MFSA MALTA FINANCIAL SERVICES AUTHORITY

Audit and Risk Committee (ARCO) Charter

Responsible Official: Secretary to the Audit and Risk Committee
Version: 1.0
Approved by the Board of Governors at its Meeting 09-2024 on Tuesday 12 November 2024

Note: This Charter replaces the MFSA's Audit Committee Charter and the Risk Committee Charter

Table of Contents

Malta Financial Services Authority

AUDIT AND RISK COMMITTEE CHARTER

1. ESTABLISHMENT AND PURPOSE

1.1 Article 12A of the Malta Financial Services Authority Act (Cap 330) (hereinafter "the MFSA Act"), refers to the establishment of an Audit Committee which shall be independent and shall act independently of the Board of Governors.

1.2 For this reason, the Board of Governors (BoG) approved at its Meeting no. 09 of 12/ November 2024 to re-designate the existing Audit Committee as the Audit and Risk Committee (hereinafter "ARCO") as one of the main internal Committees of the Malta Financial Services Authority (hereinafter "the Authority" or "the MFSA"). The ARCO is established by and reports to the BoG and shall operate in accordance with the provisions of the MFSA Act and this ARCO Charter.

1.3 The purpose of the ARCO is to support the BoG in meeting its oversight responsibilities of the internal governance, internal controls, financial statements, Risk Management and Internal Audit Functions of the Authority. The Committee may also have additional tasks as instructed or delegated by the Board.

In fulfilling its responsibilities as delineated under Section 1.3, the BoG have determined that the Committee will have oversight responsibilities of the Internal Audit Function and the Risk Management Function. In order to guarantee that the concept of objectivity is maintained, the Committee will ensure that the essential segregation is maintained between Internal Audit as the Authority's Third Line of Defence and Risk Management as the Second Line of Defence. For this reason, the BoG determined that the Committee shall have two co-chairs, each of whom shall chair meetings on risk matters and meetings on audit matters respectively.

2. AUTHORITY

2.1 In carrying out its functions the ARCO shall have full and unrestricted access to all information, documentation and personnel of the Authority and all officers and employees of the Authority shall cooperate with the Committee accordingly.

2.2 To this effect the BoG further empowers the ARCO to have full and unrestricted access to the Authority's external auditors, consultants or any other person or entity engaged by the Authority to provide it with advice, or services and such persons shall cooperate with the Committee accordingly.

2.3 The Committee may also hire outside counsel or other consultants as may be necessary in accordance with the established internal procedures of the Authority. The

Committee shall inform the BoG of such circumstances at the earliest opportunity but not later than the first meeting of the BoG following such decision and prior to such engagement. In this regard, the Authority shall make available the necessary funds to achieve this aim.

2.4 In fulfilling its Internal Audit responsibilities within the Single Supervisory Mechanism (hereinafter "SSM") of the European Central Bank (hereinafter "ECB") the ARCO is also authorised to exchange information with the Internal Auditors Committee (hereinafter "IAC") of the Eurosystem in its SSM format. The Committee is also authorised to exchange information with the International Operational Risk Working Group (hereinafter "IORWG").

2.5 The Committee shall be consulted on the appointment of suitable officers to perform the function of Head and/or Deputy Head within the Internal Audit Function and the Risk Management Function. To this effect, the BoG shall ensure consideration of such consultation through its internal procedures for the recruitment and appointment of such roles.

2.6 The Committee shall have the authority to institute and undertake or oversee internal investigations as required and as may be directed by the BoG in accordance with investigation policies, including those under the Anti-Fraud Policy of the Authority, and procedures as established under inter alia the People & Culture Guidebook, the Ethics Framework, and/or the Grievance Policy.

2.7 The Committee shall also have the authority to liaise with the Internal Audit and Investigations Department (hereinafter "IAID") in terms of the Internal Audit and Financial Investigations Act, Chapter 461 of the Laws of Malta which provides for the regulation of the internal and financial investigative functions, including the power to carry out effective independent internal audits and financial investigations, providing for the necessary safeguards to ensure the protection of the financial interests of Government including the funds it may receive or be required to manage under Malta's international obligations.

