17.22

Internal Audit Charter & Policy

Automated Services Network Co. (eNet)

Aligned with the IIA Global Internal Audit Standards (2024)

Issue Date: 22/07/2026

Version: 4.0

Approved by: Audit & Review Committee

Contents

1. Purpose & Mandate 3
2. Authority & Access Rights 3
3. Scope 3
4. Audit Objectives 3
5. Conformance with Standards 3
6. Independence & Governance 4
7. Audit Process 4
8. Roles & Responsibilities 5
9. Risk Assessment 5
10. Risk Rating Methodology 5
11. Audit Frequency 6
12. Communicating the Acceptance of Risk & Plan Changes 6
13. Quality Assurance & Improvement Program (QAIP) 6
14. Internal Audit Strategy 7
15. Audit Documentation & Record Retention 7
16. Follow-Up & Reporting 7
17. Non-Compliance & Escalation 7
18. Continuous Improvement 7
19. Charter & Policy Review 8
20. Approval 8

1. Purpose & Mandate

This document is both the Charter and the operating Policy of the Internal Audit function of Automated Services Network Co. (eNet). As the Internal Audit Charter, it establishes the purpose, authority, and responsibility of the function; as the Policy, it sets the framework by which internal audits are planned, executed, reported, and followed up. It is approved by the Audit & Review Committee (the "Committee") and reviewed at least annually.

The purpose of Internal Audit is to provide independent, objective assurance and advisory services designed to add value and improve eNet's operations. Internal Audit helps eNet accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management, and control processes, in accordance with the Central Bank of Kuwait (CBK) Governance and Risk Management standards.

The mandate of the Internal Audit function — its authority, role, and responsibilities — is established by the Committee through this Charter, consistent with Standard 6.1 (Internal Audit Mandate) and Standard 6.2 (Internal Audit Charter) of the Global Internal Audit Standards.

2. Authority & Access Rights

To fulfil its mandate, and as authorised by the Committee, the Internal Audit function is granted:

- Full, free, and unrestricted access – to all eNet functions, records, systems, physical property, and personnel relevant to the performance of any engagement.
- Direct and unrestricted access to the Committee – including the right of the Internal Audit Manager to communicate and meet with the Committee privately, without management present.
- Authority to allocate resources, set scope, and apply the techniques required to accomplish audit objectives – free from interference by any party in the selection of audit areas, scope, procedures, frequency, timing, or report content.
- Authority to obtain assistance – from personnel in the units where audits are performed, and from other specialised services within or outside eNet where required.

Internal Audit personnel are accountable for the confidentiality and safeguarding of records and information accessed in the course of their duties.

3. Scope

This Charter & Policy applies to all departments and subsidiaries of eNet, including IT, Finance, Operations, Compliance, and Customer Support, and to any outsourced or third-party service provider handling payment-related operations. No function, activity, or entity is excluded from the potential scope of Internal Audit.

4. Audit Objectives

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

5. Conformance with Standards

The Internal Audit function shall perform its work in conformance with the Global Internal Audit Standards issued by the Institute of Internal Auditors (IIA), effective 2024 (the "Standards"), and with the CBK Governance and Risk Management framework. Where CBK requirements and the Standards differ, the more stringent requirement applies.

Conformance with the Standards will be confirmed through the Quality Assurance and Improvement Program described in Section 13. Any instance of non-conformance that affects the overall scope or operation of the function will be disclosed to the Committee.

6. Independence & Governance

The Internal Audit Department operates independently of all operational functions. The Internal Audit Manager reports functionally to the Audit & Review Committee and administratively to the General Manager. This positioning is designed to preserve the organisational independence of the function (Standard 7.1).

Internal auditors must remain free from conditions that threaten their ability to carry out responsibilities in an unbiased manner, and must avoid any conflict of interest, maintaining full objectivity and confidentiality at all times. An internal auditor must not assess a particular operation for which they previously held responsibility within the preceding twelve months.

Safeguard – audit of the Finance function

Because the General Manager provides administrative oversight of Internal Audit, and to safeguard independence when Internal Audit reviews the Finance function, the results and conclusions of any engagement covering Finance are reported directly to the Committee. Neither the Financial Manager nor any member of Finance management may influence the scope, procedures, findings, or ratings of an engagement covering their own function.

