BANCA D'ITALIA

EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Proposal for a common categorisation of IT incidents

by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury

May 2021

Number 6

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento
(Markets, Infrastructures, Payment Systems)

Questioni istituzionali
(Institutional Issues)

Proposal for a common categorisation of IT incidents

by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury

Number 6 – May 2021

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

Proposal for a common categorisation of IT incidents

by Autorité de Contrôle Prudentiel et de Résolution, Banca d'Italia, Commissione Nazionale per le Società e la Borsa, Deutsche Bundesbank, European Central Bank, Federal Reserve Board, Financial Conduct Authority, Ministero dell'Economia e delle Finanze, Prudential Regulation Authority, U.S. Treasury

Abstract

This paper presents the proposal for a common categorisation of malicious cyber incidents (cyber-attacks) and other information technology (IT) incidents formulated by ten financial authorities that are members of the G-7 Cyber Expert Group (CEG) and that represent six of the G-7 jurisdictions.

The aim of the proposal is to promote the harmonisation of the various incident reports that authorities require from financial institutions by defining common principles and developing a common taxonomy for incident reporting. The adoption of these common principles and taxonomy should make incident reporting more robust and effective by facilitating a common understanding of incidents, the sharing of information, and the joint management of IT cross-border crises.

Sintesi

Questo lavoro illustra una proposta per una classificazione comune degli incidenti cyber malevoli (attacchi cibernetici) e di altri incidenti di sicurezza informatica, formulata da dieci autorità finanziarie partecipanti al G-7 Cyber Expert Group (CEG), in rappresentanza di sei giurisdizioni del G-7.

L'obiettivo è promuovere, attraverso la definizione di principi comuni e lo sviluppo di una tassonomia condivisa, l'armonizzazione delle segnalazioni di incidenti, previste da diversi *framework*, che le autorità richiedono alle entità finanziarie. L'adozione di principi e di una tassonomia comuni renderebbe la segnalazione degli incidenti più solida ed efficace, facilitando una comprensione comune degli incidenti, la condivisione delle informazioni e la gestione congiunta delle crisi cibernetiche transnazionali.

JEL Classification: F50, G20, K24, L50.
Keywords: it incidents, cyber incidents, operational incidents, taxonomy.

TABLE OF CONTENTS

Foreword 7

1. The importance of effective incident reporting to financial authorities 9

1.1. Supervisors need to be informed of incidents 9

1.2. The current situation and its shortcomings 10

2. Proposal for a common categorisation of IT incidents 12

2.1. General principles 12

2.2. A multidimensional matrix 14

2.2.1. Incidents 15

2.2.1.1. Malicious incidents 15

2.2.1.2. Non-malicious incidents 17

2.2.2. Impact 19

2.2.2.1. Technical impacts 19

2.2.2.2. Business impacts 20

2.2.2.3. Operational impacts 20

2.2.3. Affected scope 21

2.2.3.1. IT systems 21

2.2.3.2. IT assets 22

2.2.3.3. Information 23

2.2.3.4. Services affected 23

2.2.3.5. Entity affected 24

2.2.4. Severity 25

3. Area for future work: Sector Analysis Taxonomy 27

Annex 1: Proposed matrix for a common categorisation 29

Annex 2: Bibliography 30

Foreword: This CEG occasional paper presents a proposal for a common categorisation of malicious cyber incidents (cyber-attacks) and other operational IT incidents. It responds to the demand that the Finance Ministers and Central banks Governors formulated at their G-7 Finance track meeting in Chantilly in July 2019.This proposal is primarily addressed to financial authorities to help them to design effective and robust incident reporting and management, as well as to facilitate their exchange of information and understanding of incidents. It is not intended though to displace or replace existing frameworks that are tailored to the authorities' specific missions. Nothing in this paper shall be construed to alter, impair, or supersede the authority of a jurisdiction's supervisory authorities to determine the timelines or thresholds for impacted entities under their supervision to notify them of an incident, nor their mandate to ensure the safety and soundness of supervised entities, as appropriate. The proposal for a common categorisation of incidents has been elaborated by a group of the CEG member authorities[1] and has benefited from the comments made by representatives of the financial sector from the different jurisdictions. This occasional paper expresses the views of the participating authorities only. It shall not engage the CEG nor the G-7.

In the past few years, the financial authorities have increasingly focused on the cybersecurity of the financial sector. Cyber risk, and information technology (IT) risk[2] in general, has the potential to severely disrupt the functioning of the financial institutions, and ultimately of the entire financial sector.

---

1 **European Union**: European Central Bank (ECB); **France**: *Autorité de Contrôle Prudentiel et de Résolution* (ACPR); **Germany**: *Deutsche Bundesbank*; **Italy**: *Banca d'Italia*, *Commissione nazionale per le società e la Borsa* (CONSOB), *Ministero dell'Economia e delle Finanze* (MEF); **United Kingdom**: Financial Conduct Authority (FCA), Prudential Regulation Authority (PRA); **United States of America**: Federal Reserve Board (FRB), U.S. Department of the Treasury (UST).

2 This paper uses the words "Information Technology –IT" rather than "Information and Communication Technology – ICT, but the concepts are equivalent. Some authorities or regulations refer to "IT risk" in order to make clear that they not only take into account security issues in the strict sense, but also all other issues affecting the proper functioning of the IT environment.

The reasons for such impact are multiple. They first stem from the fact that the financial institutions depend almost entirely on IT tools and services to carry on their activities. A severe disruption affecting their IT systems

could prevent them from fulfilling some or all of their business obligations. The second reason is that with the digitalisation of services, the customers of the institutions also make extensive use of IT tools and connections to carry out remote transactions with them, forcing institutions to maintain high-end services. The third reason is that the cyber threat posed by cyber-criminals is generally recognised to be increasing in the financial sector.

With the objective of maintaining a resilient and well-functioning financial sector, authorities have intensified their actions in this area using a variety of instruments. The G-7 Cyber Expert Group (CEG) has often been at the forefront by publishing various documents on the good practices to be implemented, in the form of *Fundamental Elements* for authorities and financial institutions. International and national regulators have also adopted regulatory texts setting out their expectations regarding IT risk and cybersecurity. Supervisors around the world have also enriched their supervisory practices to better understand, monitor, and evaluate financial institutions' IT risks in order to intervene where necessary to impose more control over them.

The monitoring of IT incidents is an essential element of supervision. It has become necessary for authorities to understand the impact of incidents and assess the risk profile of financial institutions. It is not only used in day-to-day surveillance but also for crisis management, when incidents are of such severity that authorities might be led to activate their crisis management procedures.

Incident reporting obligations have flourished in all jurisdictions, without enough coordination and are usually based on different materiality criteria and incident taxonomies. This has diminished the capacity to assess the level of cyber-threats, compare situations, understand the trends, and analyse any systemic impact for the entire financial sector.

In July 2019, the finance ministers and central bank governors of the G-7 asked the "CEG to analyse how to make progress on a common categorisation of cyber incidents affecting the financial sector, for better measurement of their impact".

A common categorisation of IT incidents was identified as a fundamental element for effective incident reporting. With the use of such a "common language", authorities and the sector itself could understand better the characteristics and severity of incidents, and this would have benefits for all the actions that may follow an incident. It would help authorities and financial institutions in various jurisdictions to reach a common understanding about the situations, promote the sharing of information about the latter, and ultimately decide on concerted actions during international crises. It would also standardise the information that financial institutions have to manage, thereby reducing their incident-reporting burden.

This occasional paper presents a proposal to establish a common categorisation of cyber incidents and other operational IT incidents. The proposal is addressed to the financial authorities and financial institutions. It is intended to be a

building block for incident reporting, but does not imply establishing similar incident reporting obligations (timeline, thresholds and triggers). Authorities choosing the common categorisation could keep their own timelines and triggers for incident reporting and these criteria are therefore left outside the scope of this paper. Along the same line, the management of a crisis caused by an incident, and the sharing of information on incidents are two types of actions that are not covered by this paper.

