World Customs Organization

DETAILED REPORT ON THE ADOPTION OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN CUSTOMS

MARCH 2025

wcoomd.org

Funded by 中国海关 CHINA CUSTOMS

Detailed Report on

The Adoption of Artificial Intelligence and Machine Learning in Customs

March 2025

The content presented herein has been developed by a consultant under the Smart Customs Project. It does not reflect the views, opinions, or official positions of the World Customs Organization (WCO), its Members or the WCO Secretariat.

World Customs Organization

Table of Contents

Figures

Tables

Abbreviations

AI	Artificial Intelligence
CPUs	Central Processing Units
DNNs	Deep Neural Networks
DVC	Data Version Control
GACC	General Administration of China Customs
GDPR	General Data Protection Regulation
GNNs	Graph Neural Networks
GPUs	Graphics Processing Units
HITL	Human-in-the-Loop
HS	Harmonized System
IaC	Infrastructure-as-Code
IDE	Integrated Development Environment
IPR	Intellectual Property Rights
KCS	Korea Customs Service
LLMs	Large Language Models
ML	Machine Learning
MLOps	Machine Learning Operations
NLP	Natural Language Processing
OCR	Optical Character Recognition
OECD	Organisation for Economic Co-operation and Development
RAM	Random Access Memory
RBAC	Role-based Access Control
WCO	World Customs Organization
WTO	World Trade Organization

1 Executive summary

Artificial Intelligence (AI) and Machine Learning (ML) technologies are revolutionizing operations worldwide, offering unprecedented opportunities to enhance efficiency, improve decision-making and address complex challenges in global trade and border security. These technologies enable Customs administrations to automate routine processes, enhance risk assessment and fraud detection capabilities, optimize resource allocation and facilitate trade by streamlining clearance procedures. Key areas of AI/ML application include operational efficiency and trade facilitation, risk management, intelligence and surveillance, predictive analytics and real-time processing, as well as human resource management and capacity building.

To successfully implement AI/ML initiatives, Customs administrations must consider several critical factors. Legal and ethical frameworks governing AI use need to be carefully navigated to ensure compliance and responsible deployment. Data availability, quality and management are fundamental to the success of AI/ML projects, requiring significant investment in data preparation and governance. Technical infrastructure and expertise requirements must be met, necessitating both hardware and software investments as well as skilled personnel. A thorough cost-benefit analysis should be conducted to justify AI/ML investments, and pilot projects are recommended to test feasibility and effectiveness before full-scale implementation.

This Report provides Customs administrations with a comprehensive understanding of the minimum technical specifications, costs, trends, use cases, business processes, policy arrangements and legal requirements associated with AI and ML adoption. The objective is to equip WCO Members with the knowledge to make informed decisions about implementing AI/ML technologies and integrating them into their operations. By offering practical insights into these technologies, the Report seeks to reduce the digital divide among WCO Members, enabling more equitable access to AI/ML tools and helping Customs administrations address the challenges posed by an increasingly complex global trade environment.

The Report outlines a scalable technical framework for AI/ML implementation and integration, covering AI/ML development environments, data management and governance tools, model development and training platforms, and deployment options. This framework ensures that Customs administrations have a flexible technological foundation to support AI/ML initiatives effectively, allowing for gradual adoption and scaling based on individual needs and resources. Building Machine Learning Operations (MLOps) capabilities is crucial for accelerating AI development and deployment, improving model performance and reproducibility, and reducing risks associated with AI projects.

To prepare for AI/ML adoption, Customs administrations should invest in comprehensive training programmes to develop in-house expertise across various domains, including data science, software engineering and domain-specific knowledge. Fostering a culture of data literacy across the organization is essential to ensure that both technical and non-technical staff can effectively contribute to and benefit from AI/ML initiatives. Collaboration with external experts and academic institutions can provide valuable insights and keep Customs administrations at the forefront of technological advancements.

The implementation of robust data integration tools is crucial for seamless system interoperability, allowing AI/ML models to access, process and deliver actionable insights in real time across various systems. Security and compliance considerations are paramount in AI/ML adoption. Comprehensive cybersecurity measures, including data encryption, access control and compliance with data protection regulations, must be implemented to safeguard sensitive and trade data. Regular audits and monitoring of AI/ML systems are necessary to ensure ongoing compliance and detect potential biases or inaccuracies in model outputs.

The ethical implications of AI/ML in operations cannot be overstated. Customs administrations must establish clear guidelines for the responsible use of AI, addressing issues such as fairness, transparency and accountability. Regular assessments of AI systems for potential biases and unintended consequences are crucial to maintain public trust and ensure equitable treatment of all stakeholders in the trade ecosystem.

By embracing AI/ML technologies, Customs administrations can position themselves at the forefront of trade facilitation and border security. These advanced tools enable more efficient, transparent and secure international trade operations in an increasingly complex global environment. However, successful implementation requires a holistic approach that addresses technical, organizational and ethical considerations. With careful planning, investment in infrastructure and skills, and a commitment to responsible AI practices, Customs administrations can leverage these technologies to significantly enhance their capabilities, ultimately benefiting global trade and economic growth.

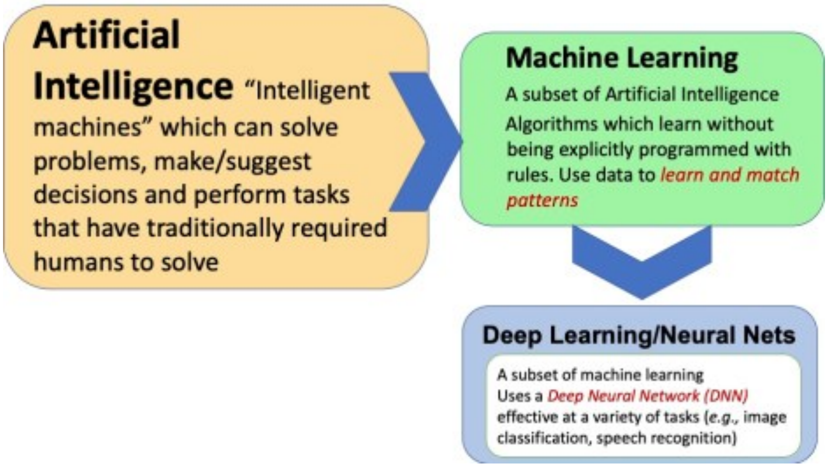
2 Overview of Artificial Intelligence (AI) and Machine Learning (ML)

Artificial Intelligence (AI) is a broad term encompassing technologies that enable machines to perform tasks traditionally requiring human intelligence. These tasks include problem-solving, decision-making and learning from experience. AI is not a singular technology but a collection of various techniques.

Machine Learning (ML) is a subset of AI. It involves training algorithms on data to recognize patterns and make predictions or decisions without explicit programming. For instance, a ML model can learn to differentiate between cats, dogs and humans on the basis of images, or to understand the content of text.

The below figures provide an overview of the relationship between AI, ML and deep learning, highlighting their definitions and key concepts, as well as explaining common terminologies used in AI and ML.

Figure 1 – What is AI/ML?[1]



2.1 AI/ML - a brief history

AI has undergone a dynamic and multifaceted evolution, marked by cycles of groundbreaking achievements and periods of scepticism due to scientific hurdles and inflated expectations.

In the foundational years of AI (1956–1974), the primary objective was to create intelligent machines through general search strategies capable of general problem-solving techniques. Scientists believed that if they represented tasks using symbols (like words or numbers), machines could use these symbols to reason and solve various problems. However, they soon realized that these broad, one-size-fits-all methods were not effective enough to achieve the desired level of intelligence or performance in machines.

In the 1980s there was a shift from a search-based paradigm to a knowledge-based paradigm, which led to embedding extensive domain knowledge into highly specialized AI expert systems, primarily designed to emulate the decision-making abilities of human experts in specific "domains". For instance, the U.S. Internal Revenue Service (U.S. IRS) experimented with expert systems to assist in tax auditing and fraud detection.[2] These systems aimed to replicate the decision-making abilities of experienced auditors by

[1] Blank, S. (2022). Artificial Intelligence and Machine Learning Explained. steveblank.com.

[2] McCoy, K. F. (1989). *The Use of Expert Systems in the IRS*. In Proceedings of the Annual Conference on Taxation (pp. 147–154). National Tax Association.

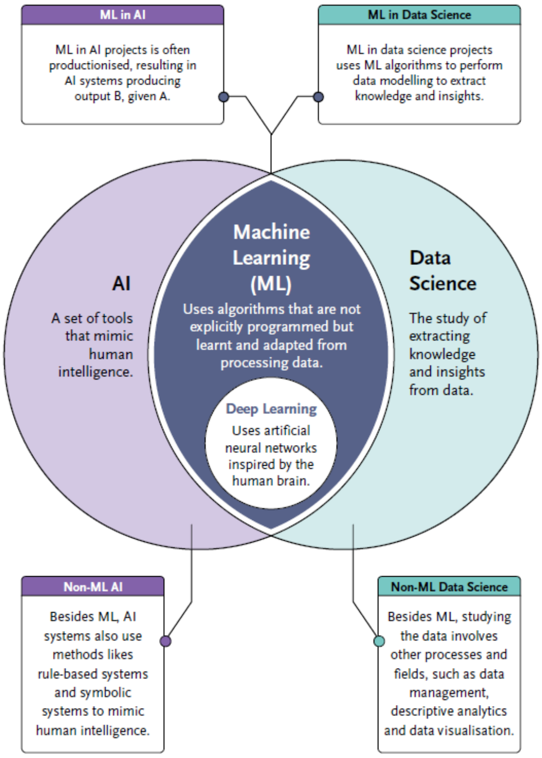
encoding tax laws and regulations into a knowledge base.[3] However, the complexity of tax codes and the nuances of individual cases often led to inaccurate assessments. Human auditors frequently had to intervene to interpret the results and make judgment calls, highlighting the systems' limitations. While expert systems showed promise, they were inherently brittle, performing well only within their narrow scope and relied heavily on human experts to bridge the gap between the designers' intentions and real-world applications.

From the 1990s to 2010, alternative approaches such as multi-agent systems and the semantic web were explored but achieved limited success. The semantic web aimed to make web content more accessible to machines by structuring data in a standardized format. Public sector initiatives like Data.gov in the United States and Data.gov.uk in the United Kingdom sought to leverage this technology for better data sharing among government departments and with the public. Projects were launched to promote open data standards. However, these systems faced challenges when scaling up to real-world complexity, including unpredictable human behaviour and environmental factors, and the lack of widespread adoption of semantic web technologies and interoperability issues limited their effectiveness.[4]

2.2 The rise of Machine Learning (ML)

While AI encompasses technologies that enable machines to mimic human intelligence, ML, a subset of AI, involves algorithms that learn from data to improve predictions. Data science integrates statistical methods and computational techniques to analyse and extract meaningful insights from structured and unstructured data sources. The figure below illustrates key AI, ML and data science terminology.

