MFSA MALTA FINANCIAL SERVICES AUTHORITY

RISK MANAGEMENT POLICY

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

CONTENTS

REVISIONS LOG

VERSION	DATE ISSUED	DETAILS
1.00	30 June 2020	Risk Management Policy – Initial version.

1. PURPOSE

This Policy sets out the Risk Management objectives and requirements for the Malta Financial Services Authority ("Authority" or "MFSA"). Management is expected to conduct structured Risk Management in accordance with this Policy.

This Risk Management Policy:

- defines the objectives and scope of Risk Management for the MFSA tasks and processes, and related outcomes i.e. products and deliverables;
- describes the roles and responsibilities of the operational risk stakeholders within the MFSA; and
- presents an umbrella methodology outlining the operational Risk Management process which is applicable to both vertical and horizontal Risk Management disciplines and to specialised frameworks. The Policy is tailored to also suit the MFSA's tasks and processes and related outcomes and is accompanied by guiding principles which describe in more detail how to apply the Policy and provide appropriate techniques for risk identification, assessment, response, reporting and monitoring. These will facilitate consistency of the approach and foster transparency of risk documentation.

The MFSA considers the strategy, assets, liabilities, processes, people, technology and resources within the Authority with the purpose of continually evaluating and managing risks on an integrated enterprise-wide basis.

The Authority's Risk Management practices are embedded throughout the MFSA's different Functions. They are applied in strategy setting and all business processes across the Authority, and their application allows the Board of Governors, Committees and Senior Management to identify, assess, respond to and monitor risks.

By applying Risk Management in a structured way, the MFSA shall be in a better position to know and control its overall operational risk situation and thereby achieve its key objectives.

All employees are expected to be familiar with the Authority's Risk Management practices and to be clear on their roles and responsibilities in this regard.

2. SCOPE

The Policy is applicable to all MFSA Functions and comprises SSM tasks and processes and related outcomes where operational risks could jeopardise the achievement of the objectives of the MFSA.

3. POLICY

The MFSA recognises Risk Management as an important element for implementing effective controls and corporate governance structures within the Authority. It is the process by which the MFSA intends to systematically identify, evaluate and manage the potential risks and opportunities attached to its activities and objectives. In order to adopt an appropriate Risk Management process at the MFSA, this Policy is prepared to:

- Highlight the objectives of Risk Management;
- Detail the roles and responsibilities;
- Outline the key components of the adopted Risk Management framework; and
- Identify the deliverables of the Risk Management process.

4. OBJECTIVES

The objectives of having a structured Risk Management process at the MFSA are to:

- Provide the Board of Governors and other Governing Councils with a regular and consistent overview of risks and related responses;
- Enhance corporate governance;
- Align risk appetite between the Board of Governors, the Management and the staff;
- Enhance risk response based on agreed risk appetite;
- Reduce operational surprises and associated exposures;
- Align, integrate and rationalise Risk Management, governance and compliance;
- Build confidence of regulatory authorities, community and stakeholders;
- Successfully respond to a changing business environment;
- Align strategic processes with corporate culture.

5. GUIDING PRINCIPLES

This operational Risk Management Policy aims at promoting the principles of responsibility, efficiency, effectiveness, integrity and transparency whilst being based on the concepts of monitoring, continuity and correctness, to develop a suitable framework to limit the risk to acceptable levels.

This integrated approach to Risk Management covers other aspects of operational risk, including those related to physical security, information system security and regulatory matters.

5.1 EFFICIENCY

Operational Risk Management aims at being efficient by allocating resources to the management processes proportional to the extent of the risks that the MFSA plans to mitigate. To this effect, efforts will be made to optimise Risk Management practices, by generating synergies, avoiding duplication of tasks and favouring a cost-benefit approach consistent with the acceptable level of risk.

5.2 EFFECTIVENESS

The use of a structured methodology that is systematically applied to all MFSA Functions and consistent with the methodology adopted by the ECB/SSM, contributes to the effectiveness of operational Risk Management. Although harmonized within the MFSA, this methodology is applied with the flexibility required to support each of the MFSA's Functions and objectives which can be inherently different and adaptable to a changing environment.