1. THE IMPORTANCE OF EFFECTIVE INCIDENT REPORTING TO FINANCIAL AUTHORITIES

1.1. SUPERVISORS NEED TO BE INFORMED OF INCIDENTS

At the time when operational risk started to be subject to capital charge under the "Basel II Accord" in 2004, supervisors mainly expected credit institutions to monitor, record and report internally their incidents with a confirmed or potential loss impact.[3] The main aim of observing operational risk incidents, especially those with a significant loss impact, was to measure the amount of capital needed to safeguard the solvency of the institutions. Besides, it was also an incentive for them to adapt their control measures and reduce their exposure to losses. There was no obligation to report losses to supervisors but only the requirement to provide these data to them upon request.

Reporting obligations were added later, often in the aftermath of the 2008 financial crisis, as supervisors focused increasingly on the severity of incidents and stepped up their efforts to ensure that institutions took action to control them. This also went hand in hand with a greater focus on the monitoring of IT and security incidents, which were not mentioned as such in the operational risk event types defined by the Basel framework.

Being timely informed of IT incidents and especially of cyber-incidents has become crucial for authorities, in particular for supervisors, for the following reasons:

- Supervisors need to assess the risk profile of each individual financial institution, which obliges them to understand their activities, their inherent risk exposure, the mitigation measures and controls in place to reduce risk, as well as the effectiveness of these measures. Being informed of the different incidents incurred gives supervisors a better insight into the actual efficiency of risk identification and mitigation. It allows them to make appropriate recommendations to institutions with a view to adapting their risk management.
- The increasing sensitivity to any IT disruption has also prompted supervisors to act urgently in the event of incidents, in particular of malicious cyber incidents. This explains the need for incidents to be reported immediately and the fact that incident monitoring is now generally supplemented by a crisis management procedure;

[3] See the latest version of the Basel Committee on Banking Supervision (BCBS), "The Basel Framework", section OPE ("calculation of RWA for operational risk"), effective as of 15 Dec. 2019.

- Supervisors and other authorities involved in financial stability are also cautious about the possibility that cyber-risks may constitute a systemic risk for the financial system as a whole. Receiving incident notifications from financial institutions helps to understand phenomena of a broader nature than those affecting only one institution. It contributes ina useful manner to the management of systemic crisis or the issuance of recommendations of good practices or regulatory requirements. It can also foster the cooperation that financial sector authorities could implement with those of other sectors in order to share information and reduce cross-sectoral threats.

Without first-hand information from the institutions they supervise, financial authorities would not be capable of measuring the seriousness of IT and cyber risks, neither to take appropriate actions in due time.

1.2. The current situation and its shortcomings

In many jurisdictions, a number of IT or security incident reporting obligations have been established to the benefit of financial authorities or non-financial authorities, such as security agencies or personal data protection authorities.

In Europe, for example, such incidents are subject to reporting requirements to authorities under a number of texts and with various scopes. This is the case of the Payment Services Directive – (UE) 2015/2366[4] for operational or security incidents affecting payment services providers, of the NIS directive – (EU) 2016/1148[5] for security incidents affecting "operators of essential services" and digital service providers, and of the General Data Protection Regulation – (EU) 2016/679[6] for personal data breaches affecting natural or legal persons processing such data. There is also a notification requirement for participants in the Eurosystem real-time gross settlement system Target 2. In 2017, the ECB Banking Supervision implemented a Cyber Incident Reporting for itssupervised Significant Institutions. National frameworks generally supplement these obligations by applying specific rules.

These reporting obligations generally suffer different shortcomings:

- Since they were adopted separately with no consideration as to their consistency, they vary from one to another in terms of the materiality criteria that trigger notification, the timeline for reporting, the designation of the incidents themselves and the information that help categorise their severity. For institutions that are subject to multiple reporting obligations, providing

---

4 PSD 2, Article 96 – Incident reporting: "1. In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider".

5 NIS Directive, Article 14 – Incident notification: "3. Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross- border impact of the incident. Notification shall not make the notifying party subject to increased liability".

6 GDPR, Article 33 – Notification of a personal data breach to the supervisory authority: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

different information with different timelines to several authorities on one single incident may represent a serious challenge and require substantial organisation;

- As was originally the case for operational risk incidents, materiality criteria have been set to limit reporting obligations to the most significant incidents, for example based on the amount of financial loss they cause. Applied to IT and especially to cyber-incidents, this approach may prove insufficient insofar as it is not the financial loss that determines the severity of the incident but rather its multiple consequences on the service provided to users. As regards cyber-incidents, it was generally decided to primarily concentrate on successful attempts and not onfailed ones. As a result, most authorities receive few incident reports, which does not allow them to fully measure the scale of the phenomenon and understand its evolution;
- The reports use different taxonomies to designate the incidents. In the absence of a reference taxonomy for IT and cyber-incidents, authorities have built classifications of their own. These taxonomies are not aligned, which does not allow for a comparison of situations. In addition, they may sometimes be incomplete as they are a selection of the most commonly observed cases. Moreover, they might also contain redundant items (e.g. ransomware is a malware but both categories can appear together). As a consequence, this can result in misinterpretation or flaws and errors in the information reported to supervisors who need additional explanations before they can complete their analysis;
- The reports do not consistently require information that categorise the severity of incidents. This information may already be encapsulated in the materiality criteria required for the notification. Therefore, supervisors might for example struggle to measure the severity of the situation and appropriately activate their crisis management procedures.

Consequently, although it might be a significant burden for institutions to provide, the data conveyed so far in incident reports are too limited to give a full picture of how the industry effectively responds to attacks and incidents. This reduces the financial authorities' understanding of the sector's resilience and the evolution of risks.

At the same time, it has also a bearing on the capacity for institutions to compare their situation with the rest of the sector, or even cross-sectors. Incomplete or inconsistent data might prevent authorities from sharing their analyses or from producing official statistics on IT operational and cyber-incidents. Firms remain dependent upon consultants' surveys or private consortiums' incident repositories to help measure the severity of IT incidents and compare their situation. Insurance companies also bear the consequences of this situation because they do not have enough data to measure the risks and propose appropriate premiums in insurance policies.

This sub-optimal situation leads to make the following proposal for a common categorisation.

2. Proposal for a common categorisation of IT incidents

The proposal for a common categorisation of IT incidents, including cyber incidents aims to alleviate the difficulties that have been identified in the practice of incident reporting so far. This proposal is intended to encourage financial authorities and industry to act more efficiently in their efforts to enhance the resiliency of the financial sector. Member authorities of G-7 jurisdictions are encouraged to consider the adoption of the proposed common categorisation. This categorisation of IT incidents is designed in the form of building blocks and can be used in different ways according to the preferences of the authorities. Adopting common categorisation would help a shared understanding and facilitate the analysis and the crisis management. It does not oblige to adopt same materiality or triggering criteria for incident reporting and crisis management. Authorities remain free to choose their own criteria.