3. COMPOSITION

3.1 In accordance with Article 12A (4) of the MFSA Act, the ARCO may be composed of either non-executive Members of the BoG, or external independent appointments or a combination of both. All members shall be appointed for not more than three years and may be eligible for reappointment. Accordingly, the Authority shall from time to time determine such remuneration payable to the members of the Audit and Risk Committee.

3.2 The BoG shall appoint the members of the Committee and the co-Chairpersons. The Deputy co-chairpersons shall be appointed from amongst the other members of the Committee.

3.3 In considering an external independent person to be appointed as a member or co-Chairperson of the ARCO, the BoG shall apply the conditions laid down under paragraph (3) of Article 6 of the MFSA Act on the eligibility of persons to be appointed as Chairperson or a

member of the BoG or of any organ of the Authority, or to hold office with the Authority. Moreover, according to Article 12A of the MFSA Act, the provisions of paragraph (6) item (a) – eligibility for appointment, item (b) – fit and proper, item (d) – relievement from office, and item (e) – resignation from office, of Article 6 of the MFSA Act shall, as far as applicable, *mutatis mutandis* apply to the co-Chairpersons and members of the Committee.

3.4 The members of the Committee shall be financially literate and at least one member shall preferably have accounting or related financial expertise.

3.5 In addition to the provisions of Article 12A of the MFSA Act, a member of the Committee shall be relieved of office on the occurrence of any situation defined in sub-paragraph (4.2) of Clause 4 of this Charter.

3.6 Moreover, members of the BoG who are also members of the ARCO and whose terms as members of the ARCO end during the tenure of the Committee, would need to be reappointed or confirmed again by the BoG. Similarly, if a member of the Board of Governors resigns, he/she cannot remain on the ARCO unless the Board confirms him/her as an external independent member of the ARCO.

3.7 The Committee shall designate one of the officers of the Authority to act as its Secretary and who shall report to both the Audit Chairperson and to the Risk Chairperson. The Committee shall also ensure that such appointment is noted in the relevant minutes. In absentia of the appointed Secretary in any Committee meeting, the Committee may appoint a temporary Secretary to the Committee to act as substitute Secretary. Such an appointment is to be recorded in the relevant Committee minutes.

4. INDEPENDENCE OF THE MEMBERS OF THE AUDIT AND RISK COMMITTEE

4.1 The Committee shall be independent and shall act independently of the BoG. Consequently, any impairments to the independence or objectivity of the Committee shall be reported to the BoG and, where and if appropriate, shall be raised with the external auditors responsible for the annual statutory audit of the Authority.

4.2 To this effect a member of the ARCO shall be considered independent when the BoG determines that such member is independent in character and judgement, and there are no relationships or circumstances which could affect, or appear to affect, his/her judgement as a member of the ARCO. Relationships or circumstances that would normally affect the independent judgement include where the member of the ARCO:

- is a former employee of the Authority until three years after employment, or any other material connection, has ended; or
- maintains, while being a member of the Committee, a material business relationship with the Authority either directly, or as a partner, shareholder, executive director or senior employee of a body corporate or non-corporate that has such a relationship with the Authority; or

- has close family ties to the first degree with any of the consultants or senior employees of the Authority.

4.3 A member of the ARCO shall declare to the other Committee members, any perceived or potential conflict of interest which s/he may have on any item/s included for discussion on the Agenda of the Committee or being discussed during Committee meetings. The member who reports the conflict of interest shall abstain from participation in deliberations on the relevant item/s placed on the Agenda of the Committee. S/he is to be directed by the respective co-Chairperson to leave the meeting for the relevant item/s on the Agenda of the Committee and discussion being held. The respective co-Chairpersons shall also ensure that the conflict of interest is noted in the relevant minutes.

5. ACCESS TO THE AUDIT AND RISK COMMITTEE

5.1 The Head of Internal Audit, the Head of Finance, the Head of Risk Management, and the statutory external auditor responsible for the annual statutory audit of the Authority shall have free and confidential access to the Committee.