5.3 TRANSPARENCY AND COOPERATION

Operational Risk Management is only relevant within a framework of cooperation between the stakeholders in an information sharing environment with full transparency, according to the respective needs, in accordance with the principle of *"need to know, need to have"*.

The treatment of an incident (identification of the sources of the incident, analysis of the original vulnerabilities, assessment of the impacts that have occurred and potential assessment of the probability of recurrence of the incident, search for preventive measures to be implemented, monitoring of adaptations and corrections implemented, factual and objective reporting) makes sense only if the necessary information is presented in a complete and accurate manner.

5.4 CONFIDENTIALITY

The confidentiality principles in force at the MFSA also apply to operational Risk Management, and this is applied without impeding the basis of transparency and essential cooperation as described above.

5.5 RESPONSIBILITY

Operational Risk Management is based on the individual's responsibility - depending on the level of intervention of each person - in terms of:

- the conduct of professional practices that help to limit operational risk,
- the full acceptance of residual risk based on the level of risk defined according to the principles being set out in this Policy.

As such, the demand for accountability on these two aspects is an integral part of operational Risk Management.

Based on these founding principles, operational Risk Management requires the collaboration of all stakeholders, as part of their roles and responsibilities.

6. METHODOLOGICAL FRAMEWORK

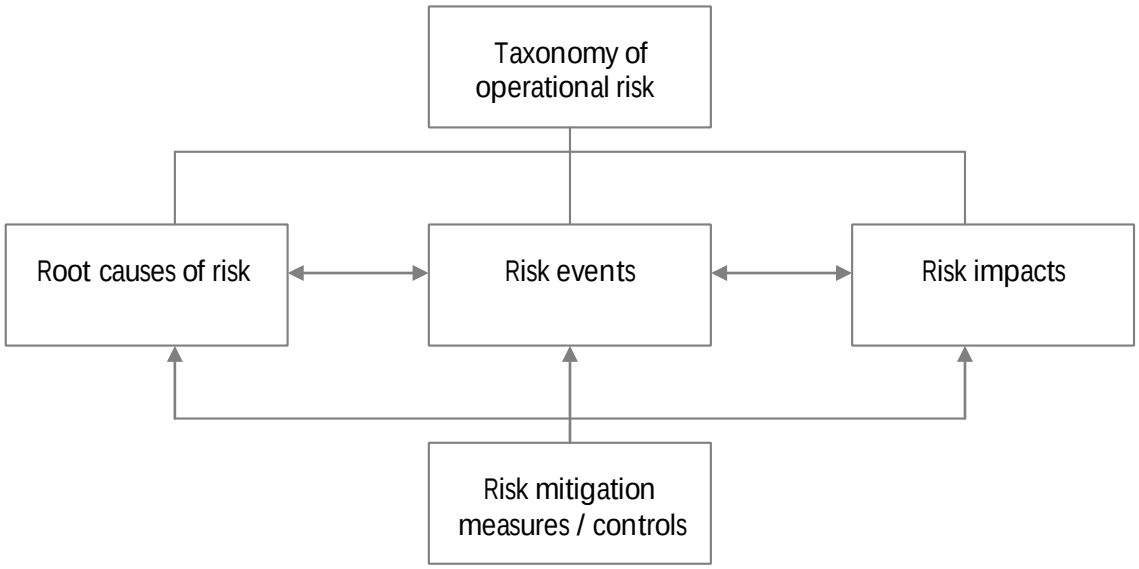
The methodology for identifying, assessing and responding to operational risks should follow the logic of the generic Risk Management process. The components defined in this Policy remain at a high level in order to ensure enough flexibility in their implementation within different areas of activity.

