Commission de Surveillance
du Secteur Financier

Circular CSSF 24/847

ICT-related incident reporting framework

Circular CSSF 24/847

ICT-related incident reporting framework

To all Supervised Entities within the meaning of the following laws, as amended, and regulations as further specified in point 2:

- Law of 5 April 1993 on the financial sector
- Law of 15 December 2000 on postal financial services
- Law of 10 November 2009 on payment services
- Law of 17 December 2010 relating to undertakings for collective investment
- Law of 12 July 2013 on alternative investment fund managers
- Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories
- Law of 17 April 2018 on benchmarks
- Law of 6 June 2018 on Central Securities Depositories
- Law of 28 May 2019 on Network and Information Systems
- Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services

Luxembourg, 5 January 2024

Ladies and Gentlemen,

The purpose of this Circular is to introduce a new ICT-related incident reporting framework in order to acquire a better and more structured overview of the nature, frequency, significance and impact of ICT-related incidents, also considering the growing ICT and security risk in the context of a highly interconnected global financial system.

The provisions of this Circular are based on Article 53(1) of the Law of 5 April 1993 on the financial sector, as amended (hereafter "LFS"), Article 31(4) of the Law of 10 November 2009 on payment services, as amended (hereafter "LPS"), Article 2 of the Law of 15 December 2000 on postal financial services, as amended, Article 147 of the Law of 17 December 2010 relating to undertakings for collective investment, as amended (hereafter "UCITS Law"), Article 50 of the Law of 12 July 2013 on alternative investment fund managers, as amended (hereafter "AIFM Law"), Article 2(1) of the Law of 15 March 2016 on OTC derivatives, central counterparties and trade repositories, as amended (hereafter "EMIR Law"), Article 2(1) of the Law of 17 April 2018 on benchmarks (hereafter "Benchmark Law"), Article 2 of the Law of 6 June 2018 on Central Securities Depositories (hereafter "CSD Law"), and Article 20-16 of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services.

According to Article 3 of the Law of 28 May 2019 on Network and Information Systems (hereafter "NIS Law"), the CSSF is also the competent authority in terms of network and information security for the credit institutions and the financial market infrastructures that have been identified as Operators of Essential Services (hereafter "OES"), as well as for Digital Service Providers (hereafter "DSP") which are already under the supervision of the CSSF ("NIS authority"). The objective of this circular is to lay down the practical details and modalities for the reporting obligations set forth in Articles 8(4), 8(5), 9(1), 11(3) and 11(4) and 12 of the NIS Law and in CSSF Regulation No 24-01

relating to the notification of incidents according to the Law of 28 May 2019[1] (hereafter "CSSF Regulation No 24-01") regarding specifically Articles 8(5) and 11(3) of the NIS Law.

This Circular brings the following changes to the current incident reporting mechanism:

- Increases the incident coverage, currently limited to fraud and incidents due to external computer attacks as per Circular CSSF 11/504, by covering more broadly ICT operational and security incidents while avoiding double reporting for incidents to be notified under other incident notification frameworks.
- Introduces reporting based on classification. Supervised Entities will be required to classify ICT-related incidents based on the criteria indicated in this Circular and to notify to the CSSF the cases where ICT-related incidents are classified as major or significant incidents.
- Introduces a new incident reporting notification form. To obtain data in a structured form, Supervised Entities will be required to complete and submit an ICT-related incident notification form in case the ICT-related incident is classified as a major or significant incident.
- Introduces a specific chapter to cover in the same Circular the incident notification requirements (previously communicated via bilateral communications to Supervised Entities that are under the scope of the NIS Law) in order to apply the new incident reporting notification forms and practical requirements to the notifications of incidents assessed as significant under the NIS Law.

