

RISK APPETITE POLICY

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk
St., fl. 2, office

TABLE OF CONTENTS

INTRODUCTION.....	3
DEFINITIONS	3
SCOPE	4
CORE PRINCIPLES	4
RISK APPETITE FRAMEWORK	5
FINANCIAL RISK.....	6
LIQUIDITY AND CAPITAL MANAGEMENT	6
CREDIT RISK AND COUNTERPARTY EXPOSURE	7
MARKET RISK MITIGATION	8
TRANSACTION AND FRAUD RISK	9
COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS	9
OPERATIONAL RISK	11
REPUTATIONAL RISK.....	11
TECHNOLOGY AND INNOVATION RISK.....	12
FRAUD AND FINANCIAL CRIME RISK	14
RISK MONITORING AND REVIEW	15
CONCLUSIONS.....	16

INTRODUCTION

At PayNox, we recognize the importance of balancing risk and opportunity in achieving our strategic and operational objectives. This Risk Appetite Policy defines the level of risk we are willing to accept in different areas of our business while ensuring compliance with regulatory requirements, maintaining financial stability, and protecting our clients and stakeholders.

Our approach to risk appetite is guided by principles of responsibility, transparency, and sustainability, ensuring that we manage risks effectively while fostering growth and innovation. This policy serves as a framework for decision-making, risk assessment, and mitigation strategies, ensuring that our operations align with our risk tolerance and regulatory obligations.

By establishing a clear and structured risk appetite, PayNox aims to protect the integrity of its financial services while enabling responsible business growth and long-term success.

DEFINITIONS

For the purpose of this Risk Appetite Policy, the following definitions apply:

Risk Appetite – The level and type of risk that PayNox is willing to accept in pursuit of its business objectives while ensuring compliance, financial stability, and operational resilience.

Risk Tolerance – The acceptable level of variation in risk exposure that the company can withstand without negatively impacting its strategic goals, regulatory obligations, or financial position.

Risk Management – The systematic process of identifying, assessing, monitoring, and mitigating risks to minimize potential negative impacts on the business.

Compliance Risk – The risk of legal or regulatory penalties, financial losses, or reputational damage due to non-compliance with applicable laws, regulations, and industry standards.

Operational Risk – The risk of losses resulting from inadequate or failed internal processes, human errors, system failures, or external events, including fraud, cyber threats, and third-party failures.

Financial Risk – The risk of financial losses due to market fluctuations, liquidity challenges, credit defaults, or economic instability.

Reputational Risk – The risk of damage to the company's reputation due to negative public perception, regulatory violations, unethical practices, or customer dissatisfaction.

Fraud and Financial Crime Risk – The risk of the company being exploited for fraudulent activities, money laundering, terrorist financing, or other illicit financial practices.

Risk-Based Approach (RBA) – A methodology that tailors risk management efforts based on the nature, likelihood, and potential impact of risks, ensuring proportionate mitigation measures.

These definitions provide the foundation for understanding and implementing PayNox's Risk Appetite Policy, ensuring consistency in risk management practices across the organization.

SCOPE

This Risk Appetite Policy applies to all aspects of PayNox's operations, ensuring that risks are managed in alignment with our business objectives, regulatory requirements, and ethical standards. It provides a structured framework for identifying, assessing, and mitigating risks while balancing growth opportunities and operational resilience.

The policy applies to all employees, management, partners, and third-party service providers engaged in activities related to our financial services. It covers key risk areas, including financial, operational, regulatory, compliance, reputational, cybersecurity, and fraud-related risks.

This policy also guides decision-making processes, ensuring that risk exposure remains within acceptable levels. It is continuously reviewed and updated to reflect changes in regulatory environments, market conditions, and business strategies.

CORE PRINCIPLES

The Risk Appetite Policy of PayNox is built upon key principles that guide our approach to risk management, ensuring a balance between business growth, compliance, and financial stability.