6.1 RISK TAXONOMY

The risk taxonomy is based on three interlinked components: risk impacts, risk events and root causes. Each risk event may have multiple root causes and impacts. The taxonomy is a comprehensive and modular toolbox used as follows:

- The taxonomy of operational risk impacts is used in risk assessment to classify the level of risks and prioritise (in combination with likelihood) detailed risk analysis and risk response measures, as it lays the emphasis on the type of negative impact on the MFSA;
- The taxonomy of operational risk events serves to identify risks;
- The taxonomy of root causes is used on a continuous basis to define and implement the most effective risk treatment measures.

Taxonomy of Operational Risk



6.2 RISK TOLERANCE POLICY

The MFSA risk tolerance policy is a Board of Governors' decision defining the principles how to respond to operational risk, depending on its level of impact severity and likelihood. The risk tolerance policy is therefore a reference point for the Risk Management assessment as to whether an individual risk needs a response and, if relevant, which risks need to be submitted to the Board of Governors for acceptance.

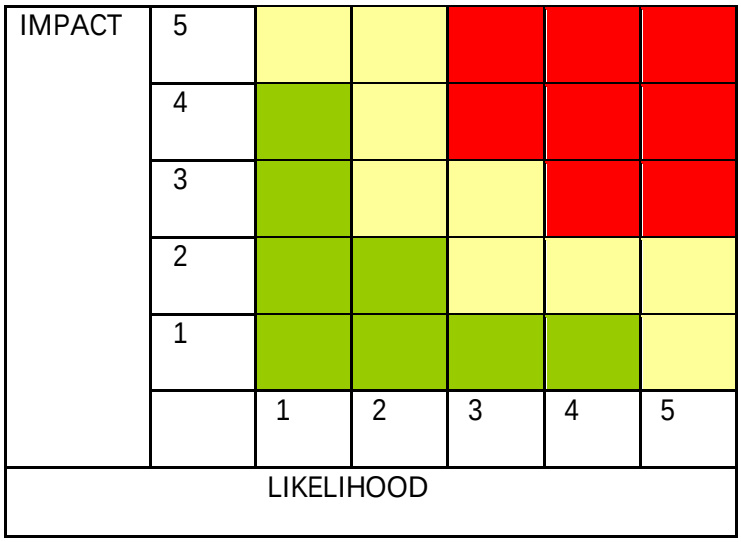
The risk tolerance policy can be represented in a graphical way (see the risk matrix below) using the three level grading scales of impact and likelihood.

These scales are the foundation for the MFSA to establish an overview of the current and foreseen risk situation for its products and deliverables and are consistent with the Internal Audit Risk Assessment scales. Each zone corresponds to specific risk management principles:

- Low and Low/Medium risks (risks in the "green zone") are considered ex ante as tolerable;
- For Medium risks (risks in the "yellow zone") - the Risk Owner shall elaborate and implement risk treatment measures for approval by the Risk Committee or, in case no

measures can be applied efficiently, provisionally accept those risks and report them to the Board of Governors on an annual basis for acceptance;

- For High and Medium/High risks (risks in the "red zone") Risk Management shall inform the Executive Committee and Risk Committee without undue delay whenever such a risk is identified and elaborate risk treatment measures for approval by the Board of Governors or, in case no measures can be applied efficiently, request that the Board of Governors accept the risk.



6.3 RISK MANAGEMENT PROCESS

Risk Management should, as a pre-condition for the subsequent exercises, conduct the following two steps:

- identify the products and deliverables;
- conduct a criticality assessment of each product.

The Risk Management process comprises the following steps: risk identification, risk assessment, risk response as well as risk reporting and monitoring.

6.3.1 Risk Identification

Risk Management should identify risks related to the MFSA's most critical products/ deliverables. Identified risks should be recorded consistently to allow for a review and for the subsequent stages of the process to be effective.

6.3.2 Risk Assessment

The risk assessment considers impact and likelihood, as well as existing controls/control objectives as a basis for determining how the risks should be managed. Depending on the available sources, the risk assessment may be qualitative (expert opinions) and/or quantitative

(statistical analysis based on an incident database). In practice qualitative analyses are often used to rank the risks.