This Circular is divided in four chapters:

- Chapter 1 (Definitions and scope of application) sets out the definitions applicable for the purpose of this Circular and defines the scope of application;
- Chapter 2 (General requirements) sets out the requirements for the classification and reporting of the ICT-related incidents;
- Chapter 3 (Specific requirements under the NIS Law and CSSF Regulation No 24-01) is dedicated to specific requirements for those Supervised Entities that are subject to the NIS Law and CSSF Regulation No 24-01 and that are defined as OES or DSP;
- Chapter 4 (Date of application) provides for the entry into force of this Circular.

[1] CSSF Regulation No 24-01 of 5 January 2024 relating to the notification of incidents according to the Law of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the European Union.

TABLE OF CONTENTS

Chapter 1: Definitions and scope of application

Section 1.1: Definitions

1. For the purpose of this Circular, the following definitions apply[2]:

   a) "Network and information system" means:
      i. an electronic communications network within the meaning of Article 2, paragraph 1, of the Law of 17 December 2021 on electronic communications networks and services[3];
      ii. any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
      iii. digital data stored, processed, retrieved or transmitted by elements covered under points i. and ii. above for the purposes of their operation, use, protection and maintenance.

   b) "Security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

   c) "ICT-related incident" means a single event or a series of linked events unplanned by the Supervised Entity that compromises the security of the network and information systems, and has an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the Supervised Entity.

   d) "Major ICT-related incident" means an ICT-related incident that has a high adverse impact on the network and information systems that support critical or important functions of the Supervised Entity.

   e) "Critical or important function" means a function, the disruption of which would materially impair the financial performance of a Supervised Entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a Supervised Entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services laws.

   f) "Operator of Essential Services" ("OES") means, in accordance with point (3) of Article 2 of the NIS Law, a public or private entity of a type referred to in the annex to the NIS Law, and which meets the criteria laid down in Article 7(2) of the NIS law[4].

[2] Definitions in points 1.f) to 1.i) are specific to Supervised Entities subject to the requirements of the NIS Law and CSSF Regulation No 24-01.

[3] 'Electronic communications network' means transmission systems, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including internet) and mobile networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

[4] In its competence as NIS authority, the CSSF already notified the relevant Supervised Entities of their identification as OES when the NIS Law entered into force. The CSSF will reconfirm the relevant Supervised Entities of their status as OES at the latest by 1 March 2024. The Supervised Entities which will not receive this notification at that date are therefore not designated as OES, without prejudice to potential future designation.

g) "Digital Service Provider" ("DSP") means, in accordance with point (5) of Article 2 of the NIS Law, a private entity that provides a digital service as defined in point (4) of Article 2 of the NIS Law[5].

h) "Essential service" means a service which is essential for the maintenance of critical societal and/or economic activities and which is listed as essential service in Article 2 of CSSF Regulation No 20-04 of 15 July 2020[6].

i) "Significant incident" means an incident having a significant impact on the continuity of the essential services provided by an OES or on the provision of a digital service provided by a DSP[7] within the European Union. For the purpose of this Circular, a significant incident is by default considered as a "Major ICT-related incident".

2. The following entities are to be considered as Supervised Entities in the frame of this Circular:

a) credit institutions and professionals of the financial sector within the meaning of the LFS;

b) approved publication arrangements (APAs) with a derogation and authorised reporting mechanisms (ARMs) with a derogation within the meaning of the LFS;

c) payment institutions and electronic money institutions within the meaning of the LPS;

d) POST Luxembourg governed by the Law of 15 December 2000 on postal financial services[8];

e) management companies incorporated under Luxembourg law and subject to Chapter 15 of the UCITS Law;

f) management companies incorporated under Luxembourg law and subject to Articles 125-1 or 125-2 of Chapter 16 of the UCITS 2010 Law;

g) Luxembourg branches of IFMs subject to Chapter 17 of the UCITS Law;

h) investment companies which did not designate a management company within the meaning of Article 27 of the UCITS Law;

i) alternative investment fund managers authorised under Chapter 2 of the AIFM Law;

j) internally managed alternative investment funds within the meaning of point (b) of Article 4(1) of the AIFM Law;

k) central counterparties (CCPs) within the meaning of Article 2(1) of EMIR[9], including Tier 2 third-country CCPs within the meaning of Article 25(2a) of EMIR, complying with the relevant requirements of EMIR in accordance with point (a) of Article 25(2b) of EMIR;

l) central securities depositories within the meaning of the CSD Law;

