MFSA MALTA FINANCIAL SERVICES AUTHORITY

THE NATURE AND ART OF FINANCIAL SUPERVISION

VOLUME III

ICT RISK AND CYBERSECURITY

28 January 2021

Contents

Table of Abbreviations

AIFMD	Alternative Investment Fund Managers Directive (and amending Directives)
BIA	Business Impact Analysis
CRD	Capital Requirements Directive
CRR	Capital Requirements Regulation
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
EMIR	European Market Infrastructure Regulation
ESA	European Supervisory Authority
ESMA	European Securities and Markets Authority
EU	European Union
ICT	Information and Communications Technology
IORP	Institutions for Occupational Retirement Provision
MiFID	Markets in Financial Instruments Directive
MFSA	Malta Financial Services Authority
NIS	Network and Information Systems
OES	Operators of Essential Services
PSD	Payment Services Directive
SIRC	Supervisory ICT Risk and Cybersecurity (function)
TPP	Third Party Provider
UCITS	Undertakings for the Collective Investment in Transferable Securities

Introduction

Information and Communications Technology (ICT) has become a critical dependency for organisations and people alike. Inevitably, we are seeing an increased interest in ICT risk and Cybersecurity by standard setters and policymakers worldwide. This is inevitably also true for the financial services sector.

ICT risk and Cybersecurity continue to present significant challenges to, and potential severe consequences on, the resilience, performance and stability of financial systems and economies. In its Threat Landscape 2020 publication Main incidents in the EU and worldwide, the European Union Agency for Cybersecurity ('ENISA') listed the financial sector as one of the top five most targeted sectors claiming that "*the number of incidents with financial organisations and not necessarily banks, increased substantially during the reporting period*" (the reporting period being January 2019 to April 2020). We are also seeing an increased relevance of third-party dependencies and risks associated with ICT outsourcing as part of ICT risk management.

The Malta Financial Services Authority ('MFSA' or 'the Authority') through its Vision 2021 and Strategic Plan 2019-2021 placed substantial importance on ICT risk and Cybersecurity, highlighting a number of "*measures and initiatives planned to ensure that regulated firms have a cybersecurity programme in place, which is designed to enhance their resilience to cyber-attacks and mitigate the risks associated with such threats, such as disruption of service, data breaches and the loss of data, amongst others*", classifying Cybersecurity and resilience as a "*Cross-sector Priority*". ICT Risk and Cybersecurity remains a cross-sectoral priority within the MFSA Supervision Priorities 2021.

The establishment of the Supervisory ICT Risk and Cybersecurity function (the 'SIRC' function) as a cross-sectoral supervisory function within the MFSA Supervision directorate in February 2020 was a critical milestone for the Authority. The function works closely with the other supervisory functions and is responsible for the supervision of licence holders in the areas of ICT risk and Cybersecurity and the management of risks associated with ICT outsourcing, collectively the area of Digital Operational Resilience.

In 2020, the SIRC function conducted a number of supervisory interactions with licence holders. This publication provides general feedback to the industry on the Authority's findings and prevailing risks and puts forward recommendations. This document also describes the MFSA's supervisory focus for 2021 in the areas of ICT risk and Cybersecurity as well as ICT outsourcing.

Background on ICT Risk and Cybersecurity Supervision

Supervisory Approach

The SIRC function, a cross-sectoral supervisory function, works closely with the Authority's other supervisory functions to supervise authorised persons from different sectors in the areas of ICT risk and Cybersecurity and the management of risks associated with ICT outsourcing. This section provides an overview of the supervisory approach taken by the SIRC function.

The obligations and expectations on providers of financial services within the European Union (EU) in the areas of ICT risk and Cybersecurity are fragmented, consisting of sets of legal requirements (e.g. requirements within the sector-specific legislative instruments) and soft law measures (typically guidelines) developed at different times. They are not specifically focused on ICT risk and Cybersecurity and are largely oriented towards the respective sector falling within scope of the particular law. Such provisions are typically found in the following legislative instruments, albeit with varying levels of detail:

- Payment Services Directive ('PSD');
- Capital Requirements Directive / Capital Requirements Regulation; ('CRD/CRR')
- Markets in Financial Instruments Directive ('MiFID');
- European Market Infrastructures Regulation ('EMIR');
- Solvency II Directive;
- Directive on undertakings for collective investment in transferable securities (UCITS) / Alternative Investment Fund Managers Directive (and amending Directives) ('AIFMD');
- Institutions for Occupational Retirement Provision (IORP) Directive.

At the national level, where applicable, the above legislative instruments have been transposed to the relevant Acts Regulations, Subsidiary Legislation and/or rules.