Figure 2 - AI, ML, data science terminology[5]



[3] A "knowledge base" is an information repository that enables knowledge sharing and problem-solving rather than just data storage, as in a "database".

[4] Heitmann, B., et al. (2009). *Implementing Semantic Web applications: reference architecture and challenges*. Proceedings of the 5th International Workshop on Semantic Web Enabled Software Engineering).

[5] Government Technology Agency of Singapore (2019), "Public Sector AI Playbook"

Expert systems from the 1980s were rule-based AI systems designed to simulate human decision-making using if-then rules and knowledge bases. While they represented early progress in AI, they had several limitations that ML later addressed. ML, a subset of Artificial Intelligence (AI), focuses on creating algorithms that enable computers to learn from data and make predictions or decisions without explicit programming. One of the most advanced forms of ML is deep learning, which relies on neural networks to identify patterns in large datasets.

Deep learning encompasses various neural network architectures, including Deep Neural Networks (DNNs) and Graph Neural Networks (GNNs). These architectures are inspired by the human brain and consist of layers of nodes (neurons) connected to each other. Each node processes information and makes decisions and passes the information and decisions along to the next layer, enabling the network to learn complex patterns and relationships within the data.

Deep Neural Networks (DNNs) emerged as a powerful alternative to earlier expert systems, leveraging data-driven learning to overcome challenges such as manually gathering expert knowledge and common-sense reasoning. DNNs excel at processing structured data in Euclidean space, such as images or text sequences. The rise of DNNs marked a turning point in AI, enabling breakthroughs like superhuman performance in image classification, game-playing, and major advancements in voice recognition and language translation.

Graph Neural Networks (GNNs), a more recent development, are designed to handle graph-structured data, addressing limitations of traditional neural networks in processing non-Euclidean data. GNNs can model complex relationships in data represented as graphs, such as social networks or molecular structures, by passing messages between nodes to capture both node features and graph structure. In Customs administration, both DNNs and GNNs play crucial roles. DNNs are often used in risk assessment and cargo inspection, analysing historical shipment data to identify patterns and detect anomalies that may indicate smuggling, fraud or misdeclarations. GNNs can be applied to analyse complex trade networks, identifying suspicious patterns in relationships between entities involved in international trade.

While these deep learning approaches have brought impressive advancements in AI, they come with challenges. They typically require large amounts of labelled data, which can create bottlenecks in development. Additionally, their complex structure with millions of parameters often makes them function as “black boxes”, making it difficult to understand how they arrive at decisions.

Despite these challenges, DNNs and GNNs continue to push the limits of AI with their high performance and ability to tackle complex tasks. DNNs excel in processing grid-like data, while GNNs open up new possibilities in handling relational data. This blend of high performance and complexity continues to shape the evolution of AI, pushing the boundaries of what machines can learn and achieve in various domains, including Customs operations.

2.3 The advent of generative AI (Gen AI)

Generative AI (Gen AI) represents one of the most advanced forms of AI, capable of producing new and original content by identifying patterns and structures within existing data. Its emergence has reshaped the AI landscape, pushing the boundaries of creativity, automation and problem-solving across industries.

Unlike traditional AI models that rely on predefined rules and structured outputs, generative AI learns to create unique outputs that resemble the data it was trained on. This capability has made it a powerful tool for applications such as text generation, image creation, video synthesis and music composition, transforming fields ranging from entertainment to marketing and education.

2.3.1 The technology behind generative AI

Many generative AI models rely on neural networks, particularly DNNs and GNNs. These neural network-based approaches have significantly contributed to the rapid growth and diversity of generative AI capabilities.

Initially, Deep Neural Networks (DNNs) laid the foundation for complex pattern recognition and data processing, enabling early generative models to create basic outputs in areas such as image and text generation. Building upon this foundation, Graph Neural Networks (GNNs) emerged, excelling at handling graph-structured data and facilitating tasks that involve relational information, such as molecule generation for drug discovery, social network analysis and recommendation systems.

A key advancement in the development of generative AI was the introduction of Transformer models - AI systems that understand and generate language by focusing on how words relate to each other in a sentence. These models transformed the field by using self-attention mechanisms, which enable them to assess and prioritize the relationships between words regardless of their position in the sentence. This innovation significantly enhanced the capability of models to manage and interpret massive datasets, leading to the creation of Large Language Models (LLMs) like GPT-3, GPT-4 and LLaMA. These LLMs demonstrated unprecedented proficiency in understanding and generating coherent, context-aware text, setting new benchmarks in natural language processing.

Concurrent with advancements in Transformer-based LLMs, the field of generative AI witnessed the emergence of diffusion models. Diffusion models create images by first adding random noise to data and then teaching the AI to remove this noise step by step. This approach allows the models to generate high-quality, photorealistic images. As a result, diffusion models have significantly improved the clarity and variety of images produced by generative AI, enhancing both their fidelity and versatility.

Hence, generative models continued to advance, supporting multimodal applications, extending their capabilities beyond text to encompass text-to-image and text-to-video generation. These multimodal generative AI systems leverage billions of parameters to produce coherent and contextually relevant content across various formats, thereby broadening the scope and applicability of generative AI in creative and analytical domains.

The expansion of generative AI beyond text has had profound implications for multiple industries. In art, design and marketing, advanced text-to-image models enable the creation of high-quality, photorealistic images from textual descriptions, fostering unprecedented levels of creativity and efficiency. Similarly, generative AI-driven video generation allows for the production of dynamic visual content from textual inputs or still images, revolutionizing content creation and media production processes.

Despite these advancements, generative AI introduces significant challenges. The complexity of these models necessitates specialized hardware, such as Graphics Processing Units (GPUs),[6] to perform computations efficiently. The substantial computational resources required for training and deploying these models raise concerns about environmental sustainability and the equitable accessibility of AI technology. Additionally, the intensive resource demands contribute to the centralization of AI capabilities, potentially limiting democratization and broader societal benefits.

Ethical considerations are paramount in the deployment of generative AI. These models can inadvertently reproduce or amplify biases present in their training data, resulting in discriminatory or inappropriate outputs. Furthermore, the potential misuse of generative AI for creating deepfakes or disseminating misinformation poses significant societal risks. Addressing these ethical challenges is crucial to ensure the responsible development and application of generative AI technologies.

---

[6] Graphics Processing Units (GPUs) handle parallel tasks, crucial for rendering images and training machine learning models.

Looking ahead, generative AI represents a significant milestone in the evolution of artificial intelligence, characterized by sophisticated neural architectures and versatile applications across various domains. The future of generative AI is poised to integrate diverse neural network architectures, including DNNs and GNNs, with rule-based systems and human expertise. This hybrid approach aims to enhance the flexibility and reliability of AI systems, enabling them to handle unexpected situations more effectively. Additionally, ongoing research focuses on improving the interpretability of AI models, ensuring ethical operations and enhancing sustainability by reducing the environmental impact of AI computations.

Table 1 outlines the hierarchical relationship between AI, ML, Deep Learning and generative AI, highlighting their definitions, focus areas, techniques, applications, advantages and data dependencies to clarify their distinctions and interconnectedness.

Table 1 - Differences between AI, ML, Deep Learning and generative AI

Category	Artificial Intelligence (AI)	Machine Learning (ML)	Deep Learning	Generative AI
Definition	A broad field of computer science focused on creating systems that simulate human intelligence, encompassing reasoning, learning and problem-solving.	A subset of AI focused on enabling systems to learn from data and improve their performance over time without being explicitly programmed.	A subset of ML that uses neural networks with many layers (Deep Neural Networks, DNNs) to model complex patterns in large amounts of data.	A subset of AI and Deep Learning designed to create new content, such as text, images, audio and video, by learning patterns from existing data.
Focus	Simulating human intelligence through reasoning, learning and decision-making to perform tasks typically requiring human cognition.	Enhancing system performance through data-driven learning, making predictions and identifying patterns based on historical data.	Processing large volumes of structured and unstructured data to recognize intricate patterns and representations, enabling tasks like image and speech recognition.	Generating new, creative outputs by understanding and replicating the underlying patterns and styles present in the training data, fostering innovation and content creation.
Techniques used	Rule-based systems, decision trees, expert systems, search algorithms, neural networks, natural language processing (NLP), computer vision.	Algorithms such as linear regression, logistic regression, decision trees, support vector machines, clustering and reinforcement learning.	Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Graph Neural Networks (GNNs), Transformers.	Variational Autoencoders (VAEs), Generative Adversarial Networks (GANs), Transformer-based models (e.g. BERT, T5), diffusion models, autoregressive models.
Examples of applications	Autonomous vehicles, virtual personal assistants (e.g. Siri, Alexa), smart home devices, robotics, game playing (e.g. AlphaGo).	Spam filtering, fraud detection, recommendation systems (e.g. Netflix recommendations), predictive maintenance, customer segmentation, stock market analysis.	Image and speech recognition (e.g. Google Photos, Siri), language translation (e.g. Google Translate), autonomous driving systems, medical image analysis.	Text generation (e.g. ChatGPT, Jasper), image creation (e.g. Midjourney, DALL·E), music composition (e.g. AIVA), synthetic media creation, video generation (e.g. Synthesia).
Key advantage	Enables automation and intelligent	Allows systems to learn and improve from data,	Highly effective for processing and	Excels at creating highly realistic and

	decision-making across a wide range of applications, enhancing efficiency and effectiveness in various domains.	making them adaptable and capable of handling complex tasks without explicit programming.	extracting meaningful insights from large and unstructured datasets, leading to superior performance in tasks like image and speech recognition.	novel outputs, fostering creativity, innovation and automation in content generation across multiple media types.
Data dependency	May or may not require large datasets; depends on the specific AI techniques and applications being utilized.	Requires structured and often labelled data for training to enable accurate learning and predictions.	Requires vast amounts of labelled or unlabelled data to effectively train deep neural networks, leveraging large-scale datasets for optimal performance.	Requires massive datasets to learn intricate patterns and styles, enabling the generation of diverse and high-quality content that mimics real-world data.

2.4 AI for Customs administrations

AI/ML are increasingly transforming Customs operations. By adopting AI/ML, Customs administrations can unlock the full value of their data, be it structured, semi-structured or unstructured. These technologies allow Customs administrations to analyse vast amounts of data and enhance decision-making in areas such as risk management, fraud detection, cargo inspection and resource allocation, thereby increasing overall efficiency. AI/ML also empowers Customs administrations to tackle global challenges like cross-border smuggling, non-compliance, and increasing volumes of e-commerce, and better adapt to the dynamic landscape of global trade and security challenges.

However, there is a growing digital divide among Customs administrations globally, with many WCO Members lacking the technical capacity or infrastructure to fully benefit from AI/ML technologies. Bridging this digital gap is critical to ensuring that all Customs administrations, regardless of their current technological capabilities, can adopt these powerful tools to modernize their operations and tackle emerging global challenges effectively.