[5] In its competence as NIS authority, the CSSF already informed relevant Supervised Entities of their consideration as DSP when the NIS Law entered into force. The CSSF will reconfirm the relevant Supervised Entities of their status as DSP at the latest by 1 March 2024. The Supervised Entities which will not receive this information at that date are therefore not considered as DSP, without prejudice to potential future information.

[6] CSSF Regulation No 20-04 of 15 July 2020 on the definition of essential services under the Law of 28 May 2019 transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a common high level of network and information system security in the European Union.

[7] Definition in alignment with the NIS Law.

[8] For the sake of clarity, the wording "postal financial services" has the meaning provided for in Article 1 of the Law of 15 December 2000, as amended.

[9] Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories.

m) administrators of critical benchmarks within the meaning of point (b) of Article 20(1) of the Benchmark Regulation[10];

n) crowdfunding Service Providers within the meaning of the Law of 16 July 2019 on the operationalisation of European regulations in the area of financial services;

o) credit institutions and the financial market infrastructures for which according to Article 3 of the NIS Law the CSSF is the competent authority in terms of network and information security and that have been identified as OES,

p) support PSF authorised in accordance with Article 29-3 of the LFS for which according to Article 3 of the NIS Law the CSSF is the competent authority in terms of network and information security and that have been informed by the CSSF of their consideration as DSP under the NIS Law.

Section 1.2: Scope of application

3. This Circular defines the supervisory expectations that must be complied with in the event of an ICT-related incident.

4. The provisions of Chapter 2 (General requirements) of this Circular are applicable to all Supervised Entities as defined in point 2 a) to n) above, hereinafter collectively referred to as "**Supervised Entities**" or individually as "**Supervised Entity**", including their branches as specified in the respective laws. Branches in Luxembourg of Entities incorporated in a third country shall be deemed to be included in the notion of Supervised Entity.

5. Branches in Luxembourg of the Entities that are part of a legal entity whose head office is located in a different Member State of the European Economic Area (EEA) (EEA branches) are subject to the supervision of the competent authority of that Member State (home Member State). However, as the CSSF is competent for ensuring that EEA branches comply with the specific requirements laid down in the sectoral legal and regulatory frameworks[11], this Circular applies if an ICT-related incident impacts areas for which the CSSF retains an oversight responsibility.

6. The provisions of Chapter 3 (Specific requirements under the NIS Law and CSSF Regulation No 24-01) of this Circular are only applicable to those Supervised Entities that are also OES[4] or DSP[5].

7. With the aim of preventing double reporting, Supervised Entities in scope of this Circular are not required to notify under this Circular the incidents they notify in compliance with:

   a) Circular CSSF 21/787 on the "Application of the EBA Guidelines (EBA/GL/2021/03) on Major Incident Reporting under PSD2", and/or;
   b) Cyber Incident Reporting for Supervised Entities defined as significant institutions falling under the direct supervision of the ECB, and/or;
   c) Article 45(6) of Regulation (EU) No 909/2014 on notification of incidents resulting from the risks that key participants, service and utility providers, other central securities

[10] Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014.

[11] Notably in the context of investment services in accordance with the MiFID Law, the AML/CFT Law, the provision of asset management services and depositary tasks for Undertakings for Collective Investments established in Luxembourg.

depositories (CSDs) or other market infrastructures might pose to the CSD's operations, and/or;

d) Article 71(4)(b) of Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 on reporting of material operational incidents to the competent authority.