6.3.3 Risk Response

The purpose of risk response and the implementation of risk response measures is to manage risks according to the risk tolerance policy. The following risk responses can be applied to a specific risk:

- avoid (e.g. not to proceed with an activity or to withdraw from it);
- mitigate (e.g. modify the likelihood or the impact of a risk event by applying operational tools and/or procedures and the corresponding controls);
- transfer (e.g. transfer or share risks by means of insurance or contractual arrangements);
- accept (to tolerate the risk, e.g. when the ability to do something about the risk is limited or the cost of acting is disproportionate to the potential benefit).

When analysing and defining risk responses, a cost-benefit analysis should be conducted to ensure the efficiency of possible solutions.

Controls/control objectives are a key mechanism for modifying and managing risks. Controls/control objectives should provide reasonable and cost-effective assurance of reducing risk levels according to the risk tolerance policy.

An appropriate action plan needs to be prepared and maintained to ensure compliance with control objectives and the progress of implementation is properly monitored. Upon implementation of the action plan, the risk situation should be reviewed. Control objectives should be reviewed regularly to continuously verify their appropriateness.

Residual with a rare likelihood can be accepted without treatment in cases where the control framework cannot be reasonably further improved under cost/benefit considerations, e.g. if the control framework is already fully aligned with good practices.

6.3.4 Risk Reporting and Monitoring

Risk reporting is a communication of the key outputs from the Risk Management process. The purpose of consistent risk reports by Risk Management to the Board of Governors, via the Risk Committee, is to provide assurance that the Risk Management process is operating effectively and consistently, and the risks are being managed in line with the risk tolerance policy.

Appropriate information and communication activities are an integral part of the Risk Management process and are related to each step of the process. The process must ensure that all stakeholders across the MFSA have access to relevant information and a sufficient overview of the risk situation.

Risk Management is an on-going process; therefore, risk reporting is not associated with a given process phase (i.e. completion of a full cycle is not a prerequisite). It aims to present an overview of the risk situation at a given point in time. Regular reports, in line with the guiding principles provided, are produced in order to inform the Board of Governors of the status of risks and risk

response and to steer decisions, where appropriate. In order to provide a comprehensive and consistent picture of the risk situation to the Board of Governors in the reports, Risk Management shall regularly perform a review to update the risks.

Operational risks must be subject to regular monitoring. It is an on-going process that continuously checks the status of the key operational risks and related controls/ control objectives, verifies that these remain in line with the operational risk tolerance policy, ensures that action plans are being implemented according to agreed schedules, scans the business environment and best practices to detect emerging new operational risks, defines control objectives, and ensures that incidents (including near misses) are proactively monitored and reported.

A key mechanism for risk awareness, knowledge and future performance is to ensure that the MFSA learn from risks that have materialised and resulted in a negative impact or from near misses. For this purpose, Risk Management should keep track of incidents (including near misses) and, where relevant to ensure a smooth operational response at Board of Governors and SSM level, establish a process of event reporting. Incidents (including near misses) with a very high, high and medium impact, according to the risk impact grading scales, should be reported to Executive Committee, Risk Committee and Board of Governors and, at least very high and high incidents (including near misses) should be reported to the Board of Governors, provided that these incidents (including near misses) are related to MFSA tasks and processes.

6.4 RISK CULTURE

Risk culture refers to the set of shared attitudes, values and behaviours that characterise how an entity considers risk in its day-to-day activities.

The MFSA aims to foster a positive risk culture. A positive risk culture promotes an open and proactive approach to managing risk that considers both threat and opportunity and is one where risk is appropriately identified, assessed, communicated and managed across all levels of the Authority.

Senior management and other identified individuals are responsible for driving the risk culture through initiatives and processes. All senior staff should proactively provide feedback through normal reporting channels on external interactions with key stakeholders regarding areas of potential risk. Every employee also has a role to play in contributing positively to this culture.

Risk influences the outcome of all work undertaken by the Authority and that all staff understand, accept and manage risk as part of their everyday decision-making processes.

6.5 RISK APPETITE

Risk is part of doing business and Risk Management is therefore part of day-to-day business management. The Authority aims to formalise risk management to the extent that Functions are able to apply best-practice techniques, to share knowledge and experience, and to make the MFSA's key risks to the Board of Governors transparent.