On a more general level, the Network and Information Systems (NIS) Directive[1] (transposed by virtue of Legal Notice ('LN'). 216 of 2018 on "Measures For High Common Level of Security of Network and Information Systems Order, 2018") which is focused on measures for a high common level of security, covers Operators of Essential Services (OES) in different industries e.g. Energy and Transport, and, from a financial services perspective, it covers certain Credit Institutions, Operators of Trading Venues and Central Counterparties.[2]

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[2] The Single Point of Contact and National Competent Authority for the NIS Directive in Malta is the Critical Information Infrastructure Protection Unit

Furthermore, European Supervisory Authorities (ESAs) have been issuing numerous Guidelines on the subject under their respective legislative regimes, notably the:

- EBA Guidelines on ICT and Security Risk Management (EBA/GL/2019/04);
- EBA Guidelines on Outsourcing Arrangements (EBA/GL/2019/02);
- EIOPA Guidelines on ICT Security and Governance (EIOPA-BoS-20/600);
- EIOPA Guidelines on Outsourcing to Cloud Service Providers (EIOPA-BoS-20-002);
- ESMA Guidelines on Outsourcing to Cloud Service Providers (ESMA50-157-2403).

Publication of Guidance Document

The SIRC function has, following a comprehensive consultation process, recently published a principle-based cross-sectoral Guidance on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements (the 'Guidance Document'). This is without prejudice to all applicable Acts, Regulations, rules, or any other sector specific guidelines. It sets out the MFSA's expectations on Technology Arrangements, ICT and Security Risk Management, and Outsourcing Arrangements for:

- Credit Institutions;
- Financial Institutions;
- Insurance Undertakings and Reinsurance Undertakings;
- Insurance and Reinsurance Undertakings which are part of a group in line with Article 212 of Directive 2009/138/EC;
- Captive Insurance Undertakings and Captive Reinsurance Undertakings;
- Insurance Intermediaries;
- Ancillary Insurance Intermediaries;
- Retirement Pension Schemes (Occupational Retirement Schemes and Personal Retirement Schemes);
- Pension Service Providers (Retirement Scheme Administrator, Investment Manager and Custodian);
- Investment Services Licence Holders:
    - Investment Firms - Categories 1 to 3;
    - Custodians of Collective Investment Schemes – Categories 4a and 4b;
    - Fund Managers: De-minimis AIFMs, full-scope AIFMs and UCITS Management Companies;
    - Self-managed Collective Investment Schemes (including Professional Investment Funds, UCITS, and Alternative Investor Funds);
    - Recognised Fund Administrators;
- Trading Venues;
- Central Securities Depositories;
- Trustees and other Fiduciaries;
- Company Service Providers;
- Virtual Financial Assets.

Licence holders should approach the Guidance Document with a view to align with the Authority's expectations therein.

Supporting Authorisations

The authorisation stage is crucial in the supervisory lifecycle. Applications for authorisation are assessed by the respective authorisation teams within the supervisory functions to ensure that criteria detailed under the respective financial services legislation are satisfied. The SIRC function provides support to supervisory functions in reviewing applications from an ICT risk and Cybersecurity perspective.

Onsite Inspections

As part of its supervisory work, the MFSA conducts onsite inspections at the offices of licence holders. Due to the COVID-19 pandemic, these were mainly carried out remotely through tele-conferencing throughout 2020. The SIRC function supports onsite inspections carried out by other supervisory functions and also conducts its own thematic onsite inspections focused on ICT risk and Cybersecurity. As a supervisory function, SIRC focuses on the licence holders' compliance with legal and regulatory requirements emanating from the relevant EU and national legislation and regulation and also monitors adherence to best practices within the industry.

Offsite Supervision

From time to time, the SIRC function may conduct its own thematic reviews as part of its offsite supervision or support offsite supervision undertaken by other functions. This is carried out in the form of self-assessments and/or questionnaires circulated to the relevant licence holders.

Incident Reporting

Without prejudice to any incident reporting obligations within the relevant Acts, Regulations, rules, or sector-specific guidelines, Licence Holders are expected to report major ICT-related incidents to the Authority.

National and International Cooperation

The SIRC function participates and contributes to local and foreign working groups, particularly, the National Cybersecurity Strategy Steering Committee, expert groups organised by the European Central Bank (ECB) and other working groups organised by the ESAs.

The SIRC function, together with other organisations, is also working with the Ministry for Finance and Employment in working parties and other activities related to the legislative proposals on digital operational resilience issued by the European Commission on 24 September 2020.

