RISK POLICY

PayNox EOOD

ID number: 208071994

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

Table of contents

INTRODUCTION

The Risk Policy is a critical component of PayNox's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) framework. It establishes a structured approach to identifying, assessing, and managing risks that could impact the organization's operations, financial stability, regulatory compliance, and strategic objectives. It ensures that risks are systematically evaluated and addressed to minimize potential threats while maximizing opportunities.

PayNox adheres to Bulgarian AML laws, EU Directive 2015/849 (4AMLD), EU Directive 2018/843 (5AMLD), EU Directive 2019/1153 (6AMLD), FATF Recommendations, and GDPR (EU Regulation 2016/679). The policy is also aligned with PSD2 (EU Directive 2015/2366), ensuring compliance with payment service regulations.

By implementing a proactive risk management framework, the organization enhances its resilience against financial fraud, cybersecurity threats, regulatory violations, and operational disruptions. This policy supports informed decision-making, protects stakeholders, and fosters a culture of transparency and accountability.

These legal frameworks guide risk mitigation efforts, ensuring compliance with anti-money laundering, anti-fraud, sanctions, and cybersecurity regulations.

DEFINITIONS

Risk – The potential for loss, harm, or adverse outcomes resulting from internal or external factors that could affect the organization's objectives, financial stability, operations, or reputation.

Risk Management – The systematic process of identifying, assessing, mitigating, and monitoring risks to reduce their impact and likelihood while ensuring business continuity.

Risk-Based Approach (RBA) – A strategy that prioritizes risk management efforts based on the level of threat or impact, ensuring that high-risk areas receive greater attention and resources.

Risk Assessment – The process of analyzing risks by evaluating their likelihood and impact to determine the necessary controls and mitigation strategies.

Risk Tolerance – The level of risk the organization is willing to accept in pursuit of its business objectives, considering regulatory requirements and strategic goals.

Residual Risk – The remaining risk after mitigation measures have been applied, which must be continuously monitored and managed.

Operational Risk – The risk of loss due to failed internal processes, human errors, system failures, or external events that disrupt business operations.

Regulatory Risk – The potential for penalties, fines, or legal consequences due to non-compliance with laws, regulations, or industry standards.

Fraud Risk – The possibility of financial loss or reputational damage due to fraudulent activities, including internal fraud, external fraud, or cyber fraud.

Cybersecurity Risk – Threats related to data breaches, hacking, ransomware, phishing, or other cyberattacks that compromise sensitive information and business systems.

Compliance Risk – The risk of failing to adhere to applicable laws, regulations, and internal policies, leading to legal liabilities and reputational damage.

Business Continuity Plan (BCP) – A framework for ensuring essential business functions can continue or quickly recover in case of disruptions, including cybersecurity incidents, natural disasters, or financial crises.

These definitions provide a foundation for understanding risk-related concepts and ensure consistency in the organization's risk management approach.

SCOPE

This Risk Policy applies to all business processes, financial transactions, compliance operations, and third-party engagements within PayNox. It ensures that risk management is fully integrated across all company functions and follows legal and regulatory frameworks in Bulgaria, the EU, and FATF jurisdictions.

This policy applies to all employees, management, executives, vendors, contractors, and business partners. It also governs the use of digital assets, blockchain transactions, and fiat currency operations.

Additionally, this policy aligns with PayNox’s Know Your Transaction (KYT) Policy, ensuring a cohesive risk management and transaction monitoring strategy.

Furthermore, the policy aligns with Bulgarian laws, EU regulations, and international risk management frameworks, ensuring adherence to legal and regulatory requirements while maintaining a proactive approach to identifying, assessing, and mitigating risks. Regular reviews and updates ensure the policy remains relevant in response to evolving threats and regulatory changes.

CORE PRINCIPLES

The Risk Policy is built on fundamental principles that guide the organization in identifying, assessing, and managing risks effectively. These principles ensure a proactive and structured approach to risk management, promoting resilience, compliance, and sustainable growth.