5.2 The Head of Internal Audit, the Head of Finance, the Head of Risk Management, and members of the Executive Committee may propose items to be placed on the agenda of the Committee meetings subject to the agreement of the Committee. To this effect, they shall liaise with the Secretary of the ARCO giving reasons for the inclusion of the proposed Agenda item.

5.3 Any item to be placed on the Agenda of the Committee in accordance with sub-paragraph (5.2) shall be accompanied by a written explanatory note to the members of the Committee detailing the reasons and objectives of such item and shall be verbally presented to the members of the Committee at the relevant Meeting as directed by the Committee through the Secretary.

6. MEETINGS OF THE AUDIT AND RISK COMMITTEE

6.1 The provisions of Article 7 of the MFSA Act governing the meetings of the BoG shall, as far as applicable, *mutatis mutandis* apply to the meetings of the Committee. Otherwise, the Committee may regulate its own procedures.

6.2 The Committee meetings are to cover separately Audit matters and Risk matters. The Committee is to cover these responsibilities sequentially or in separate meetings.

6.3 The Committee shall meet and report to the BoG as often as may be necessary but, in any case, not less frequently than once every three months. Meetings of the ARCO shall be called by any member of the Committee.

6.4 As a minimum, the Committee shall meet with the appointed external statutory

auditors of the Authority twice annually to discuss issues regarding the annual statutory audit of the Authority.

6.5 Although the Committee shall strive for all members to be present for meetings of the Committee, in exceptional circumstances a quorum for any meeting shall be of at least three members.

6.6 The Committee shall endeavour to reach an agreement by consensus but if this fails then a simple majority vote shall apply with the respective Chairperson of the section being discussed having the right to a casting vote.

6.7 Subject to prior notification to the Committee Secretary, members of the Committee may participate in a meeting of the Committee from separate locations through teleconferencing or other communication channels which allows those participating to hear each other and shall be entitled to vote or be counted in the quorum accordingly.

6.8 The Committee shall have the right to invite other members of management or any other officials and staff members of the Authority; and representatives of the external statutory auditors as it deems appropriate, to attend any, or part, of its meetings.

6.9 The Head of Internal Audit and the Head of Risk Management are to participate in the respective meetings of the Committee so as to support the Committee in its responsibilities as the subject matter experts. The Committee shall decide whether the Head of Internal Audit and, or the Head of Risk Management may be present during meetings of the Committee irrespectively whether discussing audit or risk matters.

6.10 The Committee is to determine whether any individuals, including the Head – Internal Audit and the Head – Risk Management, should be excluded during specific agenda items. If such a situation arises, it will be documented in the Committee Minutes.

6.11 The other members of the Board of Governors, not being members of the Committee shall have the right to attend any meeting of the Committee as observers by giving prior notice to the Committee and Secretary of the Committee who shall not withhold approval unless for specific reasons to be recorded in writing. They may not participate in discussions unless invited to do so by the Committees. Non-participation by the other members of the BoG shall not invalidate the proceedings of the Committee.

6.12 The Secretary, in consultation with the two respective co-Chairpersons shall prepare the agenda of each section of the Committee. The agenda of the Committee shall be divided into two separate areas of focus covering i) the Audit and ii) the Risk Management, which will be handled sequentially during a Committee meeting or in separate meetings. The agenda, together with relevant documents and briefing material, shall be circulated to all members of the Committee at least one week before the scheduled meetings.

6.13 The Committee Secretary after prior consultation with the respective co-Chairperson shall request a written explanatory note detailing the reasons and objectives of an agenda item. This explanatory note and any supporting documentation must be duly

signed and dated as appropriate by the relevant function before this is circulated by the Secretary to all members of the Committee, in accordance with sub-paragraph (6.12) of this Charter.