8. By way of exception from point 7 above, Supervised Entities falling under by point 7.b) and who are also OES, are required to report to the CSSF as per this Circular those incidents that impact the continuity of the essential services they provide, in addition to their other incident reporting obligations.

Chapter 2: General requirements

Section 2.1: Incidents to be notified

9. Supervised Entities shall notify the following incidents in accordance with the procedure defined in section 2.3:

   a) Any successful malicious unauthorised access to the network and information systems. For the purpose of this circular these successful malicious unauthorised accesses are to be considered as major ICT-related incidents.
   b) Any incident other than those referred to in point a) above, classified in line with section 2.2 as major ICT-related incident.

Section 2.2: ICT-related incident classification

10. Supervised Entities shall classify ICT-related incidents and assess their impact on the basis of the following criteria:

    a) the number and/or relevance of clients[12] or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;
    b) the duration of the ICT-related incident, including the service downtime;
    c) the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;
    d) the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality;
    e) the criticality of the services affected, including the Supervised Entity's transactions and operations;
    f) the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.

11. When the Supervised Entity's internal assessment based on the criteria listed under point 10 leads the Supervised Entity to classify an ICT-related incident as major, the ICT-related incident shall be considered as major under this circular.

12. In the case the assessment referred under point 11 does not lead to a clear outcome on whether the ICT-related incident has to be classified as major, Supervised Entities shall report the ICT-related incident to the CSSF.

13. Supervised Entities shall classify the ICT-related incident in a timely manner after the ICT-related incident has been detected, and without undue delay after the information required for the classification of the ICT-related incident is available to the Supervised Entities, but no later than 24 hours after the detection of that ICT-related incident. If longer time is needed to classify the ICT-related incident, Supervised Entities shall explain in the initial notification submitted to the competent authority the reasons thereof. Where the deadline

[12] Supervised Entities who are also OES shall consider the number of users affected by the disruption to the essential service. Supervised Entities who are also DSP shall consider the number of users affected by the incident, in particular those who use the digital service to provide their own services.

for classification falls on a weekend day or a bank holiday, Supervised Entities may classify the incident on the next working day.

Section 2.3: Major ICT-related incident notification

14. Supervised Entities shall, within the time limits laid down in Annex I, submit the following notifications of major ICT-related incidents to the CSSF:

    a) An initial notification with "Initial Information" when the ICT-related incident has been classified as major.
    b) An intermediate notification with "Incident cause, classification and impact" after the initial notification referred to in point 14.a), followed by, as appropriate, updated notifications each time a relevant update is available, as well as upon specific request by the CSSF.
    c) A final notification, when the root cause analysis has been completed, regardless of whether mitigation measures have been fully implemented, and when the actual impact figures are available to replace estimates. In this notification Supervised Entities can add any follow-up and additional information that is deemed relevant for the ICT-related incident.

15. When the ICT-related incident proves to have or will potentially have a very serious impact (e.g., complete unavailability of the systems), the Supervised Entity shall notify the CSSF as soon as possible within the given timeframe, and if necessary, before the formal submission of the notification form.

16. ICT-related incident notifications referred to in point 14 shall be submitted via the corresponding form available using the CSSF digital solution as further specified on the CSSF website.

17. Supervised Entities shall complete the relevant section of the notification form, depending on the phase they are in (i.e., section "Initial information" for initial notification, section "Incident cause, classification and impact" for intermediate notification and section "Root cause – Follow-up and additional information" for final notification). The notification form contains the data fields laid down in Annex II.

18. The sections of the notification form must be submitted in the order indicated in point 14. Should the Supervised Entity have all the information required available at the time of the initial notification, a single submission (containing all the sections of the notification form) shall be made.

19. Supervised Entities shall also notify the competent authority when, as a result of the continuous assessment of the ICT-related incident, it is identified that an already reported ICT-related incident no longer fulfils the criteria to be considered major and is not expected to fulfil them before the ICT-related incident is resolved. In this case, Supervised Entities shall reclassify the ICT-related incident as soon as this circumstance is detected and provide an explanation of the reasons justifying this reclassification in the section "Initial information" of the notification form.

