MFSA MALTA FINANCIAL SERVICES AUTHORITY

Feedback Document

Feedback Statement to the Consultation on the Reporting of Major ICT-Related Incidents

Ref: 05-2022

Date: 13 October 2022

Contents

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155

communications@mfsa.mt
www.mfsa.mt

On 12 July 2022, the Malta Financial Services Authority ('MFSA', 'the Authority') published a Consultation Document on the Reporting of Major ICT-Related Incidents ('the Consultation Document').

During the consultation period, expiring on 5 August 2022, the MFSA received various feedback from the industry for the Authority's consideration. The MFSA reviewed the feedback received. This document is the outcome of the feedback review process, the conclusions of which, can be found in Section 2.

This Feedback Statement is being released alongside a Circular, expecting eligible Authorised Persons to report Major ICT-Related Incidents to the Authority in a three-tier approach, as of the date of the Circular (13 October 2022). The Circular, in turn, refers to the release of the following documents available on the MFSA website (*Our Work > Supervisory ICT Risk and Cybersecurity*):

1. A Major ICT-Related Incident Reporting Process ('the Process Document');

2. Templates for Initial, Intermediate and Final Major ICT-Related Incident Reporting ('the Templates', 'the provided Templates');

3. User Guidelines for submitting Major ICT-Related Incident Reports to the Authority ('the User Guidelines').

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

1. Introduction

On 12 July 2022, the Authority published a Consultation Document on the Reporting of Major ICT-Related Incidents with a consultation period expiring on 5 August 2022. The MFSA received various feedback from the industry for the Authority's consideration. The feedback has been categorised as follows:

1. Eligibility and Exceptions;
2. Major ICT-Related Incident Thresholds;
3. Initial Report;
4. Intermediate Report;
5. Final Report;
6. General Feedback.

The MFSA reviewed the feedback received and the conclusions can be found in Section 2. Each feedback category is covered in a dedicated sub-section (2.1 to 2.6). For each feedback category, a summary of the feedback received, as well as the position taken by the Authority on the feedback, is provided. The position taken by the Authority includes, where applicable, whether the feedback resulted into any amendment/s to the material published for consultation.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2. Feedback Statement

2.1. Eligibility and Exceptions

Within the Consultation Document, the Authority stated that it "*will expect the reporting of ICT-related incidents, whether of an operational or security nature, that reach the specified thresholds in Annex 1 – and therefore classify as 'major'*". It also stated that "this will apply to all eligible Authorised Persons" and included an "Exceptions" section stating:

"*Credit and financial institutions are currently required to follow the EBA Revised Guidelines (EBA/GL/2021/03) on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2) and to report major incidents using the forms and methodologies stipulated within these Guidelines to the Central Bank of Malta under the Banking Act (Chapter 371 of the Laws of Malta) and the Financial Institutions Act (Chapter 376 of the Laws of Malta). Significant credit institutions are required to – in addition – report significant cyber incidents to the European Central Bank (ECB) via their allocated Joint Supervisory Team, using an agreed process and template established by the ECB. In view of this, the process being proposed within this document will not apply to credit and financial institutions.*"

Feedback Received

One respondent enquired whether this means that financial institutions will not fall in scope and shall keep reporting any major incidents to the Central Bank of Malta. The same respondent enquired whether a case may still arise where reporting will need to be submitted to both authorities.

MFSA Position

Financial Institutions (payment institutions, electronic money institutions and account information service providers) shall continue reporting major operational or security incidents to the Central Bank of Malta using the forms and methodologies stipulated within the EBA Revised Guidelines (EBA/GL/2021/03) on Major Incident Reporting under Directive (EU) 2015/2366 (PSD2). The Financial Institutions Act (and the Banking Act) states that "*upon receipt of such notification, the Central Bank shall promptly notify the competent authority*" and therefore an arrangement is in place whereby the Central Bank of Malta makes available to the Authority the incidents reported to it. This means that there is no need for financial (or credit) institutions to submit incident reports to both the Central Bank of Malta and the MFSA.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2.2. Major ICT-Related Incident Thresholds

Annex 1 of the Consultation Document included a thresholds matrix. This matrix is to be used by Authorised Persons to determine whether an ICT-Related Incident (operational or security) meets the thresholds within, therefore classifying as 'major' and making it reportable to the Authority. The final and official version of this thresholds matrix is annexed (Annex A) to the Process Document.