2.1. General principles

The participating authorities recognised the importance of some general principles in order to achieve the objective of proposing a common categorisation that could be widely adopted by authorities and supported by the industry. These general principles are described hereafter:

1. **Cover incidents affecting the security and the overall functioning of the IT environment**: Although cybersecurity incidents have received a lot of attention in the recent years, authorities continue to monitor closely incidents resulting from dysfunctions such as breakdowns or errors, which still represent a major source of potential disruption. The proposal covers both types of incident, as the reduction of each is essential to the resilience of financial institutions and important to avoid their contagion to the entire financial sector. It is also because institutions themselves might have difficulties in distinguishing at the outset of an incident whether it results from a pure operational related incidents or malicious cyber incidents. Most authorities also encompass both in their incident notification procedure.
2. **To be able to recognise incidents with variable materialisation**. When monitoring an IT system, experts generally distinguish between "events"[7], which are changes of state of any kind, and "incidents"[8], which are events having a negative impact on operation or security. The recognition of the impact might require some time, since incidents affecting the functioning or the security of an IT environment can progressively aggravate. The common categorisation should be adapted to instant notification as well as to ex- post reports and be workable for authorities irrespectively of the various thresholds that they might have for incident notification and crisis management activation. The categorisation should help identifying the

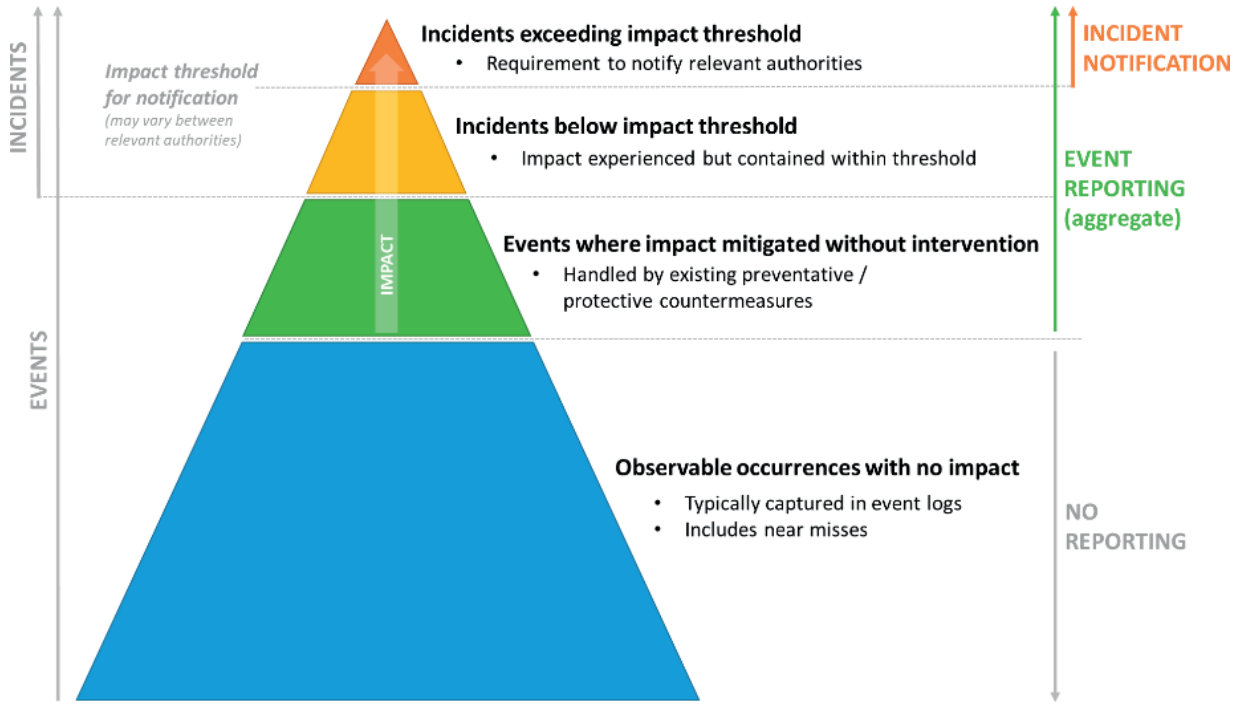
---

7 As per the National Institute of Standards and Technology (NIST) SP 800-37 Rev. 2 standard, also recognised by the FSB Cyber Lexicon, an "**event**" can be defined as "any observable occurrence in a network or information system". It signals a change in the normal behaviour of a system, process, environment or workflow.

8 As inspired by the NIST SP 800-171 Rev. 2 44 USC 3552, an "**incident**" can be defined as "an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system.

step at which an incident is occurring. In the case of malicious cyber-incidents, the taxonomy should allow categorising incidents constituting "attempts" to compromise the information system and that require active intervention by the security teams in order to be stopped. Figure 1 illustrates how notification and reports can treat events and incidents according to their impact.

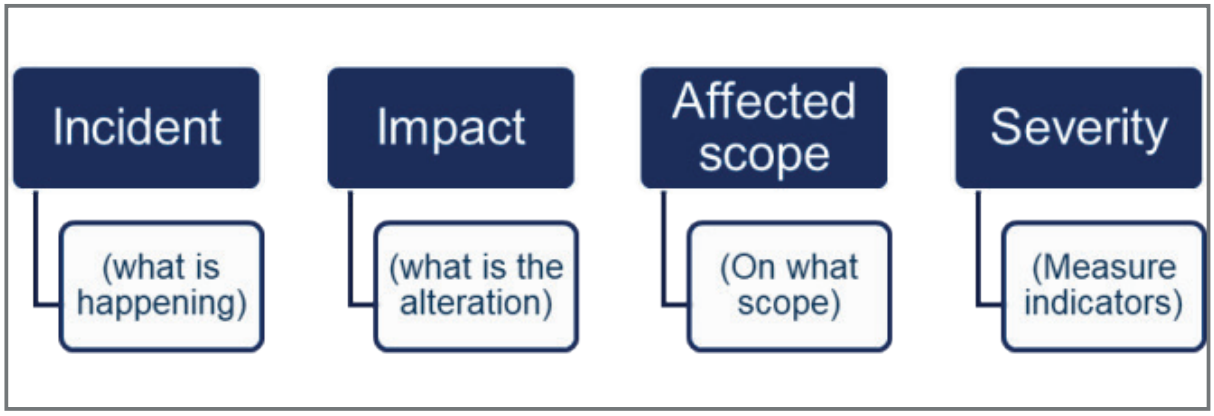
Figure 1 - Incident types in relation to notification and reporting



3. **Promote a multidimensional approach** in order to obtain the relevant information and be able to measure the seriousness of incidents: the proposal combines different perspectives to help build incident reports. These different perspectives are intended to enable authorities to obtain immediately relevant information about the type of incident, the nature of the disruption, the assets and activities impacted and the severity of the disruption. This multi-dimensional approach can foster the analysis of the incidents and help understand their importance, notably for the purpose of activating a crisis management procedure. These four dimensions should be viewed as a minimum common set of information to be adopted for the incident reports to authorities in order to improve the similarity and comparability of information. The proposal does not intend to prevent the authorities from using additional information if they wish to do so.

4. **Put oneself in the situation of the firm facing the incident in order to facilitate the provision of information:** Financial institutions may encounter serious difficulties in informing authorities when details are required that do not correspond to observable facts or easy-to-provide analysis. This can lead to delays or the provision of inaccurate information and weaken the understanding of the authority, since it is critical to have clear information promptly. The proposal includes elements that are generally observable

Figure 2 - Multi-dimensional approach



or easy to analyse by an institution's IT and business or risk teams. It is assumed that the institution in the various updates that follow an incident notification can also correct or enrich these elements.

5. **Opt preferably for well-recognised taxonomies in order to avoid creating something too specific**: The fact that financial sector authorities have created specific nomenclatures for their incident reporting has arguably made their use by institutions more complicated. The participating authorities recognise the importance of using a sector-agnostic taxonomy of IT incidents, especially for cyber-incidents, since institutions in the financial sector face similar IT incidents to those experienced by firms in other sectors. Using a reference nomenclature instead of establishing a specific one for the financial sector also facilitates its understanding and usage by the IT teams who manage the incidents. If such taxonomies were used by other sectors, it would help to compare the situation of the financial sector with others. However, the representatives of the financial sector pointed out during the industry workshops that it could be useful to marginally modify certain reference nomenclatures in order to adapt them to today's context.
6. **Follow robust design principles for the chosen taxonomies in order to conceive a coherent and perennial categorisation:** while relying as much as possible on existing and well-recognised taxonomies, the proposal for a common categorisation of incidents might require a supplement of specific on-purpose nomenclatures. Therefore, the choice of the different combined taxonomies requires robust design principles. They should ensure a comprehensive coverage of the different items, with an appropriate granularity ensuring that each component has its unique attributes. They should be based on clear definitions to ensure that the components are mutually exclusive in nature. The taxonomies should also prove to be stable over time for the sake of the stability of the categorisation.

