

INTERNAL AUDIT CHARTER

INTRODUCTION

The Internal Audit Division (IAD) of the Bank of Commerce (the Bank) is an independent unit of the Bank that conducts objective assurance and advisory activities designed to add value and improve the Bank's operations. It helps the Bank accomplish its objectives by bringing a systematic, disciplined approach to examine, evaluate and improve the effectiveness of governance, risk management and control processes of the Bank.

The Internal Audit (IA) Charter will be periodically reviewed and presented to the Audit Committee for approval and endorsement for Board approval; and Senior Management for notation.

PURPOSE STATEMENT

Internal auditing strengthens the organization's ability to create, protect, and sustain value by providing the board and management with independent, risk-based, and objective assurance, advice, insight, and foresight.

PROFESSIONALISM

The internal audit function will adhere to the purpose statement of IAD and the Global Internal Audit Standards (the 'Standards')¹ issued by the Institute of Internal Auditors (IIA), which includes the five domains covering the (1) Purpose of Internal Auditing, (2) Ethics and Professionalism, (3) Governing the Internal Audit Function, (4) Managing the Internal Audit Function, and (5) Performing Internal Audit Services; together with the corresponding 15 principles and 52 standards. This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the internal audit function's performance. The Standards' Considerations for Implementation and Examples of Evidence of Conformance issued by the IIA will also be used as reference for operations. In addition, the internal audit function will adhere to the Bank's relevant policies and procedures, other supplemental standards issued by regulatory authorities/ government agencies, as well as with the relevant code of ethics, and the internal audit function's standard operating procedures manual.

ORGANIZATION

The Chief Audit Executive (CAE) will report functionally to the Audit Committee and administratively to the President.

¹ The use of the terminology "conformance with ISPPA" in IAD audit reports will continue until January 2025, when the Global Internal Audit Standards becomes effective and the External Quality Assurance Review concludes that IAD is indeed compliant with the ISPPA and the noted gaps between internal audit practices versus the new Standards are few and far between or considered insignificant.

The Audit Committee will:

- Periodically review with CAE and endorse for Board approval the internal audit charter.
- Approve the risk-based and dynamic internal audit plan.
- Approve the internal audit budget and resource plan.
- Receive communications from the CAE on the IAD's performance relative to its plan and other matters.
- Make appropriate inquiries of management and the CAE to determine whether there is inappropriate scope or resource limitations.

Additionally, through the Chairman, the Audit Committee will:

- Approve decisions regarding the appointment, transfer or removal of the CAE.
- Approve the remuneration of the CAE.

The President and Senior Management will:

- Provide IAD full support and cooperation at all levels of operations.
- Provide IAD complete access to all records, property and personnel relative to the performance of its duties and responsibilities.
- Ensure that IAD has adequate resources (e.g., budget and staffing) to perform its responsibilities.
- Provide written response to all Internal Audit reports submitted.
- Promptly inform the IAD of known or suspected cases of a criminal nature involving Bank funds, property and employees, as well as significant changes in the Bank's risk management systems, policies and processes.

INDEPENDENCE AND OBJECTIVITY

The internal audit function will remain free from interference or influence by any element in the Bank, including the determination of the audit universe, scope, procedures, frequency, timing, or report content to permit maintenance of an independent and objective mental attitude. Internal Auditors shall not have direct operational responsibility or approval authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair the Internal Auditor's judgment. Internal Auditors will exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal Auditors will make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments. If independence or objectivity of internal audit function is impaired, in fact or appearance, the details of the impairment will be disclosed to the Audit Committee. Impairment to organizational independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding. The CAE will confirm to the Audit Committee, at least annually, the organizational independence of the internal audit function.

Internal audit staff shall avoid conflicts of interest. Internally-recruited internal auditors shall not engage in auditing the activities for which they have had previous responsibility before a one-year “cooling off” period has elapsed.

Staff of the internal audit function shall be periodically rotated, whenever practicable, and without jeopardizing competence and expertise to avoid unwarranted effects of continuously performing similar tasks or routine jobs that may affect the Internal Auditor’s judgment and objectivity.

MANDATE

IAD should be authorized full, free, direct and unrestricted access to any and all of the Bank’s units, activities, records, files, data, systems, physical properties, and personnel pertinent to carrying out any engagement. All employees are requested to assist the IAD in fulfilling its roles and responsibilities. The internal audit function will also have free and unrestricted access to the Board of Directors (BoD), through the Audit Committee. The internal audit function exercises accountability for confidentiality and safeguarding of Bank records and information. All internal audit personnel shall act with integrity in carrying out their duties and responsibilities. They should respect the confidentiality of information acquired in the course of the performance of their duties and should not use it for personal gain or malicious actions.