3 AI/ML trends in Customs and trade

3.1 Advanced AI models

Advanced AI models are transforming Customs administration by enhancing risk assessment, fraud detection and cargo inspections through data-driven learning and pattern recognition. These include models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs)[7] to analyse patterns and generate realistic data, enabling document verification, anomaly detection and predictive analytics.

Large Language Models (LLMs), such as GPT-4 and LLaMA, leverage Transformer architectures to process natural language, making them ideal for automated document classification, processing Customs declarations and responding to inquiries. These models can extract insights from unstructured data, assist in risk profiling and streamline compliance checks. Additionally, AI-powered image recognition systems, based on deep learning, improve cargo scanning by identifying concealed items and anomalies in X-ray and scanning data.

Customs administrations benefit from reduced processing times, enhanced compliance and improved detection of illicit activities. The use of deep learning and reinforcement learning[8] in Customs not only accelerates operational workflows but could also provide a data-driven foundation for policymaking, enabling Customs administrations to adapt to changing trade dynamics and emerging threats more effectively.

As AI models continue to evolve, they are expected to integrate with a wide range of technologies, including IoT sensors, blockchain-based trade records, robotic process automation (RPA), Augmented Reality (AR) and Virtual Reality (VR), enabling more robust, transparent and efficient Customs operations.

3.2 The role of generative AI in Customs operations

Generative AI has introduced transformative capabilities in Customs operations since its emergence in 2022. Leveraging the large datasets from Customs management systems and Single Window platforms, Customs administrations can establish their own foundational LLM by adapting open-source LLMs, such as LLaMA,[9] and train them with Customs-specific data, including trade regulations, tariff codes, declaration forms and historical compliance records. By harnessing the power of natural language processing and context-aware learning, these foundational LLMs trained on massive Customs-related data can support complex tasks, such as document classification, risk profiling, fraud detection and policy enforcement. They can also analyse unstructured data, identify patterns and generate insights to improve targeting strategies and border security measures. Furthermore, generative capabilities allow LLMs to interpret trade regulations and assist in scenario planning, enhance strategic planning and improve overall efficiency. By effectively leveraging their own data alongside open-source LLM models, Customs administrations can harness the full potential of generative AI.

---

[7] Generative Adversarial Networks (GANs): AI models with two parts—one creates data and the other checks if it looks real. Both work together to produce realistic outputs like images, videos or text. Variational Autoencoders (VAEs): AI models that learn patterns in data and create new, similar examples based on those patterns. They can generate new data samples that are similar to the original data by sampling from learned patterns.

[8] Reinforcement learning is learning by trial and error, maximizing rewards through feedback.

[9] LLaMA (Large Language Model Meta AI) – open-source LLM developed by Meta, designed for research purposes.

3.3 Human-in-the-Loop (HITL) approach in Customs operations

While advanced AI/ML models and generative AI offer significant benefits to Customs operations, an important trend is the adoption of the Human-in-the-Loop (HITL) approach. This ensures that AI systems assist but do not replace human decision-making. HITL involves human oversight in the AI decision-making process, allowing Customs officers to review and validate AI recommendations, providing a balance between automation and human expertise.

3.3.1 Ensuring accountability and compliance

Validation of AI outputs: Customs officers can review AI-generated insights to ensure decisions align with legal and regulatory standards. While human validation helps maintain compliance, it should be supported by a robust integrity policy to mitigate risks of bias or corruption and uphold transparency in Customs operations.

Contextual understanding: Humans provide context that AI models may not fully grasp, such as geopolitical factors, cultural nuances or exceptional circumstances affecting trade practices. This ensures that decisions are appropriate and take all relevant factors into consideration.

3.3.2 Enhancing trust and transparency

Building confidence in AI systems: Involving humans in the loop increases trust among stakeholders, as decisions are not solely made by automated systems, instilling a level of assurance in processes that include human judgment. However, integrity and transparency safeguards have to be instituted to ensure fair and unbiased decisions.

Transparent decision-making: AI-only decisions may lack transparency because complex models like neural networks operate as "black boxes", making it difficult to trace how inputs lead to outputs. Without clear explanations, it becomes challenging to justify decisions, especially in legal and compliance contexts where accountability is required. HITL allows for explanations of how decisions are made, which is essential for transparency and accountability. Customs officers can provide rationales for actions taken, which is critical in legal and compliance contexts.

3.3.3 Managing ethical and legal considerations

Preventing bias and discrimination: Human oversight helps identify and mitigate any biases in AI models, ensuring fair treatment of all traders and compliance with anti-discrimination laws. This is particularly important when AI models are trained on historical data that may contain biases.

Legal responsibility: AI systems function as advisory tools to support decision-making. The decision-making responsibility still rests with human officers, who are accountable under the law. However, the issue of liability in AI-driven decisions remains an open question, highlighting the need for clear legal frameworks to address accountability as AI systems continue to evolve.

3.3.4 Adapting to dynamic environments

Handling unpredictable scenarios: Humans are better equipped to handle unforeseen events or anomalies that AI models may not have been trained on. In cases of unexpected global events affecting trade, human judgment is crucial.

Continuous improvement: Feedback from Customs officers can be used to retrain and improve AI models. This iterative process enhances the performance of AI systems over time, making them more effective and reliable.

3.3.5 Balancing efficiency with expertise

Optimizing workflows: HITL allows AI systems to handle routine tasks, freeing up Customs officers to focus on complex cases that require human judgment. This optimizes the use of human resources and improves overall efficiency.

Leveraging experience: Experienced officers can apply their expertise to interpret AI-generated data, leading to more nuanced and effective decision-making. Their insights can also guide the development of better AI models.

3.4 Cloud-based AI in Customs operations

Cloud-based AI, which provides services hosted via the Internet on remote servers, offers scalable processing power and data storage for AI applications. It has emerged as a significant trend, with an increasing number of organizations adopting cloud platforms to develop, deploy and scale AI solutions. This shift is driven by cost efficiency, as the pay-as-you-go pricing model eliminates the need for large upfront investments in hardware and maintenance, reducing overall operational costs. Cloud-based AI platforms enable rapid deployment of AI projects, efficient scaling of AI/ML operations and processing of large datasets without requiring extensive on-premises infrastructure.

Customs administrations, depending on data sensitivity and security requirements, can opt for *private cloud* models for greater control and security or *hybrid cloud*[10] models to balance scalability with data protection. These flexible options ensure accessible, scalable and cost-effective solutions while addressing data security and compliance concerns.

3.4.1 Addressing data security concerns

Cloud providers use strong safeguards to meet Customs administrations' data security needs. One important concept is *data residency*, which allows organizations to decide where (in which country or region) their data is physically stored. This helps them follow *data sovereignty* rules - laws that apply to data based on the country where it is stored.

Customs administrations can choose a private cloud or a hybrid cloud to have more control over sensitive information. These choices let Customs administrations decide where and how their data is stored and processed, ensuring they comply with local regulations and keep data safe.

Major cloud platforms also follow strict international security standards.[11] They use advanced methods such as encryption, multi-factor authentication and role-based access controls to ensure data remains secure and that only authorized users can access it.

[10] A private cloud is a cloud computing environment dedicated to a single organization, either hosted on premises or by a third-party provider, and not shared with other customers. A hybrid cloud combines both private and public cloud resources, allowing organizations to keep data in a secure private environment while leveraging the scalability and flexibility of the public cloud for less sensitive workloads.

[11] These include: ISO/IEC 27017, which provides guidelines for information security controls applicable to cloud services; and SOC (Service Organization Control) 2: a U.S.-based standard that details how service providers should manage customer data securely, often adopted internationally as well.

4 Legal requirements for AI/ML adoption

4.1 National approaches to AI regulation

Governments around the world are adopting varied strategies to regulate AI, reflecting differences in legal traditions, policy priorities and levels of technological advancement. These approaches can be broadly categorized into formal legislation, governance frameworks and guidelines, and hybrid models that combine elements of both.

4.1.1 Formal legislation

Some countries are enacting specific laws to regulate AI, creating legally binding obligations for developers, users and other stakeholders. The European Union (EU) exemplifies this legislative path with its European Artificial Intelligence Act (AI Act) which entered into force on 1 August 2024.[12] This comprehensive legal framework seeks to classify AI systems based on their risk levels - unacceptable, high, limited and minimal - and stipulates specific obligations for each category. For instance, high-risk AI applications, which could include Customs-related systems for risk assessment or fraud detection, would be subject to stringent requirements like conformity assessments, transparency mandates and provisions for human oversight. The objective is to ensure AI systems are safe, respect fundamental rights and promote trust across EU member states.

Similarly, China has established a multi-layered regulatory framework for AI that includes both laws and binding regulations, such as its Interim Administrative Measures for Generative Artificial Intelligence Services, effective 15 August 2023,[13] and Administrative Provisions on Recommendation Algorithms in Internet-based Information Services (2021).[14] China's approach is aimed at controlling AI development in line with interests and security concerns, as well as balancing innovation with national security, ethical concerns and societal values.

4.1.2 Governance frameworks and guidelines

Other countries prefer non-binding guidelines or frameworks to steer AI development responsibly without imposing strict legal constraints. The United States, for example, employs a sector-specific, flexible approach that emphasizes innovation. In 2020, the White House issued principles for regulating AI, focusing on public trust, transparency and fairness.[15] The National Institute of Standards and Technology (NIST) provides voluntary guidance to promote trustworthy AI. The objective is to foster AI innovation while addressing risks, without hindering technological progress with heavy regulations.

Japan has issued ethical guidelines rather than formal laws, aimed at fostering innovation while ensuring responsible AI development and deployment. The Japanese government has published, in their "Social Principles of Human-Centric AI", a set of ethical guidelines for AI that provide principles for responsible AI development and use.[16] These guidelines cover various aspects, including fairness, transparency, accountability and privacy. The government has also issued cross-ministerial guidelines on AI, which outline the roles and responsibilities of different ministries and agencies in promoting AI development and addressing potential risks.

---

[12] European Commission. (2024). Regulatory framework for AI. Shaping Europe's Digital Future.

[13] Cyberspace Administration of China. (2023). Measures for the management of generative artificial intelligence services.

[14] Cyberspace Administration of China. (2022). Administrative provisions on algorithm recommendation for Internet information services (Order No. 9).

[15] The White House - Office of Management and Budget (2020). Guidance for Regulation of AI Applications.

[16] Government of Japan. (2019). Social Principles of Human-Centric AI.

Singapore has adopted a light-touch proactive approach to AI governance and regulation, introducing the Model AI Governance Framework.[17] This framework provides voluntary guidelines for organizations to adopt when developing and deploying AI systems, offering practical guidance on internal governance, risk management and stakeholder communication. An AI Ethics Advisory Council was also established to provide ongoing guidance and promote ethical AI. The objective is to build public trust and encourage responsible AI innovation.

Australia released the "AI Ethics Framework", consisting of eight principles, including privacy protection, reliability, transparency and accountability.[18] This framework provides guidance for businesses to implement AI ethically, ensuring technologies are developed responsibly and align with societal values.

