Commission de Surveillance
du Secteur Financier

CSSF FAQ – Circular CSSF 24/847

ICT-related incident reporting framework

CSSF FAQ – Circular CSSF 24/847

ICT-related incident reporting framework

TABLE OF CONTENTS

Context

The present document refers to a list of questions and answers (Q&A) in relation to a number of key aspects of the Circular CSSF 24/847 concerning the ICT-related incident reporting framework (hereafter "Circular"). The objective is to bring further clarity on the supervisory expectations of the competent authority.

This document will be updated when necessary and the CSSF reserves the right to adapt its approach to any matter covered by the Q&A at any time. You should regularly check the CSSF website in relation to any matter of importance to you to see if questions have been added and/or positions have been adapted.

Definitions

Definitions taken from the circular and relevant to the Q&A are listed here below:

a) "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 have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the Supervised Entity;
b) "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;
c) "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;
d) "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;
e) "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 within the European Union. For the purpose of this circular a significant incident is by default considered as a "Major ICT-related incident".

Update information

05/01/2024	**First publication**

Question 1: What is the link between NIS Law (NIS1) / NIS2 / DORA and this Circular?

The term "NIS Law" used throughout the Circular refers to the Law of 28 May 2019 on Network and Information Systems, which is also referred to as "NIS1 Law". This is the NIS Law that is currently applicable and is therefore the law that is referred to in the Circular.
NIS2 will become applicable when it will be transposed in Luxembourg by 17 October 2024.

DORA refers to the Digital Operational Resilience Act. DORA Regulation will only be applicable as of 17 January 2025.
DORA will be *lex specialis* for Financial Entities falling under NIS2 but neither DORA nor NIS2 are applicable yet and therefore they are not relevant in the context of the Circular at the current point in time.

Question 2: To which entities does Chapter 3 of the Circular apply?

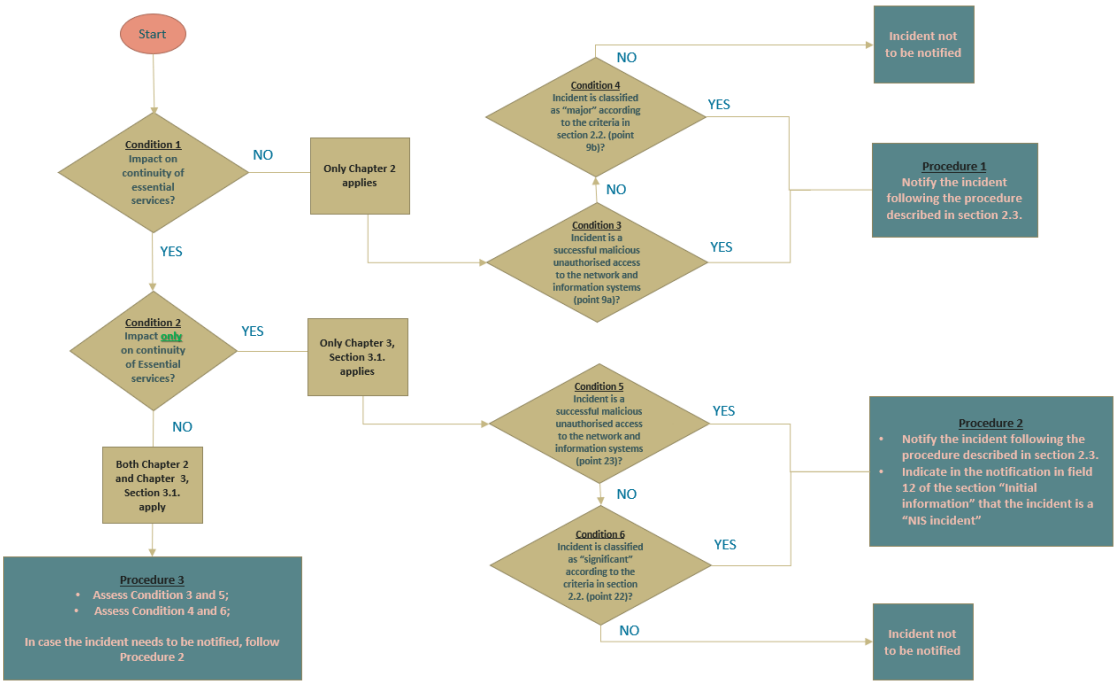
Chapter 3 of the Circular applies only to Supervised Entities that are either Operators of Essential Services "OES" or Digital Service Providers "DSP" under the NIS1 Law. These entities will have been notified of their identification as OES or informed of their consideration as DSP when the NIS Law entered into force. The CSSF will reconfirm the relevant Supervised Entities of their status as OES or DSP respectively at the latest by 1 March 2024. The Supervised Entities which will not receive this information at that date are therefore not designated as OES or considered as DSP respectively, without prejudice to potential future designation or information.

