شركة شبكة الخدمات الآلية
Automated Services Network Co.

Risk Management Policy

Version: 1.7

Date: 22-10-2025

Approved by

Sabah K. Al Ghunaim

Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

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, however, 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 to 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 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 transaction 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

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 the regulations No. (2/BS, IBS, FS, IFS, ES, PS/524/2023), 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, as the company collects corporate and e-commerce dues and does not work in areas such as buying shares, lending, or investing and its transactions are local, but may have an impact on reducing the number of executed transactions or a single service provider loss or most of the 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. Transactions that are high-risk, pending for review, or approved but reported for our attention are rejected. These filters include:

- The maximum amount of transactions per day and per month
- Determining the number of daily and monthly transactions
- COUNTRY OF ORIGIN - Payments from countries that we believe pose a business risk, like Syria, Jordan, Egypt, Turkey, Egypt, Georgia and Morocco.
- Ensure that the 3D secure system is used on the electronic payment gateway

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.

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.

AML/CFT Risks:

Considering the law 106/2013 of the state od Kuwait, Mitigating Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) risks requires stringent measures. Strategies includes:

- Customer Due Diligence: Implement robust customer due diligence processes to identify and verify customer information by adding authentication through the Civil ID to verify the customer's identity and linking the phone number to the Civil ID.
- Transaction Monitoring: Continuously monitor transactions for unusual patterns or amounts that may indicate money laundering or terrorist financing.
- Staff Training: Conduct regular staff training on recognizing and reporting suspicious activities to regulatory authorities.

Regulatory Collaboration: Collaborate with regulatory bodies to stay updated on AML/CFT regulations and ensure compliance

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.

Third-Party Risks:

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

- 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.

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.

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 does not carry out any financial transactions, including lending or borrowing, and therefore it is not exposed to these risks

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.

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 and **Blocking Proxy Usage: where any transaction executed using any type of location-masking tools or from outside the State of Kuwait will be rejected.**
- 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 taken measures 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 uses best practices to maintain its security and availability of its services. eNet uses the following levels of security:

Network Security: Our network is the most important part of our business, which is why it is imperative to maintain and operates 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

Risk Criteria Definitions

To ensure consistency and transparency in risk assessments, the company adopts a unified risk matrix based on two dimensions: **Likelihood** and **Impact**.

1. Likelihood Scale

Level	Rating	Definition	Expected Frequency
1	Rare	Event is highly unlikely to occur	Less than once in 5 years
2	Unlikely	Could occur under exceptional circumstances	Once every 2–5 years
3	Possible	Might occur at some point	Once per year
4	Likely	Expected to occur in many circumstances	Several times per year

5	Almost Certain	Expected to occur frequently	More than once per month

2. Impact Scale

Level	Rating	Definition	Expected Frequency
1	Insignificant	No material impact	Financial loss < KWD 1,000 Service outage < 1 hour No reputational effect
2	Minor	Limited impact	Financial loss KWD 1,000–2,500 Service outage 1–4 hours Limited customer complaints
3	Moderate	Noticeable but manageable impact	Financial loss KWD 2,500–10,000 Service outage 4–12 hours Local negative publicity
4	Major	Substantial and difficult to absorb	Financial loss KWD 10,000–100,000 Service outage 12–24 hours National negative publicity
5	Severe	Strategic or existential threat	Financial loss > KWD 100,000 Service outage > 24 hours Regional reputational damage license loss

3. Risk Rating Matrix

- **Risk Score = Likelihood × Impact**
- Classification thresholds:
  - ✓ 1–5 = Low
  - ✓ 6–12 = Medium
  - ✓ 15–25 = High

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.

Roles And Responsibilities

In our commitment to effective Records Management, each stakeholder, including the Risk Management Department, contributes to upholding the integrity and efficiency of our processes:

Risk Management Department: As the primary custodian of the Records Management (RM) policy, the Risk Management Department oversees its development, ensuring alignment with organizational goals. This department is responsible for identifying, assessing, and mitigating risks associated with the RM policy. Importantly, the Risk Management Department plays a crucial role in seeking Board of Directors approval, providing a strategic overview of the finalized policy.

Department Heads/Managers: At the departmental level, our leaders work collaboratively with the Risk Management Department. They translate overarching guidelines into actionable steps for their teams, communicate policy updates, reinforce compliance importance, and address department-specific record-keeping needs.

Employees: At the heart of our RM endeavors, every employee plays a vital role in translating policy into practice. Active participation in training sessions is paramount, ensuring that each team member is well-versed in proper record-keeping procedures. From creation and maintenance to disposal, employees are the frontline executors of our RM policy.

Collectively, these roles, led collaboratively by the Risk Management Department, form a cohesive unit. Each contributor plays a unique part in the successful implementation and continuous improvement of our records Management policy. Through collaboration and a shared commitment to excellence, we fortify our organization's ability to navigate the complexities of electronic payment operations.

Review

This plan is to be reviewed every one years. 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.

Sabah K. Al-Ghunaim
Chairman

Khalid Al-Ghunaim
Board Member

Afif Hussein Mukahal
Sales & Business Development Manager

Jamal Kubeer
General Manager

Linto Lawrance
IT Manager

COMMITTEE RESOLUTION

RISK MANAGEMENT COMMITTEE

Dated: 2-2-2026

SUBJECT: Approval of the Updated Risk Management Policy V.1.7

WHEREAS, the Committee has scrutinized the updated Policy framework and its alignment with the current fiscal year's 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-1.7 is approved for immediate submission to the Board of Directors for final ratification.

POSITION	NAME	SIGNATURE
Chairman	Sabah K. Al Ghunaim	
Board Member 1	Lamiaa Khaled Al Kharafi	
Board Member 2	Khaled Sabah Al Ghunaim	
General Manager	Jamal Kubeer	
Executive Manager	Afif Moukahel	
Finance Manager	Abdul Rahman El Rotel	

Prepared and Verified by: ***Elsayed Thabet***

شركة شبكة الخدمات الآلية
Automated Services Network Co.