شركة شبكة الخدمات الآلية
Automated Services Network Co.

Risk Management Policy

Version: 1.8

Dated 25/10/2026

Approved by

Sabah K. Al Ghunaim
Chairman

Contents

Policy Statement 3
Purpose 3
Definition: 4
Risk Taxonomy and Cross-Reference 5
Risk Analysis Main Issues 6
Risk Management Policy Scope 14
Objectives 14
Alignment With eNet's Mission and Values 15
Background/Context 15
Policy Position 15
Risk Management Framework and Process 15
- Identification and the Risk Register 15
- Assessment Scale 15
- Risk Appetite, Tolerance, and Limits 16
- Risk Treatment 16
- Risk Exceptions 16
- Monitoring and Assurance 16
- New Products, Services, and Material Changes 17
- Models 17
- Stress Testing, Concentration, and Resilience 17
- Reporting 17

Related Governance Documents 18
Review 19
Document Control 20
Approval of the Risk Management Policy 21

Policy Statement

Automated Services Network Company, eNet is committed to effective Risk Management as a strategy for protecting the organization, board, employees, workers, clients, stakeholders, and the community from unnecessary injury, loss or damage related to the business and activities the organization undertakes.

Purpose

The primary purpose of this policy is to promote an integrated, holistic approach to company risk management and to ensure that all risks that could affect the achievement of our objectives are identified, assessed, and treated to an acceptable level. The embedding of the Risk Management Framework into strategic and operational processes supports the company to make informed decisions.

This policy aims to provide guidance to the organization in applying risk management processes across the organization's operations, to ensure that, so far as reasonably practicable, the organization's goal and identified outcome areas that can be achieved.

This policy encompasses but is not limited to:

- Identifying, assessing, and managing risks
- Ongoing risk monitoring and review
- Communication and consultation
- Record-keeping
- Specific risk areas.

Risk is made up of two parts: the probability of something going wrong, and the negative consequences if it does. Risk can be hard to spot, let alone to prepare for and manage. And, if you're hit by a consequence that you hadn't planned for, costs, time, and reputations could be on the line. Similarly, overestimating or overreacting to risks can create panic and do more harm than good.

This makes Risk Analysis an essential tool. It helps identify the risks that eNet could face. In turn, this helps eNet to manage these risks and minimize their impact on implemented plans.

By approaching risk in a logical manner, eNet can identify what can and cannot be controlled and tackle potential problems with measured and appropriate action. This can then help to alleviate feelings of stress and anxiety, both in and outside of the work environment.

Definition:

Organization	Automated Services Network Company, eNet
Board	Means the organization's Board of Directors
AML Law	The Law 106/2013
CBK Regulations	CBK Circular No. (2/BS, IBS, FS, IFS, ES, PS/524/2023) and any relevant instructions.
Activity	Electronic Money (E-money)
Electronic Money (eMoney)	A value that has cash equivalent stored in an electronic payment instrument and accepted for payment transactions from a party other than the E-money issuer.
Customer	The natural or legal person who is a beneficiary of the provided Activity.
Payer	A customer who performs or approves the E-Payment order to transfer funds.
Payee	A customer who receives funds of an E-Payment transaction.
Payment Order	Instructions to the Activity service provider to process a payment transaction and can be issued on behalf of the payer or the payee.
Payment Transaction	A procedure that results in depositing, transferring, or withdrawing money by virtue of the payment order.
Buy Now Pay Later (BNPL)	A payment service for individuals for the purpose of purchasing consumer goods and paying for them later through a payment transaction performed by any of the electronic payment methods for the merchant.
Compliance Register	A register that assists an organization to comply with its legal obligations
Impact	Actual or potential impact that would or may occur
Likelihood	Probability or chance of an incident occurring
Personnel	The organization's staff, workers, Board members and visitors
Risk	Chance of something happening that will Impact on objectives, measured in terms of likelihood and impact
Risk Assessment	Process of analyzing and evaluating the likelihood and impact of potential risks
Risk Incident	Realization or occurrence of a risk impact
Risk Management	Process of identifying, assessing, and judging risks, assigning ownership, taking actions to mitigate them, and monitoring and reviewing progress
Risk Register	A Risk Register is a tool for documenting risks, and actions to manage each risk. The risk register is essential to the successful management of risk. As risks are identified they are logged on the register and actions are taken to respond to the risk
Risk Treatment	Identifying and implementing actions to eliminate risks or reduce impacts
Inherent Risk	The level of risk before taking account of existing controls.
Residual Risk	The level of risk remaining after existing controls; compared with the Risk Appetite Statement to decide whether a risk is within or outside appetite.