2.2. A MULTIDIMENSIONAL MATRIX

The proposal is based on a combination of four pillars. The two first relate to the nature and impact of the incident. The two others aim at identifying the assets and activities affected and measuring the severity of the disruption in

order to help understand its significance and help make crisis management or follow-up decisions.

For each pillar, the proposal integrates an existing reference taxonomy, if any. When no reference taxonomy could be identified, the proposal has been established on the basis of common practices observed among the jurisdictions of the CEG members.

2.2.1. Incidents

The first pillar sets out to describe the IT incident from the perspective of the financial institution. Both incidents affecting the security and the functioning of the IT environment are concerned since they are equally important for the resilience of the financial sector. As the terms “security” incidents and “operational” incidents may appear insufficiently differentiating, it was preferred to use the incident terms "malicious" and "non-malicious", which refer instead to the intentionality. In the proposal, those terms are equivalent to “adversarial” and “non-adversarial” which are sometimes used.

2.2.1.1. Malicious incidents

Different reference taxonomies have been considered for malicious incidents. The one that was selected to draw up the proposal is the ATT&CK[9] taxonomy established by MITRE. Created in 1958, the MITRE corporation is an American not-for-profit organisation supporting several US government agencies. It is attached to the Department of Homeland Security. ATT&CK was launched in 2013 to categorise cyber-attacker behaviour and provide a common taxonomy for attack and defence. This taxonomy has been kept up-to-date since, which represents an asset for the relevance of the common categorisation developed.

ATT&CK is structured into 12 “tactics”[10]. Each of them represent the different steps that an attacker would follow in order to infiltrate and disrupt an IT system (like “initial access”, “privilege escalation”, “lateral movement”, “exfiltration”, “impact”). Each “tactic” has a well-established definition that do not need further explanations, which is helpful for the rapid adoption of the common categorisation. The “tactics” definitions are presented in the Table 1 below.

The ATT&CK 12 “tactics” are complemented by a regularly updated sub-level of “techniques” describing the modus operandi used by the attackers[11]. They correspond to recognised patterns of attack that the defence solutions of the institutions can identify. The participating authorities believe that it could be useful to add a further piece of information for categorising malicious incidents by indicating the ATT&CK technique identified by the reporting institution.

---

9 ATT&CK stands for “Adversarial Tactics, Techniques, and Common Knowledge”.

10 In October 2020, MITRE included in the “ATT&CK” tactics the “Reconnaissance” and “Resources development”, which were previously regarded as “PRE-ATT&CK” tactics, raising their number from 12 to 14. However, the occasional paper does not include those two tactics in the incident taxonomy since they are not strictly constitutive of an incident in the meaning of the definition given in footnote 8.

11 According to the current version of MITRE ATT&CK, the framework for enterprise comprises 178 “techniques” and 352 “sub-techniques”.

Table 1 - The 12 MITRE ATT&CK tactics with definition

1	Initial Access	Techniques that use various entry vectors to gain their initial foothold within a network (include targeted spearphishing and exploiting weaknesses on public-facing web servers).
2	Execution	The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
3	Persistence	Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.
4	Privilege Escalation	Techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.
5	Defense Evasion	Techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware.
6	Credential Access	Techniques for stealing credentials like account names and passwords, such as keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.
7	Discovery	Techniques that an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective. Native operating system tools are often used toward this post-compromise information-gathering objective
8	Lateral Movement	Techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain.
9	Collection	Techniques that adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
10	Command and Control	Techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
11	Exfiltration	Techniques that adversaries may use to steal data from your network. Once they have ve collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel.
12	Impact	Techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. Adversaries might use these techniques to achieve their final goal or to cover up a breach of confidentiality.

However, the technique may only be identifiable at a later stage than the initial recognition of the incident, and therefore may not be available in the initial incident report. In order to simplify the list of techniques referred to by MITRE, it is proposed to concentrate on the group of ones corresponding to the most common attack techniques and threats exposures identified by

the European Union Agency for Cybersecurity (ENISA). Table 2 below lists those most prominent groups of techniques which could be inserted in the common categorisation, with a proposed definition inspired by the ENISA *Threat landscape* and by the FSB *Cyber Lexicon*.

Table 2 - Categorisation of techniques, with definitions

Technique (grouping)	Related ATT&CK technique(s)	Definition
Web Application Attacks	Among many; e.g. T1190 Exploit public facing application; T1102 Web Services	Web based attacks are those that use web systems and services as the main surface for compromising the victim/target. This includes browser exploitations and injections (including extensions), websites, Content Management System (CMS) exploitation, and web services. [ENISA TLR 2018]
Phishing	T1566 Phishing	Phishing is the mechanism of crafting messages that use social engineering techniques so that the recipient will be lured and "take the bait". More specifically, phishers try to lure the recipients of phishing emails and messages to open a malicious attachment, click on an unsafe URL, hand over their credentials via legitimate looking phishing pages, wire money, etc. [ENISA TLR 2018]
Denial of Service	T1498 Network Denial of Service T1499 End Point Denial of Service	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: FSB CL[12] "Adapted from ISO/IEC 27033-1:2015"
Physical manipulation/ damage/theft/ +loss	T1200 Hardware addition; T1134 Token theft; T1048 Exfiltration via physical medium	Physical attacks may not be as popular as other types of cyberthreats they can still lead to data breaches. Physical access to a device still gives the opportunity to attackers to conduct their malicious activities, e.g. ATM fraud and POS attacks. [ENISA TLR 2018]
Information leakage	9 techniques of exfiltration (TA0010)	Information leakage is one of the significant cyberthreats covering a wide variety of compromised information, from personal data collected by internet enterprises and online services to business data stored in IT infrastructures. [ENISA TLR 2018]
Identity theft	T1078 Valid account	Identity theft is the fraud committed from the theft of personal identifiable information strengthened by the massive digitisation of people's personal data which most of the times, include information related to their legal and civil substance. [ENISA TLR 2018]
Ransomware	T486 Data encrypted for impact	The ransomware attacker gains ownership of files and/or various devices and blocks the real owner from accessing them. To return the ownership the attacker demands a ransom in cryptocurrency. [ENISA TLR 2018]
Crypto-jacking	T1486 Resource Hijacking	Cryptojacking (also known as cryptomining) is a new term that refers to the programs that use the victim's device processing power (CPU or GPU) to mine cryptocurrencies without the victim's consent. This processing power is used to solve cryptographic puzzles that are recorded in the blockchain. [ENISA TLR 2018]

2.2.1.2. Non-malicious incidents

For the purpose of the proposal, non-malicious incidents refer to natural disasters, accidents, errors, inattentions or inactions that affect the proper functioning of the IT environment. There are not many reference taxonomies for such incidents. Those existing might be very detailed for the purpose of establishing the causes of the incidents, like in the domain of insurance. The proposal for a common categorisation is based on the nomenclature developed for risk assessment in the Special Publication 800-30 of the United States'

[12] The FSB *Cyber Lexicon*, Oct. 2018, defines "**Denial of Service**" as the "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" and "**Distributed Denial of Service (DDoS)**" as "A denial of service that is carried out using numerous sources simultaneously."

National Institute of Standards and Technology (NIST)[13][13]. The table 3 below represents the nomenclature used by NIST with regard to non-adversarial threats.