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy, efficiency, and effectiveness of the organization's governance, risk management, and internal controls, as well as the quality of performance in carrying out assigned responsibilities to achieve the organization’s stated goals and objectives and IA’s role in areas of public interest. This includes:

- Evaluating risk exposure relating to achievement of the organization’s strategic objectives.
- Evaluating the reliability, effectiveness, and integrity of management and financial information systems, including the electronic information system and electronic banking services and the means used to identify, measure, classify, and report such information.
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on the organization.
- Evaluating the means of safeguarding physical and information assets and, as appropriate, verifying the existence of such assets.
- Reviewing compliance of trading activities with relevant laws, rules and regulations.
- Evaluating the effectiveness and efficiency with which resources are employed.
- Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.
- Assisting in the investigation of significant suspected fraudulent activities within the organization and notifying appropriate management and the Audit Committee of the results.
- Monitoring and evaluating governance processes.
- Monitoring and evaluating the effectiveness of the organization's risk and compliance management processes.

- Coordinating with external audit and other assurance functions, including supervisory authorities, to provide optimal audit coverage to the Bank at a reasonable overall cost.
- Performing advisory services related to governance, risk management and control as appropriate for the organization. Consulting services include: counsel and advice, process evaluation, and training.
- Providing annually an assessment on the adequacy and effectiveness of the processes for controlling the Bank's activities and managing its risks.
- Performing activities required from internal audit, specified in regulations.
- Reviewing areas of interest to regulators such as monitoring of compliance with relevant laws, rules and regulations, including but not limited to the assessment of the adequacy of capital and provisions; liquidity level; regulatory and internal reporting, among others.
- Reporting periodically on the internal audit function's mandate, and performance relative to its plan.
- Reporting significant risk exposures and control issues, including fraud risks, compliance, governance and regulatory issues, and other matters needed or requested by the Audit Committee.
- Evaluating specific operations at the request of the Audit Committee or management, as appropriate.
- Maintaining professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this Charter.
- Keeping the Audit Committee informed of emerging trends and successful practices in internal auditing.
- Revisiting the internal audit manual annually and consulting with the Audit Committee and senior management, where appropriate.
- Updating engagement work programs (also known as audit program guides) during the planning stage of the audit in line with recent changes or newly issued policies, guidelines, advisories or regulations, which will require approval of the CAE or the appropriate IAD Department Head.

INTERNAL AUDIT PLAN

The CAE will submit to the Audit Committee at least annually an internal audit plan for the latter's review and approval. The internal audit plan will consist of a work schedule, as well as resource requirements, for the following year. As part of the planning, the CAE will confer and consult with the President and/or Senior Management and obtain an understanding of the organization's strategies, key business objectives, associated risks, governance, risk management and control processes. The CAE will communicate the impact of resource limitations and significant interim changes to the Audit Committee. The internal audit plan will be developed and implemented based on a prioritization of the audit universe using a risk-based methodology, including inputs from the Audit Committee, Senior Management and regulatory authorities. The CAE will review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls. Any significant deviation from the approved internal audit plan will be communicated to the Audit Committee through periodic activity reports.

The plans will include provisions or "buffer" for special engagements, projects, and/or investigations during the year, as mandated by the Audit Committee or at the request of the President or any members of Senior Management.

REPORTING AND MONITORING

A written report will be prepared and issued by the CAE or the IAD Department Head following the conclusion of each internal audit engagement and will be distributed as appropriate. Material issues and high risk findings will also be communicated to the Audit Committee. The internal audit report may include management's response and corrective action taken or to be taken to address the specific findings, identified root causes and recommendations. Management's response, whether included within the original audit report or provided thereafter by management of the audited area, should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented. The IAD will be responsible for appropriate follow-up on engagement findings and recommendations. All open 'For Resolution' issues will be monitored on a monthly basis until fully resolved. Meanwhile, 'For Compliance' audit issues shall be monitored and assessed by the auditee's Deputy Compliance Officer (DCO) semi-annually until such has been validated as 'Compliant' by the DCO or in the next audit, whichever comes first.

The audit supervisor (i.e. CAE or IAD Department Head) may issue interim reports whether transmitted formally or informally, to communicate information needing immediate attention; a change in the scope of the engagement; or the progress of a long-duration engagement. The use of interim reports does not reduce or eliminate the need for a final audit report.

In case an issued final audit report contains a significant error or omission (e.g. erroneous audit rating, critical information relayed by management but not included in report), the CAE must communicate corrected information promptly to all parties who received the original communication.

The CAE will periodically report to senior management and the Audit Committee on the internal audit function's mandate, as well as performance relative to its plan. Reporting will also include significant risk exposures and control issues, including fraud risks, governance and compliance issues, and other matters needed or requested by senior management and the Audit Committee.

QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

IAD will maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The program will include an evaluation of the internal audit function's conformance with IIA's Global Internal Audit Standards and an evaluation of whether Internal Auditors apply the Code of Ethics. The program will also assess the efficiency and effectiveness of the internal audit function and identify opportunities for improvement.