Risk Appetite	The level and type of risk the Board is willing to accept in pursuit of its objectives, as set out in the Risk Appetite Statement (RAS).
Risk Tolerance	The acceptable deviation around the approved appetite for a risk category, monitored through limits and key risk indicators.
Risk Capacity	The maximum level of risk the Company can bear without breaching regulatory capital, liquidity, or other legal requirements.
Key Risk Indicator (KRI)	A quantitative or qualitative measure with Green / Amber / Red thresholds that gives early warning of increasing risk exposure.
Risk Owner	The role accountable for managing a risk and its controls, normally the head of the department concerned.
Near Miss	An event that could have caused loss or harm but did not; recorded without a loss amount.

The Impact and Likelihood ratings defined above are formally applied through the quantitative scoring methodologies set out in the Risk Assessment and Risk Scoring for Business Sectors & Limits policy and the Key Risk Indicators (KRI) Framework, which are the Company's official reference methodologies for translating these definitions into Low/Medium/High risk classifications, RAG thresholds, and escalation triggers.

Risk Taxonomy and Cross-Reference

To keep the Risk Register, the Risk Appetite Statement (RAS), and the KRI Framework consistent, risks are classified under ten risk categories. The Risk Register category is the master classification; each category is mapped below to the section of this Policy that describes it, the corresponding RAS category, and the KRI pillar that monitors it.

Risk Register category	Covered in this Policy under	RAS category	KRI pillar	Owner function
1. Operational	Operational Risks; Transactional Risks; Payment Conflict Risk; Business Continuity Risks	Operational – IT Outage; Operational – Continuous Development; Business Continuity	Pillar 1 (Payment Operations); Pillar 4 (Business Continuity)	Operations / IT
2. Financial	Market Risk; Credit Risk; Financial or Other Business Risks	Credit Risk (RAS v1.6); Market Competition & Societal Change	Pillar 2 – Financial Risk	Finance
3. Liquidity	Liquidity Risks	Liquidity Risk	Pillar 3 – Liquidity Risk	Finance
4. IT / Cyber	Cybersecurity Risks; Security Risk	Operational – Cybersecurity; Information Management	Pillar 4 – IT & Cyber Risk	IT / Information Security Officer
5. AML/CFT	AML/CFT Risks (including CPF/WMD)	Compliance / AML-CFT	Pillar 1 (Compliance, AML/CFT Reporting, Customer & Merchant Due Diligence, Compliance Training)	Compliance
6. Fraud	Fraud Risks	Fraud & Corruption	Pillar 1 (Fraud Risk)	Compliance

7. Legal	Legal Risks (including regulatory directives)	Legal Risk	Pillar 1 (Compliance Risk; Regulatory Engagement)	Legal / Compliance
8. Third-party	Third-Party Risks; Related Party & Intra-Group Risks	Third-Party Risk	Pillar 1 (Vendor Risk)	Process owners (TPRM owner to be confirmed)
9. Strategic	Policy Statement; Alignment With eNet's Mission and Values	Strategic Risk	Pillar 2 (Revenue Risk)	General Manager / Board
10. Reputational	Reputational Risks	Reputational Risk	Pillar 1 (Reputation Risk)	Marketing / Compliance

Merchant risk scoring under the Risk Assessment and Risk Scoring for Business Sectors & Limits policy is a separate customer-risk methodology (Low / Medium / High) and does not replace the enterprise risk rating set out in this Policy.

Risk Analysis Main Issues

Within the dynamic landscape of electronic payment operations, our business encounters an array of challenges that demand meticulous attention and strategic management. In this section, we delve into the multifaceted risks that shape our industry. These risks span operational intricacies, legal considerations, reputational concerns, and the ever-evolving realm of cybersecurity.

We have designed a comprehensive guide, outlining our approach to identifying, assessing, and mitigating these risks, taking into consideration the Central Bank of Kuwait's guidelines and Regulation **No. (2/BS, IBS, FS, IFS, ES, PS/524/2023) and** relevant local regulations, and adhering to the best standard practices in the industry.

Operational Risks:

Operational risks in the context of electronic payments refer to challenges in the day-to-day functioning of systems and processes. Mitigation strategies for operational risks may include:

- **Continuous Monitoring:** Implement systems for continuous monitoring of transaction patterns and system performance to quickly identify irregularities.
- **Employee Training:** Conduct regular training sessions for employees to enhance their awareness of operational risks and equip them with the skills to respond effectively.
- **Multi-Factor Authentication (MFA):** Utilize multi-factor authentication mechanisms, especially for sensitive transactions, to add an extra layer of security.