Future Developments within the Regulatory Framework

Legislative proposals on digital operational resilience

On 8 March 2018, the European Commission issued a FinTech action plan for a more competitive and innovative European financial sector. "Enhancing security and resilience of the financial sector" was outlined as one of the initiatives within this action plan.

This initiative, *inter alia*, included a public-private workshop to explore and assess barriers limiting information sharing on cyber threats between financial market participants and to identify potential solutions while ensuring data protection standards are met. It also included an exercise by the ESAs to map the existing supervisory practices across financial sectors around ICT security and governance requirements, and where appropriate: (a) consider issuing guidelines aimed at supervisory convergence and enforcement of ICT risk management and mitigation requirements in the EU financial sector; and, (b) provide the European Commission with technical advice on the need for legislative improvements. It also included an evaluation of the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.

On 10 April 2019, the ESAs published two 'Joint Advice' to the European Commission in response to the FinTech action plan: one on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector; and another on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector.

On 19 December 2019, the European Commission published a consultation document *Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure* inviting feedback by 19 March 2020 as follows:

1. Part 1 – Stakeholder Identification, Transparency and Confidentiality;

2. Part 2 – Building Blocks for a Potential EU Initiative: Main Issues:
    a. Targeted improvements of ICT and security risk management requirements;
    b. Harmonisation of ICT incidents reporting;
    c. Development of a digital operational resilience testing framework;
    d. Better oversight of certain critical ICT third-party providers;
    e. To promote (i) effective information sharing (ii) better cooperation.

Following this consultation, on 24 September 2020, the European Commission issued a Digital Finance Package, which includes a Digital Finance Strategy; a Retail Payments Strategy; legislative proposals on crypto-assets, and legislative proposals on digital operational resilience.

The legislative proposals on digital operational resilience consist of: a proposal for a Regulation on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, and (EU) No 909/2014; and a proposal for a Directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341.

The Regulation proposal consists of the following main aspects:

1. ICT risk management - all financial institutions would be required to have in place an ICT risk management framework developed on key common principles that are risk-based and allow for a proportionate application;

2. Incident reporting - communication on ICT-related incidents would be enhanced, extended to those subsectors currently not subject to such rules and normalised;

3. Digital operational resilience testing - a proportionate and harmonised resilience testing framework;

4. Managing of ICT third party risk - enhanced monitoring of risks stemming from ICT Third Party Providers (TPPs) built upon (a) heightened outsourcing rules; and (b) oversight tools for supervisors in relation to ICT activities of TPPs;

5. Information sharing arrangements - a voluntary scheme encouraging communication on threats.

It should be noted that the Regulation on digital operational resilience for the financial sector and amending Regulations, also known as DORA, is still in the proposal stage as at the time of writing.

Supervisory Engagement, Findings, Risks, and Recommendations

During 2020, the SIRC function conducted a number of supervisory interactions and desk-based exercises. This section provides general feedback to the industry on findings and prevailing risks, and also puts forward recommendations.

ICT Governance and Strategy

Management bodies should ensure that financial entities have adequate internal governance and an internal control framework in place for ICT and cybersecurity risks. They should ensure that the ICT strategy is aligned with the overall business strategy and that the ICT budget is adequate and appropriate.

The MFSA observed instances where: [i] boards were not adequately involved in ICT matters; [ii] the ICT strategy did not adequately support the overall business strategy; [iii] ICT budgets did not adequately reflect increased and forthcoming operational requirements (e.g. ESA Guidelines in the pipeline) and needs; and [iv] boards did not ensure that their organisations have in place the necessary ICT policies and procedures.

ICT and Security Risk Management

Financial entities should have an adequate ICT and security risk management framework in place which is documented and continuously improved.

The MFSA observed instances where: [i] boards were not adequately involved in, and lacked the necessary oversight on, ICT and cybersecurity risk; [ii] ICT and cybersecurity risk was not integrated within the overall risk management framework; [iii] ICT and cybersecurity risk was not given priority; [iv] ICT and cybersecurity risk roles and responsibilities were not clearly defined and assigned; and [v] the ICT and cybersecurity risks were not being adequately managed. The Authority also observed instances whereby there was no sufficient segregation of functions in accordance with the three lines of defence model to adequately manage conflicts of interest – including cases where the control function responsible for risk management was also responsible for ICT operations. In addition, at times, the Authority also noted that the Internal Audit function was not complemented by people with the necessary skills and qualifications to carry out ICT Audits and/or did not include ICT audits within their audit plans.

ICT Outsourcing Arrangements

Licence holders should ensure that they are effectively managing risks associated with ICT outsourcing. Financial entities remain fully responsible and accountable for complying with all of their regulatory obligations and for ensuring that they continue to meet on an ongoing basis the conditions with which they must comply to remain authorised.