We are committed to full compliance with all applicable laws, regulations, and industry standards. Our risk appetite aligns with legal requirements, ensuring ethical business practices and preventing regulatory breaches.

Our risk management strategy follows a risk-based approach (RBA), where risks are assessed, categorized, and mitigated based on their potential impact on operations, financial stability, and reputation.

We maintain a zero-tolerance policy for money laundering, terrorist financing, fraud, and other financial crimes. Strict due diligence, transaction monitoring, and compliance controls are in place to prevent illicit activities.

We ensure business continuity by proactively managing operational risks, including cybersecurity threats, fraud prevention, and technology disruptions. Security measures are continuously updated to mitigate threats.

Risk management is embedded in our corporate culture, with clear accountability at all levels of the organization. Decision-making is transparent, ensuring responsible risk-taking aligned with our strategic goals.

We prioritize client security, data protection, and fair treatment, ensuring that our risk appetite does not compromise customer confidence in our services.

Risk appetite is reviewed regularly, and adjustments are made to align with evolving regulatory, market, and operational conditions. Feedback loops and audits ensure that our risk management framework remains effective and responsive.

These core principles ensure that PayNox maintains a structured, compliant, and sustainable approach to risk management while fostering innovation and business growth.

RISK APPETITE FRAMEWORK

The Risk Appetite Framework defines how PayNox identifies, assesses, and manages risk within acceptable limits. It ensures that risk-taking aligns with strategic objectives, regulatory compliance, and operational stability. The framework consists of key components that provide a structured approach to risk management.

PayNox classifies risks into key categories, each with predefined risk tolerance levels:

Financial Risk – We maintain a conservative approach to financial exposure, ensuring liquidity and capital adequacy to support operations.

Compliance & Regulatory Risk – We have a low tolerance for non-compliance with legal and regulatory requirements, with strict adherence to AML, KYC, and financial crime regulations.

Operational Risk – We proactively manage risks related to fraud, cybersecurity, IT failures, and third-party dependencies, ensuring business continuity and data security.

Reputational Risk – We uphold ethical standards and transparent operations, minimizing risks that could harm brand reputation or customer trust.

Risk exposure is continuously assessed using a Risk-Based Approach (RBA), which ensures proportionate controls and mitigation strategies. We implement real-time monitoring, risk scoring, and periodic reviews to identify emerging risks and trends.

Risk management is embedded into corporate governance, with clear responsibilities assigned to senior management, compliance officers, and operational teams. A risk

oversight function ensures that policies are implemented effectively and that decisions align with our risk appetite.

To keep risks within acceptable levels, we apply preventive, detective, and corrective controls. These include enhanced due diligence (EDD), transaction monitoring, cybersecurity measures, and regular audits to minimize exposure to financial crime and operational disruptions.

Our risk appetite is reviewed regularly to adapt to regulatory changes, market conditions, and business developments. This ensures that risk management remains aligned with the company's objectives and evolving industry standards.

Through this Risk Appetite Framework, PayNox ensures a structured, proactive, and compliant approach to managing risks while fostering sustainable business growth.

FINANCIAL RISK

PayNox takes a conservative approach to financial risk management, ensuring liquidity, capital adequacy, and financial stability while mitigating exposure to market volatility, credit risk, and operational disruptions.

We maintain sufficient liquidity to meet operational and regulatory requirements, ensuring that financial commitments can be fulfilled without disruption. Capital reserves are structured to absorb potential losses while supporting business growth.

We conduct thorough due diligence on business partners, counterparties, and payment providers to mitigate the risk of defaults or insolvencies. Risk assessment procedures ensure that only reputable and financially stable entities engage with our platform.

We closely monitor fluctuations in cryptocurrency and fiat markets, implementing hedging strategies and risk controls to minimize the impact of price volatility on transactions and holdings.

We implement real-time transaction monitoring, fraud detection, and security controls to prevent financial losses due to fraudulent activities, chargebacks, or unauthorized transactions.