Penetration Testing: Conduct routine penetration testing and vulnerability assessments to proactively identify and address potential weaknesses in the system

Market Risk

The risks arising from changes in market prices and fluctuations in the capital market or because of economic, social or political reasons in the country or in other countries, and may include risks such as recession, political turmoil and changes in interest rates.

These risks generally do not significantly affect the company's core electronic payment operations, as the Company primarily collects corporate and e-commerce dues and its transactions are local. The exception is the BNPL/eFlex product line, which carries a distinct market/credit sensitivity addressed under Credit Risk below and in the Risk Appetite Statement.

Market disruption may otherwise impact the number of executed transactions or result in the loss of a single service provider or several participating service providers.

Fraud Risks:

Fraud risks are a significant concern in electronic payment operations, and addressing them requires a multi-faceted approach:

- **Transaction Verification:** Implement robust transaction verification processes to ensure the legitimacy of each transaction and promptly identify any fraudulent activities.
- **Fraud Detection Systems:** Deploy advanced fraud detection systems that use machine learning algorithms to analyze transaction patterns and detect anomalies indicative of fraudulent behavior.

Measures taken:

We set fraud management filters to suit our business needs. High-risk transactions, pending review, or approved but reported for our attention are rejected. These filters include:

- The maximum number of transactions per day and per month
- Determining the number of daily and monthly transactions
- COUNTRY OF ORIGIN — Payments from countries assessed as high-risk. This filter shall apply the Geographic Risk methodology defined in the Risk Assessment and Risk Scoring for Business Sectors & Limits policy, and shall be operationalized through the Geographic Anomaly and Risk detection scenario in the Risk Assessment and Management Policy for AML/CFT/WMD (Section 5.1).
- Ensure that the 3D secure system is used on the electronic payment gateway

Merchant categories designated as Prohibited in the KYC Procedures for Merchant-Onboarding are not onboarded (Onboarding Denied); the Prohibited Sectors list in those Procedures is the governing reference for this control.

Confirmed fraud, whether internal or external, carries zero appetite under the Risk Appetite Statement. Every suspected case shall be reported immediately, an investigation shall be opened within five days, and the outcome escalated in line with the Corporate Fraud Policy (eNet-POL-FRD-001) and the KRI Framework.

Cybersecurity Risks:

Cybersecurity risks pose threats to the confidentiality, integrity, and availability of electronic payment systems. Key strategies to mitigate cybersecurity risks include:

- **Regular Security Audits:** Conduct regular security audits to identify vulnerabilities and ensure that security measures are up-to-date and effective.
- **Employee Awareness:** Train employees on cybersecurity best practices, emphasizing the importance of strong password management, secure Wi-Fi usage, and recognizing phishing attempts.
- **Incident Response Plan:** Develop a robust incident response plan to guide the organization in the event of a cybersecurity breach, outlining steps for containment, investigation, and recovery.

Data Encryption: Implement strong data encryption mechanisms to protect sensitive customer information during transmission and storage

Legal Risks:

Legal risks in electronic payment operations require a strong compliance framework and clear contractual agreements. Mitigation strategies may include:

- **PCI DSS Compliance:** Adhere to Payment Card Industry Data Security Standard (PCI DSS) to ensure secure handling of cardholder information.
- **Data Protection Compliance:** Ensure compliance with local and international data protection laws, with regular assessments to adapt to evolving regulations.
- **Legal Reviews:** Conduct periodic legal reviews to stay informed about changes in regulations and ensure ongoing compliance.
- **Contractual Clarity:** Clearly document contractual obligations with customers and partners to mitigate legal uncertainties.
- **Regulatory Directive Tracking:** All circulars, instructions, and directives issued by the Central Bank of Kuwait, together with their implementation deadlines and responsible owners, shall be recorded in a regulatory register maintained by the Compliance function. Overdue or unimplemented directives shall be escalated to the Risk Management Committee and tracked as risks until closure.
- **Pricing and Fee Approvals:** Any new fee, commission, or pricing structure applied to payment services shall be confirmed as approved by the Central Bank of Kuwait, where such approval is required, before it is applied to customers or merchants.
- **CBK Examinations:** Each CBK examination, information request, and remediation commitment is recorded with an owner and due date and tracked to closure. Requests answered beyond the deadline and overdue remediation actions are monitored as KRIs and reported to the Risk Management Committee.

Reputational Risks:

Maintaining a positive reputation is crucial for success in the electronic payments sector. Mitigation strategies may include:

- **Rapid Response Plan:** Develop a rapid response plan for addressing and communicating security incidents promptly.
- **Proactive Communication:** Proactively communicate security measures to customers to build trust and confidence.
- **Customer Feedback Integration:** Integrate customer feedback and satisfaction surveys to gauge and enhance reputation.
- **Social Media Monitoring:** Regularly monitor social media channels to assess public perception and address concerns.

