28 September 2026

Insurance and Pensions Supervision
Tel: (356) 21441155
Email: ipsu@mfsa.mt

Dear Chief Executive Officer and Compliance Officer,

Outcomes-Based Supervision: Implementation of an Effective Risk Management Function

You are receiving this letter as a Chief Executive Officer and Compliance Officer of a (Re)Insurance Undertaking (referred to herein as "undertakings") authorised and supervised by the Malta Financial Services Authority (referred to herein as the "MFSA" or the "Authority").

1. Background

The Solvency II Directive 2009/138/EC requires undertakings to maintain an effective system of governance that includes a robust Risk Management Function ("RMF"). Article 44 of the said Directive requires undertakings to establish a Risk Management System ("RMS") that is fully integrated into their organisational structure and decision-making processes, enabling the continuous identification, measurement, monitoring, management, and reporting of risks at both individual and aggregated levels. The RMF plays a critical role in supporting the Board and senior management by providing oversight of the undertaking's risk profile, assessing the effectiveness of risk management arrangements, and ensuring that emerging and material risks are appropriately identified, escalated, and managed. These requirements are fundamental to promoting the sound and prudent management of undertakings and safeguarding policyholder interests.

To foster and enforce effective compliance with Solvency II obligations, the Authority conducted a thematic supervisory engagement during 2025 focusing on the implementation and effectiveness of the RMF across undertakings. This engagement comprised a series of onsite supervisory inspections and a supervisory self-assessment questionnaire distributed to a representative sample of undertakings.

The objective of this supervisory work was to assess how undertakings are implementing the RMF, including governance arrangements, resourcing, operational effectiveness, and integration within the decision-making processes, in line with the requirements of the Solvency II framework.

This letter sets out the Authority's key observations arising from the thematic review and includes examples of good practices as well as recurring issues observed across the insurance market that undermine the effectiveness of the RMF. The letter also outlines the

Authority's supervisory expectations regarding the roles and responsibilities of individuals responsible for carrying out the RMF.

The RMF plays a central role within the system of governance of undertakings. It is responsible for identifying, measuring, monitoring, managing, and reporting risks to which the undertaking is or could be exposed to, both on a current and forward-looking basis. An effective RMF supports sound decision-making, ensures that the undertaking operates within its risk appetite, and contributes to the long-term protection of policyholders.

The Authority expects the RMF to operate as a second line of defence, with sufficient authority, independence, and access to information to enable it to challenge business decisions and escalate concerns where necessary. Undertakings are to ensure that they implement the Authority's expectations in a manner proportionate to the nature, scale and complexity of their operations and risk profile. Nevertheless, applying proportionality should not contribute towards ineffective governance arrangements or insufficient oversight by the function.

2. Risk Management Self-Assessment Questionnaire

The self-assessment questionnaire developed by the Authority was structured to focus on specific areas, namely, General Governance requirements, Board involvement and oversight, Risk Management Strategy and Policy, the RMF, and the Own Risk and Solvency Assessment ("ORSA").

2.1. Scope and Methodology

As part of this engagement, the Authority issued a self-assessment questionnaire to the individual responsible for conducting the RMF within selected undertakings. Through this thematic review, the participating undertakings were asked to assess the level of effectiveness of the RMS and the RMF as well as identify areas which need improvement.

The self-assessment questionnaire comprised both open-and-closed-ended questions and was developed with reference to the relevant regulatory requirements under the Solvency II Directive 2009/138/EC, Article 259 of Commission Delegated Regulation (EU) 2015/35, Article 18 of the Insurance Business Act (Cap. 403 of the Laws of Malta), and Chapter 6 of the Insurance Rules. The questionnaire was sent out to a sample representing circa 30% of the total undertakings authorised in Malta. It was issued on 20 May 2025, and the selected undertakings were given 10 weeks to complete and submit their responses. Of the selected undertakings, 90% submitted their self-assessment within the stipulated timeframe. The remaining 10% did not submit their responses by the deadline, with one undertaking failing to submit the self-assessment altogether.

2.2. Analysis

Overall, the results indicate a strong level of alignment with Solvency II requirements across the insurance market. Undertakings generally assessed themselves as either mostly compliant or fully compliant, with no significant deficiencies identified. The findings suggest that undertakings have established mature governance and risk management supported by Board oversight, clearly documented policies, effective RMF, and the ORSA.