Question 3: The provisions of Chapter 2 are applicable to all Supervised Entities as defined in point 2 a) to n). What about OES and DSP as defined in point 2 o) and p)?

Supervised Entities that are either OES or DSP are by default included in point 2 a). OES are either credit institutions or financial market infrastructures, which are professionals of the financial sector within the meaning of the LFS. DSP that are supervised by the CSSF are also professionals of the financial sector within the meaning of the LFS, more specifically support PFS according to article 29-3 of the LFS.

The following examples shall clarify the classification and notification flow:

1. **An ICT-related incident occurs at a Supervised Entity that is a credit institution, under point 2 a) of the Circular, and an OES, under point 2 o) of the Circular.**



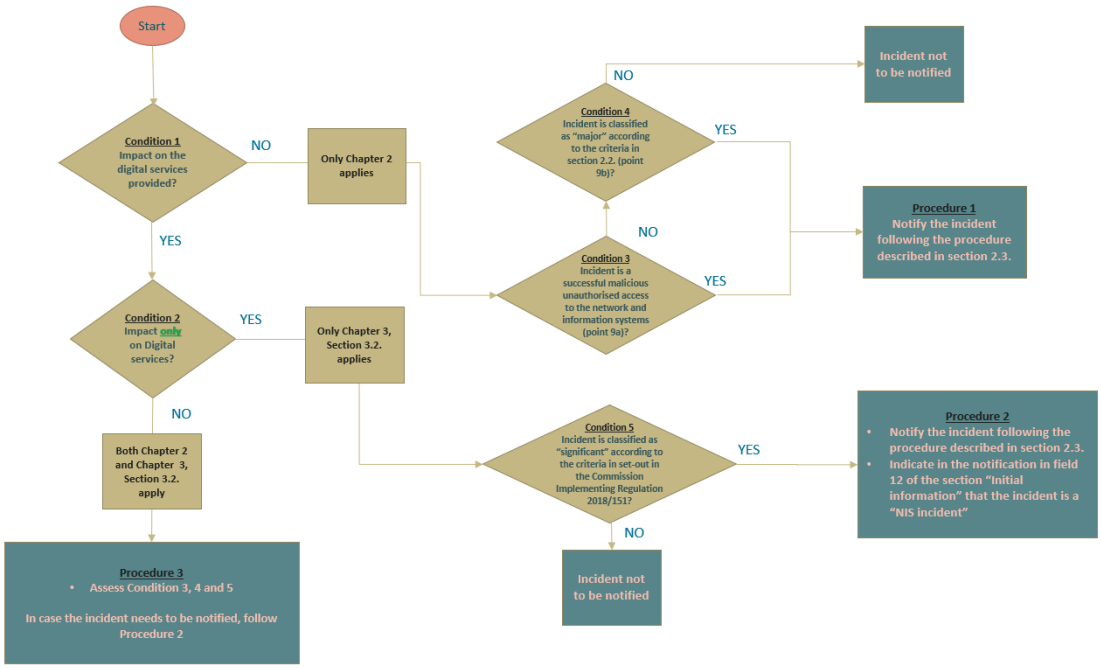
The Supervised Entity needs to assess whether the ICT related incident impacts the continuity of the essential services:

a) No (e.g. impact on other critical or important functions): only Chapter 2 of the Circular applies;

b) Yes, and only on essential services: only Chapter 3, Section 3.1. of the Circular applies. This Chapter describes the steps that need to be fulfilled to comply with the NIS Law. It refers to elements of Chapter 2 for classification criteria (2.2.) and notification requirements (2.3) as the NIS Law is silent on these points. In the notification form the Supervised Entity shall indicate that the ICT-related incident is notified under the NIS framework.

c) Yes, and it impacts both essential services and other critical or important functions: both Chapter 2 (in its entirety) and Chapter 3, Section 3.1. of the Circular apply, which refer to the same classification and notification requirements. In the notification form the entity shall indicate that the ICT-related incident is also notified under the NIS framework.

