MFSA MALTA FINANCIAL SERVICES AUTHORITY

Annual Compliance Report Submission

Guidance Notes

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Revisions Log

VERSION	DATE ISSUED	DETAILS
1.00	27/01/2026	Issuance of Document

List of Abbreviations

FIR/02	Chapter 2 of the Financial Institutions Rulebook
FIR/03	Chapter 3 of the Financial Institutions Rulebook
FS	FinTech Supervision
CMP	Compliance Monitoring Plan
ACR	Annual Compliance Report
AP	Authorised Person
AML	Anti-Money Laundering
CFT	Counter Finance Terrorism
MLRO	Money Laundering Reporting Officer

The ACR is expected to be signed using a valid qualified electronic signature in accordance with the Circular issued by the Authority on the Use of Electronic Signatures dated 15 November 2022.

The ACR should include relevant information detailing the risk assessment methodology, the frequency and the mitigation strategies to be included. As a minimum, it is expected that the risk assessment should factor in operational, legal and compliance, strategic, liquidity, reputational, cyber security, technology and financial crime risks.

The Authority expects a robust CMP based on the main risks for the AP. An assessment of these risks should be undertaken in liaison with the person leading the Risk Function, and this would also take into consideration any recent Internal Audit Findings. For each area identified in the CMP and subjected to testing, FS recommends that the CMP include the following elements:

i. A description of the area being tested
ii. The relevant procedures outlining the actions and checks to be performed
iii. The frequency of the testing
iv. The individual or function responsible for the area under review
v. The findings and/or recommendations arising from the testing
vi. The date on which the testing was conducted

It is important that the Compliance Officer and the Compliance team itself test the processes, policies and procedures and that the function should not rely on checks carried out by other departments. This is since the CMP is the responsibility of the Compliance Officer himself/herself, and thus the individual should be aware of the correctness of the checks being carried out.

Following its review of the deficiencies identified in the first submission of CMPs, FS wishes to draw the attention of APs to several areas that would be advantageous to incorporate. These elements were present in submissions that FS assessed as being of high quality and thoroughly prepared.

1. **Regulatory Compliance governance**
    - An updated organisational structure, including all outsourced functions and committees;
    - An assessment of the adequacy of the FI's second and third line functions;
    - Evidence of ongoing adherence to all pre-licensing and post-licensing conditions;
    - Confirmation of compliance with all conditions imposed by the Authority on approved key function holders;
    - Clear reporting lines and escalation procedures;
    - Defined reporting frequencies;
    - Confirmation that the MFSA Licence Holder portal has been updated and reflects all accurate and current information.

2. Policies and Procedures

- A list of policies and procedures scheduled for review during the period;
- Details of any amendments effected;
- The date of approval;
- Any documentation issues that remain outstanding and unremedied.

3. Board of Directors

- The adequacy of the Board's composition, including the number of Directors and their respective skill sets, to ensure alignment between the current structure and that approved by the Authority;
- The nature and quality of Board deliberations. This is to be supported by a review and documentation of a sample of Board meeting minutes;
- The management and disclosure of conflicts of interest among Board members;
- The regular assessment of the independence criteria applicable to Independent Non-Executive Directors;
- The contributions and effectiveness of Independent Non-Executive Directors.

4. Committees

- Evaluation of the appropriateness and effectiveness of the committee structure;
- Review of committee discussion and resulting actions.

5. Business Model and Business Strategy

- Assessment of the adequacy and sustainability of the business model;
- Strategic objectives and plans for the forthcoming three to five years;
- Alignment of the risk strategy with the overarching business strategy;
- Verification that the AP's activities remain consistent with the terms of its licence;
- Evaluation of the effectiveness of the New Product Approval process;
- Comparison of forecasted outcomes against actual performance;
- Identification of any matters requiring particular attention or escalation.

6. Financial Crime Compliance

- AML/CFT checks, with particular reference to the FIAU Implementing Procedures Part I and any applicable guidance notes and circulars issued by the FIAU;
- Business Risk Assessment, including, inter alia, reference to the most recent publication of the National Risk Assessment. Customer Risk Assessment;
- Jurisdiction Risk Assessment;
- Policies and Procedures relating to AML/CFT, Sanctions, Fraud and other types of financial crime;
- Industry Risk Assessment;
- Client Onboarding including Customer Due Diligence;
- Client reviews and updating of data with an emphasis on a risk-based approach;

- Client sanctions, Adverse Media and PEP screening; with a recommendation for periodic system testing;
- Dormant/Inactive client review;
- Internal/External reporting procedures;
- Outsourcing &/ Reliance (if applicable);
- Internal Training;
- Periodic AML/CFT Audits;
- Oversight of the AML/CFT Function / MLRO;
- Record Keeping;
- Ongoing Monitoring - Keeping information/documentation up to date & Transaction monitoring;
- Mitigation measures implemented by the FIs in relation to Fraud.