Table 3 - Categorisation of non-malicious incidents, with definitions

Non-malicious incident (based on NIST SP 800-30 Table D-2)	Definition (based on NIST SP 800-30 Table D-2)
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.
STRUCTURAL - Information Technology (IT) Equipment · Storage · Processing · Communications · Display · Sensor · Controller - Environmental Controls · Temperature/Humidity Controls · Power Supply - Software · Operating System · Networking · General-Purpose Application · Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made disaster · Fire · Flood/Tsunami · Windstorm/Tornado · Hurricane · Earthquake · Bombing · Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage · Telecommunications · Electrical Power	Natural disasters and failures of critical infrastructures on which the organisation depends, but which are outside the control of the organisation.

Figure 3 below represents the incident classification.

[13] National Institute of Standards and Technology (NIST).SP.800-30 rev 1 (Sept. 2012).

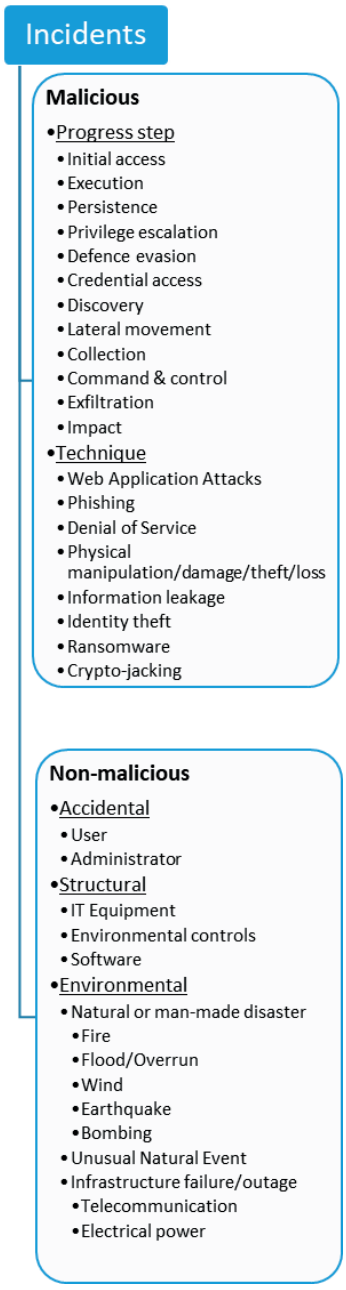
2.2.2. Impact

The proposal for a common incident categorisation is intended to capture not only the technical impacts that affect the IT environment itself, but also the business impacts that describe the organisational repercussions of the incident for the institution, and the operational impacts that inform on the possible disruptions to activities.

2.2.2.1. Technical impacts

The most usual classification of the problems affecting IT systems is the "Confidentiality-Integrity-Availability" triad ("CIA triad")[14]. The proposal for a common categorisation only focuses on these properties, but the participating authorities recognise that it could be worthwhile to expand with additional properties like authenticity, accountability, non-repudiation and reliability. Those additional properties are indeed recognised and defined by the International Organization for Standardization (ISO), and have also been taken into account in the European System Risk Board (ESRB) work on cyber risk[15]. The table 4 below represents the different properties that are used to categorise the impact of IT incidents. These properties benefit from well-recognised definitions given by the ISO.

Figure 3 - Categorisation of incidents



[14] The Financial Stability Board (FSB) *Cyber Lexicon* (Oct. 2018) provides definitions for "**confidentiality**" ("property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems"), "**integrity**" ("property of accuracy and completeness") and "**availability**" ("property of being accessible and usable on demand by an authorised entity").

[15] European Systemic Cyber Group (ESCG), *Systemic cyber risk*, February 2020.

Table 4 - Categorisation of Technical properties, with definitions

Information Security Property (ISO/IEC 27000:2018)	Definition (ISO 27000:2018, also quoted in FSB Cyber Lexicon)
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems
Integrity	Property of accuracy and completeness
Availability	Property of being accessible and usable on demand by an authorised entity
And to be considered as an expansion:	
Authenticity	Property that an entity is what it claims to be.
Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities
Reliability	Property of consistent intended behaviour and results.

2.2.2.2. Business impacts

The ISO has established a reference list of business impacts in its technical specification on business impact analysis (BIA), dated 2015[16]. The proposal is to include this classification in the common categorisation to help structuring the identification of the different impacts on the institution's activity. It would include "financial", "reputational", "legal and regulatory", "contractual" damages, as well as the inability to meet "business objectives".

Table 5 - Categorisation of business impacts, with definitions

Business impacts (ISO/TS 22317:2015 GL for BIA)	Definition (inspired by ISO/TS 22317:2015)
Financial	Financial losses due to fines, penalties, lost profits or diminished market share
Reputational	Negative opinion or brand damage
Legal and regulatory	Litigation liability and withdrawal of licence of trade
Contractual	Breach of contracts or obligations between organisations
Business objectives	Failure to deliver on objectives or take advantage of opportunities

2.2.2.3. Operational impacts

The proposal for a common categorisation includes the dimension of functional or "operational" impacts in order to capture all situations of service level reductions or disruptions. The US-CERT "*Federal Incident Notification Guidelines*", 2017, provide a classification of functional impacts to activities, which served for the table 6 below. The criticality of the services should be assessed from the perspective of the financial institution. Consequently, authorities notified through the incident should use this information in combination with the indication of the type of entity to assess the incident.

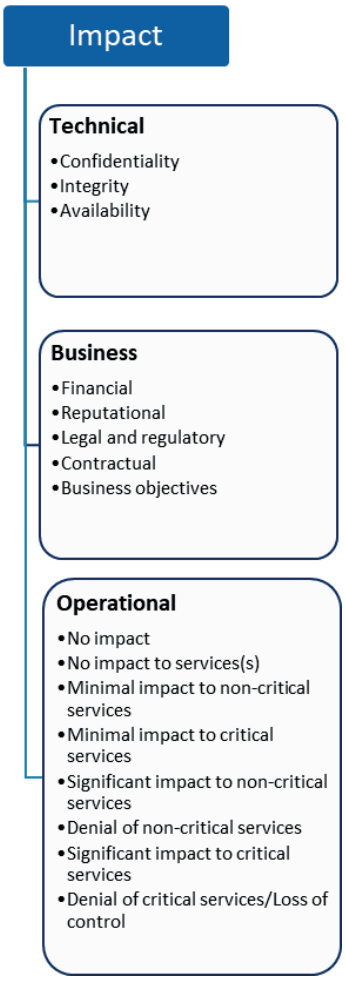
[16] ISO/TS 22317:2015 *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*.

Table 6 - Categorisation of operational impacts, with definitions

Operational impacts (U.S. CERT Federal Incident Notification Guidelines)	Definition
No impact	Event has no impact.
No impact to services	Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
Minimal impact to non-critical services	Some small level of impact to non-critical systems and services.
Minimal impact to critical services	Minimal impact but to a critical system or service, such as email or active directory.
Significant impact to non-critical services	A non-critical service or system has a significant impact.
Denial of non-critical services	A non-critical system is denied or destroyed.
Significant impact to critical services	A critical system has a significant impact, such as local administrative account compromise.
Denial of critical services/loss of control	A critical system has been rendered unavailable.

As a result, Figure 4 represents the impact categorisation.

Figure 4 - Categorisation of impacts



2.2.3. Affected scope

In a third pillar, the proposal for a common categorisation aims at presenting in a classified manner the scope of IT systems, IT assets, information, financial services and the type of entity affected by the incident. This representation is agnostic of whether the financial institution operates on its own or via external service providers (either for the business operations or for the IT services). It is recommended that if the incident affects the environment or assets of such service provider with consequences on the financial institution, the reporting template allows the financial institution to indicate which part of the affected scope is under its operation or outsourced to a service provider (including sub-outsourcing).