6.14 The Committee may, in exceptional circumstances adopt decisions by written procedures. Any member to whom the Secretary communicates a proposed decision and who fails to respond within the set deadline, which in normal circumstances should not be less than two working days following the date on which the proposed decision is sent to him/her, shall be considered to have approved the written procedure, provided that the other members are required to have responded to the written procedure to be considered adopted. The Secretary shall ensure that the documents relating to the proposed decisions are received by all members of the Committee. It shall be the responsibility of the Secretary to ensure that any decisions taken through written procedures shall be ratified by the Committee at the first opportunity that it meets. Co-Chairpersons shall also ensure that such ratification is noted in the relevant minutes.

6.15 The Secretary shall keep minutes of the proceedings of each meeting and shall, as early as possible following the meeting, circulate draft versions to all members seeking any amendments prior to the next meeting. The minutes of the Committee shall be divided into two separate areas of focus covering i) Audit and ii) Risk Management. A final version shall be tabled and approved by the Committee. The Minutes are to be signed by all Members of the Committee and the Secretary of the Committee at the following meeting and circulated to all members. Other members of the BoG not being members of the Committee may request a copy of the final approved minutes from the Secretary and the Secretary shall comply with the approval of the Committee who shall not withhold approval unless for specific reasons to be recorded in writing.

6.16 The Head of Internal Audit and Head of Risk Management shall have a copy of the committee minutes. Nonetheless, in the event that an agenda item requires the Head of Internal Audit or the Head of Risk Management, or both to be excused from the meeting for any reason deemed appropriate by the Committee, a separate set of minutes will be taken to preserve confidentiality. These minutes will be handled with the necessary discretion and will not be shared with the individuals excused from the discussion, unless otherwise decided by the Committee.

7. REPORTING TO THE BOARD OF GOVERNORS

7.1 The Committee shall report to the BoG at the first Board Meeting immediately following the approval of the Committee minutes. However, should circumstances so warrant, the Committee may request the Chairperson of the BoG to call an “ad hoc” meeting of the BoG giving specific and justified reasons therefor.

7.2 The Committee shall bring to the attention of the BoG the reports presented to it by the Head of Internal Audit in accordance with the Internal Audit Charter, together with its opinion on issues at stake.

7.3 The Committee shall keep the Chairperson of the BoG and the Chief Executive Officer informed of the risk profile and urgent high-risk matters discussed at meetings of the Committee by the Head of Risk Management on an ongoing basis.

7.4 The Committee shall present a summary of its activities at least annually to the BoG or at such other time and frequency as required by the BoG.

8. PERFORMANCE EVALUATION AND REVIEW OF CHARTER

8.1 The Committee shall conduct a biennial performance self-evaluation, which evaluation shall, among other things, compare the performance of the Committee with the requirements of this Charter. The performance evaluation shall be conducted in such an objective manner as the Committee deems appropriate, as required by the International Standards for the Professional Practice of Internal Audit published by the Institute of Internal Auditors. The Committee shall report to the BoG on this evaluation.

8.2 Where the review required in terms of sub-paragraph (8.1) of this Charter is not undertaken, the Committee shall report to the BoG and record in its Minutes reasons why such review has not been undertaken.

8.3 The Committee shall biennially review the adequacy of this Charter, taking into consideration the findings of the Committee's performance self-evaluation conducted in accordance with sub-paragraph (8.1) hereof, if any, and determine whether this Charter should be amended. If the Committee determines that any amendments to the Charter are necessary, the Committee shall propose such amendments to the BoG, who shall have the sole and ultimate authority to approve any amendments to this Charter.

8.4 This Charter and any amendments become effective, immediately upon approval of the BoG.

9. DOCUMENTATION

9.1 Any documentation submitted for the consideration of the Committee, including inter alia meeting agendas, approved minutes duly signed and Committee reports, shall be held in the hardcopy format within the assigned repository as per the Authority's Documents Retention Policy and also within the Committee's Secretary electronic repository.

9.2 In those instances whereby the Committee adopts a decision by a written procedure in accordance with sub-paragraph (6.14) of this Charter, the Secretary shall also keep an electronic record of any such consultation, including relative papers and views and/or positions expressed in the assigned repository.