A risk-based approach is central to decision-making, prioritizing risks based on their potential impact and likelihood. This ensures that high-risk areas receive greater attention and resources while maintaining efficiency in managing lower-risk activities.

A strong compliance framework ensures adherence to Bulgarian laws, EU directives, and international standards. Regulatory risks, including anti-money laundering (AML), counter-terrorism financing (CTF), and data protection laws, are continuously monitored and addressed.

Accountability and transparency are key to maintaining trust and integrity. All employees and stakeholders are responsible for identifying and reporting risks, with clear roles and responsibilities assigned for risk management. Regular training and awareness programs reinforce a culture of risk consciousness.

The organization adopts a continuous monitoring and improvement approach, regularly reviewing risk management strategies, policies, and controls. Internal audits, stress testing, and scenario analysis help identify vulnerabilities and improve response mechanisms.

A robust incident response and mitigation strategy ensures that identified risks are addressed promptly and effectively. Business continuity planning (BCP) and disaster recovery plans (DRP) are in place to minimize disruptions and maintain operational resilience.

By integrating these principles, the organization ensures a dynamic and adaptive risk management framework that safeguards its financial stability, regulatory compliance, and long-term success.

FATF COMPLIANCE AND SANCTIONS SCREENING

PayNox follows FATF Recommendations to prevent financial crime and maintains a blacklist of high-risk jurisdictions based on FATF Grey and Black Lists. Transactions involving these jurisdictions are flagged for enhanced scrutiny and require senior compliance approval.

Automated sanctions screening tools compare all transactions against sanctions lists, including:

- United Nations (UN) Sanctions List

- European Union (EU) Financial Sanctions
- U.S. Office of Foreign Assets Control (OFAC)
- Interpol & Local Bulgarian Watchlists

Any flagged transactions undergo Enhanced Due Diligence (EDD), and if concerns persist, a Suspicious Activity Report (SAR) is filed.

RISK-BASED APPROACH

The organization follows a risk-based approach (RBA) to ensure that resources and controls are proportionally allocated based on the level of risk associated with different activities, transactions, and business relationships. This approach enables a more effective and efficient risk management process by focusing on areas that pose the highest threats to financial stability, regulatory compliance, and operational integrity.

The Risk-Based Approach (RBA) categorizes transactions, clients, and business operations based on their risk exposure:

- Low-Risk: Verified customers with consistent transaction behavior, operating in regulated jurisdictions.
- Medium-Risk: Customers in industries with moderate AML concerns, such as remittance services, e-commerce, or online businesses.
- High-Risk: Transactions involving Politically Exposed Persons (PEPs), high-risk jurisdictions, crypto mixing/tumbling services, or unusual fund movement patterns.

Risk levels are continuously reviewed to adapt to evolving financial crime risks, sanctions updates, and emerging fraud patterns.

High-risk activities undergo enhanced scrutiny, while lower-risk activities are managed with proportionate controls to avoid unnecessary burdens on operations.

For financial transactions, customer relationships, and third-party engagements, a tiered due diligence process is applied. Enhanced due diligence (EDD) is conducted for high-risk customers or transactions, particularly those involving politically exposed persons (PEPs), high-risk jurisdictions, or large-volume cryptocurrency transactions. Lower-risk entities may undergo simplified due diligence, ensuring compliance without overburdening legitimate business activities.

The risk-based approach also applies to compliance monitoring and reporting, ensuring that regulatory requirements under Bulgarian law, EU directives, and international standards are met. Regular risk reviews and updates are performed to adapt to emerging threats, regulatory changes, and evolving business conditions.

By adopting a dynamic and adaptive risk-based approach, the organization effectively mitigates threats while maintaining operational efficiency and regulatory compliance.