The Company's Cashless product carries a distinct reputational sensitivity, given that its end beneficiaries are underprivileged families referred by charitable associations. Any service disruption, beneficiary-screening failure, or public perception issue affecting this product line is treated as an elevated reputational risk, and is escalated and reviewed under the beneficiary screening and NPO due diligence procedures set out in the Risk Assessment and Management Policy for AML/CFT/WMD and the KYC Procedures for Merchant-Onboarding.

Customer and merchant complaints shall be recorded with the date of receipt, the response, and resolution details, and reviewed by Compliance; trends are reported to the Risk Management Committee.

AML/CFT Risks:

Anti-Money Laundering, Counter-Financing of Terrorism, and Counter-Proliferation Financing (AML/CFT/CPF) risk; including product-specific risk factors for the Company's eFlex (BNPL) and Cashless product lines is identified, assessed, and managed in accordance with the Risk Assessment and Management Policy for AML/CFT/WMD, which is owned and maintained by the Compliance function under Law No. 106 of 2013 and applicable Central Bank of Kuwait instructions.

That policy sets out the governing methodology, customer due diligence measures, transaction monitoring scenarios, sanctions/PEP screening, staff training requirements, and regulatory reporting obligations. Risk Management incorporates the outcome of the Compliance function's AML/CFT/CPF risk assessment, including the applicable Key Risk Indicators and Risk Appetite thresholds, into the enterprise-wide risk register and reporting cycle, and escalates any material AML/CFT/CPF risk to the Risk Management Committee consistent with this Policy's escalation principles.

Liquidity Risks:

Effectively managing liquidity risks in electronic payments involves strategic planning and monitoring. Mitigation strategies may include:

- **Stress Testing:** Conduct stress testing of systems and processes to assess their capacity during peak transaction periods.
- **Liquidity Reserves:** Establish liquidity reserves to cover potential surges in transaction volume or unforeseen circumstances.
- **Settlement Process Management**: Monitor and manage settlement processes to ensure timely and efficient transactions.
- **Regular Reviews:** Conduct regular reviews of liquidity requirements based on business growth and market dynamics.

Liquidity is monitored against the thresholds in the RAS and the KRI Framework. The daily cash reserve against the CBK minimum requirement is a Priority Watch indicator: any shortfall is escalated the same day to the Head of Risk Management and the CEO.

Third-Party Risks:

Effectively managing risks associated with third-party partnerships requires thorough due diligence and clear contractual agreements. Strategies may include:

Third-party risk classification, due diligence, contractual requirements, and ongoing monitoring are governed by the Third-Party Risk Management Policy. Vendor sanctions screening and related AML/CFT due diligence are set out in the Compliance function's Anti-Money Laundering Policy and Procedures. This Policy incorporates the outcome of these assessments into the enterprise-wide risk register.

Critical vendors shall have a documented exit strategy. Where two or more registered risks depend on the same vendor or merchant, the concentration is reported to the Risk Management Committee.

- **Due Diligence**: Conduct thorough due diligence before entering into partnerships with third parties.
- **Security Audits:** Perform regular audits and assessments of third-party security measures to ensure alignment with industry standards.
- **Clear Contracts:** Establish clear contractual agreements outlining responsibilities, liabilities, and dispute resolution mechanisms.
- **Contingency Planning**: Develop contingency plans to address potential failures or disruptions from third-party partners.

Related Party & Intra-Group Risks:

Transactions, shared services, and staff secondments between eNet and its related parties (including eNet Integrated Solutions Co.) carry governance, conflict-of-interest, and operational-independence risks. These are governed by the Related Party Transactions provisions of the Third-Party Risk Management Policy (Section 14), under which each related-party arrangement is identified, independently reviewed by the Risk/Audit Committee, priced on arm's-length terms, and recorded in the Related Party Register. Where the Central Bank of Kuwait requires organizational or operational separation between eNet and a related party, Risk Management shall track implementation of the required separation as a risk treatment action and report its status to the Risk Management Committee until closure; documenting a related-party arrangement does not, by itself, satisfy a separation requirement.

Business Continuity Risks:

Mitigating business continuity risks involves thorough planning and preparation. Strategies may include:

- **Testing Plans:** Regularly test business continuity and disaster recovery plans to ensure they are effective and up to date.
- **Redundancy Mechanisms:** Implement redundancy and failover mechanisms for critical systems to minimize downtime.
- **Cross-Training:** Cross-train employees to ensure key functions can continue during disruptions or the absence of key personnel.
- **Supplier Collaboration:** Collaborate with key suppliers to ensure alignment with their business continuity plans and maintain a resilient supply chain.