9.3 All documentation related to the proceedings of the Committee shall be treated as confidential in line with the Authority's Data Classification Policy and access thereto shall only be granted to specific individuals on a need-to-know basis and subject to the prior approval of

the Committee.

10. CONFIDENTIALITY

10.1 The members of the Committee and officers attending and/or participating in the meetings of the Committee as established by this Charter, shall not disclose any information of a confidential nature coming to their knowledge during the performance of their duties to persons or bodies external or internal to the Authority except as provided for under this Charter and in accordance with the provisions of Article 17 of the MFSA Act.

10.2 In carrying out their duties, members of the Committee and officers attending and/or participating in the meetings of the Committee as established by this Charter, shall comply with the provisions of the Ethics Framework and the Anti-Fraud Policy of the Authority and with any other Code of Conduct as may be applicable from time to time to the BoG or to any other organs of the Authority.

Annex to the Audit and Risk Committee Charter

1. Audit

In respect of audit matters, the main functions of the ARCO shall be:

(a) to determine whether the governance, controls and risk management processes of the Authority in implementing agreed policies and strategies across the activities of the Authority are adequate, effective and functioning.

(b) to determine the Internal Audit Function's remit and role.

(c) to evaluate the performance of the Internal Audit Function set out under Article 12B of the MFSA Act.

(d) to carry out such other functions as may be assigned to it by the Board of Governors.

In fulfilling its responsibilities under Article 12A(1)(b) of the MFSA Act, in consultation with the Chief Executive Officer, the Committee shall prepare a three-year plan whereby the objectives and targets, including key performance indicators of Internal Audit are listed. These plans and targets shall be reviewed and approved annually by the BoG.

In further fulfilling its responsibilities under Article 12A(1)(c) the Committee shall also evaluate the performance of senior officials of Internal Audit including the Head and Deputy Head on an annual basis.

In addition to the functions under Article 12A of the MFSA Act and in accordance with item (d) of Article 12A (1) of the MFSA Act, the BoG has resolved to assign the following additional functions to the Committee:

(a) to oversee the financial reporting process, including risks and internal and other controls in that process, and compliance with laws and regulations.

(b) to review and monitor the integrity of the financial statements, and any formal public announcements relating to the financial performance of the Authority.

(c) to oversee the development and implementation of a policy on the engagement of the statutory external auditors including non-audit services and to make recommendations to the BoG in relation to the appointment and removal of the statutory external auditors, including fees payable.

(d) to monitor and review the independence, objectivity and effectiveness of the statutory external auditor.

(e) to oversee the annual independent statutory audit process, including the signing of the necessary statutory audit correspondence and the receiving of all financial statements, reports and management letters.

(f) to oversee the operational risk management process throughout the prudential regulatory, conduct of business, management processes and any other

functions of the Authority.

(g) to consider and make recommendations to the BoG for the approval of the annual Internal Audit Plan.

In fulfilling its functions, the Committee shall assume the following responsibilities:

Effectiveness

In determining the implementation, functioning and effectiveness of the governance, controls and risk management processes as applied to the agreed policies and strategies across the entire activities of the Authority the Committee shall:

- ensure that all areas of activity of the Authority are covered in the internal audit universe.
- consider the findings of the Internal Audit Function in these areas and monitor the application of timely and appropriate remedial action.
- consider the findings of the statutory external auditors' Management Letter and monitor the application of timely and appropriate remedial action.
- consider financial and operational risk management reports brought to its attention.
- ensure the adequacy of the financial reporting process.
- provide its opinion on the quality of the activities of the Authority to the BoG based on assessment reports received from the Internal Audit Function.
- review and make recommendations to the BoG on changes required to this Charter to ensure better effectiveness and efficiency as a minimum on an annual basis.