RISK IDENTIFICATION AND ASSESSMENT

The organization systematically identifies and assesses risks that could impact its financial stability, regulatory compliance, and operational integrity. Risk identification is an ongoing process that involves monitoring internal operations, market conditions, regulatory changes, and emerging threats. This proactive approach ensures that potential vulnerabilities are detected before they escalate into significant issues.

Once identified, risks are evaluated based on their likelihood and potential impact. This assessment helps categorize risks into different levels—low, medium, or high—allowing for appropriate mitigation strategies. Factors such as financial exposure, legal consequences, reputational damage, and operational disruption are considered during this evaluation.

To ensure accuracy, multiple methods are used in risk assessment, including internal audits, data analysis, employee reporting, and external threat intelligence. Advanced analytical tools may also be used to assess transaction patterns and detect suspicious activities.

A structured risk register is maintained to document identified risks, their severity, and the corresponding mitigation measures. Regular updates to this register help ensure that the organization remains prepared for evolving threats.

By implementing a robust risk identification and assessment framework, the organization strengthens its ability to detect, evaluate, and mitigate risks, ensuring compliance with Bulgarian regulations, EU directives, and international best practices.

ENHANCED DUE DILIGENCE (EDD)

Enhanced Due Diligence (EDD) is a more detailed and rigorous process of investigation and assessment that is applied when dealing with high-risk customers, transactions, or situations that require additional scrutiny beyond standard due diligence practices. EDD is typically triggered when there are higher-risk factors involved, such as transactions linked to politically exposed persons (PEPs), high-risk jurisdictions, large or unusual transactions, or suspicious financial activities. The purpose of EDD is to mitigate the risks of money laundering, fraud, terrorist financing, or other illicit activities, ensuring that the organization remains compliant with regulatory requirements and safeguards its reputation.

The EDD process involves gathering in-depth information about the individual or entity in question, including verifying their identity, assessing the source of funds, and

examining the purpose and nature of the business relationship. This may involve seeking additional documentation, conducting background checks, or even performing on-site visits for business clients. For high-risk individuals, EDD ensures that their financial history, affiliations, and any potential links to criminal activities or corruption are thoroughly investigated.

For example, when dealing with a politically exposed person (PEP), EDD requires the organization to obtain details about the person's position, business dealings, and family or close associates. Additionally, organizations must assess the risks associated with the PEP's jurisdiction, ensuring that transactions do not involve money laundering or the financing of terrorism. Similarly, transactions in countries with high corruption levels or poor regulatory oversight may also trigger EDD processes.

The source of funds is a crucial aspect of EDD, particularly for high-value transactions. The organization must be satisfied that the funds involved are not the proceeds of crime. This involves tracing the origin of the funds, understanding the financial background of the client, and ensuring that all assets are legitimate.

EDD also involves more frequent monitoring of high-risk clients or transactions, as their financial behavior may change over time. This monitoring helps identify any changes in the risk profile, enabling the organization to take swift action if needed, such as freezing assets or terminating the business relationship.

By conducting Enhanced Due Diligence, the organization minimizes its exposure to legal and reputational risks, strengthens its ability to detect illicit activities, and ensures compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

EXAMPLE OF KYC WITH ENHANCED DUE DILIGENCE (EDD)

Let's consider an example of a financial institution conducting Know Your Customer (KYC) with Enhanced Due Diligence (EDD) for a high-risk individual who is a Politically Exposed Person (PEP).

Step 1: Initial Customer Onboarding (KYC)

The institution begins the KYC process by collecting standard information from the individual (the customer), such as:

Personal details: Full name, date of birth, nationality, address, and contact information.

Identification documents: A passport, national ID, or driver's license.

Employment and business information: Occupation, employer, business activities, and source of income.

The customer is requested to provide supporting documents like a utility bill for address verification and proof of employment. This step ensures that the individual is legitimate and the information is consistent with their financial activity.