Risk Appetite is defined as the level of risk that the Authority is prepared to sustain whilst pursuing its business strategy, recognising a range of possible outcomes as business plans are

implemented. It reflects the MFSA's philosophy and influences the Authority's culture and operating style.

The Board of Governors sets its Risk Appetite in terms of (i) objectives and factors, and (ii) limits and trigger levels across.

Appetite is determined in the light of the Authority's business strategy, risk management competencies and core values, and is approved by the Board of Governors on an annual basis.

The Authority aims to take risks in an informed and proactive manner, such that the level of risk is consistent with the potential rewards and that the Authority understands and can manage or absorb the impact of the risk in the event that it materialises. Management will establish such risk responses as are required to achieve the Function objectives in accordance with the acceptability of the risk. Quantified Functions risk tolerances will be formulated and regularly updated by management at Function level.

6.6 RISK MANAGEMENT REQUIREMENTS

In order to formalise risk management across the MFSA and in order to set a common level of transparency and risk management performance, several requirements have been defined for each Function. The Authority's Functions are obliged to address the following requirements with regards to Risk Management:

- Develop and review, at least annually, a statement on the risk tolerance of the Function;
- Conduct a formalised risk assessment at least annually, this assessment is to include the identification, prioritisation, measurement and categorisation of all key risks that could potentially affect the Function's objectives;
- Report annually on the key Functional risks as identified in the Authority's risk reporting formats;
- Continuously monitor key risks and controls and implement appropriate risk responses where necessary;
- Formalise responsibilities for managing risk and for sustaining the MFSA's Risk Management framework within the Functions;
- Monitor and review the application of the Risk Management framework.

6.7 ASSURANCE

The Authority has an Internal Audit Function that conducts a systematic program of operational and financial audits across the MFSA Functions. Through the Risk Management process, the Functions themselves are responsible for assessing their risks, for implementing appropriate controls, for monitoring risks and controls, and for gaining assurance that the risks are being managed as intended. Formalised assurance from a corporate level focuses on auditing how the Functions apply the Risk Management framework. The outcome of the risk assessment process will be used as input for the audit planning by Internal Audit.

7. RISK GOVERNANCE AND CULTURE

Successfully embedding Risk Management practices into the Authority's governance and working practices is vital to the overall effectiveness of this framework. It requires the Board of Governors, Board Committees and Senior Management to consider actively the ways in which they act and behave ensuring that Risk Management becomes a core element of the MFSA's culture.

The MFSA's governance structure is based on what is known as a 'three lines of defence' framework with well-defined lines of accountability.

Responsibility for Risk Management resides at all levels within the Authority, from the Board of Governors down through the organisation. The MFSA distributes these responsibilities so that risk/return decisions are taken at the most appropriate level, as close as possible to the Function, and subject to robust and effective review and challenge.

The Authority's governance structure distinguishes between Functions owning and managing risks; Functions overseeing management of risks; and Functions providing independent assurance in relation to risks.

8. RISK MANAGEMENT ROLES AND RESPONSIBILITIES

Risk Management is primarily the responsibility of Function management. Specific responsibilities for applying, supporting and auditing the risk management process are detailed in this section.

8.1 FUNCTION MANAGEMENT

By definition, Risk Management is a normal part of day-to-day management practice. The specific responsibilities of management with respect to structured risk management are to:

- Implement the Risk Management framework within the Function;
- Develop and review the Function's risk tolerance;
- Manage through their Function Risk Officers, the identification and assessment of the risks encountered, and report material risk information annually and ad-hoc in the case of significant new risks arising;
- Manage the material risks within the Function and ensure the actual risk profile is consistent with the risk tolerance;
- Develop and maintain an appropriate organisation to facilitate the application of the Risk Management framework.