4.1.3 Hybrid approaches

Some countries combine elements of formal legislation with flexible guidelines, tailoring regulation to specific contexts. Canada's approach to AI governance is a hybrid, using a mix of mandatory policies and voluntary frameworks. The AI and Data Act (AIDA)[19] provides a legal framework for regulating AI systems, while ethical guidelines and voluntary frameworks, such as the Algorithmic Impact Assessment tool, provide guidance for organizations to develop and use AI responsibly. This hybrid approach allows Canada to balance the need for legal certainty with the flexibility to adapt to the rapidly evolving field of AI.

The United Kingdom employs a hybrid sector-specific regulation supported by overarching guidelines.[20] It focuses on principles like safety, transparency and fairness, implemented by existing regulators rather than new legislation. The UK government has published a National AI Strategy, which outlines its vision for AI development and sets out principles for responsible AI, as well as the AI Ethics Framework, which provides guidance on ethical considerations for AI development and use.

4.2 International efforts to regulate AI

International collaboration has been growing, with the United Nations (UN) and Organisation for Economic Co-operation and Development (OECD) announcing enhanced collaboration on AI governance. The OECD adopted AI Principles in 2019 (updated in 2024),[21] which is a set of guidelines to promote the development and use of trustworthy and responsible AI. The G7 and G20 have also established key recommendations to guide the responsible development and deployment of AI. The G7's AI recommendations include 11 guiding principles for safety and trustworthiness, along with a voluntary Code of Conduct promoting ethical and responsible AI development.[22] The G20 has, moreover, provided key guidance on AI governance, advocating responsible stewardship of trustworthy AI and encouraging member countries to develop national AI strategies reflecting their individual priorities and concerns.[23]

In March 2024, the UN General Assembly adopted a resolution on "Seizing the opportunities of safe, secure and trustworthy AI", emphasizing ethical AI principles and adherence to international human rights

---

[17] AI Verify Foundation (AIVF) and Infocomm Media Development Authority (IMDA) (2024). *Model AI Governance Framework for Generative AI*.

[18] Australian Government, Department of Industry, Science, Energy and Resources. (2019). *Australia's AI Ethics Framework*.

[19] Canadian Government (2022). *AI and Data Act ("AIDA")*

[20] UK Government, Department for Digital, Culture, Media & Sport. (2022). Establishing a pro-innovation approach to regulating AI: An overview of the UK's emerging approach.

[21] OECD. (2024). Shaping a human-centric approach to artificial intelligence: OECD AI Principles.

[22] G7. (2023). International Guiding Principles on Artificial Intelligence and Code of Conduct for Advanced AI Systems.

[23] G20. (2019). G20 AI Principles. In Annex to G20 Ministerial Statement on Trade and Digital Economy.

law. [24] Additionally, in 2021 UNESCO adopted the Recommendation on the Ethics of Artificial Intelligence, committing all 193 UN member states to ethical principles in AI development.[25]

4.3 Implications for Customs administrations

Globally, governments are navigating the challenge of regulating AI in a manner that safeguards societal values without hindering technological progress. Formal legislation provides clear, enforceable rules and legal certainty but may be rigid, risk stifling innovation, and can be slow to adapt to technological changes. Governance frameworks offer flexibility, encourage innovation and can be quickly updated, but their non-binding nature may lead to inconsistent adoption and enforcement. Hybrid approaches balance regulatory oversight with flexibility tailored to specific sectors, but they can create complexity in compliance and potential overlap between regulations and guidelines.

As AI laws and governance frameworks continue to evolve, Customs administrations face the complex challenge of ensuring compliance while remaining adaptable to new developments. The varied global approaches to AI regulation highlight the necessity for Customs administrations to stay vigilant and proactive in their adoption of AI/ML technologies.

To navigate this landscape responsibly and in accordance with relevant laws and guidelines, it is imperative for Customs administrations to remain informed about these diverse regulatory approaches and ongoing changes. This involves monitoring existing laws, proposed legislation and guidelines issued by national and international organizations. By understanding different regulatory models, Customs agencies can better prepare for the trustworthy and ethical integration of AI into their operations.

A proactive approach entails integrating legal obligations with ethical best practices, regardless of the specific regulatory environment in which they operate. Customs administrations can benefit from adopting best practices established in regions with advanced AI regulations, even if their own jurisdictions lack specific AI regulation. This strategy positions them to harness the benefits of AI effectively while upholding high legal and ethical standards. Key considerations include strict compliance with their jurisdiction's laws, the thoughtful adoption of international best practices and the flexibility to adjust strategies as new regulations emerge.

By embracing best practices from various regulatory models, ensuring adherence to applicable laws and maintaining readiness to modify strategies in response to regulatory evolution, Customs administrations can effectively leverage AI technologies. This approach not only enhances operational efficiency and effectiveness but also sustains public trust and supports the authority's mission to facilitate legitimate trade while ensuring security and compliance with international norms.

4.4 Data encryption, anonymization and consent management

Protecting personal and sensitive data is of paramount importance when adopting AI and ML technologies. Implementing robust technical measures is essential to mitigate risks associated with data processing. This includes the following:

- Data Encryption - it is imperative to use strong encryption protocols to safeguard data during transmission (encryption in transit) and while stored (encryption at rest), thereby preventing unauthorized access in the event of interception or breaches. Regularly updating encryption methods is also crucial to defend against evolving cybersecurity threats.
- Anonymization and pseudonymization - these are additional strategies to enhance data privacy. Anonymization involves processing data in such a way that individuals cannot be identified.

[24] United Nations. (2024). Governing AI for humanity: Final report. High-level Advisory Body on Artificial Intelligence.
[25] UNESCO. (2024). Recommendation on the ethics of artificial intelligence.

When data is fully anonymized, it often falls outside the scope of many data protection regulations, thus potentially reducing compliance burdens. Pseudonymization, on the other hand, entails replacing identifying information with pseudonyms, allowing for data analysis while offering increased privacy protection. It is important to note that pseudonymized data is still considered personal data under the GDPR and must be handled accordingly.

- Consent management - this is another critical aspect of data protection. For Customs administrations, data processing is often based on legal obligations rather than consent. However, consent is required in optional programmes such as voluntary traveller schemes or voluntary disclosure programmes. In these cases, consent must be freely given, specific, informed and unambiguous. Customs administrations should maintain records of consents obtained and provide easy withdrawal mechanisms where applicable.
- Algorithmic transparency and fairness - these are important considerations when implementing AI/ML systems. Striving to make AI/ML decisions understandable enhances trust and complies with transparency requirements outlined in regulations such as the GDPR. While complex algorithms can be opaque, providing explanations for decisions is crucial. Furthermore, it is vital to ensure that AI/ML models do not perpetuate discrimination. Regular testing and validation of models are necessary to detect and correct biases that could adversely affect decisions about individuals or groups.
- Data governance and security - this aspect must be prioritized to protect sensitive information. Implementing strict access controls limits data access to authorized personnel who require it for their roles, employing authentication and authorization mechanisms. Maintaining detailed audit trails on data processing activities is important for monitoring unauthorized access and facilitating audits.

4.5 Data use compliance and Intellectual Property Rights (IPR) compliance

When Customs administrations adopt AI/ML technologies, ensuring compliance with data use regulations and Intellectual Property Rights (IPR) is crucial. This is particularly important when handling sensitive trade information provided by traders as part of their legal obligations. Key considerations for data use compliance include the following:

- Legal basis: ensure that the use of trade data for AI/ML aligns with the legal basis under which it was collected, not exceeding the original purpose's scope.
- Confidentiality: implement robust measures to prevent unauthorized access or disclosure of sensitive information when using trade data for AI/ML.
- Data protection: mitigate privacy risks by anonymizing or aggregating trade data before AI/ML training, ensuring effective techniques to prevent re-identification.
- Third-party involvement: when external vendors are involved, ensure data sharing complies with data protection obligations through appropriate contractual clauses.
- International compliance: adhere to provisions in international trade agreements and conventions regarding trade data use and protection.

Regarding IPR compliance, Customs administrations must:

- Respect existing rights: ensure that AI models, algorithms or software used in their projects respect existing IPR laws.

- Proper licensing: obtain proper licences for AI tools and ensure that proprietary technologies are not used without authorization.
- Protect own IP: if developing custom AI solutions, protect their intellectual property to prevent unauthorized use or duplication.

By carefully managing data use, implementing robust safeguards and adhering to legal and ethical standards for both data and IPR, Customs administrations can leverage AI/ML technologies effectively while maintaining the trust and cooperation of the trading community. This approach ensures that sensitive trade information is handled responsibly and that all intellectual property rights are respected throughout the AI/ML adoption process.

4.6 Cybersecurity regulations

AI/ML adoption introduces new vulnerabilities, increases system complexity and exposes Customs administrations to potential cyber threats. These new vulnerabilities and risks must be managed to protect sensitive data, ensure the integrity of systems and maintain public trust. Compliance with cybersecurity regulations is essential to safeguard against threats that could compromise national security, disrupt trade or expose confidential information.

Therefore, a robust cybersecurity framework aligned with legal requirements is imperative. This includes:

- Complying with relevant cybersecurity regulations - Customs administrations must comply with a range of cybersecurity laws and regulations at both national and international levels. These regulations are designed to protect information systems, ensure data privacy and prevent unauthorized access or cyberattacks.
- International standards and guidelines - adhering to internationally recognized cybersecurity standards, such as ISO/IEC 27001, provides a structured approach to managing information security. Adhering to these standards helps organizations implement best practices and demonstrate compliance with international expectations.
- Comprehensive risk management - Customs administrations must conduct thorough risk assessments to identify and evaluate potential threats to their AI/ML systems and the data they handle. This involves analysing the likelihood and impact of various cyber threats, including data breaches, unauthorized access and cyberattacks specifically targeting AI algorithms.
- Advanced access controls - access control mechanisms are vital in protecting sensitive data and critical AI/ML systems. Customs administrations should enhance security beyond traditional password-based systems, for example, multi-factor authentication. Role-based access control (RBAC) should be employed to restrict access based on an individual’s role within the AI programme.
- Continuous monitoring and threat intelligence – to monitor the dynamic nature of cyber threats, Customs administrations can combine advanced monitoring tools with traditional security measures and human expertise. Regular security audits, threat hunting and manual reviews should complement automated detection systems.

5 Policy arrangements for AI/ML adoption

Adopting AI/ML technologies in Customs operations requires carefully designed policy arrangements that govern how these technologies are integrated, managed and utilized. Such policies will not only guide the responsible use of AI/ML systems but also support strategic alignment with organizational goals and ensure integration into a broader corporate digitalization strategy. These policies must also address legal requirements and ethical standards and uphold robust security measures. By establishing comprehensive policy frameworks, Customs administrations can harness the full potential of AI/ML technologies while mitigating associated risks and ensuring responsible innovation in their operations.

This section outlines the key policy arrangements for AI/ML adoption in Customs, considering the broader legal requirements already covered in the previous section, including data protection and privacy, data use and cybersecurity regulations.