7. Employee related checks

- Processes for employee onboarding and ongoing screening;
- Management of employee conflicts of interest;
- Clarity and completeness of role descriptions;
- Analysis of staff turnover levels;
- Identification and assessment of employee-related matters.

8. Safeguarding of client funds

- The adequacy of safeguarding policies and procedures;
- The adequacy of the safeguarding methods employed;
- Testing of safeguarding reconciliation processes;
- Review of the Internal Audit report on Safeguarding of Clients' Funds, and any findings emanating from this.

9. Own funds

- Adequacy of own funds policies and procedures;
- Testing of own funds calculations;
- Confirmation that own funds are in line with regulation;
- Planning for any increases in capital to meet regulatory requirements.

10. Internal Audit Reports

- Ongoing monitoring of Internal Audit cycles, which at a minimum in accordance are to be in line with the regulatory requirements;
- Documentation of outstanding items categorised by risk level, including the actions being undertaken for their closure, the responsible individual, and the target completion date;
- Planned Internal Audit cycles for the forthcoming year.

11. External Auditor Management Letter

- Review of the external auditor's comments, management replies and follow up on actions to close off any open items.

12. Regulatory Calendar of submissions (to include but not limited to)

- Risk Evaluation Questionnaire;
- Any submissions arising from the licence, including post-licensing conditions, as well as any additional submissions required under the relevant framework, such as R3-2.13 "Reporting Requirements".

13. Technology

- Compliance with the Digital Operational Resilience Act, including identified gaps and remedial actions underway; including but not limited to:
    i. Classification of ICT-related Incidents and cyber threats;
    ii. Key contractual provisions where contractual arrangements with ICT TPPs are concerned;
    iii. In general, where the ICT Risk Management Framework is concerned; and
    iv. Due diligence and governance arrangements where ICT TPPs are concerned.

14. Business Continuity

- Evaluation of the adequacy of the Business Continuity Plans, including provisions for loss of personnel (with specific reference to approved key function holders during periods of absence and/or elevated turnover, delegation and oversight arrangements), loss of systems, and loss of premises, as applicable;
- Review of Business Continuity Plan testing, including results and any follow-up action.

15. Third Party Management

- Assessment of the adequacy and effectiveness of outsourcing evaluations, policies, and procedures;
- Ensuring that all documentation pertaining to Critical Outsourced Functions as per FIR/03 is adequately maintained in accordance with the legislation;
- Management of conflicts of interest arising from outsourcing arrangements, including intra-group arrangements, where relevant;
- Evaluation of the robustness of the risk management framework in identifying, assessing, and mitigating risks associated with all third-party relationships (including, but not limited to, outsourced services);
- Assurance that sound governance structures and appropriate local substance are maintained in the context of outsourcing;
- Summary of the outcomes of risk assessments conducted on outsourcing arrangements;
- Clarity and sufficiency of exit strategies and termination rights for all outsourced functions;

- Inclusion of any sub-outsourcing arrangements within the Outsourcing Register, where applicable;
- Evidence of thorough due diligence and ongoing monitoring of third-party providers, including testing of adopted processes and disclosure of any related issues;
- Confirmation that the Authority's non-objection has been obtained for all critical or important outsourced activities.

16. Conduct

- Product/service oversight;
- Review of marketing material, website;
- List of customer complaints, timeline of events and action taken for closure.

17. Training

- Employee, director and stakeholder training;
- Adequacy of training;
- Plans for enhancements in the following period.

18. Applicable and upcoming legislation

- Details on applicable legislation;
- Identification of forthcoming legislative developments;
- A gap analysis relating to forthcoming legislation;
  Planned or ongoing projects aimed at ensuring compliance with legislative requirements.

The ACR should provide a comprehensive list of all breaches recorded during the year, as well as any open breaches carried over from previous reporting periods. Supporting information should detail the nature of each breach, its current status and the corrective measures being implemented.

FS does not have any preferences for specific formatting requirements; however, the ACR and all supporting inclusions are expected to be professionally presented, well-structured and clearly articulated, ensuring the document is self-explanatory and easily comprehensible to any third-party reviewer.

Please note that APs are advised that the details listed above are intended solely as a general guide to illustrate the type of content that an ACR and CMP might contain and what could be applicable to a licensed Financial Institution. It should also be emphasised that any examples of testing methods included are not comprehensive, nor do they necessarily address every element that may require examination. As noted earlier, the AP is responsible for ensuring that, when preparing or updating a CMP, a thorough review is carried out that reflects the AP's specific operational structure and the services it offers in line with its licence. Therefore, relying solely on the examples provided does not guarantee that the documents submitted will satisfy the Authority's expectations.

It is therefore essential that the ACR and CMP is customised to match the specific licence held by the fi since requirements may differ significantly. The AP must also decide how often and to what degree checks should be carried out during the year, based entirely on its own operational framework and, crucially, on the scale, nature and complexity of its activities.

THIS PAGE HAS BEEN INTENTIONALLY LEFT BLANK

Malta Financial Services Authority

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

www.mfsa.mt