The self-assessment consisted of the following 4 sections:

Section 1: General Governance Requirements

The survey results from the first part of this section demonstrate a high degree of alignment across all three areas mentioned in Table 1, with no undertaking reporting low ratings.

Undertakings identified opportunities to further strengthen ORSA integration, enhance communication across functions, refine risk reporting and stress-testing methodologies, and continue developing risk culture and emerging risk management practices.

Requirement	Mostly Compliant	Fully Compliant
Fit and Proper Criteria	15.8%	84.2%
Risk Management System	21.1%	78.9%
ORSA Integration	26.3%	73.7%

Table 1: General Governance Requirements

The results pertaining to the Board Involvement and Oversight indicate a strong degree of Board engagement in risk management matters across the market.

Undertakings reported strong levels of interaction between the Board and the RMF. Most undertakings assessed Board engagement as very frequent and structured, with only a small number reporting a lower level of interaction, as noted in Figure 1 below.

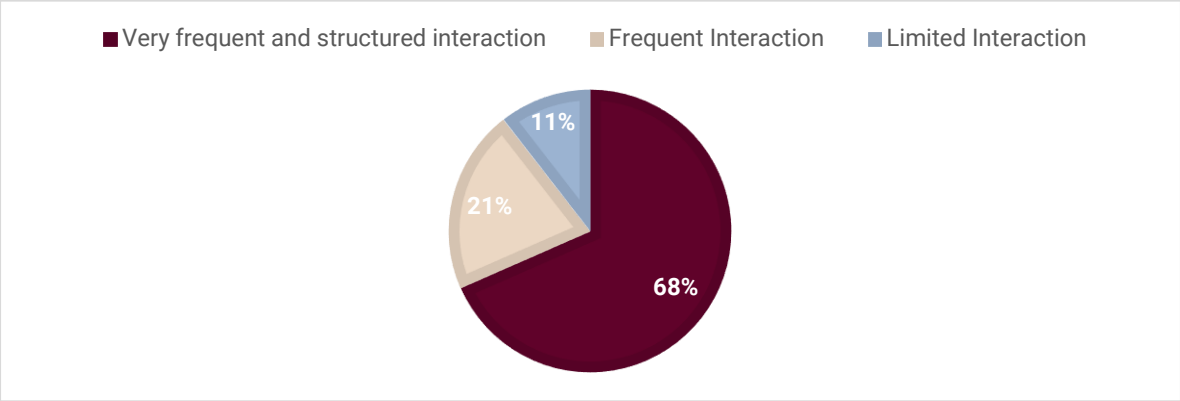

Figure 1: Board Engagement with the Risk Management Function

From the selected undertakings, one undertaking noted that it had not appointed at least one Board member with specific responsibility for overseeing the RMS, as demonstrated by Figure

2 below. This is not in line with the Para 1.5.3.15(f) of Chapter 1 of the Insurance Rules, which states that in an insurance undertaking there should be "*the identification of the Board member to oversee the risk management system on its behalf*".

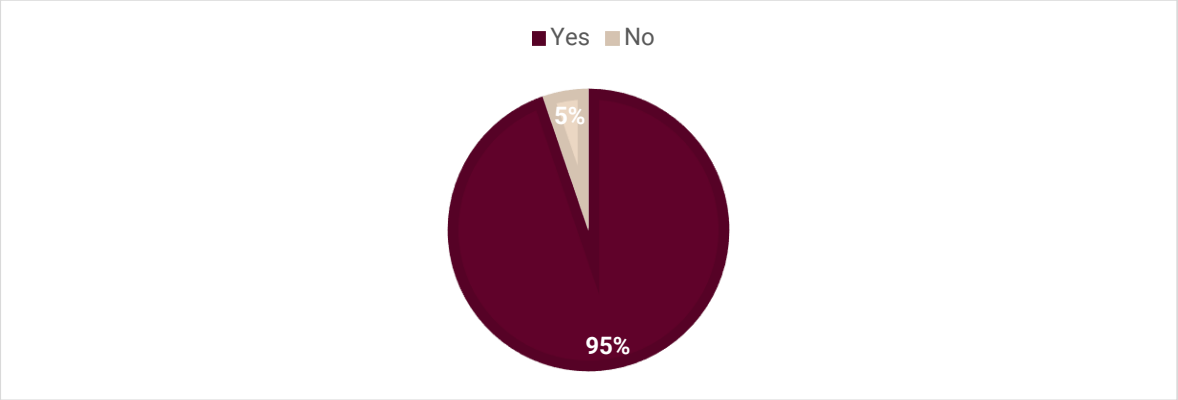

Figure 2: Appointment of a Board Member responsible for Risk Management Oversight

Overall, the undertakings indicated that the Boards play an active and accountable role in overseeing risk management and integrating risk considerations into decision-making processes, as noted in Table 2.