20. Supervised Entities may outsource the reporting obligations under this chapter to a third-party provider. In case of such outsourcing, the Supervised Entity remains fully responsible for the fulfilment of the ICT-related incident reporting requirements within the applicable timeline and for the whole content of the incident reporting.

Chapter 3: Specific requirements under NIS Law and CSSF Regulation No 24-01

Section 3.1: Incident notification by Supervised Entities who are also OES

21. In compliance with Article 8(4) of the NIS Law, Supervised Entities who are also OES shall notify, without undue delay, the CSSF of incidents having a significant impact on the continuity of the essential services they provide. The notion of "without undue delay" is considered complied with when Supervised Entities submit their incident notification in line with the time limits indicated in section 2.3 (Major ICT-related incident notification) and in Annex I.

22. In this respect, in compliance with Article 8(5) of the NIS Law and CSSF Regulation No 24-01, Supervised Entities who are also OES shall assess whether an incident is to be classified as a significant incident by applying mutatis mutandis the requirements stated in section 2.2 (ICT-related incident classification) and shall notify the significant incidents in compliance with the requirements stated in section 2.3 (Major ICT-related incident notification).

23. Successful malicious unauthorised accesses have to be considered by default as significant incidents and shall be notified in compliance with the requirements stated in section 2.3 (Major ICT-related incident notification).

24. When an incident is classified both as a significant incident and as a major ICT-related incident (e.g., the incident impacts both essential services under NIS and other critical or important functions), Supervised Entities who are also OES shall notify only once the incident and indicate in their notification that the incident is also notified under the NIS Law.

Section 3.2: Incident notification by Supervised Entities who are also DSP

25. Article 11(3) of the NIS Law and CSSF Regulation No 24-01 mentions that DSPs shall notify, without undue delay, the competent authority of incidents having a significant impact on the provision of a digital service they provide within the European Union. The notion of "without undue delay" is considered complied with when Supervised Entities submit their incident notification in line with the time limits indicated in section 2.3 (Major ICT-related incident notification) and in Annex I.

26. Supervised Entities who are also DSP shall:

    a) assess whether an incident (including successful malicious unauthorised accesses, as defined under point 9.a) of section 2.1) is to be classified as a significant incident in line with Articles 3 and 4 of Commission Implementing Regulation (EU) 2018/151 of 30 January 2018[13] providing details on Article 11(4) of the NIS Law;

[13] Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

b) apply mutatis mutandis points 12 and 13 of section 2.2 (ICT-related incident classification);
c) notify the significant incidents in compliance with the requirements stated in section 2.3 (Major ICT-related incident notification).

27. When an incident is classified both as a significant incident and as a major ICT-related incident, Supervised Entities who are also DSP shall notify only once the incident and indicate in their notification that the incident is also notified under the NIS Law.

Chapter 4: Date of application

28. This Circular shall enter into force on 1 April 2024 for the Supervised Entities as defined in point 2 a) to d) and k) to p) in Section 1.1., and on 1 June 2024 for the Supervised Entities as defined in point 2 e) to j) in Section 1.1. The Circular will repeal and replace Circular CSSF 11/504 on "Frauds and incidents due to external computer attacks" on 1 April 2024 for the Supervised Entities as defined in point 2 a) to d) and k) to p) in Section 1.1. and on 1 June 2024 for the Supervised Entities as defined in point 2 e) to j) in Section 1.1.