The CAE will communicate the results of the quality assurance and improvement program to senior management and the Audit Committee. The report shall include:

- The scope and frequency of both the internal and external assessments.
- The qualifications and independence of the assessor(s) or assessment team, including potential conflicts of interest.
- Conclusions of assessors.
- Corrective action plans.

OUTSOURCING OF INTERNAL AUDIT ACTIVITIES

External service providers may be considered to perform internal audit engagements, in accordance with existing BSP regulations on outsourcing, except for areas covered by existing statutes on deposit secrecy. Outsourcing shall, however, be done on a limited basis to have access to certain areas of expertise that are not available to IAD or to address resource constraints. The internal audit function shall not be outsourced to the Bank's own External Auditor nor to internal audit service provider that was previously engaged by the Bank in the same area intended to be covered by the internal audit function that will be outsourced, without a one-year "cooling off" period. Further, the CAE shall ensure that the knowledge or inputs from the outsourced experts shall be assimilated into the Bank to the greatest extent possible.

ADVISORY SERVICES

Senior management may seek the advice of the Internal Auditor on matters related to risks and internal controls without tainting the latter's independence. In such cases, the Internal Auditor shall not be involved in the development or implementation of policies and procedures, preparation of reports or execution of activities that fall within the scope of an audit. When performing advisory services, the Internal Auditor should maintain objectivity and not assume management responsibility. The internal audit function should also exercise due professional care in conducting advisory engagements. Some examples of advisory services that may be requested from IAD are as follows:

- Pre-implementation review for new systems
- Review of department's operating or control procedures
- Advice on the interpretation, implementation or compliance of a unit to control policies
- Membership in cross-functional groups and task forces to provide advice on control, risk management and governance processes
- Facilitation of training pertaining to internal control

COORDINATION WITH THE EXTERNAL AUDITOR, OTHER ASSURANCE PROVIDERS AND/OR SUPERVISORY AUTHORITIES

IAD may coordinate directly, or through other parties (e.g., Compliance Division), to ensure proper coverage and minimize duplication of efforts. The degree of coordination and cooperation may vary depending on circumstances, including considerations of confidentiality, independence and regulatory provisions. Modes of coordination and cooperation may include:

- Communication of audit strategy and plans
- Regular meetings between External Auditors/other assurance providers and Internal Auditors
- Arrangements for the sharing of information
- Communication of audit reports
- Temporary assignment of personnel or arrangements for joint reviews
- Organizing common training programs and courses, and sharing training materials
- Sharing methodologies, scope of work, and schedules

- Granting access to audit documentation
- Collaborating on certain audit procedures, such as collecting audit evidence or testing data.

In coordinating activities, the CAE may rely on the work of other assurance and consulting service providers, provided that competency, objectivity, and due professional care of the assurance and consulting service providers are considered. The CAE should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the CAE is still accountable and responsible for ensuring adequate support for engagement conclusions reached by IAD.

FRAMEWORK FOR EVALUATING INTERNAL CONTROL

The internal audit function helps the Bank accomplish its objectives by bringing a systematic, disciplined approach to examine, evaluate and improve the effectiveness of governance, risk management and control-processes of the Bank. To complement and align the Bank's existing policies and procedures and in the absence of such policies, IAD is guided by industry best practices and established frameworks for evaluating internal control such as, but not limited to, the following:

- Committee of Sponsoring Organizations (COSO) Internal Control and Risk Management Frameworks
- BASEL II and III and related framework, principles and documents
- Bangko Sentral ng Pilipinas (BSP) Manual of Regulations and Circulars
- The Institute of Internal Auditors' (IIA) Global Internal Audit Standards
- Information Systems Audit and Control Association's (ISACA) Control Objectives for Information and Related Technologies (COBIT) 2019 (Business Framework for the Governance and Management of Enterprise Information and Technology) and IT Assurance Framework (ITAF)

CHIEF AUDIT EXECUTIVE RESPONSIBILITIES AND ACCOUNTABILITIES

The CAE must be a Certified Public Accountant (CPA) or a Certified Internal Auditor (CIA). He must have at least five (5) years of experience as Auditor-In-Charge, Senior Auditor or Audit Manager in the regular audit of a bank.

The CAE oversees and is responsible for the internal audit activities of the Bank, including outsourced activities. The CAE, together with the President, attests in writing, at least annually, that a sound internal audit, control, compliance, risk management and governance system is in place and working effectively.

The Audit Committee and Senior Management may find that it is appropriate for the organization to expand the CAE role beyond internal auditing. When the CAE takes on roles and/or responsibilities outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.

The CAE should gain an understanding of any proposed role that falls outside of internal auditing and must discuss with senior management and the Audit Committee the reporting relationship, responsibilities, and expectations related to the role.

Additionally, if the CAE has responsibilities in areas outside the internal audit function that are subject to internal auditing, the provision of assurance would be outsourced to an objective, competent assurance provider that reports independently to the Audit Committee, rather than the CAE.