Area	**Partially Compliant**	**Mostly Compliant**	**Fully Compliant**
Board assumes responsibility for the RMS	0.0%	5.3%	94.7%
Board approves risk appetite and tolerance limits	0.0%	0.0%	100.0%
Board oversees risk management strategies and policies	0.0%	15.8%	84.2%
Board monitors the effectiveness of the RMS	5.3%	15.8%	78.9%
Board ensures framework alignment with business complexity	0.0%	10.5%	89.5%

Table 2: Board Oversight of the Risk Management Function

Section 2: Risk Management Strategy and Policy

The undertakings also indicated that they have established Risk Management Strategies and Policies that are integrated within governance arrangements and which are aligned with regulatory expectations, as noted in Table 3 below.

Area Assessed	**Result**
Documented Risk Management Strategy	94.7% confirmed a formally documented strategy
Integration into decision-making	Predominantly rated mostly compliant
Risk decision-making procedures	Predominantly rated mostly compliant
Board-approved Risk Management Policy	100% confirmed
Link between Policy, ORSA and capital requirements	100% confirmed
Stress-testing requirements documented	100% confirmed
Annual Board review and approval	100% confirmed
Regulatory alignment across risk categories	Predominantly rated mostly compliant

Table 3: Risk Management Strategy and Policy – Key Findings

The survey results suggest a strong level of maturity in the governance and application of Risk Management Strategies and Policies across the insurance sector.

Section 3: Risk Management Function

This section focused on the authority, independence, reporting arrangements, and interaction of the RMF with other key functions.

All undertakings confirmed that the RMF regularly reports to the Board on identified, existing, and emerging material risks and provides reports on specific risk areas, both proactively and upon request.

Undertakings also reported regular interaction between the RMF and Compliance, Actuarial, Internal Audit, and Senior Management functions, supporting a coordinated approach to risk management across the organisation, as noted in Figure 3.

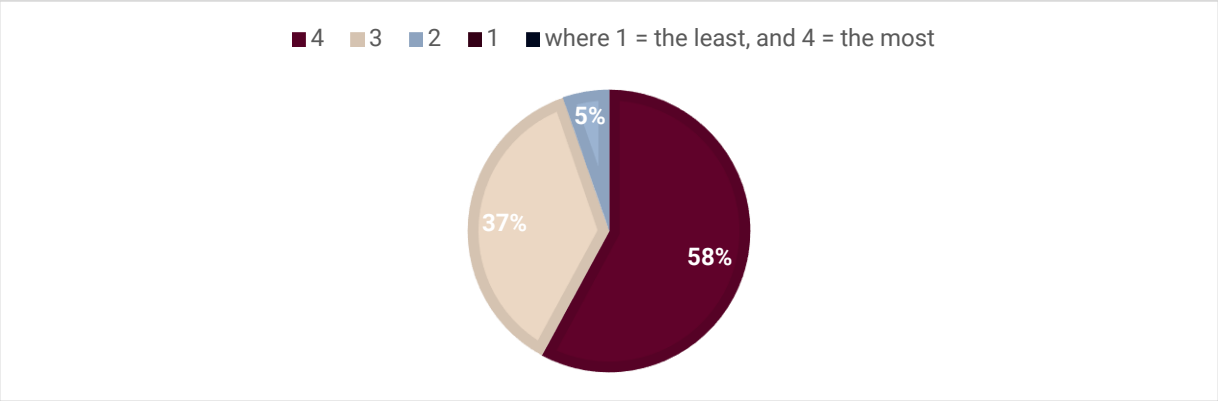

Figure 3: Authority, Visibility and Access of the Risk Management Function

Section 4: ORSA

The survey results in this section indicate an elevated level of compliance in ORSA governance and implementation.