Step 2: Triggering Enhanced Due Diligence (EDD)

As part of the KYC process, the financial institution uses an automated system to check for any red flags, such as:

The customer's name being flagged as a politically exposed person (PEP).

The customer is linked to a high-risk jurisdiction with a history of corruption or money laundering.

Given these high-risk factors, the institution triggers Enhanced Due Diligence (EDD) to further assess the customer's background and ensure there is no potential for illegal activity or reputational risk.

Step 3: Conducting Enhanced Due Diligence (EDD)

The institution now conducts a deeper investigation into the customer's background, which includes:

Verification of PEP status: The institution cross-checks the customer's name against various international PEP databases and government records to confirm their position as a senior government official, family member, or close associate of a PEP.

Source of funds and wealth: Since the customer is a high-profile individual, the institution must verify the legitimacy of their source of funds. The institution requests detailed documents, such as tax returns, business records, and income statements, to confirm that the individual's wealth comes from legitimate sources, such as a legitimate business or inheritance.

Review of financial history: The institution evaluates the customer's previous financial transactions for any suspicious activity or patterns that could indicate money laundering, such as large transactions to and from high-risk jurisdictions. They may also assess any involvement in complex financial structures that could be used to disguise the true source of funds.

Third-party checks: The institution may conduct background checks on the customer's associates or business partners, ensuring that no criminal connections or conflicts of interest exist. This may involve public records searches, checking against sanctions lists, and consulting with legal or regulatory experts to evaluate any potential risks.

On-site visit (if applicable): For businesses or entities linked to the PEP, the institution may decide to conduct an on-site visit to verify the legitimacy of the business operations, especially if the business is based in a high-risk jurisdiction.

Step 4: Risk Assessment and Ongoing Monitoring

Following the completion of EDD, the institution assesses the overall risk profile of the customer. If the risk is deemed high, the institution may decide to:

Refuse to onboard the customer if any of the findings suggest potential involvement in illegal activities.

Establish stricter monitoring measures, such as periodic reviews of the customer's transactions and accounts, setting up alerts for suspicious activities, and requesting additional documentation if certain transactions raise red flags.

Additionally, the financial institution commits to ongoing monitoring of the customer's financial activity, ensuring that any changes in the risk profile are identified promptly. This includes monitoring for unusual transactions, new associations with high-risk entities, or large international wire transfers.

CUSTOMER DUE DILIGENCE (CDD)

Customer Due Diligence (CDD) is the process that financial institutions and other regulated entities use to gather and assess information about their customers in order to understand the risks associated with doing business with them. CDD is a critical component of anti-money laundering (AML) and combating the financing of terrorism (CFT) efforts. Its primary goal is to ensure that the institution can detect and prevent money laundering, fraud, and other financial crimes.

There are several key components of CDD, including:

Customer Identification: This involves obtaining basic information to verify the identity of the customer, such as their full name, date of birth, address, nationality, and government-issued identification (e.g., passport, driver's license, or national ID). This step ensures that the financial institution knows who they are dealing with.

Risk Assessment: Financial institutions assess the risk level of the customer by considering factors like their occupation, location, the nature of the transactions they engage in, and any potential connections to high-risk jurisdictions or entities. Customers are categorized into different risk levels (low, medium, high) based on this assessment.

Verification of Information: Institutions may request supporting documents to verify the customer's identity and background. For example, utility bills may be requested to

confirm the customer's address, and business clients might need to provide corporate documents such as tax returns or business registration papers.

Ongoing Monitoring: CDD isn't just about collecting data at the time of onboarding; it also involves monitoring the customer's activity throughout the business relationship. This helps to detect any changes in behavior, suspicious transactions, or signs of illicit activities. If the customer's risk profile changes over time, additional due diligence may be required.

Enhanced Due Diligence (EDD) for High-Risk Customers: If a customer is deemed high-risk (for example, a politically exposed person or a customer from a high-risk jurisdiction), the institution must apply Enhanced Due Diligence (EDD) to obtain further information, monitor their transactions more closely, and mitigate the risks associated with that customer.