Customs legal teams and regulatory advisors play a vital role in developing policies that address how AI/ML systems interact with these requirements, particularly regarding data use, algorithmic transparency and privacy considerations. Ensuring that AI/ML systems operate within legal constraints is critical for their safe and lawful implementation in Customs operations.

These policy arrangements should address governance, ethical use, data management, system design and deployment, capacity-building, regulatory alignment and continuous improvement.

5.1 Internal policies

Governance and oversight for AI/ML adoption - One of the foundational steps in AI/ML adoption is establishing a robust governance and oversight structure. Governance policies also address the division of roles and responsibilities, ensuring clear accountability for AI/ML usage as well as for addressing any errors, biases or ethical breaches. This includes establishing oversight committees or task forces comprising senior Customs officials, data scientists, IT personnel, legal advisors and policy experts to oversee AI/ML projects, ensuring strategic alignment with Customs operations and adherence to the broader legal framework. This governance ensures that all decisions are made transparently, risks are managed proactively and policies are updated in tandem with technological and operational changes.

Data management and security policies - Data management policies are central to AI/ML adoption, to govern data collection, quality, privacy and security. These policies must also address how data is shared across Customs departments, with other government agencies and with external partners to promote interoperability and facilitate integrated approaches to AI/ML adoption.

In parallel, data privacy policies are crucial for protecting sensitive trade, business and personal data. Policies must align with data protection regulations, such as safeguarding data against unauthorized access and misuse, ensuring consent for data collection and processing, and anonymizing personal information. Security policies provide guidelines for data encryption, secure storage and access controls to mitigate risks of data breaches and cyberattacks. Together, these policies help Customs administrations responsibly manage the vast volumes of data required for AI/ML operations, while complying with existing data protection and privacy regulations.

System design, development and deployment policies - Customs administrations need to design policies that guide the design, development and deployment of AI/ML systems. These should set clear standards for model validation, accuracy and suitability to ensure the design and development effectively supports Customs functions such as fraud detection, risk profiling and trade facilitation. Deployment policies ensure that AI/ML systems are implemented systematically, including guidelines on change management, user training and system integration into existing workflows. These policies should also address compliance with cybersecurity regulations, ensuring systems are resilient against threats and vulnerabilities.

Internal capacity and skills for AI/ML - To ensure successful AI/ML adoption, Customs administrations need to invest in developing internal capacity and the necessary skills. Policies should support comprehensive training programmes for Customs officers focusing on AI/ML principles, data analytics and system usage. Besides training, Customs administrations can facilitate partnerships with academic institutions, research organizations and private sector experts to foster knowledge exchange and access to the latest developments in AI/ML.

Policy alignment - Internal AI policies must align with external legal and regulatory requirements to ensure compliant and responsible adoption. Policies should be designed to adhere to existing legal frameworks around data protection, privacy, IPR and cybersecurity, as previously discussed in detail. These internal policies ensure that AI/ML technologies respect legal boundaries, trade regulations and cross-border compliance requirements.

Integration into operations - Finally, policy arrangements for AI/ML adoption must address how these technologies are strategically integrated into Customs operations. Policies should outline how AI/ML align with Customs business processes, trade facilitation goals and national economic strategies. Developing strategic roadmaps for AI/ML adoption allows Customs administrations to prioritize initiatives based on potential impact, scalability and operational relevance. These roadmaps ensure that AI/ML technologies not only support immediate Customs requirements but also contribute to long-term modernization, risk management and global trade goals.

In summary, the policy arrangements for AI/ML adoption involve a comprehensive approach that covers governance, ethical use, data management, system development, capacity building, legal compliance, continuous monitoring and strategic alignment. These policies form the backbone of responsible AI/ML adoption, ensuring Customs administrations can effectively harness technological advancements while adhering to ethical standards, legal requirements and operational goals. By developing and refining these policy arrangements, Customs administrations can position themselves to fully leverage AI/ML technologies for more efficient, transparent and secure trade processes.

5.2 Ethical frameworks and guidelines

Incorporating AI/ML technologies in Customs activities, such as risk assessment, targeting or fraud detection, raises ethical considerations that must be addressed through sound policy arrangements. Policies must ensure that the use of AI/ML aligns with principles of fairness, transparency and accountability. Customs administrations should develop ethical guidelines for AI/ML usage, setting standards for how these technologies are deployed, how decisions are made and how biases are mitigated.

Fairness and equity - One of the primary ethical considerations is ensuring fairness and equity in how AI/ML is applied to Customs operations. Algorithms used for decision-making in Customs, such as risk profiling or targeting shipments for inspection, have the potential to introduce biases that can disproportionately affect certain traders, geographic regions or product types. Policies must, therefore, mandate the detection, assessment and mitigation of biases within AI/ML systems.

Transparency and explainability - Transparency is critical to building trust in AI/ML systems. Policies must emphasize explainability, ensuring that AI/ML decision-making processes are understandable and interpretable. This is particularly important where AI/ML tools are used for risk assessment, determining which shipments are flagged for inspection and identifying potential compliance issues. Transparency policies should address the rationale behind AI/ML decisions and be documented and communicated clearly to stakeholders, offering insights into how certain conclusions are reached.

Human-in-the-loop decision-making - It is important to maintain human oversight in critical decision-making processes. Policies that promote a “human-in-the-loop” approach ensure that AI/ML outputs are reviewed and validated by trained Customs officers. Policies should define criteria for where and when a human review is required, i.e. a process in which Customs officers are needed to apply their expertise, judgment and contextual understanding to decisions, particularly in complex or high-stakes scenarios where AI/ML systems may face limitations.

Privacy and data ethics - The use of AI/ML in Customs operations involves processing large amounts of data, including sensitive trade information. To ensure ethical data use, policies must emphasize privacy protection and data ethics, going beyond mere compliance with legal regulations. Policies should ensure that only relevant data is used for AI/ML purposes, respecting the principles of data minimization and purpose limitation. Additionally, policies should promote transparency around data usage, informing stakeholders about what data is collected, how it is used and the protections in place to safeguard their information.

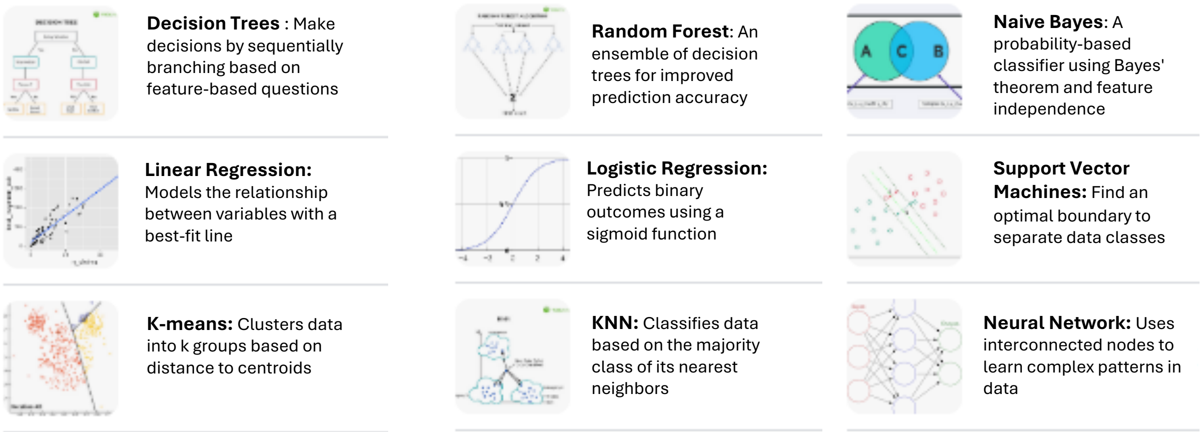
5.3 Bias mitigation in AI/ML models

Bias in AI/ML models is a critical concern for Customs administrations as it can lead to unintended consequences that compromise fairness, accuracy and trust in Customs operations. In Customs operations, biased AI/ML models can disproportionately flag certain traders, countries or goods as high risk, resulting in unfair treatment, trade barriers and a potential loss of credibility for the Customs administration. Mitigating bias is therefore essential for ethical and effective use of AI/ML, requiring targeted policy measures to identify, address and monitor potential biases throughout the model lifecycle.

Understanding sources of bias - To effectively mitigate bias, it is important to understand the different sources from which it can originate. Bias in AI/ML models can come from data-related issues, such as historical imbalances in the data used for training, incorrect or incomplete labelling of data and unrepresentative sampling that fails to capture diverse scenarios in Customs operations. For instance, if an AI/ML model is trained predominantly on data from specific export markets or product types, it may develop biased patterns that misjudge risk levels. Algorithmic bias can also occur if the model's design and feature selection inherently favour certain outcomes or reinforce existing prejudices. For example, if models overemphasize the country of origin in risk assessments, unfairly flagging certain nations; or feature selection prioritizes historical data patterns that reflect outdated prejudices in trade relationships. Policy considerations for bias mitigation must address these sources holistically, ensuring that both data and algorithm design processes are carefully scrutinized.

Data quality and representativeness - One of the primary strategies for bias mitigation is to improve data quality and ensure representativeness in AI/ML models. Policies should enforce data collection protocols that capture diverse and balanced datasets representing all segments of Customs operations, including different types of goods, trade routes, traders and compliance behaviours. This diversity helps prevent models from developing one-sided perspectives that may disproportionately impact certain groups or activities. Policies should also emphasize data cleaning and validation to remove errors, inconsistencies and outliers that may distort model learning and lead to biased predictions. Furthermore, guidelines should require that data be periodically refreshed and updated to reflect current trade patterns and behaviours, reducing the risk of biases stemming from outdated information.

Figure 3 – Common ML algorithms



Algorithm design and fairness policies - Addressing algorithmic bias requires careful consideration of how AI/ML models are designed, trained and validated. Policies should mandate fairness constraints during model development, ensuring that the algorithm does not favour one group, region or type of trade over others without justified operational reasons. This can involve applying fairness learning techniques, such as balanced weighting of features, re-sampling of training data and incorporating fairness metrics as part of model evaluation criteria. For instance, Customs administrations may establish policies requiring that AI/ML models achieve balanced accuracy across different trader profiles or trade lanes, preventing disproportionate flagging or scrutiny of specific entities. Policies should also outline processes for algorithm testing against multiple scenarios to detect and rectify any biases before deployment.

Regular monitoring for bias - Bias mitigation is not a one-time effort but an ongoing process that requires continuous monitoring and evaluation. Policies must establish frameworks for regular audits of AI/ML models, focusing on identifying signs of bias and unintended disparities in model outcomes. Such audits can be conducted by internal teams or external, independent experts to objectively assess whether AI/ML predictions align with fairness principles and operational goals. Monitoring policies should include routine checks of model outputs to detect any systematic patterns of biased decision-making and require timely corrective actions when such biases are identified. These corrective actions could involve retraining the model with more representative data, adjusting algorithms to better balance outcomes, or revising operational processes to ensure fairer use of AI/ML decisions.