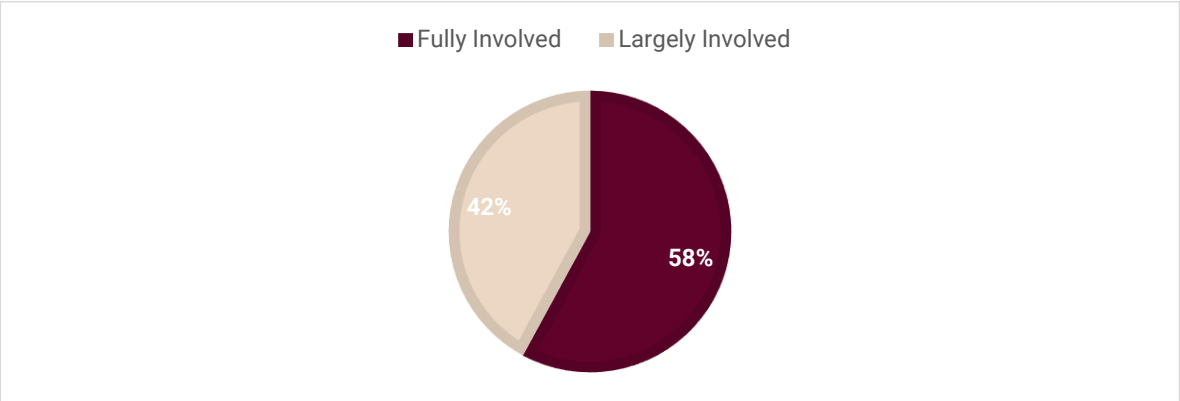

Figure 4: Board Involvement in reviewing, challenging, and approving the ORSA.

All undertakings confirmed that:

- The Board formally approves the ORSA policy and any subsequent amendments;
- The ORSA policy includes stress-testing requirements;
- The ORSA policy includes triggers for ad hoc ORSAs;
- The ORSA process reflects the proportionality principle.

The results demonstrate that ORSA frameworks are well established and supported by strong governance arrangements, active board oversight, and comprehensive policy documentation.

Conclusion on the self-assessment

The self-assessment results indicate that participating undertakings are confident that they have established mature governance, risk management, and ORSA frameworks that are broadly aligned with Solvency II requirements. Across all areas assessed, undertakings reported strong adherence with the applicable legal and regulatory framework, strong Board engagement, implementation of effective RMF, and well-developed policies and procedures.

While the overall findings are positive, undertakings recognised the importance of continuous improvement, particularly in relation to the further integration of ORSA into decision-making processes, the enhancement of stress-testing and risk reporting practices, and the management of emerging risks.

3. Supervisory Inspections

The supervisory inspections were structured to focus on the implementation of an Effective Risk Management Function within the chosen insurance undertakings.

3.1. Scope and Methodology

This initiative was in line with the MFSA Supervisory Priorities 2025, specifically within the framework of Governance, Risk & Compliance (GRC), and forms part of the Authority's ongoing commitment to strengthening risk management across the sector.

As part of this engagement, the Authority sought to assess and gain a better understanding of the effectiveness of the RMF across a selected sample of undertakings while identifying best practices and common shortcomings across the market. The supervisory inspections were conducted at the premises of a sample of 5 undertakings during the year 2025.

The Authority’s evaluation was based on discussions with relevant personnel as well as an analysis of the Company’s documentation provided prior to and during the inspection. The documentation consisted of key documents, including, the Risk Register, Risk Management Policies, Internal Audit Review Reports, Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs), and the Work Planner. Following each supervisory inspection, a Schedule of Findings was issued for each undertaking, outlining the observations and recommendations that resulted from the supervisory inspections.

Following these inspections, the Authority gathered and assessed all the observations as identified in the analysis below.

3.2. Analysis – Good Practices observed.

i. The ORSA Process

The Authority observed that undertakings with more mature governance frameworks treated the ORSA as an ongoing strategic process rather than a periodic regulatory exercise. Good practices identified included the following:

- Early planning and structured ORSA timelines

Undertakings commenced the ORSA process well in advance of Board approval deadlines, with clearly defined planning milestones, responsibilities, and timelines. This enabled sufficient time for meaningful challenge, management discussion, stress testing, and refinement of assumptions and conclusions. In several cases, the ORSA process was aligned with the undertaking's strategic planning and budgeting cycle, supporting greater integration between risk, capital, and business planning.