One respondent made a number of queries related to various criteria within the thresholds matrix as follows.

Transactions Affected (where applicable)

Feedback Received

Could the Authority clarify in more detail what is understood by transactions? Is this specifically referring to transactions typically with 'retail' clients and/or suppliers (i.e., high frequency low value transactions) or is it to be interpreted in a wider context including transactions with other Authorised Persons (i.e., low frequency high value transactions)?

MFSA Position

The *Explainers* within the Templates state that Authorised Persons should interpret the regular level of transactions to be the daily annual average of domestic and cross-border transactions carried out with the same services that have been affected by the incident and do not specifically exclude any of the scenarios provided by the respondent.

Users Affected

Feedback Received

Would the term 'users' refer to clients (e.g. 'retail' clients), employees or both?

MFSA Position

'User' refers to the recipient of the service/s provided by an Authorised Person affected by the incident – a customer (either domestic or from abroad, consumers or corporates). The *Explainers* within the Templates provide further information/details.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Service Downtime

Feedback Received

Could the Authority please provide more clarity as to what is meant by "service downtime"? Is it to be interpreted as a complete halt of the company's offering? Or is to be interpreted as a system-by-system "service downtime" (e.g. Microsoft Exchange Online (e.g. Office 365) downtime) which would be disruptive but not necessarily fully halt the operations of the company?

MFSA Position

'Service' refers to a financial service provided by an Authorised Person. A service downtime of more than two hours complemented by another two (2) Lower Impact Level thresholds would render an incident as 'major' (thus reportable) whether it is one service provided by the Authorised Person, more than one service, or all the services.

Breach of Security of Network and Information Systems

Feedback Received

Our view would be to move away from 'any' breach and to move to a more risk-driven criteria limiting it to breaches of personal, financial or confidential data.

MFSA Position

Breach of Security of Network and Information Systems shall be revised to "*Whether any malicious action has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of services*". The *Annex* to *Explainers* within the Templates provide further information on malicious action. A **Breach of Security of Network and Information Systems** is a Higher Impact Level Threshold and hence a Major ICT-Related Incident (and reportable). In times of heightened cyber-threat it is expected that any and all such breaches are reported to the Authority as was the case with Circular titled Cybersecurity – Threat Mitigation (now being superseded). This may be revised in the future.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Economic Impact

Feedback Received

Is it possible for the Authority to provide more detail on its expectations of the components making up the calculation of 'Economic Impact'? In the unfortunate event of an incident, our expectation is that it would be very difficult for undertakings to immediately assess the economic impact in the early stages of the incident.

MFSA Position

Information related to this is provided within the *Explainers* sheet of the Templates. Please note that details pertaining to the quantum of the **Economic Impact** would not be expected to be provided within the *Initial Report* but later on within the *Intermediate Report/s*.

High Level of Internal Escalation

Feedback Received

Could the Authority please clarify what the difference is between the lower impact threshold and the higher impact level criteria? Is for example the triggering of the 'Business Continuity Plan' of an undertaking the distinguishing threshold between the two levels?

MFSA Position

Authorised Persons are to classify as major those operational or security incidents that fulfil one or more criteria at the 'higher impact level'; or three or more criteria at the 'lower impact level'.

One of the criteria is **High Level of Internal Escalation**, whereby in order for it to reach the lower impact level threshold, the Management Body (as defined by the MFSA Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements) has been or will likely be informed. To reach the higher impact level threshold, the Authorised Person would need to go into crisis mode (or equivalent). ISO 22300 defines a crisis as an "unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property or the environment". The context surrounding the triggering of a Business Continuity Plan is normally a severe business disruption. While this may qualify as a crisis for some organisations, others may then pre-define different escalation points for transitioning into a crisis.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Geographical Spread

Feedback Received

Could the Authority provide more clarity on the interpretation of geographical spread? Our organisation is a fully licensed financial entity in Malta with no other presence (such as branches or subsidiaries) in the European Union, although it does provide its services to international clients.

MFSA Position

Geographical Spread is linked to **Country/Countries Affected by the Incident** within the *Initial Report* and explained within the Templates' *Explainers*. It is related to presence rather than clients.

Other Authorised Persons or Relevant Infrastructures Potentially Affected

Feedback Received

Could the Authority please clarify what is meant by "other authorised persons" in our case? In the event of a major incident specifically at our organisation, our organisation could only identify whether or not such an incident has repercussions on any of its own clients (which are also authorised persons, not necessarily only in Malta but also in other jurisdictions) – is this the correct interpretation? Moreover, what is meant by "relevant infrastructures potentially affected"?

