, Definition of 'attack': *Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.*

15 NIST CNSSI 4009-2015, Definition of 'attack': *Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.*

16 ISO 8000-2:2022: Definition of 'data': *Reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.*

17 NIST IR 4734, Definition of 'data': *A representation of information as stored or transmitted.*

18 ISO 8000-2:2022: Definition of 'information': *Knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning.*

19 ISO 19770-1:2017: Definition of 'information technology': *Development, maintenance, and use of technology to acquire, process, store and distribute digital information.*

- **Information and Communication Technology (ICT)**: '*Technology for gathering, storing, retrieving, processing, analysing and transmitting information.'* The inclusion of the transmission concept within the ICT definition (as per ISO[20]) is intended to augment the IT definition to capture those technologies involved in the transfer of information. Hence, Figure 1 depicts IT as a subset of ICT.

- **Cyber**: *'Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.'* The Cyber Lexicon's definition, which draws on CPMI-IOSCO which in turn is based off of NICCS[21], captures the interactions that occur between physical, logical, and social/cognitive planes. Accordingly, the cyber domain includes interaction with elements which fall outside of the ICT and information domains, such as people or operational technology. Conversely, aspects of other domains are not covered by cyber, e.g. analogue activities, or physical aspects of information systems. Importantly, the cyber definition does not contain or portray any negative connotation as it only describes a domain. However, use of the term, especially in mainstream media and popular culture, typically conveys a malicious overtone[22].

- **Operational**: *'Relating to people, processes, information, information systems, facilities, or external dependencies used to deliver one or more activities, functions or services.'* The operational domain encompasses all previously defined domains, as well as other elements not covered in this annex. In the absence of definitional sources from international standard setters, the definition above draws from, and blends, well established definitions from financial standard setting bodies[23,24,25].

- **Security**: *'Freedom from those conditions that can cause loss of assets with unacceptable consequences.'* Leveraging NIST sources[26] rather than ISO[27] for their broader applicability, the term 'security' can be appended to any of the previous domains as a transversal that is specifically focused on the preservation of security of assets within that given domain.

---

20 ISO 30145:2020, Definition of 'Information and Communication Technology (ICT)': *Technology for gathering, storing, retrieving, processing, analysing and transmitting information.*

21 NICCS Glossary, Definition of 'cyber ecosystem': *The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.*

22 Another common example of popular misrepresentation is the term 'hacker' or 'to hack', which is often used with negative connotations, but would be incorrect when used to describe ethical hackers.

23 BCBS Basel II, Definition of 'operational risk': *The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk.*

24 Joint Forum, High Level Principles for Business Continuity (2006), Definition of 'critical operation or service': *Any activity, function, process, or service, the loss of which would be material to the continued operation of the financial industry participant, financial authority, and/or financial system concerned. Whether a particular operation or service is "critical" depends on the nature of the relevant organisation or financial system.*

25 BCBS Principles for Operational Resilience, Definition of 'supporting assets' (in the context of operational resilience): *People, technology, information and facilities necessary for the delivery of critical operations.*

26 NIST SP 800-160v1r1, Definition of 'security': *Freedom from those conditions that can cause loss of assets with unacceptable consequences.*

27 ISO/IEC/IEEE 24765:2017, Definition of 'security': *2. defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of a system*