Financial Reporting

In fulfilling its responsibilities for overseeing the financial reporting process including the soundness of the annual financial statements, the Committee shall:

- understand significant accounting, reporting and auditing standards that have an impact on the financial statements of the Authority and the audit process.
- review any formal public announcements relating to the financial performance of the Authority.
- review the audited annual financial statements with the Chief Executive Officer, the Chief Officer Operations, the Head of Internal Audit, the Head of Finance and the statutory external auditors (as necessary), consider their completeness and consistency with information available to the Committee and make recommendations before these are submitted to the BoG for approval. In particular, the Committee shall focus on:
  - any changes in accounting policies and practices in compliance with generally accepted accounting standards.

- major judgemental areas, estimates and assumptions that underlie the financial statements.
- significant adjustments arising from the audit; and
- the findings of the statutory external auditors' audit and their report
- thereon.

- understand how management develops interim financial information, and the nature and extent of internal and statutory external auditor involvement; and
- review such interim financial reporting with management and the statutory external auditor as appropriate before submission to the BoG ensuring they are complete and consistent with the information known to the Committee.

Risk Management and Internal Control

In order to oversee the financial and operational risk management process and consequently advise the BoG on the effectiveness and soundness of risk management and internal control the ARCO shall:

- consider the application of sound risk management practices including the implementation of information security framework based on acceptable international standards.
- understand current areas of high operational and financial risks and evaluate the processes applied to manage and mitigate these risks.
- consider the respective scope of work and audit plans of the internal auditor and the statutory external auditor to ensure completeness of coverage, avoid duplication of effort and promote the efficient, effective and economic use of audit resources.
- review the adequacy of internal controls including computerised information systems and business continuity processes.
- review and discuss with internal and external auditors and risk officers' reports on any evaluations or assessments affecting risk management and controls within the Authority.

Compliance

In overseeing compliance with laws, rules and regulations governing the operations of the Authority, the ARCO shall assume responsibilities to:

- consider the findings of the internal and external audit functions in this regard and review the appropriateness of the management's actions to address these findings.
- discuss and obtain updates of any internal legal compliance matters as identified through Internal Audit engagements.

Internal Audit Function

The monitoring and reviewing of the effectiveness of the internal audit function requires the ARCO to undertake responsibilities related to:

- reviewing and making recommendations to the BoG for the approval of the annual internal audit plan and all major changes thereto prior to implementation.
- ensuring there are no restrictions or limitations to the internal audit function.
- providing the Head of Internal Audit with direct access to the ARCO and/or its Chairperson.
- periodically reviewing the Internal Audit Charter and any proposed amendments thereto to continually ensure the independence of the internal audit function.
- monitor review of the Internal Audit Manual and any proposed amendments thereto to ensure the completeness of the audit coverage of the activities of the Authority.
- consider major findings included in the Internal Audit Reports and Internal Investigations and periodically follow up and monitor the cooperation of all auditees in the timely implementation of agreed remedial measures through the Internal Audit function.
- consider quarterly and annual reports submitted by the Head of Internal Audit on the activities and results of the internal audit function in accordance with the Internal Audit Charter.
- evaluate the performance of the internal audit function through the reporting received and annually report to the BoG; accordingly, and
- assess periodic internal self-assessment reports on the quality of the internal audit function and within a minimum period of five years assess a report undertaken by an external independent reviewer appointed specifically by the Authority upon the recommendations of the Committee to assess the internal audit function including any related audit obligations and work for the purposes of the IAC of the Eurosystem in its SSM format.

External Audit Function

To review the relationship of the Authority with the statutory external auditors and in order to oversee the external audit process leading to the completion of the statutory annual financial statements of the Authority, the ARCO shall:

- review the performance of the statutory external auditors.
- make recommendations to the BoG for the engagement or removal of the statutory external auditors in line with the 'Good Practices for the Selection and Mandate of External Auditors' according to Article 27.1 of the ESCB/ECB Statute, including the fees due.

