© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

IMPROVING THE LEGAL FRAMEWORK FOR AI-BASED RISK MANAGEMENT IN CUSTOMS AUTHORITIES

Yusupov Baxit Sarsenbay uli
Head of the Division of the Legal Department
Customs Committee under the Ministry of Economy and Finance of the Republic of Uzbekistan
E-mail: bakhit@bk.ru
ORCID: 0000-0003-2745-1832

Introduction

The rapid development of digital technologies has significantly changed the methods and approaches used in public administration. Among these technologies, artificial intelligence (AI) is becoming an increasingly important instrument for processing large volumes of information, identifying patterns, forecasting potential risks and supporting administrative decision-making. Customs authorities are one of the areas where artificial intelligence can provide significant practical benefits because customs administration involves the processing of large amounts of information related to goods, customs declarations, transport vehicles, importers, exporters, countries of origin, customs values and international trade transactions.

Modern customs administration is increasingly based on the principle of risk management. The main purpose of customs risk management is to identify potential violations and concentrate control resources on transactions that require additional attention while facilitating the movement of low-risk goods. The World Customs Organization considers risk management one of the fundamental elements of modern customs administration and emphasizes the importance of risk assessment, profiling and targeting in customs control [1].

The development of artificial intelligence creates new opportunities for improving this process. AI-based systems can process large volumes of customs data, compare current declarations with historical information, identify unusual patterns, detect potential valuation anomalies and generate risk indicators. According to the World Customs Organization, artificial intelligence and machine learning can be applied in customs risk management, fraud detection, predictive analysis, image recognition and operational decision support [2].

For Uzbekistan, the introduction of artificial intelligence is also becoming an important component of digital transformation. The Presidential Resolution No. PQ-358 of 14 October 2024 approved the Strategy for the Development of Artificial Intelligence Technologies until 2030. The Strategy provides for the development of the regulatory framework for artificial intelligence, the establishment of security and ethical requirements, the development of standards and the expansion of AI applications in public administration and other areas [3].

At the same time, the implementation of AI-based risk management in customs creates a number of legal risks. An artificial intelligence system may produce an incorrect risk assessment due to inaccurate or incomplete data, algorithmic errors, outdated information or inappropriate model parameters. If such an assessment directly affects customs control, it may result in additional inspections, delays in customs clearance and other consequences for participants in foreign economic activity. Therefore, the development of AI-based customs risk management should be accompanied by an appropriate legal framework.

The purpose of this study is to examine the legal and organizational foundations of artificial intelligence-based risk management in customs authorities and to identify directions for improving its legal regulation. Particular attention is paid to algorithmic errors, data quality, transparency, human

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

oversight, accountability, cybersecurity and protection of the legitimate rights and interests of participants in foreign economic activity.

Main Part

Artificial intelligence-based risk management represents a new stage in the development of customs administration. Traditional customs risk management is generally based on predetermined rules, indicators and profiles. For example, a customs declaration may be considered potentially risky if the declared value of a product differs substantially from historical values, if the characteristics of the transaction are unusual, if the importer has a history of customs violations or if other established risk indicators are present.

Artificial intelligence can expand this approach by identifying complex relationships between multiple variables. Machine learning algorithms can analyze historical customs declarations and determine patterns associated with previous violations or unusual transactions. Based on these patterns, the system can generate a risk score for a new customs declaration. Consequently, the customs authority can use its limited control resources more efficiently.

The general mechanism of AI-based customs risk management can be described as follows: customs data are collected and processed, the artificial intelligence system analyzes the relevant information, a risk score or risk category is generated, the result is reviewed by a customs officer, and an appropriate customs control decision is subsequently adopted. This sequence demonstrates that the technological assessment and the legal decision should not be considered identical.

This distinction is particularly important from a legal perspective. An artificial intelligence system is capable of processing information and identifying statistical probabilities, but it does not independently possess the legal authority of a state official. Therefore, AI-generated risk assessments should generally be regarded as analytical information supporting the work of customs officers rather than as independent legal decisions.

The application of artificial intelligence in customs risk management can cover several areas. One of the most important is the automated analysis of customs declarations. An AI system can compare the information contained in a current declaration with historical transactions and identify unusual characteristics. Another important area is customs valuation. Machine learning models can identify significant deviations between declared values and comparable historical transactions. Artificial intelligence can also support commodity classification by analyzing product descriptions and comparing them with commodity codes.