Transparency and accountability mechanisms - Transparency in AI/ML operations is critical for bias mitigation, to understand how models work and identify potential areas of concern. Policies should require that Customs administrations document and communicate the design, development and deployment processes of AI/ML models, including the steps taken to identify and mitigate bias. Such transparency enables stakeholders, whether internal staff, traders or external partners, to provide feedback and hold the Customs administration accountable for fair outcomes.

In summary, mitigating bias in AI/ML models is a multifaceted effort requiring policies that address data quality, algorithm design, transparency and continuous monitoring. By implementing these policies, Customs administrations can ensure that their AI/ML systems support fair decision-making, enhance operational effectiveness and maintain stakeholder trust. Bias mitigation not only upholds ethical standards but also ensures that AI/ML technologies are aligned with the principles of fairness, equality and accountability in Customs operations.

6 Stakeholder engagement and communication

Engaging stakeholders effectively in AI/ML initiatives is critical for a Customs administration to ensure that these technologies are effectively adopted and address the needs and concerns of all parties involved. Stakeholder engagement should be extensive and inclusive, involving internal staff, external partners, other government agencies, industry associations, academia and the general public. The engagement process aims to foster collaboration, obtain feedback and ensure alignment with overall objectives, enhancing the efficiency, transparency and responsiveness of Customs operations.

Internal staff engagement - For internal stakeholders like Customs officers, IT teams and management, engagement starts with capacity-building initiatives and awareness programmes. Customs administrations can hold training sessions and workshops to educate internal staff about the potential of AI/ML technologies and how they can streamline Customs procedures. Regular open meetings across the administration and cross-departmental forums enable open dialogue on concerns, suggestions and practical considerations for implementing AI/ML. Involving staff early in the process builds ownership and ensures that operational insights are integrated into AI/ML solutions. An internal advisory group consisting of management, Customs officers and IT personnel can provide continuous feedback on the development and deployment of AI/ML initiatives, fostering an environment where staff feel they are contributors rather than just end-users.

External partner engagement - External partner engagement is crucial for successful AI/ML implementation in Customs operations. Customs administrations can create forums and working groups to bring stakeholders like importers, exporters and logistics companies together to discuss how AI/ML tools can improve trade processes. Stakeholder roundtables and focus groups allow partners to voice operational challenges, ensuring their needs are considered during project design. Regular updates and consultations ensure transparency and provide feedback opportunities.

Engaging industry associations provides access to a collective voice of businesses affected by Customs operations. Collaborative workshops and pilot programmes with industry participation can lead to more effective AI/ML solutions tailored to specific needs. This approach facilitates smoother implementation due to pre-established buy-in from member companies. By fostering open dialogue and collaboration, Customs administrations can develop effective solutions, address challenges proactively and gain broader support for their digital transformation efforts.

Engagement with other government agencies - Collaboration with other government agencies, such as border security, law enforcement and regulatory authorities, is crucial for the alignment of AI/ML initiatives across governmental functions. Customs administrations can set up inter-agency task forces to discuss shared goals and identify synergies between different agencies' AI/ML programmes. These task forces serve as coordination platforms to avoid duplication of efforts and ensure seamless data sharing, promoting efficient inter-agency processes. A Memorandum of Understanding (MoU) between agencies can outline specific collaboration mechanisms, roles and responsibilities for developing and implementing AI/ML initiatives that support broader government objectives like national security and regulatory compliance.

Engagement with academia - Involving academia, including universities and research institutions, is a valuable for integrating cutting-edge research and technological advancements into AI/ML projects. Customs administrations can collaborate with academic institutions through partnerships, research grants or joint projects to leverage AI/ML expertise for Customs applications like predictive analytics, risk assessment and data analysis. By engaging academic experts, Customs administrations can stay informed about emerging trends and best practices in AI/ML and incorporate innovative approaches to problem-solving. Regular academic symposiums or roundtable discussions can ensure ongoing dialogue, enabling academia to provide constructive feedback on the effectiveness and ethical considerations of AI/ML tools in Customs operations.

Public engagement - For public stakeholders, transparency and openness are key. Customs administrations can use public consultations, information sessions and online platforms to inform the public about AI/ML initiatives, solicit feedback and address concerns regarding data privacy, security and overall impact. Surveys and questionnaires distributed through digital channels provide a way to gather public input efficiently, ensuring that the implementation of AI/ML initiatives aligns with societal expectations and regulatory standards. Open dialogues, such as open meetings across the Customs administration or online discussion forums, enable the public to voice their opinions and gain clarity on how AI/ML will enhance Customs processes while safeguarding public interests.

6.1 Feedback mechanisms and integration into planning and execution

To collect and analyse stakeholder input effectively, Customs administrations should establish robust feedback mechanisms, such as surveys, focus group discussions, advisory committees and continuous monitoring systems. Regular surveys targeting different stakeholder groups (e.g. internal staff, external partners and the public) can gauge awareness, perceptions and satisfaction regarding AI/ML initiatives. Public consultations provide a forum for open feedback, while advisory committees consisting of representatives from each stakeholder group ensure that input is gathered in a structured manner. These feedback mechanisms allow Customs administrations to understand the diverse needs and concerns of all stakeholders, enabling informed decision-making.

Input gathered from these feedback mechanisms should be considered carefully in project planning and execution, ensuring that it influences project design, deployment and optimization. This process involves analysing feedback, prioritizing suggestions based on impact and feasibility, and communicating back to stakeholders on how their input is being integrated. Regular updates and transparent reporting on AI/ML projects foster trust and demonstrate that stakeholder concerns are taken seriously. By aligning these feedback mechanisms with stakeholder engagement strategies, Customs administrations can build stakeholder buy-in, facilitate smooth adoption and improve the effectiveness of AI/ML initiatives. This continuous cycle of engagement and feedback not only ensures project success but also promotes long-term stakeholder collaboration and support for future technological advancements.

6.2 Transparency and communication

To ensure transparency and maintain open communication, it is essential to effectively communicate the outcomes and success stories of AI/ML projects to stakeholders and the public. This communication builds trust, encourages engagement and showcases the value these technologies bring to Customs operations and trade processes. Various strategies can be employed to reach different audiences while highlighting the benefits and successes of AI/ML initiatives.

Success stories and case studies - Publishing detailed success stories and case studies can effectively demonstrate the tangible benefits of AI/ML projects. These case studies should highlight specific challenges faced, how the AI/ML solutions were implemented and the measurable improvements achieved, such as reduced clearance times, improved accuracy in risk profiling or enhanced trade facilitation.

Stakeholder events and workshops - Regular stakeholder events, such as workshops, forums and briefings, are important platforms for presenting AI/ML project outcomes directly to targeted audiences, including internal staff, industry partners and other government agencies. These events facilitate two-way communication where successes are not only shared but also discussed openly, allowing stakeholders to ask questions and provide feedback. Demonstrations of AI/ML tools in action during these events offer an opportunity to showcase their functionality and impact firsthand.

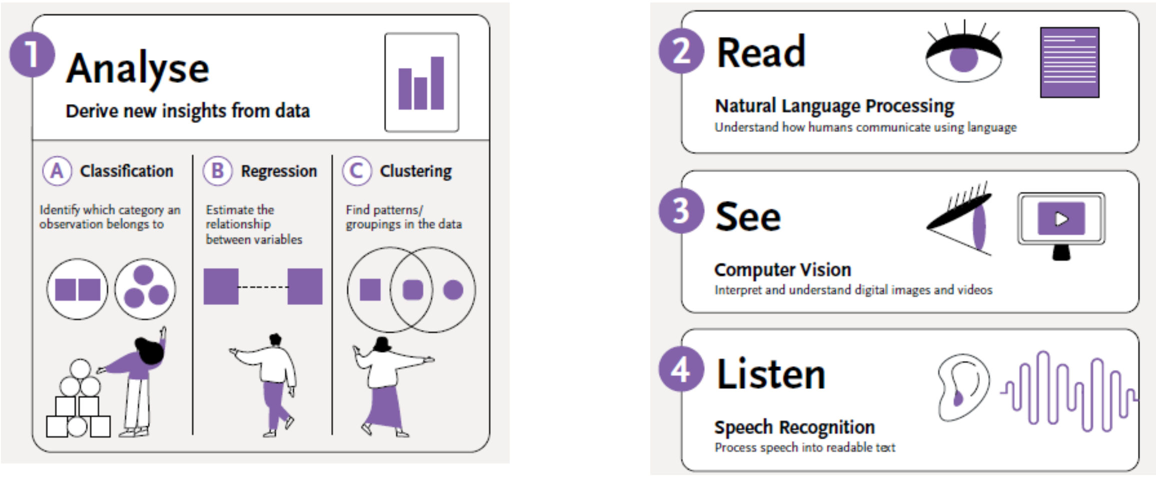
Public information and social media campaigns - Launching public information campaigns and outreach programmes tailored for the public can enhance transparency and help demystify AI/ML technologies used in Customs. Leveraging traditional media (e.g. press releases, television interviews) and social media platforms (e.g. LinkedIn, Twitter and YouTube) provides broad outreach for sharing project achievements. This helps reach a wide audience and establish public awareness. Social media campaigns using posts, infographics and videos can communicate complex AI/ML outcomes in a simple, engaging manner and encourage public interaction.

Conferences and Academic Publications - Participating in international conferences, industry events and academic forums provides opportunities to share best practices, lessons learned and AI/ML project outcomes with a broader audience, including other Customs administrations, policymakers and researchers. Publishing white papers, research articles and technical documentation in academic journals or industry publications can establish the Customs administration as a leader in adopting AI/ML technologies and provide a platform for deeper engagement with the academic and research community.

7 Key considerations for Customs administrations embarking on AI/ML projects

The figure below depicts some of the key capabilities of AI/ML technologies. Not all challenges are suitable for AI/ML solutions; for example, highly nuanced issues involving the interpretation of complex trade regulations may still require human oversight. While AI/ML offers immense potential for enhancing Customs operations, embarking on these projects requires a thoughtful and strategic approach.

Figure 4 – Key capabilities of AI/ML technologies26



Building upon the legal, ethical and governance considerations discussed in previous sections, this section focuses on practical factors that Customs administrations should evaluate when pursuing AI/ML initiatives. Addressing the following considerations ensures the successful implementation and sustainable integration of AI/ML technologies within Customs operations:

7.1.1 Problem definition and alignment

Problem definition is a crucial first step to ensure that the project targets the right issue and maximizes the potential benefits of AI/ML solutions.

Customs administrations should begin by identifying specific pain points in their processes, such as long clearance times, inefficient inspections or difficulties in detecting non-compliant activities. AI/ML technologies lend themselves particularly well to areas where large volumes of data need to be processed, or where repetitive, rule-based tasks, such as document processing, risk assessments, can be automated to improve efficiency.