- review the independence of the statutory external auditors and the audit team through statements made by the external auditors to this effect.
- review the statutory external auditors' proposed audit scope and approach, including coordination with internal audit, through a review of the engagement letters and letters of representation.
- agree on the audit plan outlining the proposed approach, timing, and continuity with regard to any forthcoming statutory external audit.
- agree on the completion of the audit exercise and findings.
- review the statutory external auditors' Management Letter and management's.
- respond and make recommendations to the BoG.
- provide the partner responsible for the statutory external audit with direct access to the Committee and/or its Chairperson; and
- periodically meet separately with the statutory external auditors to discuss any matters that the Committee or the statutory external auditors believe should be discussed privately.

2. Risk Management

In respect of risk matters, the main function of the ARCO is to assist the BoG, which has the ultimate responsibility for the Risk Management Framework within the Authority, in fulfilling its overall oversight responsibilities with regard to the risk appetite of the Authority and the Risk Management Function and the governance structure that supports it. The Committee shall also advise ExCo on the management of risk within the Authority. To this effect, through its Risk Management Policy, the 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.

Risk identification, risk assessment, and risk management are and remain primarily the responsibility of the Authority's management. The Committee has an oversight role and in fulfilling that role, it relies on the reviews and reports it receives or requests from management and/or the BoG. The Committee shall therefore advise the BoG on the management of risk within the Authority.

In fulfilling its functions, the Committee shall assume the following responsibilities:

a. In setting the tone for the management of risk, the Committee develops a culture of risk within the Authority, promotes open discussion regarding risk, integrates 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.

b. Review and discuss with management the risk governance structure of the Authority and make recommendations to the BoG as may be necessary.

c. Assist the BoG in establishing the Authority's Risk Appetite.

d. On an ongoing basis, review and discuss presentations as provided by the Heads of the various Functions of the Authority, on *inter alia* the strategies, policies, procedures, and systems established by management to identify, assess, measure, and manage major risks emanating from their most critical processes and making recommendations to the BoG as may be necessary.

e. Review and discuss management's assessment of the Authority's aggregate enterprise-wide risk profile and make recommendations to the BoG for the approval of the risk matrix of the Authority.

f. Review and discuss management's assessment and make recommendations to the BoG 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.

g. Scrutinise the Risk Register and the procedures for maintaining and managing the Risk Register and adopt management proposals to the review procedures.

h. Evaluate the scope of work of the Risk Management Function and its planned risk management activities.

i. Review the performance and effectiveness of the Risk Management Function.

j. Periodically request and review reports from the Head of Finance regarding asset quality and main financial risks.

k. Review the effectiveness of operational risk management policies and controls.

l. Periodically request and review management's assessment of the information security risk management programme, including cybersecurity risk, of the Authority.

m. Report the Committee's activities and significant decisions and risks to the BoG and the Chief Executive Officer in accordance with this Charter.

It shall be the responsibility of the Head of the Risk Management Function of the Authority to organise and develop work processes for the identification, assessment, and management of risks and the reporting of risk within the Authority. The Head of the Risk Management Function shall:

a. Instill a risk management culture within the entire business areas of the Authority.

b. Report to the co-Chairperson (Risk) of the Committee, and to the BoG and to the Chief Executive Officer as may be necessary on risks as established within this Charter and in accordance with any other internal rules and procedures of the Authority.

c. Deliver presentations to the BoG and ExCo in accordance with this Charter.

d. Maintain and advise the Committee on the Risk Register and the Authority's Risk Appetite

For the purpose of this Charter the term '**risk**' is defined as:

'Risk is a condition in which there exists a quantifiable dispersion in the possible outcomes from any activity. It can be classified in a number of ways.' (Ref. *CIMA Official Terminology, 2005*)·

'Uncertain future events which could influence the achievement of the organisation's strategic, operational and financial objectives.' (Ref: *International Federation of Accountants, 1999*).

The term '**risk management**' is in turn defined as:

'A process of understanding and managing the risks that the entity is inevitably subject to in attempting to achieve its corporate objectives. For management purposes, risks are usually divided into categories such as operational, financial, legal, compliance, information and personnel. One example of an integrated solution to risk management is enterprise risk management.' (Ref: *CIMA Official Terminology, 2005*)