Participation of the Head of Internal Audit in the Committee

The Internal Audit Manager is a permanent member of the Audit & Review Committee. Attendance and participation in all formal Committee meetings must be documented, contributing to discussions on audit plans, reports, findings, and control observations.

Committee meetings

The Audit & Review Committee shall meet at least semi-annually (twice a year). Minutes must document the attendance of executive management, the independent external auditors, and the Internal Audit Manager, and record discussion of audit reports, internal and external review outcomes, and corrective actions.

Evaluation of external auditors

The Committee shall annually evaluate the qualifications, performance, and independence of the external auditors, including the Lead Audit Partner. Results are documented in the Committee minutes and related recommendations submitted to the Board of Directors for approval.

7. Audit Process

Planning

- Annual Risk-Based Audit Plan – developed from a comprehensive risk assessment covering all business units, systems, and operations, prioritising high-risk areas such as payment processing, AML/CFT compliance, data protection, and vendor management.
- Resource allocation – assign qualified resources with expertise in financial systems, IT security, and compliance.
- Scope definition – specify audit objectives, scope, criteria, and timelines for each engagement.
- The draft plan shall be reviewed and approved by the Committee prior to implementation; any significant revision shall be re-submitted for Committee approval (see also Section 12).

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 appropriate sampling methods to review transactions and controls.

Reporting

- Draft report – prepare a detailed report setting out findings, risks, and recommendations.
- Management review – share the draft with responsible management for review and response.
- Final report – issue a final report incorporating management responses to the Committee.

Follow-Up

- Track and verify implementation of agreed corrective actions (see Section 16).

8. Roles & Responsibilities

Internal Audit

- Conduct audits in accordance with this Charter & Policy and report findings.
- Maintain independence and objectivity throughout the audit process.

Management

- Facilitate the audit process by providing access to information, systems, and resources.
- Implement corrective actions arising from audit recommendations.

Audit & Review Committee

- Approve this Charter & Policy and the annual audit plan.
- Monitor the implementation of audit recommendations and corrective actions, and oversee the independence and quality of the function.

9. 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 prioritisation – focus audit effort on the highest-risk areas, 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, considering both inherent and residual risk and informed by management input, incident reports, and regulatory findings. The results form the basis for the annual Risk-Based Audit Plan. The Internal Audit function shall maintain a Risk Universe covering all auditable entities and update it periodically.

10. Risk Rating Methodology

A standardised risk rating methodology is applied to ensure consistent evaluation and prioritisation across all auditable areas. Each risk is assessed on two dimensions — Impact (the consequence to eNet if the risk materialises) and Likelihood (the probability of occurrence) — each scored on a 1–5 scale:

Score	Impact	Likelihood
1	Insignificant	Rare
2	Minor	Unlikely
3	Moderate	Possible
4	Major	Likely

Score	Impact	Likelihood
5	Critical	Almost Certain

The overall risk rating is calculated as Risk Score = Impact × Likelihood, and categorised as follows:

Score Range	Rating	Action
1 – 5	Low	Monitor under normal procedures
6 – 12	Medium	Include in periodic audit coverage
15 – 25	High	Prioritise in the annual audit plan

Risk rating results are reviewed annually or whenever significant operational or regulatory changes occur. Ratings are approved by Internal Audit and validated with Senior Management before the annual audit plan is finalised. Any significant change in risk profile is reported to the Committee.

11. Audit Frequency

Audit coverage follows a three-tier, risk-based approach:

Risk Tier	Minimum Audit Frequency
High-risk areas	Annually
Medium-risk areas	Every 2 years
Low-risk areas	Every 3 years

12. Communicating the Acceptance of Risk & Plan Changes

Where the Internal Audit Manager concludes that management has accepted a level of risk that may be unacceptable to eNet, the matter shall be discussed with management in the first instance. If it is not resolved, the Internal Audit Manager shall communicate the matter to the Audit & Review Committee for its consideration and decision, in conformance with Standard 11.5 (Communicating the Acceptance of Risks).