Claude WAMPACH
Director

Marco ZWICK
Director

Jean-Pierre FABER
Director

Françoise KAUTHEN
Director

Claude MARX
Director General

Annexes
I. Deadlines and explanations for submission of notifications
II. Data fields

Commission de Surveillance du Secteur Financier

Annex I: Deadlines and explanations for submission of notifications

Relevant section to be filled in and submitted	Deadlines	Explanatory notes
N/A	*Classification of the incident as major* Within 24 hours after the detection of the ICT-related incident Where the deadline for classification falls on a weekend day or a bank holiday, Supervised Entities may classify the incident on the next working day.	*Classification of the incident as major* Reminder of point 15: When the ICT-related incident proves to have or will potentially have a very serious impact (e.g., complete unavailability of the systems), the Supervised Entity shall notify the CSSF as soon as possible within the given timeframe, and if necessary, before the formal submission of the notification form.
INITIAL INFORMATION	Within 4 hours after the classification of the incident as major Where the deadline for notification falls on a weekend day or a bank holiday, Supervised Entities may notify the incident on the next working day.	The "INITIAL INFORMATION" section contains the general information about the incident that shall be included in the notification the first time it is submitted.
INCIDENT CAUSE, CLASSIFICATION AND IMPACT	Within 3 working days after the submission to the CSSF of the INITIAL INFORMATION	The section "INCIDENT CAUSE, CLASSIFICATION AND IMPACT" provides a more detailed description of the incident, its consequences and the corrective measures that were taken to

		recover. If the Supervised Entity has updates to previous reports (of the same incident), an updated version of the section of the form may be submitted.
ROOT CAUSE – FOLLOW-UP AND ADDITIONAL INFORMATION	Within 20 working days after the submission to the CSSF of the INCIDENT CAUSE, CLASSIFICATION AND IMPACT	The section "ROOT CAUSE – FOLLOW-UP AND ADDITIONAL INFORMATION" provides information regarding the root cause analysis, lessons learned and any other relevant information. When submitting this information, the Supervised Entity shall review the other sections of the form and update these, where appropriate.

Annex II: Data fields

Section – Initial Information

Data Field description / Question	Field type	Proposed options
1. Contact person within the supervised entity for updates: Name and surname	Alphanumeric	
1. Contact person within the supervised entity for updates: Email	Alphanumeric (email format)	
1. Contact person within the supervised entity for updates: Phone	Number (telephone format)	
2. Second contact person within the supervised entity for updates: Name and surname	Alphanumeric	
2. Second contact person within the supervised entity for updates: Email	Alphanumeric (email format)	
2. Second contact person within the supervised entity for updates: Phone	Number (telephone format)	
3. Country(ies) affected by the incident	Choice (multiple) - Select all that apply	List of world countries
4. Date and time of detection of the incident	yyyy-mm-dd hh:mm	
5. Date and time of classification of the incident as major	yyyy-mm-dd hh:mm	
6. Criteria triggering the major ICT-related incident report	Choice (multiple) - Select all that apply	• Clients or financial counterparts affected • Transactions affected • Reputational impact • Service downtime • Geographical spread • Data losses entailed in relation to availability, authenticity, integrity or confidentiality • Criticality of the services affected • Economic impact

Data Field description / Question	Field type	Proposed options
7. The incident was detected by	Choice (multiple) – Select one option	• IT security • Staff member • Internal audit • Consumer / payment service user • External auditor • Third party provider • Attacker / warning • Other
7.1. If "Other", specify	Alphanumeric	
8. General description of the incident Provide a general description of the incident, its immediate impact and including the measures that have been taken so far	Alphanumeric	
9. Short description of impact in other EU member states	Alphanumeric	
10. Has the incident been reported to other authorities?	Boolean (Checkbox)	
10.1. If checkbox was ticked, specify	Alphanumeric	
11. If the incident caused a service interruption, is the service restored (even in degraded mode) at the time of this notification?	Alphanumeric	
12. Is the incident notified under NIS (Network Information System) framework?	Boolean (Checkbox)	