- Active involvement of the Board of Directors

The Authority observed the Board was actively engaged throughout the ORSA process, rather than only at the final approval stage. This included:

  - participation in defining the scope and key assumptions of the ORSA;
  - discussion and challenge of stress and scenario testing results;
  - consideration of the implications of the ORSA on strategy, capital management, business planning, and risk appetite; and
  - documented evidence within Board and committee minutes demonstrating effective oversight and challenge.

Such practices support compliance with Article 45 of Solvency II, which requires the ORSA to form an integral part of the business strategy and to be considered on an ongoing basis in strategic decisions.

Undertakings demonstrated a strong coordinating role by the RMF in the ORSA process. The RMF was responsible for:

  - coordinating inputs from relevant business functions;
  - ensuring consistency of methodologies, assumptions, and risk assessments;
  - challenging first-line inputs where necessary;
  - assessing the completeness of material risks considered; and
  - providing independent analysis and reporting to senior management and the Board.

The Authority also observed positive practices where the RMF holder maintained direct engagement with the Board throughout the ORSA process and provided clear explanations of key vulnerabilities, emerging risks, and management actions.

ii. Oversight of the RMF

The Authority identified a number of good practices relating to the oversight of the RMF when such function is outsourced to third party service providers ("TPSPs"). This aligns to the requirements of Article 44 of Solvency II, which requires undertakings to maintain an effective RMS that is fully integrated into governance and decision-making processes.

In particular, positive practices also included the appointment of individuals to carry out the oversight of the RMF who have sufficient authority, expertise, and independence to ensure that accountability and strategic control remain within the undertaking. The Authority also observed that effective oversight extends beyond the review of periodic reports, and includes regular engagement with the outsourced TPSP, supported by appropriate challenge and discussion. Good practice further included maintaining sufficient in-house expertise to understand, assess, and challenge risk methodologies, assumptions, and outputs, thereby avoiding excessive reliance on the outsourced RMF and ensuring that risk management remains embedded within the undertaking.

Undertakings are reminded that outsourcing does not remove their responsibility for maintaining an effective RMS. Boards and individuals responsible for the oversight of a key function remain fully accountable for ensuring that outsourcing arrangements do not adversely affect governance, operational effectiveness, or supervisory oversight. Whether performed internally or outsourced, the RMF should remain effective, continuous, and fully integrated into governance and decision-making processes.

Effective oversight should be supported by appropriate governance and reporting arrangements, including regular reporting on key risk exposures, emerging risks, methodologies, assumptions, and control weaknesses. Individuals responsible for the oversight of the RMF are expected to exercise independent judgement and challenge, ensuring that outputs produced by such outsourced function are appropriately reviewed and that methodologies remain suitable for the undertaking's business model and risk profile.

The Authority further expects undertakings to maintain high standards of data quality, integrity, and timeliness, as well as compliance with all applicable regulatory requirements. Where weaknesses are identified, prompt remediation should be supported by clear action plans, ownership, timelines, and ongoing monitoring. Undertakings should also maintain appropriate business continuity arrangements and credible exit strategies to ensure the continued effectiveness of the RMF and minimise disruption should outsourcing arrangements need to be amended or terminated.

iii. Risk Registers

The Authority also identified a number of good practices relating to the maintenance and use of Risk Registers. As a key component of an effective risk management framework, the Risk Register provides a structured and consolidated view of the material risks faced by an

undertaking and supports ongoing risk monitoring, accountability, and informed decision-making.

The Authority noted that several undertakings maintained well-structured Risk Registers that were treated as live documents and updated regularly to reflect changes in the risk profile. Good practice included the clear categorisation of risks, comprehensive risk descriptions, and assessments of both inherent and residual risk levels. Controls were clearly documented and linked to individual risks, enabling undertakings to assess control effectiveness, determine whether residual risks remained within risk appetite, and identify areas requiring further attention.

The Authority also observed the consistent use of likelihood and impact assessments to determine overall risk ratings, together with the clear allocation of risk ownership. These practices support accountability for the ongoing management, monitoring, and timely escalation of risks, while ensuring that Risk Registers remain a practical and effective tool within the broader risk management framework.

iv. Key Risk Indicators

KRIs are considered to be a powerful tool in Risk Management because they provide early warning signs of emerging risks, which could eventually impact various areas of the business including underwriting performance, claims experience, capital adequacy, regulatory compliance as well as operational effectiveness. By monitoring key exposures, such as claims trends, lapse rates, reserving adequacy, market risks, and operational or cyber risks, KRIs support a more proactive and forward-looking approach to risk management.