2.2.3.1. IT systems

This item aims to inform on the different IT systems where the incident is located. Leveraging on the classification of IT environments by the U.S. National Cybersecurity and Communications Integration Center (NCCIC)[17], the proposal classifies the IT systems according to their

[17] The NCCIC Cyber Incident Scoring System (NCISS), itself acknowledging the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide, comprises eight "levels of Location of Observed Activity".

criticality. Should the incident result from a natural disaster affecting an entire data centre, the different types of IT systems managed in this data centre would have to be reported as affected.

Table 7 - Categorisation of IT systems affected, with definitions

IT systems affected	Definition (based on US National Cyber Incident Scoring System)
Level 0 – Unsuccessful	No system affected. E.g. in case of malicious incident, the existing network defenses repelled all observed activity.
Level 1 – Business demilitarized zone	The incident affects the business network's demilitarized zone (DMZ). These systems are generally untrusted and are designed to be exposed to the Internet. Examples are a company's Web server or email server.
Level 2 – Business network	The incident affects the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems.
Level 3 – Business network management	The incident affects the business network management systems such as administrative user workstations, active directory servers, or other trust stores.
Level 4 – Critical system DMZ	The incident affects the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay "jump" boxes into more critical systems.
Level 5 – Critical system management	The incident affects high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems.
Level 6 – Critical systems	The incident affects the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments.
Level 7 – Safety systems	The incident affects critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system.
Unknown	An incident occurred, but the IT system affected could not be identified

2.2.3.2. IT ASSETS

This item aims to inform on the different types of information technology assets (equipment, software, data) that have been lost or corrupted as an effect of the incident. The proposal leverages on the event model developed by the European Telecommunications Standards Institute (ETSI)[18].

Table 8 - Categorisation of IT assets affected, with definitions

IT asset affected (simplification of ETSI -ISI Event Model)	Description (based on the ETSI -ISI Event Model)
Databases and applications	Enterprise standard applications (ERP, supply chain), Web applications, internal database or data warehouse
Systems	Servers running applications or specialised services, including directory servers, web servers, mainframes and SCADA
Networks and telecoms	Include low level devices (router, switch, hub, etc…), high level communication (such as proxies), middleware (SAN, transactional engine), wireless access points, security devices such as firewalls
Offline storage devices	Paper, USB sticks, smartcards, external hard disks, back-up tapes, CDs, DVDs
End-user devices	Desktop, laptop, telephone, smartphone, PDA, user authentication device, ATM, POS terminal

[18] ETSI, Information Security Indicators (ISI) Event Model - A security event classification model and taxonomy (ETSI GS ISI 002 v1.2.1), November 2015.

2.2.3.3. Information

This item aims to inform on the different types of information that have been lost or corrupted as an effect of the incident. The proposal also leverages on the NCCIC/US CERT scoring system but with some minor adaptation. As a complementary information, incident reporting could expand on the internal level of classification of the information affected, but since this one depends on the classification scheme of the financial institution, it could not be subject to the proposal for a common categorisation.

Table 9 - Categorisation of information affected, with definitions

Information affected (adapted from US-CERT Federal Incident Notification Guidelines)	Description (adapted from US-CERT Federal Incident Notification Guidelines)
Suspected but not identified	An impact on data is suspected, but no confirmation/detail exists.
Personal data	Data protected by personal/privacy data law (such as the General Data Protection Regulation in the EU)
Proprietary information	Proprietary information of the institution, such as intellectual property, or trade secrets
Non-critical systems data	Data pertaining to a non-critical system
Critical systems data	Data pertaining to a critical system
Core credential	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems

2.2.3.4. Services affected

Another important item that needs to be included in the common categorisation is about the activities and services of the financial institution. Since incidents can affect large international groups with imbricated or decentralised IT environments, this item aims to provide information on the name(s) of the most affected business area(s) or function(s) in the institution. The proposal leverages mainly on the classification developed by the FSB in its *Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical*

Functions and Critical Shared Services (2013). Specific items were added for capturing the activity of insurance companies, liquidity providers and trading venues. Besides, an "other" category has also been added for financial institutions' ancillary activities which are not included in this classification. This "other" category could be also be used to mention some support functions (e.g. legal services, human resources) that could be affected.

As a complementary information, incident reporting could expand on the "Customer segment" as per the reporting entity's own classification (retail, businesses, B2B, etc.).

Table 10 - Categorisation of services affected, with definitions

Services (based on FSB Guidance on Identification of Critical Functions and Critical Shared Services)	Definition (based on FSB Guidance on Identification of Critical Functions and Critical Shared Services)
Deposit taking	Deposit taking refers to the acceptance of deposits from non-financial intermediaries. It does not include borrowing from other financial intermediaries, which is dealt with separately as "Wholesale activities"
Lending and Loan Servicing	Lending refers to the provision of funds to non-financial counterparties, such as corporates or retail customers. Lending to financial counterparties is a distinct activity and assessed as "Wholesale activities"
Payments, Clearing, Custody & Settlement	Payments, clearing and settlement function.
Wholesale Funding Markets	Wholesale activities refer to lending and borrowing in wholesale markets to and from financial counterparties. It does not include intra-group flows.
Capital Markets and Investments activities	Capital markets activities refer to the issuance and trading of securities, related advisory services, and related services such as prime brokerage. They also include investment of the firm's own capital in private equity or similar principal investments.
Finance-related shared services	Finance-related shared services involve the management of financial resources of the firm
Operational shared services	Operational shared services do not involve financial resources, but provide the necessary infrastructure to enable the firm or parts of it to function.
Insurance	Insurance services
Liquidity services	Provision of liquidity services to financial institutions
Organisation and management of Trading venues	Trading venues' activity
Other	Any other service or activity

2.2.3.5. Entity affected

In order to refer to financial institutions in a similar way and facilitating further the analysis of the incident and the exchange of information at sector or jurisdiction levels, the proposal for a common categorisation includes a nomenclature indicating the type of entity affected by the incident. There is no reference taxonomy for describing the different financial sector's regulated entities. In each jurisdiction, regulations may differ and apply to regulated entities with different names and for a different scope of activities.

Nevertheless, the proposal provides in Table 9 below a common reference table that aims to match in a neutral way the types of entities in the financial sector according to US and European regulations. Further work could be carried out at international level to agree on a reference typology of financial institutions. It has to be noted that if several entities of a financial Group come to be affected by an incident, the incident report template should include the possibility to inform about this situation and refer to these different entities by using the proposed nomenclature according to their activity.

Table 11 - Categorisation of entities affected (mapping of US and EU typologies)

Entity type (mapping)	US types	EU types
Institution providing banking services	Global retail and commercial bank Mid-Size/Regional banks or credit unions Community Banks/Credit Unions	Credit institution (large/medium/ specialized)
Institution providing securities services	Major Broker dealers, ECNs/ATS/ and investment advisors/companies	Investment firm
	Minor Broker Dealers, ECNs/ATS and Investment Advisers/Companies Financial Service Provider	Managers of alternative investment funds
Institution providing payment services	Payment processers	Payment institution, e-money institution
Institution providing insurance services	Insurer	Insurance and reinsurance undertakings, insurance and reinsurance intermediaries, institutions for occupational retirement pensions
Financial Market Infrastructure (FMI)	Financial Market Infrastructure and Clearinghouse	Financial Market Infrastructures (FMIs) regroup: • Payment systems • Central securities depositories • Securities settlement systems • Central counterparties • Trade repositories
Financial Market	Exchanges	Trading venue
Credit rating agencies	Other Market Participants (credit agencies, self-regulatory organizations, etc.)	Credit rating agencies
Third party service provider	Non-Financial Service Providers (law firms, etc.), technical service providers	Third party providers (critical or non-critical)
Other	Other	Other

Figure 5 represents the categorisation for the affected scope.