Business continuity and disaster-recovery plans are tested against defined recovery time and recovery point objectives, and the results, including any failed test, are reported to the Risk Management Committee. Recovery tolerances are set in the Risk Appetite Statement.

Financial or Other Business Risks Related to the Activity:

Understanding and mitigating financial risks is crucial for sustained business success. Strategies may include:

- **Market Trend Analysis:** Regularly analyze market trends to anticipate changes in customer behavior and technological advancements.
- **Financial Audits:** Conduct regular financial audits and reviews to identify potential risks and ensure financial stability.
- **Diversification**: Diversify revenue streams to mitigate dependence on a single source and adapt to changing market conditions.
- **Scenario Planning**: Engage in scenario planning to anticipate and prepare for economic uncertainties, regulatory changes, or other external factors

Credit Risk

The Company is exposed to credit risk through its Buy Now, Pay Later (BNPL/eFlex) product, which extends consumer credit and is therefore subject to customer default and merchant-concentration risk. This exposure is assessed and managed in accordance with the Risk Appetite Statement (Credit Risk category and Section 9, eFlex Risk Appetite), which sets the applicable individual exposure limits, merchant-concentration thresholds, and default hard stops, and is monitored through the credit-quality indicators in the Key Risk Indicators (KRI) Framework. Outside of BNPL/eFlex, the Company does not carry out other lending or borrowing activities.

The BNPL credit-scoring engine is a model subject to the model-risk requirements in the Risk Management Framework and Process section of this Policy. [References above to RAS Section 9 apply once RAS v1.6 is approved; until then the Credit Risk limits are those in the approved RAS — confirm the version in force.]

Payment Conflict Risk:

One of the characteristics of electronic payment systems is that payments are not processed by humans but by an automated electronic system. The system is prone to errors, particularly when it has to deal with large amounts of payments on a recurring basis with multiple beneficiaries involved.

Measures taken:

- Special software has been developed to ensure the integrity of the information and the absence of defects.
- The system is constantly checked to avoid payment conflicts resulting from technical glitches or irregularities. Where the employee in charge of the information systems reviews the alerts of the system daily.

For the eFlex (BNPL) product specifically, payment-processing risk factors, including third-party settlement inconsistent with the registered customer, abnormal repayment patterns, and installment-related processing anomalies — are assessed under the eFlex-specific risk evaluation in Section 3.2.1 of the Risk Assessment and Management Policy for AML/CFT/WMD, and shall be monitored through the eFlex-specific transaction monitoring scenarios in Section 5.1 of that policy as those scenarios are activated in the transaction monitoring system.

Security Risk

With the increasing number of electronic payment transactions, there are new opportunities for cybercriminals who pose a significant threat to business.

Measures taken:

We put in place some rules, procedures, and tools to ensure that we provide secure transactions and that our customers do not have to worry about their data. Therefore, we secure the following:

- **Network security:** This includes using firewalls and building a security policy
- **System security:** This includes updating operating systems, using antivirus software.
- **Data security:** This includes data encryption, encrypting passwords and important data in storage.
- **Transaction security:** This includes securing transactions using the SSL protocol to send data
- **Cyber Security:** Securing protection for the network from attacks and intrusions by conducting special tests

In addition, the company also relies on educating its customers from time to time to protect themselves from exposure to fraud through its social media channels, including:

- Not to disclose the payment cards information to anyone
- Change the payment card periodically
- Ensure that there are no counterfeit devices in the ATMs
- Use of prepaid cards only, especially while traveling
- Do not photograph mobile payment cards
- Providing text messaging service for payment cards verification

Transactional Risks

Companies are exposed to transactional risks that may result in the potential for loss resulting from inadequate or failed procedures, systems, or policies. And it may include employee errors or systems failure, as well as cases of fraud or any other criminal activity or any event that disrupts business operation or process.

Measures taken:

- Periodically evaluate the procedures and policies taken by the company
- Extensive testing of the company's systems before they are released to avoid any errors
- Implementing a strict measures for controlling the use of the company's systems and users' permissions
- Develop contingency plans to ensure business continuity

Other measures taken to protect the activity and contingency to ensure business continuity

The company hosts all its applications locally at its headquarters in Kuwait City. It has a fiber optic cable that connects its data center with other service providers. eNet applies the following measures to maintain the security and availability of its services; any control gaps identified through risk assessments, audits, or testing are recorded in the Risk Register and tracked to remediation. [IT to confirm that the measures below are current as at the date of approval.] The following levels of security are applied:

Network Security: Our network is the most important part of our business, which is why it is imperative to maintain and operate 24/7. To maintain this, we apply the following measures:

- The network is secured by a Firewall. Internal and external traffic is monitored, and firewall security policies established by the network administrator are followed.
- All communications with service providers are established using VPN tunnels to secure data
- Monitoring applications are running all the time to check communication with different parties and between servers and database

Web Application Security: The web servers are using Windows Server 2022 and 2019 version. All our applications are built using Microsoft .NET. The following protocols are mainly used:

- SFTP - for Secure File Transfer Protocol and provides an extra layer of protection. SFTP closes any vulnerability during file transfer.
- SSL - SSL stands for Secure Socket Layer. SSL provides an encrypted path between the browser and the web server. This will help prevent customer information theft and protect the payment process.
- The applications that require the authentication process (Login) are secured with a username and password, and all passwords that are stored in the database are encrypted.

Risk Management Policy Scope

This policy applies to all employees, merchants, distributers, and anyone in relation to eNet's activities and outlines the expectations and processes for managing risk

Objectives

The key objectives of our risk management are to:

- Develop and embed a culture of effective risk management by taking a systems approach to integrating risk management.
- Provide the business with appropriate tools to support risk decision making and management reporting by providing mechanisms for employees to assess, prioritize, manage and monitor all material risks in a consistent and effective manner.
- Facilitate the achievement of strategic, operational and project objectives and priorities by reducing threats and maximizing opportunities.
- Provide assurances that critical risks are being managed effectively.

Alignment With eNet's Mission and Values

eNet continues to build upon its culture of risk management as an integral part of corporate governance and operations, developing strategies and systems to minimize risks. The identification and management of risk will continue to be undertaken in a systematic process, implementing the principles set out.

Background/Context

Company maintains a strong culture of risk management practices and is working towards developing a consistent and systemic process across the company.

Policy Position

eNet is committed to embedding enterprise risk management to create and maintain an environment that enables eNet to deliver high quality services. To meet this commitment, risk management is every employee's responsibility.

Risk Management Framework and Process

This section sets the common process that every department follows. Detailed thresholds and limits are held in the Risk Appetite Statement and the KRI Framework; this Policy does not restate them.

Identification and the Risk Register

All risks are recorded in the central Risk Register maintained in the Company's GRC platform, which is the system of record. Each entry shall have a risk category (see Risk Taxonomy), an owner identified by role, inherent and residual ratings, linked controls, and a review date. Risks are reviewed at least quarterly, and whenever a new product, regulatory change, incident, or audit finding affects them. Access follows need-to-know: a department head sees only the risks of their own department, and changes to risk records are kept in an audit trail.

Assessment Scale

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

Risk score = Likelihood × Impact (1–25). Rating bands: Low 1–5; Medium 6–10; High 11–15; Critical 16–25. The inherent rating is assessed before controls and the residual rating after existing controls; the residual rating is compared with the RAS to decide whether the risk is within or outside appetite.

Risk Appetite, Tolerance, and Limits

The Board sets risk appetite through the RAS, which distinguishes risk capacity, risk appetite, risk tolerance, and risk limits. Zero appetite applies to fraud and corruption and to money laundering and terrorist financing. Residual risks outside appetite, and any breach of a RAS limit or hard stop, are escalated to the Risk Management Committee and the Board in accordance with the RAS and the KRI Framework escalation matrix.

Risk Treatment

Each High or Critical residual risk, and each risk outside appetite, requires a treatment decision: Accept, Mitigate, Transfer, or Avoid. Mitigate, Transfer, and Avoid decisions need a named owner and a target completion date; Accept decisions need a documented rationale and are re-examined at the next register review. The person who proposes a treatment decision cannot approve it. A Transfer decision is valid only while an insurance policy or contractual transfer is in force. Approval authority follows the Delegation of Authority Matrix [proposed: Low — risk owner with Risk Management review; Medium — department head with Risk Officer concurrence; High and Critical — General Manager and Risk Management Committee; outside appetite — Board].

Risk Exceptions

Deviations from an approved policy, procedure, risk appetite threshold, or control requirement are permitted only as formally approved exceptions recorded in the Exception Register. No exception is permanent; every exception has an expiry date; renewal is a new approval, not a date extension; and the approval level rises with the risk rating and duration of the exception. The register is owned by Risk Management [owner to be confirmed] and reported to Internal Audit.