The Authority identified several good practices adopted by undertakings in the development and implementation of KRIs, including:

- Strong alignment between KRIs, the undertaking's risk appetite, key risk categories, and strategic objectives, ensuring that risk monitoring remains relevant and supports business decision-making;
- Clearly defined and meaningful thresholds, enabling the timely identification of deviations from expected risk levels and facilitating prompt management action; and
- Clear ownership and accountability structures, supported by well-defined escalation procedures to ensure that emerging issues are reported and addressed at the appropriate level without undue delay.

The Authority also notes positively that KRIs are generally well integrated into governance processes and are subject to regular review and updates, ensuring their continued effectiveness and relevance.

The Authority expects all undertakings to continue building on this momentum, acting pro-actively to refine their approaches and leverage KRIs as a strategic tool for informed decision-making and sustainable growth.

v. Integration of Risk Appetite into Day-to-Day Operations

The Authority observed that several undertakings had successfully embedded the Risk Appetite Framework ("RAF") into operational and strategic decision-making processes across the business. These undertakings did not treat, risk appetite as a standalone governance document, but rather as an active management tool supporting risk-informed decision-making.

Good practices observed included the following:

- Clear articulation of risk appetite and tolerances;
- Risk appetite statements that were sufficiently granular, measurable, and aligned to the nature, scale, and complexity of the undertaking's operations. This included:
    - quantitative risk limits and tolerances supported by appropriate metrics and thresholds;
    - qualitative statements addressing non-financial and emerging risks; and
    - clearly defined escalation triggers and management actions in the event of breaches or near-breaches.
- Risk appetite metrics tailored to the undertaking's specific risk profile and business model rather than relying solely on generic or high-level indicators.
- Undertakings maintain regular monitoring of risk appetite indicators and tolerances through structured reporting to senior management and the Board. Such reporting:
    - highlighted breaches, near-breaches, and deteriorating trends;
    - included forward-looking analysis and emerging risk considerations; and
    - supported timely escalation and management action where required.
- The RMF played a key role in supporting the effective implementation of the RAF by:
    - coordinating the development and periodic review of risk appetite metrics;
    - independently monitoring adherence to approved limits and tolerances;
    - challenging business decisions where risk exposures approached or exceeded established thresholds; and
    - reporting material concerns directly to senior management and the Board.

Undertakings with a more mature risk management framework were able to demonstrate clear linkages between approved risk appetite metrics and operational decision-making processes. This included evidence that breaches or near-breaches of risk tolerances triggered timely management discussion, escalation procedures, and, where necessary, corrective actions. In several cases, underwriting limits, investment exposures, reinsurance arrangements, and product approval decisions were directly linked to the undertaking's approved risk appetite framework. The RMF demonstrated sufficient authority and independence to provide effective challenge and oversight in line with Article 44 of Solvency II.

3.3. Analysis - Areas of Improvement Observed

i. Risk Identification and Assessment

Based on discussions held during onsite inspections and documentation reviewed, the Authority has identified weaknesses in the robustness and formalisation of risk identification and risk assessment processes in a number of undertakings.

In particular, several undertakings lack sufficiently structured and formally documented procedures outlining how risks are identified, assessed, challenged, and escalated. This deficiency may impair the undertaking's ability to demonstrate that risk identification is conducted in a consistent, comprehensive, and forward-looking manner, as required under Article 44 of the Solvency II Directive, which mandates an effective Risk Management System covering all material risks.

The Authority notes with concern that, in some instances, risk identification relies predominantly on informal discussions, while in others it is limited to desk-based analyses. This contrasts with observed good practices in those undertakings, where risk identification is supported by structured processes, including dedicated workshops, cross-functional engagement, formal documentation of outcomes, and the use of IT tools to ensure a comprehensive capture of all relevant risk exposures.

Besides risk identification, it is equally critical that undertakings maintain a clearly defined and documented methodology for risk assessment. This should include consistent criteria for evaluating risks and ensure a clear linkage between inherent and residual risk positions. In an instance, the Authority observed that inherent risk assessments were not formally recorded, making it difficult to ascertain whether risk mitigation measures are appropriately designed, implemented, and functioning effectively. Such practices may undermine the undertaking's ability to adequately monitor and manage its risk profile, as required under Article 44(1)(a) and (b) of the Solvency II Directive, as well as the forward-looking risk assessment requirements under Article 45 (ORSA).