Section – Incident cause, classification and impact

Data Field description / Question	Field type	Proposed options
1. Detailed description of the incident, Provide a detailed description of the incident, including (if known and/or applicable): - How the incident started - Background and incident detection, who was involved, what happened, how did it evolve? - Cause of the incident	Alphanumeric	
2. What are the main areas/systems/channels that were affected as the incident evolved?	Alphanumeric	
3. Was it related to a previous incident(s)?	Boolean (Checkbox)	
3.1. If checkbox was ticked, specify	Alphanumeric	
4. Date and time of beginning of the incident - if known	yyyy-mm-dd hh:mm	
5. Who is leading the investigation of the incident?	Choice (multiple) – Select one option	• Group • Supervised entity • Service provider • Security company • Other
6. Cause and type		
6.1. Details regarding incident cause and type (Select all that apply). Select at least one of the main options. Then, as applicable, select the subcategories	Choice (multiple) - Select all that apply	• Under investigation • Malware • Social engineering • Insider/Third Party Provider Threat • Intrusion/Unauthorised access

Data Field description / Question	Field type	Proposed options
		• Denial of service • System/Process failure • Human error • Other
6.1.1. If "Other", specify	Alphanumeric	

6.2. As applicable, select the subcategories	Choice (multiple) - Select all that apply	• Malware
		  ○ Ransomware
		  ○ Trojan horse
		  ○ Virus/Worm/Spyware
		  ○ Other (Malware)
		• Social engineering
		  ○ Phishing/*ishing
		  ○ Other (Social engineering)
		• Insider/Third Party Provider Threat
		  ○ Accidental data leakage/corruption
		  ○ Intentional misuse of access rights by insider
		  ○ Intentional misuse of access rights by service provider
		  ○ Other (Insider/Third Party Provider Threat)
		• Intrusion/Unauthorised access
		  ○ Brute force attack
		  ○ Malicious script injection and/or OS commanding
		  ○ Unauthorized use of resources, copyright
		  ○ Account/application compromise
		  ○ Other exploited vulnerability
		  ○ Other (Intrusion/Unauthorised access)
		• Denial of service
		• System/Process failure
		  ○ Hardware failure
		  ○ Software/application failure
		  ○ Network failure
		  ○ Database/Storage failure
		  ○ Physical damage
		  ○ Other (System/Process failure)

Data Field description / Question	Field type	Proposed options
		• Human error • Other
7. If this incident is related to a cyber-attack, provide information regarding the attacker(s) (select all that apply)	Choice (multiple) - Select all that apply	• Terrorists • Hacktivists • Foreign agencies • Inside job/Unaware employee • Unknown • Other
7.1. If "Other", specify	Alphanumeric	
8. Users impacted		
8.1. Number of internal users impacted	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.1.1. As a % total internal users (values allowed from 0 to 100, rounded, no decimals, percentage sign not allowed)	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.2. Number of customers impacted	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
8.2.1. As a % total customers (values allowed from 0 to 100, rounded, no decimals, percentage sign not allowed)	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available

Data Field description / Question	Field type	Proposed options
9. Service downtime?	Boolean (Checkbox)	
9.1. If checkbox was ticked, provide the total service downtime (DD:HH:MM)	Alphanumeric (DD:HH:MM)	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
10. Economic impact		
10.1. Direct financial loss in EUR	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
10.2. Indirect financial loss in EUR	Numeric	
Actual or estimated	Choice (multiple) – Select one option	• Actual figure • Estimation • Not yet available
11. Were crisis management (or equivalent) procedures activated or is it likely to be activated?	Boolean (Checkbox)	
11.1. If checkbox was ticked, specify the actions taken	Alphanumeric	
12. Were any legal or regulatory requirements breached?	Boolean (Checkbox)	
12.1. If checkbox was ticked, specify	Alphanumeric	
13. Was there any media coverage?	Boolean (Checkbox)	
13.1. If checkbox was ticked, specify the media/newspapers/blogs that covered the topic	Alphanumeric	