Monitoring and Assurance

- **Key risk indicators:** KRIs with Green / Amber / Red thresholds are defined in the KRI Framework, linked to registered risks, and reported monthly. Indicators designated "Priority Watch" (CBK regulatory violations, confirmed fraud, core infrastructure availability below threshold, cash reserve below the CBK minimum, cybersecurity incidents, and settlement failures) trigger same-day escalation to the Head of Risk Management and the CEO [subject to the KRI Framework being updated to include them].
- **Control assurance:** Each department periodically assesses its key controls through Risk and Control Self-Assessment (RCSA), reviewed by someone other than the assessor. A control's effectiveness rating shall rest on a test of design performed before a test of operating effectiveness.
- **Loss and near-miss events:** Loss events and near misses are recorded in a Loss Event Register using the Basel operational-risk event categories and linked to the Risk Register. A near miss carries no loss amount, and events not linked to a registered risk are reported as findings.
- **Findings:** Findings from Internal Audit, external audit, and CBK examinations are entered in the register with owners and due dates and tracked to closure.

New Products, Services, and Material Changes

No new product, service, or material change to an existing one (including a new merchant category, credit product, or wallet type) may be launched before a New Product Approval (NPA) risk assessment covers seven dimensions; Credit, Operational, Compliance/AML-CFT, Technology/Cyber, Reputational, Legal/Regulatory, and Liquidity/Financial — and is signed off by Risk Management, Compliance, Finance, IT/Security, and the Business Owner. A rejection by any signatory means the product is not approved.

Models

Models that drive customer, credit, fraud, or AML decisions (including the BNPL credit-scoring engine and transaction-monitoring scenarios) shall be recorded in a model register, independently validated by someone other than the model owner, monitored for performance drift against back-test results, and changed in production only after the approval required by the Delegation of Authority Matrix.

Stress Testing, Concentration, and Resilience

- **Scenario analysis:** Stress tests are performed at least annually, and each scenario links at least two registered risks.
- **Concentration:** Where two or more registered risks depend on the same vendor or merchant, the concentration is reported to the Risk Management Committee.
- **Capital adequacy:** Assessed annually against the audited financial statements, in addition to the monthly capital KRI.
- **Business continuity:** Plans are tested against defined recovery time and recovery point objectives, with pass/fail results reported to the Risk Management Committee.

Reporting

Risk Management reports: a monthly KRI dashboard to the Risk Management Committee; a quarterly risk and KRI report to the Board (Board Risk Committee); and an aggregated, anonymised whistleblowing report to the Audit Committee. Material events are escalated immediately in line with the KRI Framework escalation matrix.

Roles And Responsibilities

In our commitment to effective enterprise risk management, each stakeholder contributes to upholding the integrity and effectiveness of our risk management processes:

Risk Management Department: As the primary custodian of this Risk Management Policy, the Risk Management Department oversees its development and periodic review, ensuring alignment with organizational goals and with the Company's Risk Appetite Statement and Key Risk Indicators (KRI) Framework.

This department is responsible for identifying, assessing, and coordinating the mitigation of enterprise-wide risks, maintaining the Risk Register, aggregating risk assessments produced by specialist functions (including the Compliance function's AML/CFT/CPF risk assessment), and escalating material risks to the Risk Management Committee. The Risk Management Department is responsible for seeking Risk Committee and Board of Directors approval of this Policy and any material amendments.

Department Heads/Managers: At the departmental level, our leaders work collaboratively with the Risk Management Department. They translate enterprise-wide risk guidance into actionable steps for their teams, maintain their department's risk register entries, communicate policy updates, reinforce compliance with the Company's risk appetite, and escalate department-specific risks in a timely manner.

Employees: Every employee plays a vital role in translating this Policy into practice. Active participation in risk-awareness training is paramount, ensuring that each team member can identify, escalate, and help mitigate the risks relevant to their role.

Three Lines: Risk ownership follows the Three Lines Model. First line: department heads, process owners, and employees own and manage risks and controls. Second line: Risk Management, Compliance, and the Information Security Officer set frameworks, monitor, and challenge. Third line: Internal Audit provides independent assurance.

Board of Directors / Board Risk Committee: Approves this Policy and the RAS and its limits, reviews the quarterly KRI and risk report, and decides on risks outside appetite [confirm whether a Board Risk Committee exists; otherwise the Board].

Risk Management Committee: Reviews the monthly KRI dashboard and the Risk Register, approves corrective action plans and exceptions within its delegated authority, and escalates material breaches to the Board.

Compliance Function (including the MLRO): Owns AML/CFT/CPF risk assessment and the regulatory register, and provides independent challenge on compliance risk. The MLRO's reporting decisions are not subject to approval by business management.

Information Security Officer: Owns IT and cyber risk assessment and the related KRIs, independent of IT operations.

Internal Audit: Provides independent third-line assurance to the Board and Audit Committee. Audit findings are entered in the Risk Register, and Internal Audit is neither a risk owner nor an approver.

Collectively, these roles, led by the Risk Management Department, form a cohesive risk management structure. Through collaboration and a shared commitment to sound risk governance, the Company strengthens its ability to navigate the complexities of electronic payment operations.