2.2.4. Severity

Besides the three first pillars that can leverage on existing taxonomies, a fourth pillar is worth being added to measure the severity of the incident. Since no reference categorisation could be found on the items related to the severity, the proposal is only indicative on this. Such items would need to be developed and adapted by financial authorities according to their own objectives in terms of incident reporting. The implementation of these indicators should take into account the business activities of the financial institution, as the number of clients or transactions affected by an incident may not indicate the same level of criticality for a retail or wholesale institution.

The proposal mentions at least three groups of indicators on the "significance", the "duration" and the "disclosure" related to the incident. These groups of indicators are developed hereafter:

- **Significance** can be measured through a variety of indicators like i) the "number of customers" affected, and the percentage in comparison to the total number of customers; ii) the "number and percentage of operations" (such as card payments); iii) the "number and percentage of IT assets"; or iv) the "number and percentage of end-users' devices (e.g. PCs, tablets,

phones). Those indicators could be referred to in quantiles (e.g. 0 to 10%, etc.) in order to simplify the measure.

- **Duration** is important to provide information about pre-existence of the incident and give an idea of the extent to which it may have gained momentum. The proposal for a common categorisation is to include at least indicators on i) the "Moment of occurrence" (i.e. the point in time at which the incident effect was identified), ii) the "Probable date of onset" (i.e. the estimated moment of occurrence of the incident if it was already active before it was detected), and iii) the "Estimated moment of resolution" (i.e. the estimated moment when the institution plans to resume normal service);
- **Disclosure** provides information on the dissemination of information about the incident, both internally and externally. Incident reports could include at least indicators on whether: i) the "information has been escalated to senior management" (which indicates its importance and provides information on the level of attention given to the incident), and ii) the "information publicly disclosed" (gives an indication of the public attention given to the incident and the possible damage to the reputation of the institution).

Finally, as an indication, incident reports could also bring additional information that cannot be categorised, such as the indication that:

- the incident has spilled over to other financial institutions,
- the countries where the affected entity(ies) operate,
- whether the institution has activated its crisis management mode.

Figure 6 represents the severity classification. All in all, the common categorisation would combine those different aspects in order to report on the information. The complete matrix is presented in Annex 1.

Figure 5 - Affected scope categorisation

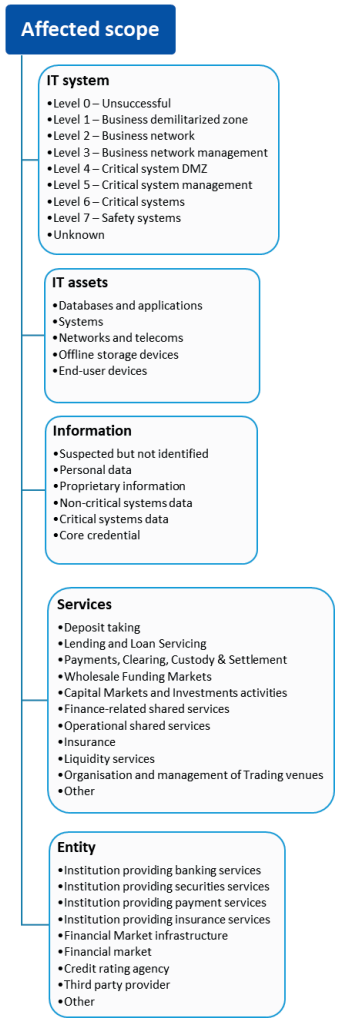
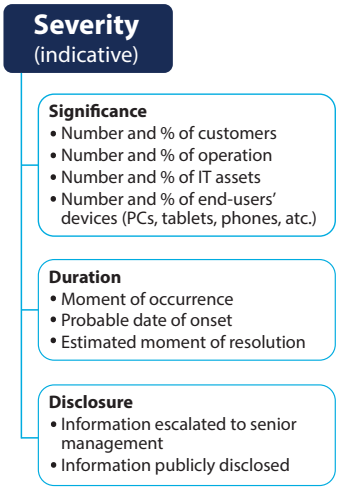


Figure 6 - Indicative items for severity



3. Area for future work: Sector Analysis Taxonomy

The participating authorities believe that the proposed common categorisation of IT incidents will help restructuring and homogenising incident reports. It will serve as a building block and facilitate the actions of incident analysis, crisis management, and information sharing that are the responsibility of supervisors. Further work will be required to develop successfully these actions. This is particularly the case for understanding and gauging incidents affecting a wider scope than a single firm.

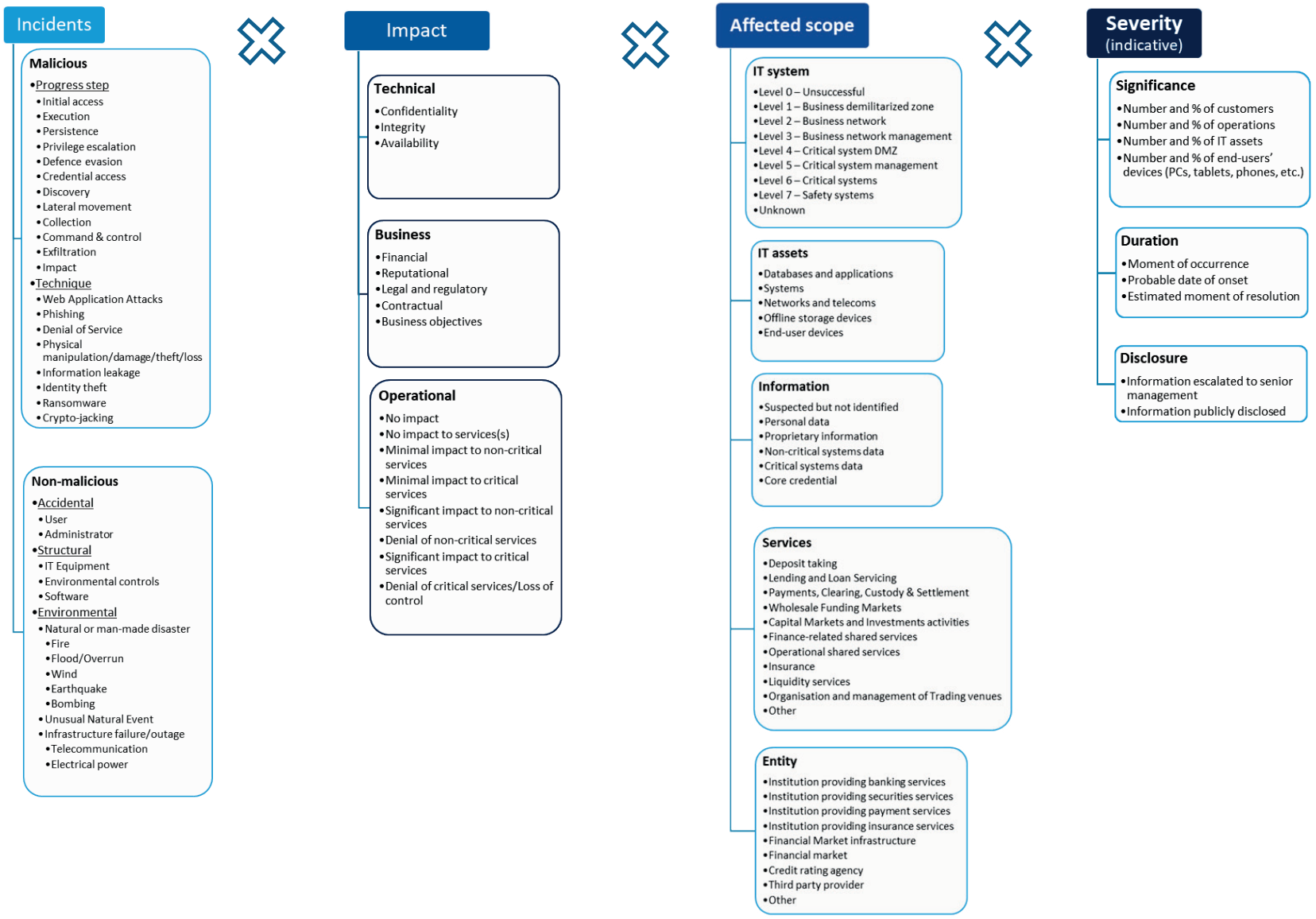
The primary frame of reference for this proposal of a common categorisation of incidents is the impacted firm, including the nature of the incident, impacts on its information systems, operations capabilities, and business functions. The four pillars of the taxonomy leverage existing reference taxonomies to facilitate incident reporting and information sharing across jurisdictions with a well-understood terminology. However, the focus on firms has revealed a shortfall in existing taxonomies to describe how the impacts on one or several firms may impact the availability of a financial service for an entire sector or jurisdiction, i.e. the function of a service. There is no established reference taxonomy to describe different levels of service availability from a sector-level perspective. Further, different jurisdictions may have different standards of what constitutes a critical or non-critical service.