Furthermore, the Authority identified practices that may weaken accountability and ownership over risk management. In particular, assigning risks / control ownership to multiple individuals or entire departments, rather than to clearly designated individual owners, may lead to

ambiguity in responsibility, diffusion of accountability, and overreliance on collective ownership. This increases the risk that identified risks are not effectively managed or subject to appropriate oversight. Undertakings are therefore expected to ensure that clear and individual accountability for risk ownership is established and documented.

ii. Operational Risk Incident Management

Operational Risk Incident Management is the systematic process of identifying, assessing, mitigating, monitoring, and reporting events, including "near misses", arising from failed internal processes, people, systems, or external events. It aims to minimise financial and reputational damage by implementing response and recovery plans. Effective management involves root cause analysis, developing action plans to prevent recurrence, remediation and fostering a risk-awareness culture.

Several weaknesses were identified by the Authority in undertakings' Operational Risk Incident Management processes, which may weaken the overall control environment. A primary area of improvement relates to the systemic capture and recording all operational risk incidents. Failure to maintain such reports limits undertakings' ability to identify risk trends, assess vulnerabilities and implement appropriate mitigating measures. Particular attention should be given to near misses, which provide valuable insight into emerging risks and control weaknesses before losses materialise. Failure to appropriately record, analyse, and escalate such events may result in missed opportunities to strengthen risk management, address underlying issues at an early stage, and prevent underlying issues from escalating further.

Additional areas of improvement noted by the Authority include inconsistent reporting thresholds across business lines, unclear definitions of incidents and losses, and excessive reliance on management judgement to decide whether an event should be recorded. These practices undermine data completeness and comparability and fall short of regulatory expectations regarding the consistency and reliability of risk information.

Other areas for improvement include the timely escalation of incidents and the performance of robust root cause analyses. It was noted that incidents are often treated as isolated events, with investigations focusing primarily on financial impact rather than the underlying process, system, or behavioural weaknesses. In addition, weaknesses in accountability and governance over incident ownership, coupled with poor tracking of remedial actions, may impede the effective resolution of issues, and reduce the effectiveness of corrective measures.

The Authority also identified shortcomings in the use of incident and near-miss data to inform broader risk assessments, scenario analysis, ORSA processes, and management decision-making. This may result in missed opportunities to strengthen operational resilience and to enhance undertakings' overall risk management framework.

iii. Risk Management Policies

The Authority positively notes that all undertakings reviewed have a Risk Management Policy ("RMP") in place, which is subject to formal approval by the Board of Directors. Notwithstanding this, a recurring finding was that a significant number of RMPs remain overly generic and high-level in nature, and are not sufficiently tailored to the business model, risk profile, and operational complexity of the undertaking.

In particular, the Authority observed that several RMPs lacked sufficient detail and were not fully aligned with Chapter 6, Annex I of the Insurance Rules. Deficiencies were noted in areas such as:

- the absence of a clearly defined methodology for how the undertaking manages each relevant category, area of risks and any potential aggregation of risks;
- limited articulation of how the risk management framework links to the undertaking's overall solvency needs assessment as identified in the ORSA, the regulatory capital requirements and the undertaking's risk tolerance limits;
- insufficient detail on the frequency, scope, and triggers for both regular and ad-hoc stress testing; and
- insufficient detail in various sub-policies under Chapter 6, Annex I of the Insurance Rules.

Furthermore, the Authority noted that, despite the annual reviews conducted, the documentation provided did not always evidence meaningful evolution over time. In several cases, changes were purely cosmetic, rather than reflecting substantive updates in response to changes in the undertaking's strategy, risk exposures, or operating environment.

Undertakings are expected to revise and strengthen their RMPs to ensure full alignment with the regulatory framework. The RMP is expected to be relevant, effective, and specific to the undertaking. In cases where the RMP is kept high-level, it must be appropriately supported by additional Board approved sub-policies and documented procedures.

iv. Risk Management Workplan

Whilst acknowledging that most of the undertakings inspected adopted a Risk Management Workplan, the Authority notes that in most instances, these plans need to be enhanced further.

In particular, the Authority expects that workplans should contain sufficient detail and provide a realistic, structured, and comprehensive overview of all planned activities. Furthermore, as part of the planning, scheduling, and monitoring of risk management–related tasks, undertakings are expected to adopt a forward-looking and proactive approach. Consequently, all activities within this area should be formally documented and captured in the Risk Management Workplan, to ensure adequate visibility of the work performed by the RMF, including clear deadlines for specific tasks and ongoing tracking of progress throughout the year.