A well-defined problem, grounded in the understanding of AI/ML's strengths and limitations, is essential to successfully implementing AI/ML projects that deliver tangible, impactful results for Customs operations.

By ensuring that the identified problem aligns with areas where AI/ML can offer significant value, Customs administrations can avoid investing in complex technologies for issues that may be more effectively resolved by simpler automation or rule-based systems.

[26] Government Technology Agency of Singapore (2019), "Public Sector AI Playbook"

7.1.2 Data availability and quality

Data availability and quality are critical considerations for Customs administrations embarking on AI/ML projects. Customs administrations collect vast amounts of data, often reaching terabytes annually, as part of their regulatory mandate. This includes structured information, such as import/export declarations, transaction records and tariff classifications, as well as unstructured data, including scanned documents, communication logs and multimedia files from inspections. Additionally, much of this data is historical and archival, providing a wealth of information accumulated over years or even decades.

While AI/ML models require large volumes of data for training and validation, the success of these initiatives depends not just on the volume, but also on the quality and relevance, of the data. For instance, developing an AI model for fraud detection would require detailed historical trade data, transaction records and known patterns of fraudulent activities. This data should capture a wide range of variables, such as product classifications, declared values, trade routes and entities involved, allowing AI/ML models to learn complex patterns and make accurate predictions.

However, simply having a large volume of data is insufficient; it must also be of high quality and relevant to current operations to ensure that AI/ML models produce useful and actionable results. Poor data quality, characterized by inaccuracies, incomplete records, inconsistencies or outdated information can severely impact model performance, leading to flawed predictions. High-quality data must be accurate, complete, consistent, timely and relevant. Achieving this level of quality is challenging for Customs administrations, particularly because much of the data comes from legacy systems or is archival and may contain errors due to manual entry, inconsistencies in classifications or incomplete documentation. Moreover, the evolution of data formats over time can create additional inconsistencies in how information is recorded, making it difficult to ensure uniformity across different datasets.

To mitigate these issues, Customs administrations must invest time and resources into data cleansing and preparation. This process will involve correcting errors, standardizing formats and ensuring that the data is comprehensive and up to date, ultimately improving the reliability of AI/ML model outputs. Section 9 of this Report, on data management, outlines the essential steps for managing data within Customs, serving as a foundational prerequisite for launching AI/ML projects.

7.1.3 Technical feasibility

When embarking on AI/ML projects, one of the key considerations for Customs administrations is technical feasibility. This involves assessing whether the necessary infrastructure, expertise and resources are available to support the implementation and success of AI/ML initiatives. The first step in this assessment is evaluating the existing technical expertise within the Customs administration.

AI/ML projects require specialized skills in data science, ML and data engineering, as well as proficiency with the necessary hardware and software tools. If these skills are lacking, Customs administrations may need to invest in staff training or seek external expertise through partnerships with technology vendors, consultants or academic institutions.

In addition to expertise, the availability of the necessary hardware, such as high-performance computing systems capable of handling large datasets and software, including AI/ML frameworks, is crucial. Customs administrations must ensure that their infrastructure is capable of supporting the storage, processing and analysis of vast amounts of data, as well as the iterative nature of AI/ML model development.

Section 10 of this Report subsequently outlines the minimum technical specifications and human resources required for AI/ML implementation and integration. Customs administrations can use these guidelines to assess both the technical feasibility of their projects and their organizational capacity to support AI/ML initiatives. This includes evaluating whether they possess the necessary infrastructure, expertise and resources to effectively implement AI/ML solutions. By referencing these specifications, Customs administrations can determine whether their current capabilities align with the demands of AI/ML projects or whether investments in training, technology or external partnerships are needed.

7.1.4 AI output challenges

The accuracy of the outputs generated by AI is paramount for Customs administrations. AI/ML models are not inherently neutral; they are shaped by the data they are trained on and the methods used to develop them. One significant concern is the risk of **biases** in the data, as discussed above.

Another key issue is the occurrence of **hallucinations and inaccuracies** in AI/ML models. AI/ML systems sometimes generate outputs based on incomplete or ambiguous data, leading to "hallucinations", where the model provides inaccurate or misleading predictions. In a Customs context, this could result in incorrect flagging of shipments for inspection or improper risk assessments. Ensuring the accuracy of the AI models and verifying their predictions against real-world outcomes is critical to maintaining fairness and trust in AI/ML-based decisions. The table below provides examples of common biases, hallucinations and inaccuracies in AI/ML models.

Table 2 - Most common biases, hallucinations and inaccuracies in AI/ML models

	Type of issue	Description	Example in Customs operations
1	Selection bias	Occurs when training data is not representative of the full range of Customs scenarios, leading to models favouring specific cases.	An AI model trained predominantly on high-value cargo data might overlook risks associated with low-value shipments.
2	Historical bias	Reflects patterns and biases in historical data, potentially reinforcing outdated trends and prejudices.	A model may disproportionately flag shipments from certain countries based on outdated risk data.
3	Algorithmic bias	Results from model design where certain features are over-emphasized, leading to skewed predictions.	A model may overestimate the value of goods, causing frequent inspection of high-value items only.
4	False positives in risk detection	When the model incorrectly flags shipments as high risk, leading to unnecessary inspections.	A harmless shipment may be flagged as containing prohibited items, causing trade delays.
5	False negatives in risk detection	When the model fails to identify actual high-risk shipments, allowing them to pass undetected.	A shipment of illegal goods might be labelled as "low risk", failing to trigger proper inspections.
6	Overfitting bias	Occurs when the model is overly trained on specific patterns, failing to generalize to new data effectively.	A model focused on specific seasonal data might fail to accurately assess shipments outside that context.
7	Hallucination of risk factors	When the AI fabricates or overstates risk factors without factual basis, leading to incorrect assessments.	A model might flag innocuous shipments as high risk based on unfounded correlations or assumptions.
8	Data drift misinterpretation	When changes in input data are not recognized, leading to inaccurate predictions or outdated risk profiles.	An AI model trained on pre-pandemic data may not adapt to post-pandemic trade patterns.

7.1.5 Cost-benefit analysis

When embarking on AI/ML initiatives, Customs administrations must conduct a thorough cost-benefit analysis to make informed decisions that balance immediate financial considerations with long-term strategic objectives. This assessment should factor in the long-term strategic value of AI adoption, including its potential to transform operational paradigms and enhance decision-making capabilities.

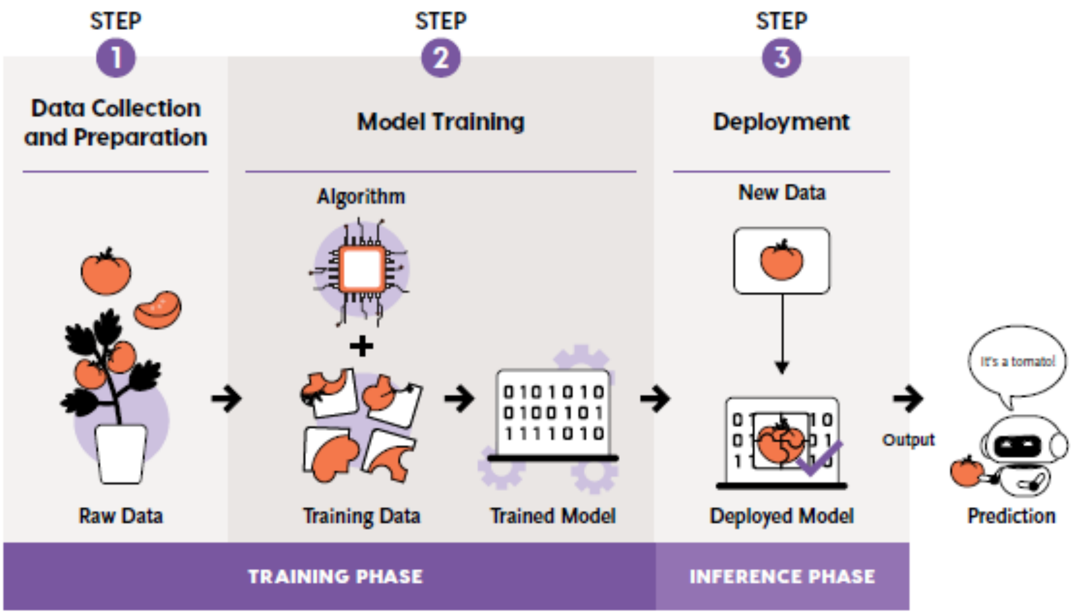
Customs administrations should evaluate the hidden costs associated with data governance, infrastructure upgrades and ongoing maintenance of AI systems.

The analysis should also consider the potential for AI to unlock new revenue streams through improved fraud detection and more efficient resource allocation. Intangible benefits, such as enhanced stakeholder trust and improved trade facilitation, should be quantified where possible. Customs should assess the opportunity costs of not adopting AI, particularly in light of evolving global trade dynamics and emerging security threats. The cost-benefit framework should be flexible enough to account for the rapid pace of technological advancement, allowing for iterative adjustments as AI capabilities evolve.

7.1.6 Pilot projects

When starting AI/ML projects, Customs administrations should consider launching a pilot project to test the feasibility and effectiveness of AI/ML solutions in a controlled environment. A pilot project allows Customs to assess the performance of the AI/ML models, gather feedback and make adjustments before a full-scale implementation. By following a structured three-step approach, Customs administrations can evaluate the practical benefits and limitations of these technologies while minimizing risks.

Figure 5 - Stages of developing and deploying an AI pilot system[27]



The first step in this approach is **data collection and preparation**. Customs administrations should begin by gathering the relevant training data, which could include historical Customs declarations, transaction records or inspection data. This data needs to undergo careful processing, such as removing duplicates, standardizing formats and handling missing values. Additionally, many AI/ML projects require labelled data, especially for supervised learning, where the desired outcome needs to be clearly defined. Labelling can be time-consuming but is essential for ensuring that the model learns from accurate and relevant examples. Once the data has been prepared, it is typically split into three sets: a training set to develop the model, a validation set to fine-tune it, and an evaluation set to test the final performance. Further details of data preparation are elaborated in the following As on data management.

[27] Government Technology Agency of Singapore (2019), "Public Sector AI Playbook"

The second step involves **model training**, which consists of several key phases. First, Customs administrations must select the most appropriate algorithm for their problem. This decision is guided by the nature of the data and the specific task the model is designed to address, such as classification, prediction or anomaly detection. Once the algorithm has been chosen, the training process begins, where the model learns to perform a task by analysing the training data. During this phase, the model is regularly validated using the validation dataset to adjust parameters and improve accuracy. Finally, the model is evaluated using the evaluation dataset to ensure it performs well on unseen data, simulating real-world conditions. This rigorous process ensures the model is reliable and ready for the next step.

The third step is **deployment**, where the trained model is introduced into the Customs administration's operational processes. At this stage, the model begins predicting new input data based on what it has learned from the training process. Since this is a pilot project, the deployment is closely monitored and the model's performance is continuously assessed. This allows Customs administrations to identify potential improvements or adjustments and address any issues before wider implementation. Monitoring the model in a real-world setting ensures that it continues to provide valuable insights and predictions, even as the data or environment may change.