Another area is supply-chain analysis. Customs authorities can use AI to analyze relationships among importers, exporters, suppliers, transport operators and other participants in international trade. This makes it possible to identify unusual networks and transaction patterns. AI technologies can also be used for analyzing X-ray images and other scanning information in order to identify potentially suspicious objects. International customs practice demonstrates that these technologies are already being tested and implemented in different customs administrations [2].

The World Customs Organization has identified risk management, predictive analytics, fraud detection, image recognition and other analytical functions as important areas for AI and machine learning in customs. At the same time, the organization emphasizes that the successful implementation of AI requires not only technical capacity but also appropriate governance, data management, cybersecurity, legal safeguards and human oversight [2].

One of the most significant legal risks associated with AI-based customs risk management is algorithmic error. Artificial intelligence systems depend heavily on the quality of the data used for training and operation. If the data contain errors, inconsistencies or incomplete information, the AI system may produce inaccurate results. For example, if historical customs information contains

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

incorrect valuation data, the algorithm may learn an incorrect relationship between certain goods and their customs values. As a result, a legitimate transaction may be classified as potentially risky.

This demonstrates that an AI-generated risk score cannot automatically be considered a legally established fact. It should be treated as an analytical indicator requiring verification. A customs officer should have the possibility to review the information underlying the risk assessment and determine whether additional control is actually justified.

Another important legal issue is algorithmic bias. Algorithmic bias occurs when an AI system systematically produces disproportionate results for certain categories of persons, companies, goods or transactions. In customs administration, this may occur when historical enforcement data are used without considering the circumstances under which those data were generated.

For example, if a particular group of importers was historically inspected more frequently, more violations may have been recorded among this group simply because the group was subject to more inspections. If the AI model learns from such historical data, it may subsequently assign higher risk scores to the same group. This may create a self-reinforcing cycle in which previous inspections generate more risk indicators, and those indicators generate further inspections.

Such a situation creates a potential conflict with the principles of equality, objectivity and proportionality in public administration. Therefore, AI models used by customs authorities should be periodically evaluated for statistical bias and excessive false-positive results. The World Customs Organization emphasizes the importance of fairness, transparency and accountability in the responsible use of AI and machine learning in customs [2].

Data quality is another fundamental issue. Customs risk management depends on a large amount of information, including declarations, commodity codes, values, quantities, countries of origin, transportation information and compliance history. If this information is incomplete, duplicated, outdated or inconsistent, the reliability of AI-generated risk assessments will decrease.

Consequently, data quality should be considered not merely a technical issue but also a legal and administrative issue. An inaccurate database can ultimately lead to an inaccurate administrative action. For this reason, customs authorities should establish procedures for data validation, correction, updating and quality monitoring before such information is used by artificial intelligence systems.

The protection of personal and commercially sensitive information is also an important legal consideration. Customs authorities process information that may concern individuals, companies, financial transactions, suppliers and international trade operations. When such information is processed through AI systems, additional risks associated with unauthorized access, disclosure or misuse may arise.

Uzbekistan has established legal mechanisms for the protection of personal data and cybersecurity, while the national AI strategy also emphasizes security and ethical requirements in the development and application of artificial intelligence [3]. Therefore, AI-based customs systems should be designed in accordance with data protection requirements and cybersecurity standards.

The principle of data minimization should also be considered. AI systems should process only information that is necessary for a clearly defined customs purpose. Access to sensitive information should be limited according to the responsibilities of individual users. System activities should be recorded, and unauthorized access should be prevented through appropriate technical and organizational measures.

Another important issue is the legal responsibility for AI-generated results. If an artificial intelligence system incorrectly identifies a customs declaration as high risk and this leads to an unnecessary inspection or delay, it becomes necessary to determine who bears responsibility for the resulting consequences.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

The AI system itself cannot independently bear legal responsibility in the same way as a state institution or authorized official. Therefore, the legal framework should clearly identify the responsibilities of the customs authority, officials responsible for the use of the system and, where relevant, private technology providers.

This requires the introduction of the principle of human responsibility. AI should provide analytical support, while the legally significant decision should remain attributable to an authorized official or institution. Such an approach is consistent with the broader principle that the use of technology by public authorities should not eliminate established procedural and legal safeguards.