Data Field description / Question	Field type	Proposed options
14. Overall impact (select all that apply)	Choice (multiple) - Select all that apply	• Integrity • Availability • Confidentiality • Reputational
15. Was the incident affecting you directly, or indirectly through a service provider?	Choice (multiple) – Select one option	• Directly • Indirectly
15.1. If "Indirectly", specify the service provider's name	Alphanumeric	
16. Other impacts	Alphanumeric	
17. Corrective actions/measures that have been taken so far or are planned to recover from the incident	Alphanumeric	
18. Was a business continuity plan activated? If yes, when and how?	Boolean (Checkbox)	
18.1. Date and time	yyyy-mm-dd hh:mm	
18.2. Describe	Alphanumeric	
19. Was a disaster recovery plan activated? If yes, when and how?	Boolean (Checkbox)	
19.1. Date and time	yyyy-mm-dd hh:mm	
19.2. Describe	Alphanumeric	
20. Is the incident in any way related to remote access (e.g., teleworking, remote connectivity, etc.)?	Boolean (Checkbox)	
20.1. If checkbox was ticked, specify	Alphanumeric	

Section - Root cause, follow-up and additional information

Data Field description / Question	**Field type**	**Proposed options**
1. Additional information Provide details regarding the following: Lessons learned (including main actions/measures taken/planned to prevent the incident from happening again in the future)	Alphanumeric	
2. Root cause and/or Vulnerabilities/weaknesses identified (select all that apply)	Choice (multiple) – Select all that apply	• Inadequate Change Management • Migration failure • Inadequacy of internal procedures and documentation • Improper operations • Latency issues • Recovery issues • Lack of staff awareness and/or compliance • Unauthorised software/wrong version • Inadequate privileged account management • Inadequate email/web browser protection • Inadequate malware defences • Inadequate identity access management • Inadequate security configurations for secure hardware and software on devices, laptops, workstations, servers • Inadequate boundary defences • Inadequate control of network ports, protocols and services • Inadequate resilience and/or back-up of systems or files • Unsecured network devices (firewalls, routers, switches) • Inadequate maintenance and monitoring of logs • Inadequate DDoS defences • Inadequate penetration and security testing • Inadequate patch management • Inadequate application software security controls (web-based and other applications) • Other

Data Field description / Question	Field type	Proposed options
2.1. If "Other", specify	Alphanumeric	
3. Other relevant information on the root cause (e.g., What went wrong with the change, New technical vulnerability exploited, etc.)	Alphanumeric	
4. If this incident is related to a cyber-attack, what was the entry vector of the incident? (select all that apply)	Choice (multiple) – Select all that apply	• Website • Instant messaging • Phone • Insider attack (privileged user) • E-mail • Third party network • Unauthorised devices • Insider attack (regular / business users) • Lost / stolen devices • Chat rooms / social media • Other
4.1. If "Other", specify	Alphanumeric	
5. Who is leading the remediation actions?	Choice (multiple) – Select one option	• Group • Supervised entity • Service provider • Security company • Other
5.1. If "Other", specify	Alphanumeric	
6. Are Police/other security agencies involved in the investigation?	Choice (multiple) – Select one option	• Police • Other • None
6.1. If "Other", specify	Alphanumeric	
7. If the incident is related to ICT security, was the incident reported to the national CERT (e.g., CIRCL, GOVCERT)?	Boolean (Checkbox)	
8. Has any legal action been taken (e.g., complaint with prosecutor against provider or perpetrator)?	Boolean (Checkbox)	

Data Field description / Question	Field type	Proposed options
8.1. If checkbox was ticked, specify	Alphanumeric	
9. Assessment of the effectiveness of the action taken	Choice (multiple) – Select one option	• Highly effective • Moderately effective • Not effective • Not yet available
9.1. Details	Alphanumeric	
10. What is the current status of the incident?	Choice (multiple) – Select one option	• Resolved • Contained • Ongoing • Unknown
10.1. Provide the date and time when then incident was closed or is expected to be closed if known	yyyy-mm-dd hh:mm	