MFSA MALTA FINANCIAL SERVICES AUTHORITY

Major ICT-Related Incident Reporting Process

CONTENTS

Introduction 4
Scope and Applicability 5
Definitions 6
The Process 9
Annex A – Major ICT-Related Incident Thresholds 10
Annex B – Exceptions 12

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	13 October 2022	First release

Introduction

In line with paragraph 4.8.11 of the Guidance Document, and in view of the outstanding times of heightened cyber threats, and in preparation for the entry into force of the Digital Operational Resilience Act (DORA), the Malta Financial Services Authority ('the Authority') is herewith establishing an updated Major ICT-Related Incident Reporting Process as communicated on 13 October 2022 through Circular titled Reporting of Major ICT-Related Incidents.

In establishing this process, the Authority has taken into consideration the challenges with the preceding incident reporting process (an Authorised Person may not have all the incident details in place at the time of initial reporting, for instance), the course that DORA is expected to be taking, established incident reporting guidelines[1] and the public consultation process that has taken place. This process will eventually have to be aligned with DORA when it enters into force.

This process is being released alongside the following material, available on the MFSA website (Our Work > Supervisory ICT Risk and Cybersecurity):

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

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

[1] EBA Revised Guidelines on major incidents reporting under PSD2 (EBA/GL/2021/03)

Scope and Applicability

This process applies to **all Authorised Persons** except for Authorised Persons referred to in *Annex B*, which at the time of writing are required to follow alternative Major ICT-Related Incident reporting mechanisms.

This process and its accompanying material apply from the **date of publication** of Circular titled Reporting of Major ICT-Related Incidents and this document, i.e. 13 October 2022.

Definitions

Authenticity	Property that an entity is what it claims to be (ISO/IEC 27000:2017).
Authorised Person	Any person that is licensed, registered or otherwise authorised by the Malta Financial Services Authority. The term 'Licence Holder' is also used by the Authority.
Availability	Property of being accessible and usable on demand by an authorised entity (FCB Cyber Lexicon, 2018).
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems (FCB Cyber Lexicon, 2018).
DORA	Digital Operational Resilience Act (not in force at the time of writing).
Event	Any observable occurrence in an ICT. Events sometimes provide indication that an Incident is occurring (adapted from the FCB Cyber Lexicon, 2018). The responsibility of the identification of Incidents from Events lies with the Authorised Person.
ICT-Related Incident	A single event or a series of linked events unplanned by the Authorised Person that compromises or will likely compromise the security of the network and information systems, and has an adverse impact on the availability, authenticity, integrity, or confidentiality of data or of the services provided by the Authorised Person (adapted from the latest available text of DORA and the EBA Guidelines on Major Incident Reporting under the PSD2 - EBA/GL/2021/03).
Information and Communication Technology (ICT)	ICT encompasses all technologies for the capture, storage, retrieval, processing, display, representation,

	organization, management, security, transfer, and interchange of data and information (NIST Glossary accessed before the date of this document).
Integrity	Property of accuracy and completeness (FCB Cyber Lexicon, 2018).
Major ICT-Related Incident	An ICT-Related Incident that has a high adverse impact on the network and information systems that support critical functions of the Authorised Person (adapted from the latest available text of DORA). A Major ICT-Related Incident meets the thresholds for the determination of Major ICT-Related Incidents in *Annex A*.
MFSA	Malta Financial Services Authority (the "Authority").
Operational Incident	Incident stemming from inadequate or failed processes, people and systems or events of force majeure that affect the integrity, availability, confidentiality and/or authenticity of a financial service/s (adapted from the Final Report on the Revised Guidelines on Major Incident Reporting under PSD2 – EBA/GL/2021/03).
Resolution	Actions taken to recover from an incident and restore any capabilities or services that were impaired due to an incident (adapted from the definition of "Recovery" within the FCB Cyber Lexicon, 2018). The responsibility of the resolution of Incidents lies with the Authorised Person.
Response	Actions taken to mitigate or resolve a Major ICT-Related Incident, including those taken to protect and restore the normal operational conditions of an ICT and the information stored in it (adapted from ISO/IEC 27035-1:2016).