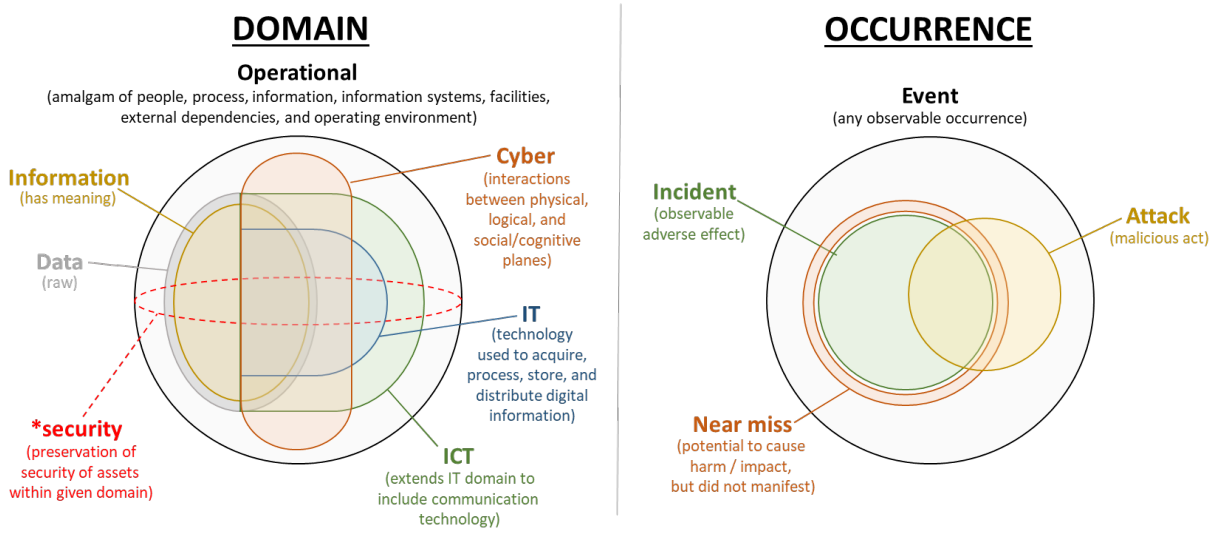
Compound terms

In the context of the Cyber Lexicon, there are three existing or new compound terms which leverage domain and occurrence: cyber event, cyber incident, and cyber attack. Using the terms previously described in this annex, it is possible to construct many other compound terms using the following formula[28] which combines domain (blue) and occurrence (red):

(cyber | data | ICT | IT | information | operational) + (security)* + (event | incident | attack | near-miss)

This formula can be used to generate both commonly used combinations (e.g. IT security incident, operational event) as well as other compound terms which, although technically accurate, would rarely or never be used (e.g. data security attack).

Conceptual maps for domain and occurrence terms **Figure 1**



Source: FSB.

The FSB's definition of 'cyber incident' is predicated on this thought process, and thus encapsulates an event that transitions to an incident due to clear adverse effect within the specifics of the cyber domain, which is in essence an intersection of all the components (e.g. data, information, IT, ICT) and can be from malicious activity or not.

[28] The asterisk indicates that 'security' can optionally be appended to change the scope of the domain.

Annex C: Sources

CERT Glossary	Carnegie Mellon Software Engineering Institute, CERT® Resilience Management Model, Version 1.2, Glossary of Terms
CPMI-IOSCO	CPMI-IOSCO, Guidance on cyber resilience for financial market infrastructures (June 2016)
FFIEC	FFIEC (Federal Financial Institutions Examination Council) IT Examination Handbook Infobase, Glossary
FIRST	FIRST Traffic Light Protocol (TLP), Version 2.0
G7 Cyber Expert Group	G-7 Fundamental Elements for Threat-Led Penetration Testing
ISACA Fundamentals	ISACA Cybersecurity Fundamentals Glossary (2016)
ISACA Full Glossary	ISACA Glossary
ISO/IEC 2832:2015	ISO/IEC 2832:2015
ISO 21188:2018	ISO 21188:2018
ISO/IEC 27000:2018	ISO/IEC 27000:2018
ISO/IEC 27032:2012	ISO/IEC 27032:2012
ISO/IEC 27033-1:2015	ISO/IEC 27033-1:2015
ISO/IEC 27035-1:2016	ISO/IEC 27035-1:2016
ISO/IEC 27039:2015	ISO/IEC 27039:2015
ISO/IEC 27040:2015	ISO/IEC 27040:2015

NICCS	NICCS (National Initiative for Cybersecurity Careers and Studies), Explore Terms: A Glossary of Common Cybersecurity Terminology
NIST	NIST, Glossary of Key Information Security Terms, Revision 3 (July 2019)
NIST 800-150	NIST Special Publication 800-150, Guide to Cyber Threat Information Sharing (October 2016)
NIST Framework	NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (16 April 2018)
STIX	Structured Threat Information Expression (STIX™) 2.1