Related Governance Documents

This Policy sets the Company's overarching risk management framework and governance principles. Detailed methodology, quantitative thresholds, and operational procedures for specific risk domains are set out in the following subordinate governance documents, which this Policy incorporates by reference:

Document	Owner	Role
Risk Assessment and Management Policy for AML/CFT/WMD	Compliance	Governing policy and procedures for AML/CFT and counter-proliferation financing (CPF/WMD) risk, including product-specific risk evaluations (eFlex/BNPL, Cashless) and beneficiary/merchant screening procedures.

KYC Procedures for Merchant-Onboarding	Compliance	Operational onboarding procedures for merchants, including risk profiling factors, the Prohibited Sectors list, and product-specific merchant due diligence (dual-use goods, eFlex-accepting merchants, charitable associations).
Third-Party Risk Management Policy	Risk Management	Governs third-party risk classification, due diligence, contractual requirements, and monitoring, and the identification, independent review, arm's-length pricing, and registration of related-party arrangements.
Risk Appetite Statement (RAS)	Risk Management	Defines Board-approved risk capacity, appetite, tolerance, and limits across all risk categories, including eFlex/BNPL credit risk and merchant concentration limits.
Key Risk Indicators (KRI) Framework	Risk Management	Defines the quantitative early-warning indicators, RAG thresholds, and escalation matrix used to monitor risk across all pillars (Operational, Financial, Liquidity, IT & Cybersecurity).
Risk Assessment and Risk Scoring for Business Sectors & Limits	Risk Management	Defines the sector-level risk scoring methodology and the merchant transaction limits used in merchant risk classification.
MCC Risk Scoring	Risk Management	Operational register mapping individual Merchant Category Codes (MCC) to sector-level risk scores for day-to-day merchant classification.
Code of Conduct & Whistleblowing Policy	Compliance	Standards of conduct, conflict-of-interest and anti-bribery rules, and the protected whistleblowing framework (reporting channels, non-retaliation, case handling).
Corporate Fraud Policy	Compliance	Governs fraud definitions, investigation, and sanctions; referenced by the Code of Conduct & Whistleblowing Policy.

In the event of any inconsistency between this Policy and a subordinate document listed above regarding domain-specific methodology or operational detail, the subordinate document's owning function is the authoritative source for that domain, and this Policy is updated to reflect it at the next scheduled review. Documents shown above as pending approval take effect only upon formal approval and, until then, do not take precedence over this Policy or any approved document.

Review

This Policy is reviewed annually, at minimum, or upon any material change to the Company's risk profile, regulatory environment, or product suite, consistent with the review cycle applied to the Company's Risk Appetite Statement, KRI Framework, and other subordinate risk governance documents. In reviewing, these points need to be considered:

- Are the objectives still relevant and appropriate?
- Are the objectives being met to successfully manage Company's risk?
- Has there been any significant changes to the operating conditions?
- Has there been any changes to our risk maturity which should be reflected in this framework.

Document Control

Field	Detail
Document Title	Risk Management Policy — Automated Services Network Company (eNet)
Version	→ 1.7 (proposed update)
Status	Draft — pending Risk Management Committee review and Board of Directors approval
Classification	CONFIDENTIAL — Internal Use Only
Prepared By	Risk Management Department
Reviewed By	Risk Management Committee
Approved By	Chairman
Regulatory Basis	Law No. (106) of 2013; CBK Circular No. (2/BS, IBS, FS, IFS, ES, PS/524/2023) and any relevant instructions; ISO 31000:2018
Review Frequency	Annually, at minimum, or upon any material change
Next Review Date	1/11/2027

Approval of the Risk Management Policy

WHEREAS, the Committee has scrutinized the updated Risk Management policy and its alignment with the current strategic objectives;

WHEREAS, the Committee has benchmarked the Policy against prevailing regulatory requirements and found it to be robust;

IT IS HEREBY RESOLVED that the Risk Management Policy V 1.8 is approved for immediate submission to the Board of Directors for final ratification.

Dated: 20/10/2026

POSITION	NAME	SIGNATURE
Chairman	Sabah K. Al Ghunaim	
Board Member 1	Lamiaa K. Al Kharafi	
Board Member 2	Khaled Al Ghunaim	
General Manager	Jamal Kubeer	
Admin &HR Manager	Nesrine Zakaria	
Sales & Marketing Manager	Afif Moukahel	
Compliance Officer	Michael Basily	
Finance Manager	Abdul Rahman El Rotel	

Risk Department Verification:

Prepared and verified by	Elsayed Thabet
Signature	
Date	20/10/2026