By applying a risk-based approach to financial risk management, PayNox ensures stability, resilience, and long-term sustainability while safeguarding client assets and regulatory compliance.

LIQUIDITY AND CAPITAL MANAGEMENT

PayNox prioritizes financial stability through a structured Liquidity and Capital Management framework. Our approach ensures that we maintain sufficient financial resources to support business operations, meet regulatory obligations, and withstand market fluctuations.

We maintain a strong liquidity position to ensure smooth transaction processing and operational resilience. This includes monitoring cash flow, managing liquidity reserves, and ensuring access to reliable financial partners to handle customer transactions efficiently. Our liquidity risk management strategy involves stress testing and scenario analysis to prepare for potential liquidity shortfalls.

To mitigate financial risks, PayNox maintains capital reserves that align with regulatory requirements and business needs. We assess capital adequacy regularly to ensure that we can absorb potential losses, fund business growth, and meet operational commitments without compromising financial stability.

We diversify our financial relationships to reduce counterparty risk, ensuring that we partner only with reputable institutions for banking and payment processing. Treasury operations follow a conservative approach, balancing fiat and crypto holdings to effectively manage volatility and operational needs.

A robust contingency framework is in place to address liquidity crises or unexpected financial disruptions. This includes emergency funding mechanisms, backup payment channels, and predefined response strategies to ensure uninterrupted service.

PayNox ensures financial resilience, operational efficiency, and long-term sustainability through a proactive liquidity and capital management strategy.

CREDIT RISK AND COUNTERPARTY EXPOSURE

PayNox takes a conservative approach to credit risk and counterparty exposure, ensuring that financial transactions and business relationships are conducted with reliable, financially stable entities. Our framework focuses on assessing, monitoring, and mitigating risks associated with counterparties, clients, and financial institutions.

Credit risk arises when counterparties fail to meet their financial obligations. To minimize this risk, we conduct thorough due diligence on clients, business partners, and payment service providers (PSPs) before establishing financial relationships. Our risk assessment process includes evaluating financial stability, payment history, and regulatory compliance.

Before engaging with counterparties, we conduct a comprehensive risk evaluation, considering factors such as:

- Financial strength and solvency to ensure they can meet their obligations.
- Regulatory compliance and reputation, verifying adherence to AML, KYC, and financial crime regulations.
- Operational history and performance, including transaction behavior and reliability.

To limit exposure, we implement risk-based limits on transactions, ensuring that no single counterparty represents a disproportionate financial risk. We also use diversification strategies, working with multiple partners to reduce dependency on any one institution.

We continuously monitor counterparties using real-time transaction tracking, adverse media screening, and financial stability checks. If a counterparty's risk profile deteriorates, we take corrective actions such as reducing transaction limits, requiring additional security measures, or terminating the relationship.

By maintaining strict credit risk controls and counterparty due diligence, PayNox ensures financial stability, protects against defaults, and safeguards the integrity of its operations.

MARKET RISK MITIGATION

PayNox employs a structured market risk mitigation strategy to manage exposure to fluctuations in cryptocurrency and fiat markets. Given the volatility in digital assets and external economic conditions, we take a proactive approach to protect financial stability, minimize losses, and ensure operational continuity.

To reduce exposure to price fluctuations in cryptocurrencies, we utilize hedging techniques such as real-time conversion mechanisms and partnerships with liquidity providers. This ensures that funds retain their value and are not significantly impacted by market downturns.

We maintain a balanced portfolio of fiat and digital assets, ensuring that dependency on any single currency or asset class is minimized. Our treasury management strategy includes diversification across multiple stable coins, fiat currencies, and regulated financial institutions to enhance financial security.

We employ advanced analytics and monitoring tools to track market trends, price volatility, and external economic factors. This enables rapid response strategies, such as adjusting exchange rates, implementing trading safeguards, or temporarily limiting exposure to high-risk assets.