	The responsibility of the response to Incidents lies with the Authorised Person.
Security Incident	Unauthorised access, use, disclosure, disruption, modification or destruction of the Authorised Person's assets that affects the integrity, availability, confidentiality and/or authenticity of a financial service/s. This may happen, among other things, when the Authorised Person experiences a breach of security of network or information systems (adapted from the Final Report on the Revised Guidelines on Major Incident Reporting under PSD2 – EBA/GL/2021/03).
SIRC	The Supervisory ICT Risk and Cybersecurity Function within the Malta Financial Services Authority.

The Process

The Authority expects Authorised Persons to report ICT-Related Incidents, whether of an operational or security nature, that reach the specified thresholds in *Annex A,* and therefore classifying as 'Major'.

Reporting is expected to occur in a three-tier approach: an Initial Report; an Intermediate Report; and a Final Report using the provided Templates, and by following the User Guidelines published alongside this Process.

Authorised Persons are expected to submit:

1. An *Initial Report* within **four (4) hours** after an incident has been classified as major. Such classification is expected to take place within **twenty-four (24) hours** after an incident has been detected.

2. An *Intermediate Report* within **three (3) working days** from the submission of the *Initial Report*, irrespective of whether the incident has been resolved. An Authorised Person may provide one or more Intermediate Report/s at different stages within the resolution process.

3. A *Final Report* within **twenty (20) working** days after business is deemed back to normal.

This Process does not replace or supersede any legal obligation by Authorised Persons to report incidents to other competent authorities, inter alia:

- the competent authority under Directive (EU) 2016/1148 (NIS Directive), transposed into Legal Notice 216 of 2018 of the Laws of Malta;

- the competent authority under Regulation (EU) 2016/679 (GDPR).

Authorised Persons may request further information or assistance by calling the SIRC function on +356 2548 5260 or by sending an email to mirt@mfsa.mt.

Annex A – Major ICT-Related Incident Thresholds

Criteria	Threshold for Lower Impact Level	Threshold for Higher Impact Level
TRANSACTI-ONS AFFECTED (WHERE APPLICABLE)	More than (>) **10%** of the regular level/number of transactions **AND** a duration of the incident of more (>) than **one (1) hour *** **OR** A total value of more than (>) **EUR 500,000 AND** a duration of the incident of more (>) than **one (1) hour ***	More than (>) **25%** of the regular level/number of transactions **OR** A total value of more than (>) **EUR 15,000,000**
USERS AFFECTED	More than (>) **10% AND** a duration of the incident of more (>) than **one (1) hour *** **OR** More than (>) **5,000 AND** a duration of the incident of more (>) than **one (1) hour ***	More than (>) **25%** **OR** More than (>) **50,000**
SERVICE DOWNTIME	More than (>) **Two (2) hours**	Not applicable
BREACH OF SECURITY OF NETWORK OR INFORMATION SYSTEMS	Not applicable	Whether any malicious action (see the Major ICT-Related Incident Reporting Templates' Explainers and their Annexes) has compromised the availability, authenticity, integrity or confidentiality of network or information systems (including data) related to the provision of the services provided by the Authorised Person
ECONOMIC IMPACT	Not applicable	More than (>) the maximum of (**0.1% Tier-1 Capital ****, **EUR 200,000**) **OR** More than (>) **EUR 5,000,000**

HIGH LEVEL OF INTERNAL ESCALATION	Yes	Yes, and a crisis mode (or equivalent) is likely to be triggered
GEOGRAPHI-CAL SPREAD	Up to **two (2) Member States**	More than (>) **two (2) Member States**
OTHER AUTHORISED PERSONS OR RELEVANT INFRASTRUC-TURES POTENTIALLY AFFECTED	Yes	Not applicable
REPUTATION-AL IMPACT	Yes	Not applicable

***** The threshold concerning the duration of the incident for a period longer than one hour applies only to operational incidents that affect the ability of the Authorised Person to provide the service.

****** Tier-1 capital as defined in Article 25 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

Authorised Persons are to classify as major those operational or security incidents that fulfil:

1. one or more criteria at the 'higher impact level'; or

2. three or more criteria at the 'lower impact level.

Annex B – Exceptions

Credit and financial institutions (payment institutions, electronic money institutions and account information service providers) 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 reporting templates 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 Document will not apply to credit and financial institutions.

Malta Financial Services Authority

Triq L-Imdina, Zone 1

Central Business District, Birkirkara, CBD 1010, Malta

communications@mfsa.mt

www.mfsa.mt