Any significant deviation from the approved annual audit plan — whether the deferral, removal, or addition of an engagement — shall be documented in the Audit Plan Change-Control Log and formally approved by the Committee before, or as soon as practicable after, the change takes effect, consistent with Standard 9.4 (Internal Audit Plan).

13. Quality Assurance & Improvement Program (QAIP)

The Internal Audit function maintains a Quality Assurance and Improvement Program covering both internal and external assessments, in conformance with Standard 12 (Enhance Quality), specifically Standards 12.1–12.4. The QAIP is designed to evaluate conformance with the Global Internal Audit Standards and the efficiency and effectiveness of the function, and to identify opportunities for improvement.

Internal assessment

- Ongoing monitoring – supervision and review of engagement working papers, adherence to methodology, and timeliness of reporting, performed as part of day-to-day management of each engagement.
- Periodic self-assessment – a documented internal self-assessment of conformance with the Standards performed at least annually, with results reported to the Committee.

External assessment

An external quality assessment shall be conducted at least once every five years by a qualified, independent assessor or assessment team from outside eNet. As no external assessment has previously been performed, the Internal Audit function shall complete its first external quality assessment no later than 31 December 2031.

The external assessment may take the form of either a full external assessment or a self-assessment with independent external validation (SAIV), as approved by the Committee. The results of every external assessment, including any conformance rating and improvement recommendations, shall be reported to the Committee and to the Board of Directors as appropriate.

14. Internal Audit Strategy

The Internal Audit function maintains a documented strategy that supports the mandate and is aligned with eNet's objectives, in conformance with Standard 9.2 (Internal Audit Strategy). The strategy sets the medium-term direction of the function and is reviewed annually alongside this Charter & Policy. It addresses:

- Vision & objectives – the intended role and value of Internal Audit at eNet over a three-year horizon, aligned to the company's strategic and regulatory priorities as a CBK-licensed payment service provider.
- Capability & resources – the skills, tools, and capacity (including co-sourcing for specialist areas such as IT security or data analytics) required to deliver the audit plan, recognising the function's current single-person structure.
- Methodology & technology – planned enhancements to audit methodology, data analytics, and continuous-monitoring capability.
- Stakeholder & coordination – how Internal Audit coordinates with the external auditors, Compliance, and Risk to provide combined assurance and avoid duplication (Standard 9.5).
- Quality – the roadmap toward the first external quality assessment and ongoing conformance with the Standards.

15. Audit Documentation & 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 authorised personnel only.

16. Follow-Up & Reporting

- **Action tracking** – maintain a log of all audit findings and recommendations.
- **Monitoring** – conduct follow-up audits to confirm corrective actions have been implemented effectively.
- **Reporting** – regularly update senior management and the Committee on the status of follow-up actions.

17. Non-Compliance & 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 in line with company policy.

18. Continuous Improvement

- **Policy review** – regularly review and update this Charter & Policy to reflect changes in regulation, technology, and business operations.
- **Training** – provide ongoing training on emerging risks, new technologies, and best practice, and maintain relevant professional competence.

- **Feedback loop** – incorporate lessons learned from previous audits and from the QAIP into future audit planning.

19. Charter & Policy Review

This Charter & Policy shall be reviewed at least annually, or upon major regulatory or operational change. The Audit & Review Committee must approve all revisions. The Charter component shall additionally be reviewed with the Committee to confirm the mandate, authority, and independence of the function remain appropriate.

20. Approval

By approving below, the signatories confirm that this Internal Audit Charter & Policy is adopted and shall be complied with. The Charter is approved by the Audit & Review Committee.

Name: Jinto Joy Signature:	Name: Jamal Kubeer Signature:	Name: Sabah K. Al Ghunaim Signature:

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Revision History

Version	Date	Author	Summary of Change
2.0	01/10/2025	Internal Audit Manager – Jinto Joy	Prior issue.
3.0	01/11/2025	Internal Audit Manager – Jinto Joy	Policy update; approved by General Manager.
4.0	22/07/2026	Internal Audit Manager – Jinto Joy	Upgraded to a combined Charter & Policy aligned with the IIA Global Internal Audit Standards (2024): added conformance statement, authority/mandate, QAIP, Internal Audit Strategy, and risk-acceptance escalation. Approval routed to the Audit & Review Committee.