Internal Audit Policy

Issue Date: 01/11/2025

Version: 3.0

Approved by

General Manager

Jamal Kubeer

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

Purpose

This policy establishes a structured framework for conducting independent internal audits across all company operations, in accordance with the Central Bank of Kuwait (CBK) Governance and Risk Management standards. It ensures that internal audits assess compliance, control effectiveness, operational efficiency, and risk mitigation.

Scope

This policy applies to all departments and subsidiaries, including IT, Finance, Operations, Compliance, Customer Support, and any outsourced or third-party service providers handling payment-related operations.

Audit Objectives

1. Compliance – Verify adherence to CBK, AML/CFT, PCI-DSS, and internal control requirements.
2. Security – Evaluate the adequacy of information security controls and data protection.
3. Risk Management – Identify, assess, and monitor key operational, financial, and reputational risks.
4. Efficiency – Review processes for optimization and cost-effectiveness.
5. Accuracy – Confirm reliability and integrity of transaction and financial records.

Independence and Governance

The Internal Audit Department operates independently from all operational functions and reports functionally to the Audit and Review Committee, while the General Manager maintains administrative oversight only.

Internal auditors must avoid any conflicts of interest and maintain full objectivity and confidentiality at all times.

Participation of the Head of Internal Audit in the Audit and Review Committee:

The Head of the Internal Audit Department is a permanent member of the Audit and Review Committee. His/her attendance and participation in all formal committee meetings must be documented. The Head contributes to discussions on audit plans, reports, findings, and control observations.

Audit and Review Committee Meetings:

The Audit and Review Committee shall meet at least semi-annually (twice a year). The meeting minutes must document the attendance of executive management, independent external auditors, and the Head of Internal Audit to discuss audit reports, internal and external review outcomes, and corrective actions.

Evaluation of External Auditors and the Lead Audit Partner:

The Audit and Review Committee shall annually evaluate the qualifications, performance, and independence of the external auditors, including the Lead Audit Partner, in accordance with recognized professional and regulatory standards. The evaluation results shall be documented in the committee's minutes, and related recommendations shall be submitted to the Board of Directors for approval.

.

Audit Process

- Planning:
  - Risk-Based Audit Plan: Develop an annual audit plan prioritizing areas with the highest risk (e.g., payment gateways, transaction processing).
  - Resource Allocation: Assign qualified auditors with expertise in financial systems, IT security, and compliance.
  - Scope Definition: Specify audit objectives, scope, criteria, and timelines.

  • Annual Risk-Based Audit Plan: An annual audit plan shall be developed based on a comprehensive risk assessment covering all business units, systems, and operations.
  • The plan shall prioritize high-risk areas such as payment processing, AML/CFT compliance, data protection, and vendor management.
  • The draft plan shall be reviewed and approved by the Audit & Review Committee prior to implementation.
  • Any significant revisions shall be re-submitted for committee approval.
- Execution:
  - Data Collection: Gather data on transaction flows, system logs, financial records, and compliance reports.
  - Testing: Conduct tests on system controls, financial reconciliations, and compliance with security protocols.
  - Interviews: Engage with key personnel to understand processes and identify potential gaps.
  - Sampling: Use statistical sampling methods to review transactions and controls.
- Reporting:
  - Draft Report: Prepare a detailed report highlighting findings, risks, and recommendations.
  - Management Review: Share the draft report with senior management for review and feedback.
  - Final Report: Issue a final report, incorporating management responses, to the Audit Committee or Board.
- Follow-Up
  - Track and verify implementation of corrective actions.

Roles and Responsibilities

Internal Audit Team:

- Conduct audits according to the plan and report findings.
- Maintain independence and objectivity throughout the audit process.

Management:

- Facilitate the audit process by providing access to necessary information and resources.
- Implement corrective actions based on audit recommendations.

Audit Committee/Board:

- Review and approve the audit plan.
- Monitor the implementation of audit recommendations and corrective actions.

Risk Assessment

- Risk Identification: Identify key risks such as fraud, money laundering, system failures, and data breaches.
- Risk Evaluation: Assess the likelihood and impact of identified risks.
- Risk Prioritization: Focus audit efforts on areas with the highest risk, such as high-volume transaction systems and customer data protection.
- A comprehensive risk assessment shall be conducted annually to identify and evaluate key operational, financial, compliance, and cybersecurity risks.
- The risk assessment shall consider both inherent and residual risks, informed by management input, incident reports, and regulatory findings.
- The results shall be documented and used as the basis for the annual Risk-Based Audit Plan.
- The Internal Audit Team shall maintain a Risk Universe covering all auditable entities and update it periodically.