2. An ICT-related incident occurs at a Supervised Entity that is a support PFS, under point 2 a) of the Circular, and a DSP, under point 2 p) of the Circular.



The Supervised Entity needs to assess whether the ICT related incident impacts the provision of digital services provided by the entity:

a) No (e.g. impact on other services): only Chapter 2 of the Circular applies;

b) Yes, and only on digital services: only Chapter 3, Section 3.2. of the Circular applies. This Chapter describes the steps that need to be fulfilled to comply with the NIS Law. The entity shall assess whether the incident is to be classified as a significant incident under the NIS Law in line with the thresholds indicated in the Commission Implementing Regulation (EU) 2018/151 (point 26.a)). Section 3.2. also refers to Chapter 2 only for some points of the section 2.2. (not related to the classification) and for section 2.3 (for notification requirements) as the NIS Law and the Commission Implementing Regulation are silent on these points. In the notification form the Supervised Entity shall indicate that the ICT-related incident is notified under the NIS framework.

c) Yes, and it impacts both digital services and other services: both Chapter 2 (in its entirety) and Chapter 3, Section 3.2. of the Circular apply. In the notification form the entity shall indicate that the ICT-related incident is also notified under the NIS framework.

Question 4: What is the meaning of the term "successful" in the context of section 2.1. point 9 a) "*Any successful malicious unauthorised access to the network and information systems*"?

With the use of the term "successful" when referring to malicious unauthorised accesses, the CSSF aims to differentiate these from simple "attempts" without intrusion.

Some examples are provided here below:
Use case 1: Social engineering, such as phishing, where an employee of the Supervised Entity clicked on a link received via email:

- If the Supervised Entity had protection mechanisms in place and blocked the intrusion, these social engineering attempts are not considered successful and don't have to be notified to the CSSF.
- If the Supervised Entity did not have protection mechanisms in place, or they were in place but not sufficient, to block the intrusion, the CSSF considers that the intrusion occurred, and the incident has to be notified as a successful malicious unauthorised access.

Use case 2: A Supervised Entity gets hacked, and the hackers were able to encrypt 2% of the files. However, the Supervised Entity was able to detect and isolate the issue:

- The example shows that a vulnerability existed and was exploited by a malicious actor. Even if the impact was considered limited by the Supervised Entity and no evident business impacts were identified at the moment of the incident, the CSSF considers that such unauthorised intrusions, even if the impacts are not immediately known or considered minor, may lead to serious consequences, in particular data breaches and data leakages.
- The CSSF considers this incident has to be notified as successful malicious unauthorised access.

Phishing attacks against clients of the Supervised Entities are not in scope of the Circular.

Question 5: What is the difference between the terms "authenticity" and "integrity"?

The CSSF considers the basic definitions of the ISO/IEC 27000:2018 as documented in the Cyber Lexicon of the Financial Stability Board (FSB):

- Authenticity: property that an entity is what it claims to be;
- Integrity: property of accuracy and completeness.

In the context of the Circular 24/847, the CSSF considers that an ICT-related incident has an impact on the authenticity respectively integrity when:

- The incident has compromised the trustworthiness of the source of data (authenticity)
- The incident has resulted in a non-authorised modification of data that has rendered it inaccurate or incomplete (integrity).

Question 6: Are physical security incidents included in the scope of the Circular?

A physical security incident is considered as an ICT-related incident, and therefore in the scope of the Circular, if, following such incident, the security of the network and information systems is compromised, and this has an adverse impact on the availability, authenticity, integrity or confidentiality of data or on the services provided by the Supervised Entities.
For example, fibre network cable cuts are to be considered as ICT-related incidents.