

If you cannot see this email, please [click here](#).



Luxembourg Newsflash - 25 January 2024

ICT-related incident reporting – new CSSF Circular and Regulation

On 5 January 2024, the CSSF issued Circular CSSF 24/847. At the same time, it also provides a comprehensive FAQ on Circular CSSF 24/847 and CSSF Regulation no. 24-01. Together, these releases shape the new landscape of the ICT-related incident reporting framework.

Reading time: 3 minutes, 39 seconds

On 5 January 2024, the Commission de Surveillance du Secteur Financier (**CSSF**) issued Circular CSSF 24/847 (**CSSF Circular**). At the same time, the CSSF also provided a comprehensive FAQ on Circular CSSF 24/847 (**CSSF FAQ**) and CSSF Regulation no. 24-01 (**CSSF Regulation**) was published in the Luxembourg Official Journal. Together, these releases shape the new landscape of the ICT-related incident reporting framework.

All three published documents should be read together for a comprehensive understanding of the CSSF's supervisory approach and regulatory framework.

1. Aim

The CSSF Regulation outlines the requirements for incident classification and major incident notification under the law of 28 May 2019 on Networks and Information Systems (NIS Law) for **Operators of Essential Services** (OES) and **Digital Service Providers** (DSP) subject to this law. Consequently, the process for classification and reporting of ICT-related incidents will be standardised for all entities under CSSF supervision.

Circular CSSF 24/847 will repeal and replace Circular CSSF 11/504 on "Frauds and incidents due to external computer attacks". It details the new supervisory expectations to be complied with in the event of an ICT-related incident. The new ICT-related incident reporting framework aims to establish a more comprehensive and structured overview of the nature, frequency, significance and impact of such incidents. This will be achieved by outlining the practical details and requirements governing the reporting obligations.

2. Scope

The CSSF Circular and CSSF Regulation are applicable to all entities under the supervision of the CSSF across several financial sector regulatory frameworks. These encompass credit institutions, professionals

of the financial sector, payment institutions, central securities depositories and entities subject to the NIS Law (**Supervised Entities**).

3. The CSSF Circular and CSSF FAQ

The CSSF Circular introduces four main changes to the existing incident reporting framework, enhancing both its scope and efficiency:

- **Expanded scope of incident to be notified:**
 - The reporting scope will be expanded as it is currently limited to fraud and incidents from external computer attacks (as per Circular CSSF 11/504). The new CSSF Circular mandates the notification of a wider range of ICT operational and security incidents.
- **Classification-based reporting system:**
 - Supervised Entities are now mandated to categorise ICT-related incidents based on the CSSF-specific criteria given in the Circular. Incidents classified as major or significant must be promptly notified to the CSSF no later than 24 hours after detection.

Detailed timelines and requirements for incident classification and initial information submission are clarified and explained in CSSF Circular Annex I and CSSF FAQs.

- **New incident reporting notification form:**
 - A structured ICT-related incident notification form is introduced to facilitate streamlined data acquisition. Supervised Entities must complete and submit this form for incidents classified as major or significant.

The details of the form are outlined in CSSF Circular Annex II and CSSF FAQs.

- **Consolidate incident notification requirements.**
 - A dedicated chapter is incorporated to align the CSSF Circular framework with incidents deemed as significant under the NIS Law. This consolidation aims to harmonise the application of new incident reporting forms and practical requirements.

Therefore, Supervised Entities categorised as OES or DSP need only to notify once for incidents classified both as significant under the NIS Law and a major ICT-related incident.

4. The CSSF Regulation

The CSSF Regulation issues a crucial framework to OES and DSP under the NIS Law as it provides for the integration of the CSSF Circular into incident classification and the mandatory notification requirements for major incidents under the NIS Law.

5. Next Steps

The CSSF Regulation on the application of the updated ICT-related incident reporting framework to the NIS Law will enter into force on 1 April 2024. The CSSF will confirm the classification of relevant Supervised Entities as OES or DSP by no later than 1 March 2024.

The CSSF Circular will enter into force on 1 April 2024 for a subset of Supervised Entities and will become universally applicable to all remaining Supervised Entities as from 1 June 2024.

How can we help?

For more information on ICT-related incident reporting framework, please contact our experts from the following teams:

- **If you are active in the banking and financial services sectors:** **Banking & Financial Services:** [Marc Mouton](#)
- **If you are active in investment management:** **Regulatory & Consulting:** [Yann Fihey](#), [Jasper Ronda](#) and [Bénédicte d'Allard](#)
- **For any advice on data protection:** **IP, Communication & Technology:** [Astrid Wagner](#), [Faustine Cachera](#), [Sophie Calmes](#) and [Julien Pétré](#)

[Read the CSSF Circular here_](#)

[Read the CSSF Regulation here_](#)

[Read the CSSF FAQ here_](#)

your contacts

Banking & Financial Services



MARC MOUTON

Partner

[Learn more_](#)

Regulatory & Consulting



YANN FIHEY

Partner

[Learn more_](#)



JASPER RONDA

Director

[Learn more_](#)

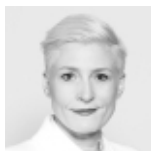


BÉNÉDICTE D'ALLARD

Senior Manager

[Learn more_](#)

IP, Communication & Technology



ASTRID WAGNER

Partner

[Learn more_](#)



FAUSTINE CACHERA

Senior Associate

[Learn more_](#)



SOPHIE CALMES
Senior Associate

[Learn more_](#)



JULIEN PÉTRÉ
Senior Associate

[Learn more_](#)



Arendt & Medernach SA
Registered with the Luxembourg Bar
RCS Luxembourg B 186371

[arendt.com](https://www.arendt.com)

41A avenue JF Kennedy
L-2082 Luxembourg
T +352 40 78 78 1

This publication is intended to provide information on recent developments and does not cover every aspect of the topics with which it deals. It was not designed to provide legal or other advice and it does not substitute for the consultation with legal counsel before any actual undertakings.



I am informed that I can object to the processing of my personal data for marketing purposes at any time either by e-mail addressed to unsubscribe@arendt.com or by clicking [here](#).

[Update e-mails preferences](#) | [Forward this e-mail](#)