MFSA Position

This refers to the systemic implications of the incident – its potential to spill over beyond the initially affected Authorised Person to other financial entities or, for instance, financial market infrastructures. Further information is provided within the Templates' *Explainers*.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

2.3. Initial Report

Another respondent provided feedback on the *Initial Report*.

Feedback Received

The Consultation proposes for an Initial Report to be sent "within 4 hours of an incident being classified as major. Such classification is expected to take place within twenty-four (24) hours after an incident has been detected".

While we are cognisant of the Authority's current reporting timeframes for material cyber incidents, we would outline that it [might] not always be possible to adequately classify an incident as being major or not (using the criteria laid out by the Consultation) within the first 24 hours of an incident. We would recommend aligning reporting more closely to GDPR reporting timescales and for reporting to the regulator and for a classification of incidents as major to be made within seventy-two (72) hours rather than twenty-four (24) hours and an initial report to be made to the regulator within eight (8) hours of that classification being made.

MFSA Position

While the Authority understands the respondent's concern, a Major ICT-Related Incident may have – either singularly or in combination with other incidents – systemic implications which is why the Authority would need to have that information as quickly as possible. If in doubt, an Authorised Person may consult the Authority. If it transpires that a reported incident is afterwards determined not to qualify as 'major', the Authorised Person will have the facility to withdraw its submission.

2.4. Intermediate Report

One respondent provided feedback on the *Intermediate Report*.

Feedback Received

The Consultation proposes that an Intermediate Report is expected to be sent "within three (3) working days from the submission [of] the Initial Report". We would propose that in order to effectively investigate and recover from an incident and a meaningful update to be given, an intermediate report is made within five (5) working days of the initial report having been made. Further intermediate reports can be made at regular intervals following the initial five (5) day report.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

MFSA Position

Please note that an Authorised Person may send multiple *Intermediate Reports* if the information is not completely available at the point in time in which the Authorised Person is submitting the first *Intermediate Report*. An Authorised Person is expected to send an updated *Intermediate Report* after every three (3) working days until the incident is resolved (B1.9 within the template).

2.5. Final Report

A respondent provided feedback on the *Final Report*.

Feedback Received

The Consultation proposes that a Final Report is required "within 20 working days after business is deemed as being back to normal". However, the 'Major ICT-Related Incident Report instructions' that go along with the Consultation say (on page 1) that a final report is to be submitted "within 20 working days from the submission of the Intermediate Report". We assume that the 20 working days refers to once business is deemed as being back to normal and NOT from the date of submission of the Intermediate Report. We would appreciate the Authority's clarity on this matter. Incidents can obviously vary widely in the time taken to recover and may exceed the 20 working day limit to be fully back to normal for a major incident.

MFSA Position

The twenty (20) working days should start counting after business is deemed as being back to normal. This will be corrected as necessary.

2.6. General Feedback

Other respondents provided an element of other, more general feedback.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt

Feedback Received

Our financial entity is a subsidiary of a group. The ICT services of the company are outsourced to the group. On this basis, it is still our understanding that, the assessment of whether a local incident or the impact of a group-wide incident is to be classified as major or not, rests within the local senior management of financial entity [licensed in Malta].

MFSA Position

The understanding of the respective respondent is correct.

Feedback Received

In the early stages of identifying an incident, there are a number of responsibilities that we have as a business, including: mobilising our incident response team / possibly also our Business Continuity process; liaising with our cyber security partners to identify the scale and severity of an incident; contacting our cyber security insurance provider to agree steps to take with their support; contracting third parties within our supply chain; reporting to our board and executive governance; communicating with our clients and staff as well as with data supervisory authorities and regulatory bodies. With these responsibilities in mind, we will need time to focus on identifying and classifying the scope and severity of an incident and classification may change over time.

MFSA Position

While the Authority appreciates the respondent's concern, please refer to the feedback provided earlier on, particularly in sub-section 2.3.

2.7. Other Feedback

Authorised Persons may request further feedback or clarifications by sending an email to the Supervisory ICT Risk and Cybersecurity function within the MFSA on mirt@mfsa.mt.

Triq l-Imdina, Zone 1 Central Business District, Birkirkara CBD 1010
+356 2144 1155
communications@mfsa.mt
www.mfsa.mt