EXAMPLE OF KYC WITH CUSTOMER DUE DILIGENCE (CDD)

Step 1: Customer Onboarding (KYC and CDD)

A user registers on the cryptocurrency exchange platform to buy and sell digital assets. The platform starts by gathering basic information as part of the KYC process:

Personal Details: The user submits their name, address, date of birth, nationality, and email address.

Government-Issued ID: The user uploads a clear copy of their passport or national ID for identity verification.

Selfie Verification: To confirm that the person registering is the same as the one shown on the identification documents, a selfie is required alongside the submitted ID.

Proof of Address: A utility bill or bank statement, showing the user's current address, is provided.

For the platform, this step ensures that the individual's identity is genuine, and the account is tied to a legitimate person or entity.

Step 2: Risk Assessment (CDD)

Once the basic KYC information is collected, the platform assesses the user's risk level:

Geographical Risk: The user is from a country that is considered high-risk due to limited regulatory oversight or a history of financial crimes. This triggers the need for additional scrutiny.

Transaction Risk: The user plans to deposit a large amount of cryptocurrency (e.g., over $10,000 worth), which could indicate a higher risk of money laundering.

Industry Risk: The user indicates they are involved in a business that deals with online gaming and virtual assets. While this is a legitimate business, it could be linked to industries that are sometimes targeted for illicit activities, prompting further checks.

Based on these factors, the platform classifies the user as medium-high risk.

Step 3: Verification of Information (CDD)

The platform proceeds with verifying the details provided by the user:

Identity Verification: The user's passport or national ID is cross-checked with public databases and records to ensure it's not a fake or altered document.

Address Verification: The utility bill or bank statement is confirmed by ensuring it matches the user's details and is recent (typically within the last three months).

Source of Funds: Since the user intends to deposit a large amount, the platform requests additional documentation, such as proof of income or the source of the funds. This may include transaction records showing the origins of the cryptocurrency (e.g., from a peer-to-peer exchange or another wallet).

These verifications confirm that the user is legitimate and their source of funds is lawful.

Step 4: Ongoing Monitoring (CDD)

Once the user is onboarded, the platform continues to monitor their activity:

Transaction Monitoring: The platform sets up automated systems to track the user's transactions, flagging any unusual or suspicious behavior (e.g., large, rapid transactions).

Risk Reassessment: If the user's activity changes significantly (e.g., they suddenly start withdrawing large sums to high-risk jurisdictions), the platform reassesses the user's risk profile.

If the user begins to make transactions to countries known for money laundering or terrorism financing, or if they make unusual, large withdrawals, the platform may take further action, such as freezing the account or requesting additional documentation.

Step 5: Enhanced Due Diligence (EDD) for High-Risk Users

If, during monitoring, the user's transactions raise significant concerns, the platform escalates to Enhanced Due Diligence (EDD):

In-depth Investigation: The platform may ask the user to provide more detailed information about the source of their funds, or they might seek external help to track the funds through blockchain analysis tools.

Background Checks: The platform might run additional checks to determine if the user is listed on any sanction lists, such as OFAC (Office of Foreign Assets Control) or FATF's high-risk jurisdictions.

Step 6: Suspicious Activity Reporting (SAR)

If the platform detects activities that indicate money laundering, terrorist financing, or other illicit activities (e.g., multiple withdrawals to a known criminal network), it will file a Suspicious Activity Report (SAR) to the appropriate regulatory authorities.

BLOCKCHAIN ANALYTICS FOR RISK MITIGATION

PayNox integrates advanced blockchain analytics tools (e.g., Chainalysis, Elliptic, TRM Labs) to monitor digital asset movements and detect illicit transactions. These tools provide real-time alerts on transactions linked to:

- Darknet markets
- Crypto mixers/tumblers
- Sanctioned wallet addresses
- Suspicious on-chain behaviors (e.g., rapid fund movement across multiple wallets)

These analytics enhance PayNox's ability to detect, investigate, and prevent cryptocurrency-based money laundering and fraud.