A strong liquidity buffer ensures that funds are available to cover transactions even during periods of high volatility. This prevents service disruptions and protects users from sudden market movements.

Regular stress testing and risk modeling help us anticipate extreme market conditions and formulate contingency plans. By analyzing historical market trends and potential economic shocks, we maintain resilience against unexpected downturns.

Through robust risk management protocols, PayNox effectively mitigates market risks, ensuring financial stability, secure transactions, and long-term business sustainability.

TRANSACTION AND FRAUD RISK

PayNox prioritizes the security and integrity of financial transactions by implementing a risk-based approach to transaction and fraud risk management. Our framework is designed to detect, prevent, and mitigate fraudulent activities while ensuring seamless and secure transactions for legitimate users.

To minimize fraud risks, we employ real-time transaction monitoring, behavioral analysis, and automated fraud detection tools. Suspicious activities, such as unusual transaction patterns, rapid fund movements, and high-risk counterparty interactions, are flagged for further investigation.

Each transaction undergoes risk assessment based on predefined parameters, including transaction size, geographic origin, counterparty reputation, and historical user behavior. High-risk transactions trigger enhanced due diligence (EDD) measures, such as additional identity verification or manual review.

We implement strong authentication protocols, encryption, and access controls to protect user accounts from unauthorized access and fraudulent transactions. This includes two-factor authentication (2FA), anti-phishing measures, and biometric verification where applicable.

All transactions and counterparties are screened against international sanctions lists, politically exposed persons (PEPs), and known fraud databases. This ensures compliance with AML and CTF regulations while preventing interactions with high-risk or illicit entities.

To mitigate financial losses from fraudulent claims or unauthorized transactions, we have a structured dispute resolution and chargeback management process. Customers must provide supporting documentation for claims, and fraudulent disputes are escalated for investigation.

Fraud patterns evolve, and PayNox continuously updates its fraud detection models using machine learning, industry best practices, and real-time risk intelligence. Regular audits and compliance reviews ensure our fraud prevention strategies remain effective.

By maintaining a proactive stance on transactions and fraud risk management, PayNox ensures secure financial operations, regulatory compliance, and enhanced customer trust.

COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS

PayNox is committed to full compliance with all applicable local, European, and international legal and regulatory requirements. Our compliance framework ensures that all operations align with anti-money laundering (AML), counter-terrorist financing (CTF), sanctions screening, data protection, and financial regulations.

We operate in strict compliance with Bulgarian financial regulations, EU directives, and international compliance standards. This includes adherence to:

- The Bulgarian Measures Against Money Laundering Act (MAMLA)
- The Bulgarian Measures Against the Financing of Terrorism Act
- EU Anti-Money Laundering Directives (AMLD 5 & 6)
- The General Data Protection Regulation (GDPR)
- The Markets in Crypto-Assets Regulation (MiCA) (once applicable)
- Financial Action Task Force (FATF) recommendations
- Know Your Customer (KYC) and Know Your Business (KYB) Compliance

To prevent financial crime, PayNox implements robust KYC and KYB procedures, verifying the identities of individual and corporate clients. This includes:

- Identity verification using government-issued documents and biometric checks
- Business verification through company registration documents and Ultimate Beneficial Owner (UBO) disclosure
- Ongoing monitoring of customer activity and risk levels
- Transaction Monitoring and Reporting

We conduct real-time transaction monitoring to detect and report suspicious activities in compliance with regulatory obligations. Any flagged transactions are reviewed, and if necessary, Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) are filed with the relevant authorities.

All customers, transactions, and counterparties are screened against global sanctions lists, Politically Exposed Persons (PEPs), and adverse media databases to prevent dealings with high-risk individuals or entities.

As part of our regulatory obligations, PayNox complies with GDPR to ensure the lawful processing, storage, and security of customer data. Strict confidentiality policies and data encryption measures are in place to protect sensitive information.

