FSB public consultation on Cyber Lexicon

The FSB invites comments on the following specific questions and the draft lexicon definitions that follow.

For the questions below, please provide supporting reasons for your views

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?

Answer	Reason
It is proposed that the lexicon includes terms that are more related to Financial Institutions and their activities.	Given the risks faced by Financial Institutions, the lexicon criteria should take into account related terms (see input for Q3 below).
It is proposed to include the following criterion of selection: "Inclusion of terms suitable for describing attack methods as well as possible mitigation options."	One of the objectives of the lexicon is to create a common vocabulary among actors for describing cyber threats, actual attacks and what can be done to prevent, detect, respond, recover, etc. The additional criterion proposed does not refer to deeply technical terms, but high-level ones relating to a few widely used attack methods and explained in plain language, e.g. 'ransomware' or 'Advanced Persistent Threat'. For the updating of the lexicon see Q5.
For a better understanding of the criteria for selection of terms, a clarification of the criterion "*Exclusion of technical terms*" would be welcome.	It is not completely clear what the FSB means by technical, considering the inclusion of terms such as "Access Control", "Authentication", "Configuration Management" or "Recovery Point Objective (RPO)."
A better clarification of the intended users of this lexicon (regulators, supervisors, etc.) would be desirable.	Depending on the profile and knowledge of the users, the definitions might need to be more or less detailed (what could be obvious for a security expert is not necessarily clear for non-technical person).

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?

Answer	Reason
'Reliance on existing sources' can be challenging, as sources may provide conflicting/different definitions. The proposal is in such situations to use the newest sources and preferably those which have dealt specifically with cybersecurity.	The provided proposal would contribute to a more up to date and accurate Lexicon.
Add the ENISA *Incident Classification Taxonomy* (2018) as a source for the terms included in the Lexicon.	The ENISA incident taxonomy is the reference at European level. Such reference could, moreover, be useful if the scope of the lexicon is extended in the future to include sub-categories of existing terms.
Depending on the intended users of this lexicon, the terms could be defined more technically, including examples.	Cybersecurity is a very technical field and examples could help towards a better understanding.

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.

Answer	Reason
Proposal to add the term "**APT**" (Advanced Persistent Threat): *an advanced persistent threat (APT) is a cybersecurity attack in which an unauthorized person gains access to a network by using advanced techniques and tools staying undetected for a long period of time*.	In order to make information sharing easier, the inclusion of terms referred to common cyber-attack methods is proposed.
Proposal to add the term "**IT-security**".	Is not uncommon that generic terms create confusion and can mislead the reader. Defining "IT-security" and demonstrating the difference with "Cybersecurity" can be very useful.
Proposal to add the term "**Likelihood of occurrence of a threat**": *Probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.* (source: NIST)	Considering the presence of terms such as "Malware", "DoS" and "DDoS", we propose to add this term in order to provide a more comprehensive coverage of cyber security events taxonomy.

Proposal to add the term "**Likelihood of success of a threat**": *Probability that a given threat, once initiated, will result in adverse impact.* (source: NIST)	Same as above
Proposal to add the term "**Social Engineering**": *Psychological manipulation of individuals (customers or employees) to induce certain actions or to disclose confidential information.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Insider/Third Party Provider Event Misuses of access rights**": *An event that is made by employees or former employees, as well as third party suppliers, which involves the accidental or intentional failure to respect the security policies and the right of access to the systems.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Unauthorised access (intentional)**": *A wide range of incidents through which a hacker intentionally accesses networks, data or systems in an unlawful manner.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Sabotage (physical attack)**": *Sabotage/destruction of equipment and/or assets through physical access.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Accidental events**": *Non-voluntary events, such as human errors*. (source: adapted from ECB)	Same as above
Proposal to add the term "**External events**": *Events caused by external factors.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Internal events**": *Events caused by internal factors.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Software problem/ system failure**": *Malfunctions of applications or basic software programs/ Performance degradation of services.*	Same as above

(source: adapted from ECB)	
Proposal to add the term "**Hardware problem**": *Incidents due to malfunctions of hardware systems and components.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Infrastructural issue**": *Incidents due to infrastructure malfunctioning, communication networks or shared platforms. Such events may arise due to external factors or internal.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Key Persons/Skills Unavailability**": *Events due to the unavailability of key persons or specific skills during the process activity.* (source: adapted from ECB)	Same as above
Proposal to add the term "**External Provider Issues**": *Events due to technical and/or operational issues of Third Party Providers.* (source: adapted from ECB)	Same as above
Proposal to add the term "**Certification**": *Formal procedure by which an accredited or authorized person or agency assesses and verifies (and attests in writing by issuing a certificate) the attributes, characteristics, quality, qualification, or status of individuals or organizations, goods or services, procedures or processes, or events or situations, in accordance with established requirements or standards.*	In light of regulations, guidelines and technical standards, there appears to be a clear need to include the terms proposed herewith.
Proposal to add the term "**Chief Information Security Officer**": *The person responsible for ensuring cybersecurity risks are managed within an organization.*	Same as above
Proposal to add the term "**Cloud Computing**": *Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows storing, processing and use of data on remotely located computers accessed over the Internet.*	Same as above