Risk Management Workplans are also expected to be tailored specifically to the undertaking's business model, ensuring that these appropriately reflect the nature, scale, and complexity of risks faced. They should also be designed in a manner that is manageable and executable within the resources available to the RMF, thereby supporting consistent and effective delivery.

In addition, sufficient capacity, time, and resources should be embedded within the workplan to accommodate any ad-hoc second-line deep dives or reviews, as necessary. This flexibility will enhance responsiveness to emerging risks and ensure that oversight and decision-making bodies are able to assess, in a timely and informed manner, the adequacy and effectiveness of the undertakings' Risk Management System and RMF.

v. Business Continuity and Succession Planning

Based on discussions held during onsite inspections and documentation reviewed, the Authority identified several deficiencies in business continuity and succession planning.

Although all undertakings had a documented Business Continuity Plan ("BCP") in place, significant shortcomings were observed in both its governance and implementation. Discussions revealed that the RMF was often detached from the development, maintenance, and testing of the BCP, with limited awareness of its content and the outcomes of any reviews undertaken. Furthermore, in several cases, no formal Business Impact Analysis ("BIA") was conducted as part of the BCP development process, and BCPs were often not subject to regular testing, limiting assurance as to their effectiveness in practice.

It was also noted that certain undertakings considered the COVID-19 pandemic to represent a sufficient test of their business continuity arrangements. However, the Authority emphasises that business continuity extends beyond remote working to address a broad range of scenarios, including system outages, cyber incidents, and operational disruptions.

Succession planning was similarly found to be underdeveloped across several undertakings, with responsibility often assigned to the Human Resources function, with limited or no involvement from the RMF. In several cases, undertakings had not established a documented succession plan identifying key roles, potential successors, or interim arrangements, nor were such plans subject to regular review or Board oversight.

The Authority expects undertakings to maintain comprehensive, documented and regularly reviewed and tested business continuity and succession arrangements, with active RMF involvement and oversight.

4. Conclusion

The good practices and areas of improvement identified during this thematic review on the effective implementation of the RMF are being shared with the market via this letter as an instrument to highlight areas of potential vulnerabilities as well as sharing best practices in the implementation of such key function. The practices contained within this letter shall not

be considered as an exhaustive list of weaknesses and/or strengths. The Authority notes the considerable time and effort being invested by individuals responsible to carry out the RMF and Board of Directors, which demonstrate the importance and value being given to implement and continue strengthening the Risk Management framework of the undertakings they are responsible for.

At the same time, undertakings are expected to ensure that the RMF is adequately resourced at all times, to be able to accomplish its responsibilities effectively and in line with Solvency II requirements. Effective risk management enables re/insurers to identify, assess, monitor, and mitigate underwriting, market, credit, operational, and regulatory risks. It also strengthens decision-making, supports regulatory compliance, protects policyholders, and enhances stakeholder confidence, ensuring long-term sustainability and resilience in an industry built on uncertainty.

The Authority expects that all undertakings take this opportunity to review and assess their Risk Management Systems including the Risk Management Framework which is a core component within the Risk Management System, in order to identify gaps and areas of improvement, and take the necessary actions to bring them in line with the applicable regulatory framework and the Authority's expectations, adopting a proportionality approach corresponding to the nature, size and complexity of their business.

Should you require any clarification on the above, please do not hesitate to contact the Authority's IPS Function on ipsu@mfsa.mt.

Yours Sincerely,

Malta Financial Services Authority

Christopher Peter BUTTIGIEG (Signature)

Digitally signed by Christopher Peter BUTTIGIEG (Signature)
Date: 2026.09.28 13:27:27 +02'00'

Christopher P. Buttigieg

Chief Officer Supervision

Raymond SCHEMBRI (Signature)

Digitally signed by Raymond SCHEMBRI (Signature)
Date: 2026.09.28 12:02:57 +02'00'

Ray Schembri

Head – Insurance & Pensions Supervision

The MFSA ensures that any processing of personal data is conducted in accordance with Regulation (EU) 2016/679 (General Data Protection Regulation), the Data Protection Act (Chapter 586 of the Laws of Malta) and any other relevant European Union and national law. For further details, you may refer to the MFSA Privacy Notice available on the MFSA webpage.