RISK MITIGATION AND CONTROL MEASURES

To minimize the impact of identified risks, the organization implements structured risk mitigation and control measures that align with Bulgarian regulations, EU directives, and international best practices. These measures ensure that financial, operational, cybersecurity, and regulatory risks are effectively managed.

Mitigation begins with preventive controls, such as strong internal procedures, multi-factor authentication for system access, and transaction monitoring tools to detect suspicious activities. Detective controls, including real-time alerts, internal audits, and anomaly detection systems, help identify risks before they escalate. If a risk materializes, corrective controls—such as incident response plans and fraud investigations—are deployed to minimize damage and prevent recurrence.

For high-risk transactions, customers, and third-party engagements, the organization applies enhanced due diligence (EDD) and continuous monitoring. This ensures that suspicious patterns are flagged, and appropriate action is taken in line with regulatory requirements. Employees receive regular training and awareness programs to strengthen compliance and risk management culture.

Risk mitigation strategies are continuously reviewed and updated to reflect emerging threats, regulatory changes, and operational needs. By integrating a dynamic risk control framework, the organization ensures resilience, operational stability, and strict compliance with applicable laws and industry standards.

PREVENTIVE CONTROLS

Preventive controls are proactive measures designed to reduce the likelihood of risks occurring by strengthening internal processes, ensuring compliance, and minimizing exposure to financial, operational, and cybersecurity threats. These controls are embedded into daily operations to detect and stop potential risks before they escalate.

One of the key preventive controls is strong internal policies and procedures, which provide clear guidelines for risk management, financial transactions, customer due diligence (CDD), and regulatory compliance. These policies align with Bulgarian laws, EU directives, and international standards to ensure adherence to legal and ethical requirements.

To prevent fraud, unauthorized access, and data breaches, the organization implements strict access controls and authentication mechanisms such as multi-factor authentication (MFA), role-based access permissions, and encryption of sensitive information. These measures protect against insider threats and cyberattacks.

Automated transaction monitoring systems help prevent illicit activities by detecting suspicious patterns in real time. These systems flag transactions exceeding predefined risk thresholds, preventing financial crime, money laundering, and sanctions violations.

Additionally, employee training and awareness programs serve as a critical preventive measure. Regular training ensures that employees can identify red flags related to fraud, bribery, cybersecurity risks, and compliance violations, reducing the risk of human error or negligence.

By continuously reviewing and strengthening these preventive controls, the organization minimizes vulnerabilities and maintains a proactive and resilient risk management framework.

DETECTIVE CONTROLS

Detective controls are mechanisms designed to identify and expose risks, irregularities, and potential violations after they have occurred. These controls provide continuous oversight of financial transactions, operational activities, and compliance processes, allowing the organization to detect suspicious activities, fraud, or regulatory breaches in a timely manner.

A key detective control is real-time transaction monitoring, which analyzes financial activities for unusual patterns, such as high-risk transactions, rapid fund movements, or interactions with sanctioned entities. This helps in identifying money laundering attempts, fraud, or illicit financial activities.

Internal audits and compliance reviews serve as another crucial layer of detection. Regular audits assess adherence to Bulgarian laws, EU directives, and industry regulations, ensuring that internal controls remain effective and up to date. Compliance teams review operational processes to identify gaps, policy violations, or weaknesses that could lead to risks.

Automated alerts and anomaly detection systems provide immediate notifications when suspicious transactions or unusual behaviors are detected. These systems flag deviations from normal transaction volumes, geographic locations, or customer profiles, allowing for quick investigation and response.

Additionally, whistleblower programs and employee reporting mechanisms help detect internal fraud, misconduct, or unethical behavior. Employees and third parties are encouraged to report suspicious activities anonymously, ensuring that potential risks are identified before they cause significant harm.