Human oversight is therefore one of the most important principles of AI-based customs risk management. A customs officer should be able to examine the reasons for an AI-generated risk assessment, verify relevant information and determine whether additional customs control is justified.

The concept of "human-in-the-loop" provides a practical model for achieving this objective. Under such a model, the artificial intelligence system analyzes the available data and produces a risk assessment. The customs officer then reviews the result, considers additional circumstances and makes the final procedural decision. This approach allows the benefits of automation to be combined with human judgment and legal accountability.

Transparency is closely related to human oversight. If an AI system classifies a customs declaration as high risk, the customs officer should be able to understand the principal factors that influenced this classification. These factors may include significant differences in declared value, unusual commodity descriptions, inconsistencies in trade information, unusual transportation patterns or previous compliance information.

Full disclosure of the technical architecture or source code of an AI system may not always be necessary. However, the system should provide sufficient information to allow authorized officers to understand and review its main analytical factors. This is particularly important when the AI-generated result influences a decision affecting the rights or legitimate interests of a business.

The concept of explainable artificial intelligence can therefore play an important role in customs risk management. Explainability enables customs officers to understand why a particular transaction received a certain risk score and provides an opportunity to identify potential errors.

Cybersecurity is another major element of the legal framework. AI-based customs systems may become attractive targets for cyberattacks because they contain valuable commercial and administrative information. Unauthorized modification of risk parameters could potentially affect the selection of customs declarations for inspection.

Therefore, AI-based customs systems should incorporate strong authentication mechanisms, access control, encryption, activity logging, secure data storage and regular cybersecurity assessments. Changes to algorithms, risk parameters and system configurations should also be documented to ensure accountability and traceability.

The legal framework should also regulate relationships between customs authorities and private technology providers. If an external company develops or maintains an AI system for a customs authority, the relevant contractual arrangements should establish rules concerning data ownership, confidentiality, cybersecurity, access rights, system maintenance, intellectual property and liability.

The improvement of the legal framework for AI-based customs risk management should therefore be based on several fundamental principles. First, AI should be used only within legally established powers and procedures. Second, the final legally significant decision should remain under appropriate human oversight. Third, AI systems should be transparent and capable of providing understandable reasons for their outputs. Fourth, data used by AI systems should be accurate, relevant and regularly updated. Fifth, AI systems should be protected against cybersecurity threats. Sixth, responsibility for the use and results of AI systems should be clearly established.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

For Uzbekistan, the development of a specialized regulatory framework for AI-based customs risk management could significantly improve the predictability and accountability of AI applications. Such a framework could establish requirements for the testing, implementation, monitoring and auditing of AI systems used by customs authorities.

The first stage could involve a legal review of existing customs, personal data, cybersecurity and digital government legislation. The second stage could involve classifying AI systems according to their potential impact on the rights and interests of individuals and businesses. High-impact systems should be subject to stricter testing and monitoring requirements.

The third stage should involve pilot implementation. Before being used on a large scale, AI models should be tested in controlled operational environments. Their accuracy, stability, false-positive rates and legal implications should be evaluated. The fourth stage should involve regular algorithmic audits. These audits should examine whether the model remains accurate, whether data quality is sufficient and whether systematic bias has emerged.

The fifth stage should involve continuous monitoring. AI models cannot be considered permanently reliable because economic conditions, trade patterns, legislation and customs practices change over time. Therefore, models should be periodically updated and validated.

International experience can provide useful guidance for Uzbekistan. The World Customs Organization has developed extensive recommendations concerning the use of AI and machine learning in customs and emphasizes the importance of responsible adoption, data governance, cybersecurity, transparency and accountability [2]. India, for example, has developed AI and machine learning applications for customs risk management, including the analysis of suppliers, goods descriptions, supply-chain relationships and valuation risks [4].

However, international practices should not simply be copied. They should be adapted to Uzbekistan's national legislation, customs procedures, institutional structure and information infrastructure. The national Strategy for the Development of Artificial Intelligence Technologies until 2030 provides an important basis for developing such a national approach [3].

In this context, the creation of a specialized internal regulation for AI-based customs risk management could be considered. Such a document could define the objectives of AI use, categories of permitted applications, data governance requirements, human oversight mechanisms, algorithmic audit procedures, cybersecurity requirements, documentation standards and responsibility mechanisms.