Our compliance team continuously monitors changes in legal and regulatory frameworks, updating policies and procedures as required. Employees receive regular training on AML, CTF, and compliance best practices to maintain the highest standards of regulatory adherence.

By integrating comprehensive legal and regulatory compliance measures, PayNox ensures secure, transparent, and legally compliant financial operations while maintaining trust with clients, partners, and regulators.

OPERATIONAL RISK

PayNox recognizes operational risk as a key component of its risk management framework. Operational risk arises from internal processes, systems, human errors, and external events that can disrupt business operations. To mitigate these risks, we implement robust internal controls, contingency planning, and continuous monitoring.

We conduct regular operational risk assessments to identify vulnerabilities across our processes, including transaction handling, IT infrastructure, cybersecurity, and customer interactions. These assessments help us anticipate potential failures and implement preventive measures.

Given our reliance on digital infrastructure, we enforce strong cybersecurity protocols, including data encryption, secure cloud storage, multi-factor authentication (MFA), and real-time threat detection systems. Regular penetration testing and system audits ensure the security of customer data and transactions.

Operational risks related to fraud, financial crime, and regulatory non-compliance are managed through real-time transaction monitoring, automated fraud detection, and AI-driven risk analytics. Any anomalies trigger enhanced due diligence (EDD) and internal investigations.

To ensure uninterrupted service, we maintain a Business Continuity Plan (BCP) that includes backup data centers, emergency response strategies, and alternative processing arrangements. In case of cyberattacks, technical failures, or regulatory incidents, our Disaster Recovery Plan (DRP) allows for quick restoration of operations.

Operational risk stemming from human errors or process failures is mitigated through standardized procedures, automation, and employee training programs. We implement segregation of duties to prevent conflicts of interest and unauthorized transactions.

Compliance with AML, CTF, GDPR, and financial regulations reduces operational risks related to non-compliance. Internal compliance audits and risk assessments ensure that policies are followed, and any gaps are addressed proactively.

By maintaining a proactive operational risk management strategy, PayNox ensures secure, efficient, and resilient business operations, minimizing disruptions and safeguarding client trust.

REPUTATIONAL RISK

Reputational risk refers to the potential for damage to PayNox's brand, trust, and market standing due to negative public perception, compliance failures, or association with illicit activities. In the financial services and cryptocurrency sector, reputational damage can arise from regulatory violations, security breaches, poor customer experiences, or partnerships with high-risk entities.

- Regulatory Non-Compliance – Failure to meet AML, CTF, and KYC/KYB requirements may lead to legal actions, fines, and loss of operating licenses.
- Association with Illicit Activities – Processing transactions linked to fraud, money laundering, or sanctioned entities can result in reputational harm.
- Cybersecurity Breaches – Hacks, data leaks, or unauthorized access to customer funds can significantly damage customer trust.
- Negative Publicity and Media Exposure – Adverse media coverage related to financial misconduct, customer complaints, or unethical practices can lead to loss of credibility.
- Poor Customer Service – Delayed transactions, unresponsive support, or unresolved complaints can result in negative reviews and customer dissatisfaction.
- Partnerships with High-Risk Entities – Engaging with businesses involved in questionable activities can expose PayNox to reputational damage.

To safeguard its reputation, PayNox implements:

- Strict Compliance Controls – Adherence to AML, KYB, and sanctions screening to avoid regulatory penalties.
- Robust Transaction Monitoring – Continuous tracking of crypto transactions to detect and prevent illicit activities.
- Proactive Cybersecurity Measures – Implementation of advanced encryption, multi-factor authentication, and threat detection systems.
- Transparent Communication – Clear policies, timely customer updates, and proactive issue resolution to maintain trust.
- Crisis Management and Incident Response – A dedicated strategy to address reputational threats, including public statements and corrective actions.

By maintaining a high level of compliance, security, and transparency, PayNox minimizes reputational risks and strengthens its standing as a trusted financial service provider.