By integrating detective controls into its risk management framework, the organization ensures continuous monitoring, early detection, and swift corrective actions, reinforcing its commitment to operational integrity and regulatory compliance.

CORRECTIVE CONTROLS

Corrective controls are designed to address and remedy issues or risks that have already occurred, minimizing the damage and preventing future recurrence. These controls come into play once a risk is identified or an incident occurs, helping the organization to contain the impact, recover, and restore normal operations while enhancing future resilience.

One critical corrective control is the incident response plan, which outlines the steps the organization will take when a security breach, fraud, or regulatory violation is detected. This plan includes procedures for investigating the issue, mitigating

immediate harm, notifying relevant stakeholders, and restoring systems to normal functionality.

For financial fraud or compliance violations, forensic investigations are conducted to trace the origin and extent of the issue. This could involve working with external auditors or legal advisors to gather evidence, identify responsible parties, and resolve the situation.

Once the cause of the risk or violation is identified, remediation actions are implemented to fix the underlying issues. This might involve revising internal policies, enhancing security protocols, updating risk assessments, or retraining employees to ensure the same issues do not arise in the future.

Another important corrective measure is the legal and regulatory reporting process. If a violation or non-compliance incident is detected, corrective controls include the timely reporting to regulatory authorities, such as financial regulators or law enforcement, in accordance with the applicable laws and regulations.

Finally, feedback loops are put in place to continuously learn from past incidents. This helps in adjusting preventive and detective controls to prevent similar occurrences in the future. Regular post-incident reviews ensure that lessons learned are applied across the organization to continuously improve risk management strategies.

Through effective corrective controls, the organization can respond quickly to mitigate damage, restore operations, and strengthen its risk management framework, minimizing future vulnerabilities.

MONITORING AND REVIEW

Monitoring and review are essential components of an effective risk management framework, ensuring that the organization's risk management practices remain robust, relevant, and effective over time. These processes involve continuous oversight, assessment, and updates to controls, policies, and procedures to adapt to evolving risks, regulatory changes, and business conditions.

Continuous monitoring involves real-time surveillance of key activities, transactions, and business operations to identify potential risks as they arise. Automated systems track financial transactions, customer behavior, and system access for signs of fraud, regulatory non-compliance, or cybersecurity threats. By promptly detecting suspicious activities, the organization can take immediate corrective actions to minimize risks.

Regular reviews of the risk management policies and procedures are conducted to ensure they align with current laws, regulations, and industry best practices. These reviews assess whether the organization's risk tolerance has changed, if new risks have

emerged, or if there are gaps in the existing controls. Any identified gaps or weaknesses are addressed through updates to policies, procedures, or risk mitigation strategies.

Internal audits play a crucial role in the review process, evaluating the effectiveness of the organization's risk controls and compliance measures. Auditors examine financial records, operational processes, and security protocols to ensure that risks are being effectively managed and that all regulatory requirements are being met.

Incident analysis and reporting also contribute to the monitoring and review process. When an issue or breach occurs, detailed post-incident analyses are conducted to understand the root cause, the response effectiveness, and what changes are needed to prevent recurrence. This feedback loop ensures continuous improvement of the risk management approach.

Additionally, management and board reviews ensure that senior leadership is regularly updated on the effectiveness of the risk management program. This ensures alignment between risk management efforts and the organization's strategic objectives.

Through systematic monitoring and review, the organization can proactively adjust its risk management practices, ensuring that it stays resilient and compliant in the face of dynamic challenges. This approach enhances decision-making, maintains stakeholder trust, and reduces the likelihood of significant risks materializing.

CONTINUOUS MONITORING

Continuous monitoring is an ongoing process that involves the real-time tracking of activities, transactions, and business operations to identify and address risks as they emerge. This proactive approach ensures that potential threats, whether related to fraud, compliance violations, cybersecurity breaches, or operational inefficiencies, are detected and mitigated promptly, minimizing their impact on the organization.