The ultimate objective should not be the complete automation of customs decision-making. Instead, AI should be used to improve the ability of customs authorities to identify genuine risks while facilitating the movement of low-risk goods. Such an approach would combine technological innovation with the principles of legality, proportionality, transparency and accountability.

Conclusion

Artificial intelligence has significant potential to improve customs risk management by enabling customs authorities to process large volumes of information, identify unusual transaction patterns, predict potential risks and allocate control resources more efficiently. International experience demonstrates that AI and machine learning are increasingly being used in customs risk assessment, valuation analysis, commodity classification, supply-chain analysis, image recognition and fraud detection [2].

At the same time, the implementation of AI in customs administration is not exclusively a technological issue. It also represents a significant legal and institutional challenge. Algorithmic errors, algorithmic bias, poor-quality data, insufficient transparency, cybersecurity threats, unclear responsibility and excessive automation may create risks for both customs authorities and participants in foreign economic activity.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

The analysis demonstrates that AI-generated risk assessments should not automatically be regarded as legally binding decisions. They should primarily function as analytical tools supporting the activities of authorized customs officials. The final legally significant decision should be made in accordance with established legal procedures and subject to appropriate human oversight.

For Uzbekistan, the Strategy for the Development of Artificial Intelligence Technologies until 2030 creates an important foundation for establishing appropriate legal, ethical and security requirements for AI applications [3]. The development of customs digitalization provides an opportunity to incorporate these principles into the country's customs risk management system.

A modern AI-based customs risk management model should therefore be based on the following sequence: data collection and validation, AI analysis, risk assessment, explanation of the analytical result, human verification, legal decision and subsequent audit. Such a model can combine the analytical capabilities of artificial intelligence with the principles of human responsibility and legal accountability.

The improvement of the legal framework should include provisions concerning algorithmic testing, data quality, human oversight, transparency, cybersecurity, audit procedures and responsibility for AI-related errors. High-impact AI systems should be subject to stricter requirements because their outputs may directly affect customs control measures and the legitimate interests of businesses.

The effective use of artificial intelligence should ultimately contribute not to the indiscriminate expansion of customs control, but to its greater precision. The identification of genuinely high-risk transactions should be combined with the facilitation of low-risk trade operations.

Therefore, improving the legal framework for AI-based risk management in customs authorities should be regarded as an integral part of the digital transformation of customs administration. The combination of advanced analytical technologies with clear legal requirements, reliable data, human oversight, cybersecurity and accountability can create a more transparent, predictable and efficient customs risk management system.

References

1. World Customs Organization. Customs Risk Management Compendium. Brussels: World Customs Organization.
2. World Customs Organization. Detailed Report on the Adoption of Artificial Intelligence and Machine Learning in Customs. Brussels: WCO Smart Customs Project, 2025.
3. President of the Republic of Uzbekistan. Resolution No. PQ-358 of 14 October 2024 “On Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030”. Tashkent, 2024.
4. World Customs Organization. Artificial Intelligence and Machine Learning-Driven Codification of Entities and Goods Descriptions: Transforming Risk Management in Indian Customs. WCO News, 2025.
5. Republic of Uzbekistan. Customs Code of the Republic of Uzbekistan. Law No. O‘RQ-400 of 20 January 2016.
6. World Customs Organization. Risk Management Compendium: Volume 1. Brussels: WCO.
7. World Customs Organization. SAFE Framework of Standards to Secure and Facilitate Global Trade. Brussels: WCO.
8. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.
9. OECD. Recommendation of the Council on Artificial Intelligence. Paris: OECD, 2019.

© 2026 International Conference on Multidisciplinary Sciences and Innovations . All Rights Reserved.

10. European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024.
11. Republic of Uzbekistan. Law “On Personal Data”. No. O‘RQ-547 of 2 July 2019.
12. Republic of Uzbekistan. Law “On Cybersecurity”. No. O‘RQ-764 of 15 April 2022.
13. World Trade Organization. Trade Facilitation Agreement. Geneva: WTO.
14. World Customs Organization. WCO Data Model. Brussels: WCO.
15. World Customs Organization. Smart Customs Project. Brussels: WCO.