8.2 EXECUTIVE COMMITTEE

- Contribute to formulating and updating the MFSA Risk Management Policy;
- Contribute to formulating and reviewing the MFSA Risk Appetite Statement;

- Determine, communicate and support the Authority's Risk Management approach;
- Review the Functional risk reporting critically and provide feedback to the Functions as part of the planning process;
- Ensure that the appropriate structure, processes and competences are in place across the MFSA in order to address the requirements set out in this Policy;
- Report to the Risk Committee on material risks.

8.3 RISK COMMITTEE

- Assist the Board of Governors, who has the ultimate responsibility for the Risk Management framework within the Authority, in fulfilling its overall oversight responsibilities regarding the Risk Appetite of the Authority and the Risk Management Function and the governance structure that supports it;
- Advise the Executive Committee on the management of risk within the Authority;
- To this effect, through its Risk Management Policy, the Risk Committee shall set the tone for the management of risk in the Authority and shall indicate how Risk Management should support the Authority's strategy;
- In setting the tone for the management of risk, the Risk Committee develops a culture of risk within the Authority, promotes open discussion regarding risk, integrate Risk Management into the Authority's goals and compensation structure, and creates a corporate culture such that people at all levels identify, assess and manage risks rather than reflexively avoid or heedlessly take them;
- Review and discuss with management the risk governance structure of the Authority and make recommendations to the Board of Governors as may be necessary;
- Assist the Board of Governors in establishing the Authority's Risk Appetite;
- Review and discuss management's assessment of the enterprise-wide Risk Management framework of the Authority, including the strategies, policies, procedures, and systems established by management to identify, assess, measure, and manage the major risks facing the Authority and make recommendations to the Board of Governors as may be necessary;
- Review and discuss management's assessment of the Authority's aggregate enterprise-wide risk profile and make recommendations to the Board of Governors for the approval of the Risk Matrix of the Authority;
- Review and discuss management's assessment and make recommendations to the Board of Governors for the approval of the Authority's Risk Appetite statement on an annual basis, including the adoption of tolerance limits in respect of the operational risk, financial risk and legal Risk Management framework;
- Scrutinise the Risk Register and the procedures for maintaining and managing the Risk Register and adopt management proposals to the review procedures;
- Evaluate the scope of work of the Risk Management Function and its planned risk management activities;

- Review the performance of the Head of Risk Management and the effectiveness of the Risk Management Function;
- Review reports from the Head of Finance regarding asset quality and main financial risks;
- Review the effectiveness of operational Risk Management policies and controls;
- Review management's assessment of the information security Risk Management programme, including cybersecurity risk, of the Authority;
- Review reports from Risk Management, Information Technology, Legal, and Internal Audit Functions relating to risk and compliance issues and management's responses to such reports;
- Report to the Audit Committee on the activities and actions of the Risk Committee and escalate to the Audit Committee for discussion at a joint session with the Audit Committee any items that may have significant impact on financial statements or require significant financial statement/regulatory disclosures, and any other significant issues;
- Report the Committee's activities and significant decisions and risks to the Board of Governors and the Chief Executive Officer.

8.4 HEAD OF RISK

The Head of Risk ensures that Risk Management is conducted in a structured, systematic and continuous manner across the Authority's Functions. The Head of Risk specific responsibilities are to:

- Organise and develop work processes for the identification, assessment and management of risks and for the reporting of risk within the Authority;
- Instil a Risk Management culture within the Authority;
- Report to the Chairman of the Risk Committee, and to the Board of Governors, to the Chief Executive Officer and to the Chairman of the Audit Committee as may be necessary on risks as established and in accordance with any other internal rules and procedures of the Authority;
- As a member of the Risk Committee report, advise and guide the Risk Committee on matters related to risk and its management;
- Deliver presentations to the Board of Governors, the Executive Committee and the Audit Committee in accordance with the Risk Committee Charter;
- Maintain and advise the Risk Committee on the Risk Register and the Authority's Risk Appetite;
- Maintain MFSA's Risk Management framework (tools and methodologies);
- Support Functions in their use of these tools and methodologies;
- Maintain Risk Management communication within the Authority;
- Facilitate the risk assessment as part of the Plan and as part of support for key decisions;

- Provide an annual risk report for the Authority, as well as a consolidated risk report;
- Coordinate and supply training in Risk Management.