The key goal of continuous monitoring is to maintain an active oversight of all critical areas, including financial transactions, employee actions, system activities, and customer behaviors, to detect any anomalies or irregularities. Automated monitoring systems play a crucial role in this process by using algorithms to flag suspicious activities, such as unusual transaction volumes, high-risk locations, or discrepancies in account behaviors, which may indicate fraudulent or illegal activities.

Real-time alerts are generated by these systems to notify relevant personnel immediately when an irregularity is detected. These alerts help mitigate potential risks by enabling quick responses and the initiation of appropriate actions, such as blocking suspicious transactions, initiating investigations, or escalating issues to senior management or regulatory bodies.

In addition to transaction and system monitoring, continuous monitoring involves overseeing compliance with internal policies and regulatory requirements. Regular checks ensure that employees, contractors, and third-party vendors adhere to set standards, and that any deviations are addressed before they lead to significant compliance risks.

The organization also applies continuous monitoring to cybersecurity, where systems are constantly scanned for vulnerabilities or unauthorized access attempts. This helps in identifying and neutralizing cyber threats in real time, ensuring that sensitive data is protected and that the integrity of the organization's IT infrastructure is maintained.

Employee monitoring is another critical aspect, focusing on adherence to ethical guidelines and policies. This includes reviewing access controls to sensitive information, monitoring for any signs of fraud or misconduct, and ensuring that employees are following the appropriate protocols in their day-to-day operations.

Through continuous monitoring, the organization creates a dynamic and responsive risk management environment. It allows for real-time risk detection, quick decision-making, and immediate action, ensuring that risks are minimized and operations remain smooth and compliant.

POLICY UPDATES AND COMPLIANCE REVIEW

To ensure continued relevance and effectiveness, this policy is subject to regular updates:

- Quarterly Internal Reviews: Compliance teams assess emerging threats and regulatory changes.
- Annual External Audits: Independent risk assessments validate compliance with EU AML Directives, FATF Guidelines, and GDPR regulations.
- Regulatory Adjustments: The policy is updated immediately in response to new AML laws, FATF sanctions updates, and EU financial crime directives.

Any significant changes are communicated to all employees and compliance teams through structured training sessions.

CONCLUSIONS

PayNox maintains a robust risk management framework that integrates AML, CTF, and cybersecurity controls. By continuously refining its Risk-Based Approach (RBA), leveraging blockchain analytics, and complying with FATF and EU AML directives, PayNox ensures regulatory compliance, financial security, and operational resilience.

This policy will be reviewed quarterly and updated as necessary to reflect the latest financial crime trends and regulatory requirements.

The implementation of a risk-based approach to decision-making helps prioritize high-risk areas and ensures resources are allocated efficiently to manage them. By adopting robust risk identification and assessment strategies, businesses can recognize vulnerabilities in their operations, whether they are related to customer activities, third-party relationships, or market conditions.

Furthermore, a comprehensive Risk Policy supports continuous improvement through regular monitoring and review of risk mitigation strategies, ensuring that they evolve with the changing business landscape. When accompanied by prevention, detection, and corrective controls, the policy can effectively reduce the likelihood of risks materializing.

Adopting ongoing monitoring allows businesses to adapt quickly to changes in the risk environment, making it easier to manage emerging threats, such as fraud or compliance issues. Additionally, maintaining an effective reporting system ensures that any potential issues are escalated and addressed in a timely manner, reducing the chance of major incidents that could affect the organization's integrity.

In conclusion, a solid Risk Policy helps ensure that your business is not only compliant with relevant regulations but is also prepared to handle various challenges and protect its assets, stakeholders, and reputation. By continually assessing risks and implementing appropriate controls, your business can maintain stability, foster customer trust, and safeguard long-term success.