Following this proposal for a common categorisation of IT incidents, future work may focus on developing a taxonomy and scale to understand impacts to service functional availability and the potential consequences to help guide financial authorities in determining the appropriate level of response and information-sharing across jurisdictions. Table 12 is a proposed new taxonomy to describe impacts to the ability of the financial services sector collectively to provide a service. It is based on the U.S. CERT *Federal Incident Notification Guidelines*, 2017, functional impact taxonomy used to describe operational impact to a firm, also used in Section 2.2.2.3 of this paper. It has been scaled up here to describe the state of a function that a system or firm provides to the sector, rather than on an individual system or firm. It is not included in the taxonomy matrix in Annex 1 of this paper to maintain the firm-level focus of the matrix and incident reporting. Financial authorities of a given jurisdiction may be better placed to determine the sector-level assessment of functional impact, as they are better able to put a reported incident and impact into the context of the entire sector.

Table 12 - Categorisation of Functional Impacts to Financial Sector Services

Functional Impacts to Financial Sector Services (U.S. CERT Federal Incident Notification Guidelines)	Description
No Impact to Sector	The financial services sector is unaffected
No Impact to Sector Services	The functions provided by the financial services sector are unaffected
Minimal Impact to Sector Non-Business-Critical Services (Degradation of 25% or less)	A non-critical function of the financial services sector has been degraded by 25% of its capacity or less.
Minimal Impact to Sector Business-Critical Services	A critical business function of the financial services sector has been degraded by 25% of its capacity or less
Significant Impact to Sector Non-Business-Critical Services (Degradation of more than 25%)	A non-critical business function of the financial services sector has been degraded by more than 25%
Denial of Sector Non-Business-Critical Service(s)	A non-critical business function of the financial sector has been rendered completely unavailable.
Significant Impact to Sector Business Critical Service(s)	A critical business function of the financial sector has been degraded by more than 25%.
Denial of Sector Business Critical Service(s)	A critical financial sector function has been rendered completely unavailable for the entire sector

Annex 1: Proposed matrix for a common categorisation



Annex 2: Bibliography

Banca d'Italia, CODISE Working Group for operational crisis management coordination in the Italian financial marketplace, *Guide*, 2014, www.bancaditalia.it

Bank of England, *CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations, Version 2.0*, 2016, www.bankofengland.co.uk

CRO Forum, *Supporting on-going capture and sharing of digital event data*, February 2018, www.thecroforum.org

Computer Security Resource Center, Online *Glossary of Key Information Security Terms NISTIR 7298 Rev. 3*, July 2019, https://csrc.nist.gov/glossary

Cybersecurity and Infrastructure Security Agency, *US-CERT Federal Incident Notification Guidelines,* April 2017, https://us-cert.cisa.gov/incident-notification- guidelines

eCISRT (Don Stikvoort), "Incident Classification/Incident Taxonomy according to eCSIRT.net – adapted (2012-current mkVI version)", March 2015, www.eCSIRT.net

ENISA, Europol, EC3, *Common taxonomy for Law enforcement and the National Network of CSIRTs*, December 2017, www.europol.europa.eu

ENISA, *Incident Handling Management Handbook, Document for Teachers*, December 2016, www.enisa.europa.eu

ENISA, *Overview of cybersecurity and related terminology,* September 2017,_www.enisa.europa.eu

ENISA, *Reference Incident Classification Taxonomy Task Force Status and Way Forward*, January 2018, www.enisa.europa.eu

ENISA, *Threat Landscape 2020 – Sectoral/thematic threat analysis*, October 2020, www.enisa.europa.eu

ESRB, *Systemic cyber risk*, February 2020, www.esrb.europa.eu

ETSI, Information Security Indicators (ISI) Event Model - A security event classification model and taxonomy (ETSI GS ISI 002 v1.2.1), November 2015, www.etsi.org

ETSI, Information Security Indicators (ISI) Guidelines for security event detection testing and assessment of detection effectiveness (ETSI GS ISI 005 v1.1.1), November 2015, www.etsi.org

European Banking Federation, *EBF position on Cyber incident reporting [EBF_038702],* October 2019, www.ebf.eu

Federal Reserve Bank of New York, *Cyber Risk and the U.S. Financial System: A Pre- Mortem Analysis*, Staff Report No 909, January 2020, https://www.newyorkfed.org/

Federal Reserve Bank of Richmond, *Cyber Risk Definition and Classification for Financial Risk Management*, August 2019, www.richmondfed.org

Financial Stability Board, *Cyber Lexicon*, November 2018, www.fsb.org

FINCEN, *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*, October 2016, www.fincen.gov

FinSAC (WorldBank), *Financial Sector's Cybersecurity: A Regulatory Digest*, 2017, https://www.worldbank.org/en/programs/financial-sector-advisory-center

ISO/TS 22317:2015 *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*.

Information Societies Technology, *Final Report of the eCSIRT.net Project*, January 2004, www.ecsirt.org

Institute and Faculty of Actuaries, Cyber Risk Investigation Working Party, *Cyber Operational Risk Scenarios for Insurance Companies*, 2018, www.actuaries.org.uk

JRC Science Hub, *European Cybersecurity Centers of Expertise, Map Definitions and Taxonomy*, 2018, https://ec.europa.eu/jrc/en/publication/european-cybersecurity-centres-expertise-map-definitions-and-taxonomy

Lockheed Martin (Hutchins, Cloppert and Amin), *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, 2010, www.lockheedmartin.com

MITRE, *MITRE ATT&CK™: Design and Philosophy*, July 2018, www.mitre.org

National Cybersecurity and Communications Integration Center, *NCCIC Cyber Incident Scoring System,* June 2016, www.us-cert.gov

National Institute of Standards and Technology (NIST), *Special Publication 800-30 Rev. 1, Guide for conducting Risk Assessments*, September 2012, https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

National Institute of Standards and Technology (NIST), *Special Publication 800-61 Rev. 2, Computer Security Incident Handling Guide,* August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2

North American Electric Reliability Corporation, *Cyber Security – Incident Reporting and Response Planning, Implementation Guidance for CIP-008-6 (Draft),* November 2018, www.nerc.com

ODNI, *A common Cyber Threat Framework: a Foundation for Communication*, January 2016, www.dni.org

OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, 2017, http://dx.doi.org/10.1787/9789264282148-en

OFSI Canada, *Advisory Technology and Cyber Security Incident Reporting*, January 2019, www.osfi-bsif.gc.ca

ORX, *Cyber: a risk management perspective*, March 2019, www.orx.org

SANS Institute (Steven Launius), *Evaluation of Comprehensive Taxonomies for Information Technology Threats*, March 2018, www.sans.org

UK Department for Digital, Culture, Media and Sport, *Cyber Security Breaches Survey 2019*, 2019, https://www.gov.uk/government/collections/cyber-security- breaches-survey