The MFSA observed instances of significant overreliance on outsourcing service providers. The Authority also came across deficiencies in the performance of adequate due diligence on TPPs. Outsourcing policies were sometimes observed not to be sufficiently comprehensive and/or failed to address ongoing assessments on the performance of TPPs.

Occasionally, the MFSA observed that licence holders placed a false sense of security on their outsourcing arrangements, particularly with respect to intra-group outsourcing setups. The Authority continues to point out that intra intra-group outsourcing is essentially a form of outsourcing and is therefore also subject to the Authority's expectations on outsourcing. Instances were observed where intra-group outsourcing arrangements were not regarded as outsourcing resulting in potential risks (associated with intra-group outsourcing arrangements) not being analysed. The MFSA also came across instances where management of potential conflicts of interest was inadequate.

Business Continuity Management

Financial entities should establish adequate business continuity management practices that maximise their ability to continue to provide their services on an ongoing basis and to limit adverse impact in the event of a disruption. As part of sound business continuity management, Licence Holders should conduct Business Impact Analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity, and availability).

The Authority has observed instances where: [i] BIA was not performed; [ii] business continuity plans were broad and did not necessarily reflect the specificities of the respective organisation; and [iii] management bodies were not adequately involved in business continuity management, did not ensure that their organisations have adequate procedures, which are periodically being reviewed, in place and over-relied on the business continuity management practices of TPPs without ensuring that they are able to continue to provide their services in case of a disruption on the part of their providers.

The MFSA's 2021 Supervisory ICT Risk and Cybersecurity Focus

The MFSA intends to continue building on the work carried out in 2020 and shall retain ICT Risk and Cybersecurity as a cross-sectoral area of focus for 2021. The Supervisory ICT Risk and Cybersecurity function will continue to support the sectoral supervisory functions to ensure that regulated entities have an adequate cybersecurity programme in place designed to enhance resilience to cyber-attacks and mitigate the risks associated with such threats.

In view of the ever-increasing dependency on ICT, an enhancement, in terms of breadth and depth of supervisory activities (see section on Supervisory Approach in page 4) throughout the year, is to be expected. Authorised persons are expected to demonstrate a clear commitment that they are indeed raising the bar on ICT Risk and Cybersecurity matters.

The function plans to develop an ICT and Cybersecurity risk model for supervision as a process for mapping out, and prioritising key risk areas within the industry.

The function plans to also carry out a comprehensive and cross-sectoral thematic desk-based review on ICT Risk and Cybersecurity matters, including outsourcing. The Guidance Document (see page 5) will be used as a basis for this exercise.

Participation and contribution in local and foreign working groups is expected to intensify throughout 2021 and significant progress on the legislative proposals on digital operational resilience is also anticipated.

The Authority plans to engage with the industry and carry out education and awareness activities for stakeholders.

Concluding Remarks

This document provides context to the activities that the MFSA is currently working on in the field of ICT risk and Cybersecurity. It provides information about how the Authority carries out ICT risk and cybersecurity supervision, future significant developments within the regulatory framework and observations from the various supervisory interactions.

ICT risk and Cybersecurity, however, go beyond supervision and regulatory compliance. Breaches and successful cyber-attacks (including on government infrastructures, ICT services providers, and even cybersecurity organisations), coupled with the increased reliance on ICT, continue to highlight the need to:

- set the right tone and commitment at management body level;
- own ICT risk and Cybersecurity;
- own oversight on outsourcing arrangements;
- look at ICT and Cybersecurity as an investment and not a cost;
- have an adequate Cybersecurity framework and controls in place;
- ensure that the quantity and skills in terms of human capital are adequate, including at board level;
- plan and prepare (including the regular testing of procedures) for the eventuality of an incident;
- increase training and awareness at all levels;
- ensure that clear roles and responsibilities are in place;
- ensure that the organisation has the necessary and proportionate monitoring and detection mechanisms in place, including following and keeping abreast with reputable cybersecurity advisories and cyber threat intelligence;
- manage vulnerabilities efficiently and effectively;
- audit ICT and Cybersecurity regularly;
- test the security of the ICT infrastructure regularly (e.g. penetration testing and red team exercises);
- adopt a continuous learning and improvement culture.

The Authority expects regulated entities to note the contents of this publication and to adopt recommendations or take corrective action, where appropriate, in order to meet the Authority's expectations.

Malta Financial Services Authority
Triq L-Imdina, Zone 1
Central Business District, Birkirkara, CBD 1010, Malta
communications@mfsa.mt
www.mfsa.mt