Risk Rating methodology

The Internal Audit Department shall apply a standardized risk rating methodology to ensure consistent evaluation and prioritization of risks across all auditable areas.

1. Risk Criteria
   Each identified risk shall be assessed based on two main dimensions:
   - ❖ Impact – The potential consequence to the organization if the risk materializes (e.g., financial loss, reputational damage, regulatory penalty, operational disruption).
   - ❖ Likelihood – The probability or frequency of the risk occurring.
2. Scoring System
   Both impact and likelihood shall be rated on a scale from 1 to 5, as follows:

Score	Impact	Likelihood
1	Insignificant	Rare
2	Minor	Unlikely
3	Moderate	Possible
4	Major	Likely
5	Critical	Almost Certain

3. Risk Rating Formula
   The overall risk rating shall be determined using the formula:

   Risk Score = Impact × Likelihood

   The resulting score will be categorized as follows:

4. Risk Scoring Level Action:

1 – 5	Low	Monitor under normal procedures
6 – 12	Medium	Include in periodic audit coverage
15 – 25	High	Prioritize in the annual audit plan

5. Review and Validation
   - The risk rating results shall be reviewed annually or whenever significant operational or regulatory changes occur.
   - Risk ratings shall be approved by the Internal Audit and validated with Senior Management before finalizing the annual audit plan.
   - Any significant changes in risk profiles shall be reported to the Audit & Review Committee.

Audit Frequency

Audit coverage shall follow a three-tier approach:

- High-risk areas – annually
- Medium-risk areas – every 2 years
- Low-risk areas – every 3 years

Audit Documentation and Record Retention

All audit reports, working papers, evidence, and related documentation shall be securely retained for a minimum of Ten (10) years or longer where required by CBK or legal obligations. Access shall be restricted to authorized personnel only.

Follow-Up and Reporting

The Internal Audit Department shall maintain the following:

- Action Tracking: Maintain a log of all audit findings and recommendations.
- Monitoring: Conduct follow-up audits to ensure corrective actions have been implemented effectively.
- Reporting: Regularly update senior management and the Audit Committee on the status of follow-up actions.

Non-Compliance and Escalation

Failure to comply with audit requirements, concealment of information, or obstruction of the audit process shall be considered a serious violation. Such incidents will be escalated to the Audit & Review Committee and may result in disciplinary action as per company policy.

Continuous Improvement

- Policy Review: Regularly review and update the audit policy to reflect changes in regulations, technology, and business operations.
- Training: Provide ongoing training for the audit team on emerging risks, new technologies, and best practices.
- Feedback Loop: Incorporate lessons learned from previous audits into future audit planning.

Policy Review

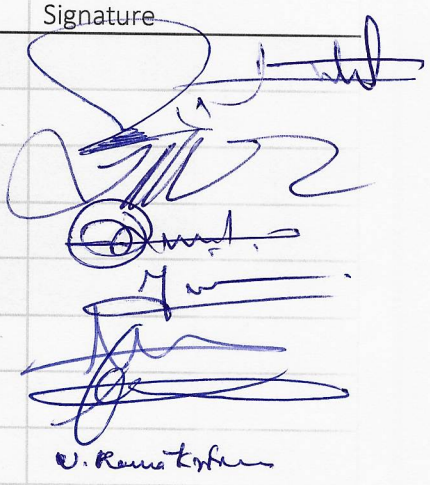
This policy shall be reviewed annually or upon major regulatory or operational changes. The Audit & Review Committee must approve all revisions.

Signature

By signing below, I agree to the following terms:

I confirm that the above have read and received and read a copy of the "Internal Audit Policy" and agree to comply to it.

Full Name	Designation	Signature
Abdulrahman ElRotel	Financial Manager	
Afif Hussein Mukahal	Executive Manager	
Jamal Eldeen A. Kubeer	General Manager	
Linto Lawrance Neelamkavil	Application Support Manager	
Michael Mansour Basily	Compliance Manager	
Nesrine Zakaria Emam	HR & Administration Manager	
Omar Mahmoud Hagras	Project Manager	
Rama Krishna Uddarraju	Information Security Manager	



Revision History

Version	Date	Author	Signature
2.0	01/10/2025	Internal Audit Manager Jinto Joy