8.5 FUNCTION RISK OFFICER

- Reporting and escalating significant risk events and delivering Root Cause Analysis reports for relevant events;
- Central point of contact for all related risks subject within the Functions;
- Promoting the Risk Culture within the Functions;
- Assessing the control environment;
- Maintaining the risk-based supervisory tool within the Functions.

ANNEX 1 - GLOSSARY

assurance structure	An accompanying assurance structure, including Internal Audit, which monitors and assures the application of the Risk Management framework within MFSA's Functions.
control objective	A guidance to design appropriate risk mitigation measures to prevent, detect, correct or minimise the impact or the likelihood of a risk event for MFSA tasks and processes.
deliverable	An outcome of a process.
frequency	The number of times that a specific type of risk event occurs within a specified interval.
horizontal risks	Risks related to information security, physical security, legal or compliance issues, human resources, business continuity, procurement, etc., that impact several products/deliverables across the MFSA.
internal control	Any action taken by the Board of Governors, Committees, management and staff to manage risks in an efficient and effective manner, thereby increasing the likelihood that the objectives of the MFSA will be achieved.
incident	An event which had or could have had (near miss) a negative impact and lead to, business disruption, reputational or financial loss.
level of risk	Magnitude of a risk expressed in terms of the combination of impact and its likelihood.
likelihood	The frequency of risk event occurrence observed in the past or the possibility that a given risk event will occur in the future.
maximum tolerable outage (MTO)	The period after which the disruption of a product would create an intolerable impact on the MFSA according to the risk tolerance policy.
operational risk	The risk of negative financial, business and/or reputational impacts on the MFSA resulting from inadequate or failed internal governance and business processes, people, systems, or from external events.
product	An outcome of one or a bundle of processes which encompasses several deliverables.
process	An end-to-end sequence of activities.
risk	The effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of occurrence.
risk acceptance	Informed decision to tolerate a residual risk.
risk appetite	The amount of risk, on a broad level, the Authority is willing to accept in pursuit of its business objectives. It is a statement or series of statements that describes the entity's attitude toward risk taking.
risk event	Something that may happen, triggered by specific root causes internal or external to the MFSA, which generates a risk impact (negative).
risk impact	The ultimate negative result of a risk event. The risk impact grading scale provides qualitative and quantitative criteria to assess the level of risk in terms of negative business, reputational or financial impact on the MFSA.
risk management framework	A set of integrated mechanisms, tools, policies, procedures, people and processes, including management oversight, to manage Risks.

risk management process	A common four-step process for identifying, assessing, responding to and monitoring risks with the Functions.
risk tolerance policy	A Board of Governors decision defining the principles on how to respond to operational risk considering its level. It is built on the risk impact and risk likelihood grading scales.
roles and responsibilities	Clearly defined responsibilities for managing and reporting on risks within line management and separately for supporting and auditing the risk management process.
root cause	The origin and initial explanation of a given risk event.
review cycle	Regular review of the risk situation to keep the risk portfolio up to date for reporting purpose, by means of a light and/or a detailed review.
support structure	A dedicated support Function (Risk Officers) and a set of common user-friendly tools that allow the Functions to implement and apply the elements of the Risk Management framework.
taxonomy	A specific categorisation of items. The risk taxonomy provides a clear and common language for all operational risks. It facilitates consistency in operational risk analysis and reporting, supports the quality and comprehensiveness of analysis by providing concrete examples for risk events and root causes, and facilitates the design and implementation of relevant controls.
three lines of defence model	A concept referred to in corporate governance, structuring the internal controls around a three-tier system. Operational management acts as the first line of defence and is responsible for maintaining and executing effective internal controls on a day-to-day basis. Whereas the second line of defence are Functions monitoring and facilitating the implementation of effective controls by the first line, e.g. risk management, compliance and quality assurance. The Internal Audit Function acts as the third line of defence providing independent and objective assurance on the effectiveness of governance, risk management and internal controls to the ECB decision-making bodies.

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