

Notice No: FSRA/13/2025

By email

04 February 2025

To: Senior Executive Officers (SEO) and Principal Representatives (PR) of Authorised Persons
Cc: Compliance Officers

Dear SEO/ RP,

Information Technology ("IT") and Cyber Incident Reporting.

The FSRA is establishing a procedure to facilitate standardised reporting of IT and cyber incidents using a common reporting template.

What constitutes a reportable incident

FSRA's Authorised Persons are to notify the FSRA immediately of any incidents having an impact that require notification to the FSRA under GEN 8.10.6.

In particular to IT and cyber incidents, Authorised Persons are to report to the FSRA when it encounters an **IT failure** (e.g., unscheduled disruptions to online services and/or business operations, etc.) or falls victim to a **cyber-attack** (e.g., illicit intrusions into computer networks, such as hacking, disruption or downgrading of computer functionality and network space, such as malware and denial of service attacks, etc.).

Expected timeline for reporting

The FSRA expectation of an immediate notification (GEN 8.10) is to happen as soon as possible upon discovery of the incident.

Notification mechanism by Authorised Persons to the FSRA

The FSRA is adopting an incremental approach to reporting which balances the FSRA's requirement for timely reporting, whilst also recognizing the Authorised Person's need to contain the incident and restore business operations.

Authorised Persons are to submit an initial report to the FSRA using the template under Annex A – "Initial IT & Cyber Incident Report Template" and email it to the FSRA Incident Reporting mailbox - incidents.fsra@adgm.com. Authorised Persons are to copy their FSRA lead supervisor or pooled supervision on their email.

Subsequently, Authorised Persons are to complete and submit progressive reports with the most up-

to-date information using the template under Annex B – “IT & Cyber Incident Progressive Report Template”. The FSRA supervisor will determine the frequency of updates on a case-by-case basis depending on the severity and complexity of the incident.

Enclosed are the templates for Cyber Incident Initial and Progressive Reports:

- Annex A: IT & Cyber Incident Initial Report Template
- Annex B: IT & Cyber Incident Progressive Report Template

Both templates are available on the following webpages:

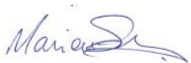
- FCCP - [Financial and Cyber Crime Prevention Forms](#)
- IT Risk Management - [IT Risk Management \(adgm.com\)](#)

Authorised Persons are also reminded of reporting obligations to other regulatory bodies (data protection breach or suspicious activity/transaction report) and law enforcement agencies where appropriate.

This Notice sets out interim supervisory expectations for Authorised Persons on the reporting of IT and cyber incidents. As communicated in the [2023 Discussion Paper on IT Risk Management](#), the FSRA is considering specific rules on the reporting of IT and cyber-related incidents. The FSRA is deliberating on the feedback received and will issue a consultation paper proposing such rules in due course.

For any clarifications, Authorised Persons are to reach out to their lead supervisor or send an email to the Pooled Supervision team (pooledsupervision@adgm.com), as appropriate.

Sincerely,



Mary Anne Scicluna

Senior Executive Director - Supervision
Financial Services Regulatory Authority