Proposal to add the term "**Cybersecurity Certification**": *Formal evaluation to attest that ICT products, services and processes comply with the cybersecurity requirements specified in a corresponding cybersecurity certification scheme.*	Same as above
Proposal to add the term "**Risk assessment**": *A process of determining the extent to which adverse circumstances or events could impact an enterprise.*	Same as above
Proposal to add the term "**Risk Management**": *Systematic application of policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.*	Same as above
Proposal to add the term "**Security Control**": *A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.*	Same as above
Proposal to add the term "**Third Party Service Provider**": *Person or entity that is not an affiliate of the Entity, provides services to the Entity, and maintains or processes information through its provision of services to the Entity.*	Same as above
Proposal to add the term "**Phishing**"*: The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically, the e-mail and the web site look like they are part of a bank the user is doing business with.* (source: SANS)	Considering the presence of terms such as "Denial of Service", we propose to add this term in order to provide a more comprehensive coverage of cyber security events, testing and assessment taxonomy.
Proposal to add the term "**Threat assessment**": *Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.* (source: NIST)	Considering the presence of terms such as "Threat Actor", we propose to add this term in order to provide a more comprehensive coverage of cyber security events, testing and assessment taxonomy.

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.

Answer	Reason
"**Access Control**": *Means to ensure access by first verifying the identity of an entity (authentication) and then checking, if the identity has the relevant access rights*.	Proposal to improve wording for clarity.
"**Authentication**": *Provision of assurance by one party in a communication that the other party has a certain claimed identity, or that a received message does originate from a certain claimed identity.*	Proposal to improve the scope of the definition.
"**Availability**": *Property of information (or an information system) that it is accessible and usable on demand by an authorized entity.*	Proposal to improve wording for clarity.
"**Confidentiality**": *Property of information that is not made available or disclosed to unauthorized individuals, entities, processes or systems.*	Proposal to improve wording for clarity.
"**Continuous Monitoring**": proposal to rename into "**Threat Monitoring"**	'Continuous monitoring' is a common phrase and narrowing down its meaning does not seem to serve a clear purpose. There are types of monitoring that are relevant to cybersecurity but not covered by the given definition e.g. monitoring of cyber incidents.
"**Cyber Incident**": *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.*	Proposal to improve the scope of the definition: a cyber incident should be always understood as a malicious event, so as not to risk overloading the reporting obligations of banks (at both national and European level) and avoid creating overlaps with the definition of operational incidents.
"**Cyber Risk**": *The risk emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – being related to individuals, companies, or governments.* (source: IAIS (2016) Issues Paper on Cyber Risk to the Insurance Sector).	Proposal to improve wording for clarity.

"**Cybersecurity**": *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.*	Proposal to merge the original FSB definition with the text originally labelled as an additional note for more clarity.
"**Cyber Threat**": *A circumstance or cyber event with the potential to exploit one or more vulnerabilities, resulting in a loss of confidentiality, integrity or availability.*	Proposal to improve wording for clarity
"**Detect**": *Implement the appropriate activities to identify the occurrence of a cyber event.*	Proposal to replace with the definition proposed herewith. In our opinion, 'to detect' is different from 'to develop'.
"**Distributed Denial of Service (DDoS)**": *A denial of service that is carried out using numerous sources simultaneously.*	Proposal to improve wording for clarity.
"**Identify**": *Organizational understanding to manage cyber risk to assets.*	Proposal to replace with the definition proposed herewith, with the assumption that the term "asset" already includes people, information, infrastructure, finances and reputation.
"**Identity Access Management (IAM)**": *Encapsulates people, processes and systems managing the data used in a system that can authenticate users and grant or deny access to Information system resources. The goal of IAM is to support appropriate access control.*	Proposal to improve wording for clarity.
"**Integrity**": *The property of information or an information system (or component thereof) that it has not been modified in an unauthorized manner.*	Proposal to improve wording for clarity.
"**Protect**": *Implement and/or develop appropriate safeguards to ensure delivery of services and to guarantee confidentiality, availability and integrity of data.*	Proposal to replace with the definition proposed herewith, which goes beyond the delivery of services.
"**Recover**": *Implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber event.*	Proposal to replace with the definition proposed herewith (omitting "develop").
"**Respond**": *Implement the appropriate activities to take action regarding a detected cyber event.*	Proposal replace with the definition proposed herewith (omitting "develop").

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?

Answer	Reason
The lexicon should be a “living” document and the groups and fora which are using it, should be able to propose updates. The Lexicon should be reviewed at least twice a year, every six months. However, changes and/or events can trigger extra-reviews. Changes and/or events that can trigger extra-reviews should be properly defined. Moreover, as a public consultation for every minor review could make the Lexicon inflexible, a process should be defined for the kind of changes that can be handled centrally. For example, when a simple update is proposed (like a name and description of a new type of attack method), a simple approval by a central office should suffice. More fundamental changes of concepts should undergo a more comprehensive approval procedure including public consultations with members and engaged stakeholders.	To be useful for information sharing, the lexicon must strive to be up to date and that will require a quick process for simpler updates and a more comprehensive one for more complex updates. The positive contribution s that both members and engaged stakeholders can provide to the updating process should be taken into account.

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