TECHNOLOGY AND INNOVATION RISK

Technology and innovation risk refers to the potential disruptions, failures, or security vulnerabilities associated with adopting and implementing new technologies within PayNox's operations. As a digital financial services provider operating in the cryptocurrency sector, the company must manage risks related to system failures, cybersecurity threats, regulatory challenges, and technological obsolescence while continuously innovating to stay competitive.

Sources of Technology and Innovation Risk

- System Downtime and Technical Failures – Interruptions in platform functionality, transaction processing delays, or server outages can impact customer trust and financial stability.
- Cybersecurity Threats and Data Breaches – Hacking attempts, ransomware attacks, and unauthorized access to customer data or funds can result in financial losses and reputational damage.
- Regulatory and Compliance Risks – Rapid changes in regulatory requirements for blockchain and cryptocurrency technology can create uncertainty and compliance challenges.
- Third-Party Dependency Risks – Reliance on external service providers for cloud infrastructure, blockchain analytics, and payment processing can introduce operational vulnerabilities.
- Scalability and Performance Risks – Growth in transaction volume or user activity may strain existing technology, requiring continuous system upgrades.
- Obsolescence and Innovation Challenges – Emerging blockchain technologies, smart contracts, and DeFi solutions can make current systems outdated, necessitating continuous R&D investment.

To minimize technology and innovation risks, PayNox implements:

- Robust IT Infrastructure – Ensuring high system uptime, redundancy, and performance scalability to handle increasing transaction volumes.
- Advanced Cybersecurity Measures – Implementing end-to-end encryption, multi-factor authentication (MFA), and regular penetration testing to safeguard against cyber threats.
- Regulatory Compliance Monitoring – Keeping up with EU, Bulgarian, and global regulatory changes to ensure platform security and legality.
- Diversification of Service Providers – Reducing reliance on a single third-party vendor for critical services like blockchain analytics, transaction monitoring, and cloud hosting.
- Continuous Technology Upgrades – Investing in AI-driven risk analysis, smart contract auditing, and decentralized identity verification to stay competitive.
- Incident Response and Disaster Recovery – Having predefined protocols for data breaches, cyberattacks, and system failures to ensure rapid recovery and minimize business disruptions.

By proactively addressing technology and innovation risks, PayNox ensures a secure, scalable, and compliant digital financial ecosystem, fostering trust among clients and regulators.

FRAUD AND FINANCIAL CRIME RISK

Fraud and financial crime risk refers to the potential for money laundering, terrorist financing, fraud, and other illicit activities within the PayNox platform. Given the nature of cryptocurrency transactions, pseudonymity, speed, and global reach, there is a heightened risk of misuse by bad actors. Managing these risks is critical to ensuring regulatory compliance, protecting clients, and maintaining the integrity of financial transactions.

Sources of Fraud and Financial Crime Risk

- Money Laundering and Terrorist Financing (ML/TF) – Criminals may attempt to conceal illicit funds through layering, structuring, or integrating crypto transactions into the legitimate financial system.
- Identity Fraud and Synthetic Identities – Fraudsters may use stolen or fake identities to create accounts and conduct unauthorized transactions.
- Crypto Investment Scams – Fraudulent schemes such as Ponzi schemes, phishing attacks, and fake ICOs can result in financial losses for customers.
- Insider Fraud and Employee Misconduct – Internal actors may engage in misuse of privileged access, collusion, or unethical activities.
- Sanctions and Prohibited Transactions – Users may attempt to circumvent international sanctions by using crypto to send or receive funds in restricted jurisdictions.

