

30 September 2026

Cyber Reporting Updates

This Circular is an update to Circular titled [Cyber Reporting Management System \(CRMS\)](#) published by the Authority in January 2025. As outlined by the latter circular, Authorised Persons within scope (see Article 2 of the DORA Regulation) of [Regulation \(EU\) 2022/2554](#) (the 'DORA Regulation'): 1) shall report Major ICT-Related Incidents, 2) are to notify Significant Cyber Threats on a voluntary basis, and 3) shall notify their voluntary participation in, or, as applicable, the cessation of their membership from, Information-Sharing Arrangements to the Authority.

The Authority is implementing a number of changes, including the introduction of Frequently Asked Questions (FAQs), updates to the CRMS within the Licence Holder (LH) Portal, and revisions to supporting documentation. These updates are intended to provide further guidance to Authorised Persons.

Frequently Asked Questions (FAQs)

The Authority released FAQs covering each of the three Cyber Reporting areas (Major ICT-Related Incidents, Significant Cyber Threats, and Information-Sharing Arrangements) under the DORA Regulation.

The three sets of FAQs are available on the MFSA website (our work > Supervisory ICT Risk and Cybersecurity), under the following tabs; 'Major ICT-Related Incident Reporting', 'Significant Cyber Threat Notification' and 'Information-Sharing Arrangement Notification'.

Cyber Reporting Management System ('CRMS')

The Authority will introduce a number of enhancements to the CRMS, as outlined below:

1. Introduction of a reclassification functionality. This functionality will enable incidents initially reported as major to be reclassified as non-major, in line with Article 5 of [Commission Implementing Regulation \(EU\) 2025/302](#). This functionality will replace the current withdrawal functionality, which will be removed;
2. Introduction of submission controls to prevent access to, and submission through, subsequent reporting panes where preceding reporting steps have not been completed;

3. Enhancements to user access management, including enabling users to view incidents submitted by, or on behalf of, the same Authorised Person;
4. General system enhancements and minor portal adjustments to improve usability.

Supporting Documentation

The Authority is making available, illustrative examples to support Authorised Persons with their Cyber Reporting. These illustrative examples are available on the MFSA website (under Our Work > Supervisory ICT Risk and Cybersecurity) and include a:

1. Major ICT-Related Incident Report;
2. Significant Cyber Threat Notification;
3. Information-Sharing Arrangement Notification.

Additionally, the Authority will update the following supporting documentation, which will also be made available on the MFSA website (under Our Work > Supervisory ICT Risk and Cybersecurity):

1. Major ICT-Related Incidents

- a. Major ICT-Related Incidents Reporting Process;
- b. User Guidelines for submitting Major ICT-Related Incident Reports to the Authority.

2. Significant Cyber Threats

- a. Significant Cyber Threats Notification Process;
- b. User Guidelines for submitting Significant Cyber Threat Notifications to the Authority.

3. Information Sharing Arrangements

- a. Information-Sharing Arrangement Notification Process;
- b. User Guidelines for submitting Information-Sharing Arrangement Notifications to the Authority.

The Malta Financial Services Authority expects all Authorised Persons to ensure that they have the necessary access to the CRMS Project within the LH Portal.

Failure to submit the required notifications and reports under the DORA cyber reporting framework within the applicable timelines may result in regulatory action by the Authority by virtue of [S.L. 330.20](#) and the [MFSA Act](#).

Authorised Persons may request further information by sending an email to the Major Incident Reporting Team at mirt@mfsa.mt.