To combat fraud and financial crime, PayNox employs:

- Comprehensive AML and KYC/KYB Procedures – All customers and businesses undergo strict verification, ongoing monitoring, and risk assessments before transacting.
- Real-Time Blockchain Analytics and Screening – Transactions are analyzed for suspicious activity using blockchain forensics tools (e.g., Chainalysis, Elliptic, Crystal Blockchain).
- Transaction Monitoring and Red Flags Detection – The system flags high-risk behaviors, such as rapid fund transfers, use of mixers/tumblers, and transactions linked to illicit wallets.
- Enhanced Due Diligence (EDD) for High-Risk Users – Users or entities with large transaction volumes, politically exposed persons (PEPs), or complex fund flows undergo deeper scrutiny.
- Fraud Detection and AI-Powered Risk Scoring – Machine learning algorithms detect anomalous patterns, account takeovers, and fraudulent behaviors in real time.

- Collaboration with Authorities and Industry Partners – Compliance teams report suspicious transactions to regulators and cooperate with financial crime enforcement agencies.

By integrating advanced fraud prevention technologies, strict compliance controls, and real-time monitoring, PayNox minimizes exposure to fraud and financial crime risks, ensuring a secure, transparent, and regulatory-compliant financial ecosystem.

RISK MONITORING AND REVIEW

Risk monitoring and review is an essential part of PayNox's risk management framework, ensuring that risks are continuously assessed, mitigated, and aligned with regulatory requirements and business objectives. Given the dynamic nature of the cryptocurrency industry, PayNox implements a proactive approach to monitor, detect, and respond to emerging risks in financial transactions, technology, compliance, and security.

Risk monitoring at PayNox involves continuous surveillance of operational, financial, regulatory, and fraud risks to prevent potential threats and ensure compliance with AML, KYC/KYB, and sanctions regulations. The company employs real-time monitoring systems, periodic risk assessments, and internal audits to detect anomalies and strengthen its risk mitigation strategies.

Risk review ensures that risk management policies and procedures remain effective and relevant. Regular evaluations, reporting, and governance reviews help identify areas that require improvement and allow for the adaptation of new controls in response to changing regulatory landscapes and emerging threats.

PayNox employs a combination of automated tools and manual oversight to track risks, including:

- Real-Time Transaction Monitoring – Continuous tracking of crypto transactions for unusual patterns, high-risk jurisdictions, and potential fraud indicators.
- Blockchain Analytics and Screening – Utilizing blockchain forensics tools to identify suspicious wallet addresses, illicit fund flows, and potential money laundering schemes.
- Internal Audits and Compliance Reviews – Regular assessment of internal processes to ensure compliance with AML, KYC, sanctions, and regulatory obligations.
- Risk Scoring and Alerts – Assigning risk scores to customers, transactions, and counterparties based on predefined risk criteria.
- Incident Reporting and Escalation – Any detected anomalies or compliance breaches are escalated to the compliance and risk management team for immediate review.

PayNox conducts periodic risk reviews to reassess the effectiveness of its risk management framework. These reviews include:

- Quarterly and Annual Risk Assessments – Evaluating risk exposure across financial, operational, and regulatory domains.
- Policy and Procedure Updates – Adjusting risk controls based on new compliance requirements, emerging threats, and industry best practices.
- Stakeholder Engagement – Collaborating with regulators, auditors, and financial institutions to ensure transparency and adherence to legal obligations.

Through real-time monitoring, regular risk reviews, and continuous adaptation, PayNox ensures a robust risk management framework that minimizes threats, enhances compliance, and protects the integrity of its operations in the cryptocurrency industry.

CONCLUSIONS

PayNox is committed to maintaining a proactive and adaptive risk management approach to ensure the security, compliance, and operational integrity of its services. By implementing real-time monitoring, advanced analytics, and regular risk assessments, the company effectively mitigates threats related to fraud, financial crime, regulatory non-compliance, and technological vulnerabilities.

Continuous evaluation and improvement of risk management policies enable PayNox to stay ahead of emerging risks in the cryptocurrency industry, ensuring that its operations remain secure, transparent, and aligned with legal and regulatory requirements. By integrating automated tools, manual oversight, and industry best practices, PayNox fosters a resilient and trustworthy financial ecosystem for its clients and partners.