8 Data management

Customs administrations routinely collect vast amounts of data in various forms - structured, semi-structured and unstructured - as part of their day-to-day operations. According to a 2018 WCO News article, even then the Korea Customs Service (KCS) was accumulating 45 GB of structured data and 30 GB of unstructured data every day,[28] amounting to over 25 TB annually, a figure that is likely to be considerably higher today. This data ranged from structured Customs declarations and cargo manifests to semi-structured data, e.g. Electronic Data Interchange (EDI) messages from Internet of Things (IoT) devices, and unstructured formats like scanned documents, x-ray images and surveillance footage. Despite the abundance and richness of this data, many Customs administrations have yet to fully harness its potential to enhance their core functions, such as revenue collection and protection, trade facilitation and border security.

The current challenge lies in effectively integrating and analysing this diverse data to draw actionable insights. Traditional data processing methods often fall short in dealing with the sheer volume, variety and complexity of the data, leaving valuable information underutilized. This is where AI/ML technologies provide Customs administrations with the tools to leverage and maximize the use of their collected data. AI/ML can automate the analysis of structured and semi-structured data, extract insights from unstructured data through techniques like natural language processing (NLP) and computer vision, and enable predictive analytics to anticipate risks and streamline processes.

Data management is the cornerstone of AI/ML projects in Customs administrations, as it ensures that the data collected and processed is both reliable and suitable for analysis. Managing data for AI/ML applications in Customs administrations requires handling diverse types of structured and unstructured data, ensuring its quality and integrity and securing it against privacy and security threats. When applied to Customs administrations, data management involves transforming raw trade data into formats ready for AI model development and processing.

By implementing robust data management strategies, Customs administrations can harness the power of AI/ML to improve operational efficiency, enhance risk management and ensure regulatory compliance. These strategies should incorporate comprehensive data governance frameworks and leverage advanced data quality tools.

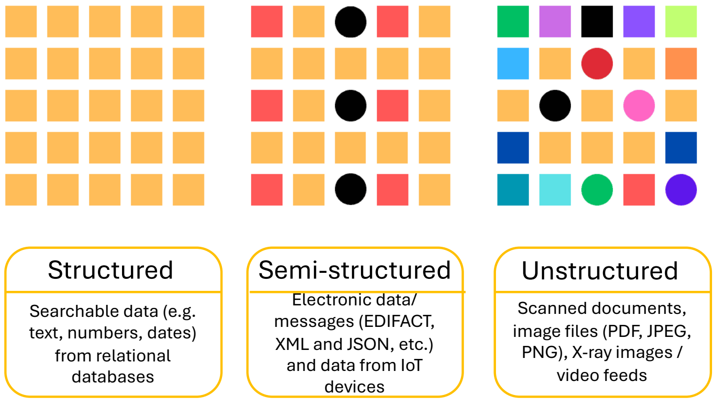
8.1 Types of data used for AI/ML projects

Structured data typically includes import/export declarations, tariff classifications, transaction records and valuation data. These datasets fit neatly into databases, making them ideal for algorithmic processing. In contrast, unstructured data, such as scanned documents, images, emails and intelligence reports, requires more advanced processing techniques, including text mining and image recognition, to extract useful insights.

Further expanding on this, Customs administrations also utilize real-time data, from sensors, tracking systems and IoT devices, alongside historical data from previous transactions and inspections. These datasets serve as the backbone for training AI models that predict risk, optimize logistics and detect fraud.

[28] WCO News 86. (June 2018) Panorama: “Clearance of express cargo and postal items: Korea tests new analytical tools to root out fraud”

Figure 6 – Structured, semi-structured and unstructured data in Customs operations



8.2 Data quality and integrity

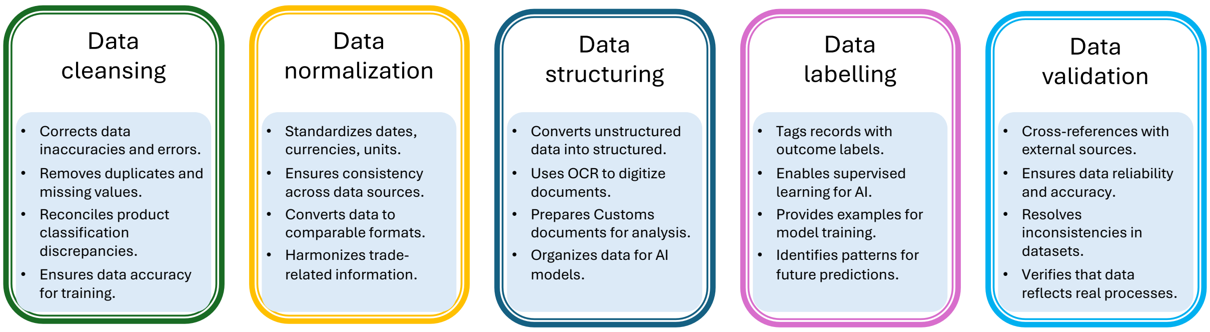
Data quality and integrity are crucial to the effectiveness of AI/ML models. For Customs administrations, ensuring that data is accurate, complete, consistent and up to date is paramount. High-quality data allows models to generate reliable predictions and decisions, such as identifying potentially fraudulent shipments or determining optimal inspection schedules.

Customs data must undergo rigorous pre-processing, including cleaning, validation and augmentation, to enhance data quality. This may involve error detection and correction, ensuring that data entries are free from inconsistencies and gaps. Data augmentation techniques such as cropping, scaling and contrast adjustment help increase the volume and diversity of training data, which is especially beneficial in Customs environments where variability is high.

8.3 Data preparation

Data preparation is a crucial phase for Customs administrations embarking on AI/ML projects, especially given the vast amounts of data they manage. High-quality outcomes from AI/ML models rely on well-prepared data, and Customs administrations must invest in comprehensive data cleansing and preparation to ensure the success of their projects. The following diagram provides the steps of data preparation which involves several essential steps that transform raw Customs data into a form suitable for AI/ML analysis.

Figure 7 – Steps of data preparation



Data cleansing - The first step is data cleansing, which involves identifying and correcting inaccuracies, errors and inconsistencies in the data. Customs administrations frequently deal with large volumes of historical data that may contain misclassified goods, inconsistent units of measure, missing values or duplicate entries. For example, variations in Harmonized System (HS) codes used to classify products over time may introduce discrepancies. Reconciling these inconsistencies is critical for ensuring consistent product classification, a fundamental requirement for any AI/ML model that seeks to assess trade compliance, detect fraud or optimize inspection processes.

Data normalization - Following data cleansing, data normalization ensures that the information from various sources is consistent and comparable. Customs data often comes from diverse systems, regions or departments, leading to differences in formats, measurement units and currency values. Standardizing dates, currency values and units of measurement, such as converting all weights to metric tons or standardizing currency exchange rates, is crucial for creating uniform datasets. Normalization enhances the accuracy of analysis and allows AI/ML models to process data from multiple sources without introducing biases due to format variations.

Data structuring - Next, as Customs administrations handle a wide array of data types – including semi-structured data (e.g. data in XML/JSON formats) and unstructured data (e.g. scanned documents), data structuring is necessary, to convert data into a structured format suitable for AI/ML analysis. Techniques like XML/JSON parsing can be used for semi-structured data, while Optical Character Recognition (OCR) can transform scanned documents into machine-readable text.

Data labelling – This is a vital step, particularly for supervised ML, which requires historical records to be accurately labelled with predefined outcomes. In Customs operations, this could mean labelling historical data to indicate whether specific shipments were compliant or were flagged for fraud or irregularities. These labels allow AI/ML models to learn from past patterns and to make predictions based on new data. For example, a risk assessment model may be trained to predict whether a particular shipment is likely to involve non-compliance based on past data labelled as “fraud detected” or “compliant”. This process is resource-intensive but essential for creating models that can provide valuable insights and improve Customs operations.

Data validation – Lastly, data validation is crucial for ensuring that the data accurately reflects the underlying reality. Customs administrations need to cross-reference their data with external sources, such as trade databases, industry reports and trusted third-party data providers, to verify the accuracy and reliability of that data. For instance, Customs administrations can validate trade volumes and product descriptions against global trade databases or consult industry reports to ensure that the data used in AI/ML models is both current and credible. Data validation helps to avoid the risks associated with incorrect or outdated information, which could lead to flawed predictions or decision-making.

Additionally, dataset version control is crucial for managing the lifecycle of datasets used in model training. Customs administrations must be able to track and manage different versions of their datasets, ensuring that the most current and relevant data is used for AI/ML model development.

Through these carefully executed steps - data cleansing, normalization, structuring, labelling and validation - Customs administrations can ensure that their AI/ML models are built on a solid foundation of high-quality data.

9 Scalable technical framework for AI/ML implementation/integration

The “scalable technical framework” recommended in this section serves as a foundational blueprint for Customs administrations aiming to incorporate AI/ML into their operational workflows. It encompasses essential aspects such as development, automation, data management, model training, platform architecture and infrastructure, hardware and networking requirements, ML Operations (MLOps) and data integration tools. It offers a flexible approach that Customs administrations can use to set up an AI/ML environment that can be expanded over time, aligning with cost-effective adoption strategies rather than imposing a fixed set of potentially overwhelming or costly upfront requirements.

These technical specifications support a wide range of AI/ML applications and use cases and facilitate streamlined model development from prototyping to production. They also incorporate MLOps practices for systematic management of the entire ML lifecycle.

9.1 AI/ML development environment

9.1.1 AI/ML frameworks

AI/ML frameworks provide the foundational libraries and tools for building, training and deploying ML models. Supporting popular frameworks like TensorFlow, PyTorch and R ensures versatility, enabling the development of a wide range of ML tasks, from neural networks to statistical models.

TensorFlow, PyTorch and R are open-source ML frameworks. This means they are freely available and can be modified and distributed by anyone. This openness has contributed to their widespread adoption and popularity in the ML community. They are best suited for projects ranging from basic data analysis to advanced deep learning applications, such as Customs risk assessment, predictive analytics and image recognition for cargo inspection.

Specifications:

- support TensorFlow (v2.x+), PyTorch (v1.7+) and R (v4.x+), and compatibility with Kubernetes for deployment;
- pre-installed libraries for common ML tasks (e.g. scikit-learn, Keras).

Supporting TensorFlow and PyTorch is often a requirement for AI/ML platforms as they offer the following features:

- community and ecosystem: both frameworks have large and active communities, which means there are abundant resources, tutorials and support available for developers;
- flexibility and versatility: TensorFlow and PyTorch are highly flexible and versatile frameworks that can be used for a wide range of ML tasks, from simple linear regression to complex deep learning models;
- integration with other tools: both frameworks integrate well with other popular ML tools and libraries, making it easier to build and deploy AI applications.

While TensorFlow and PyTorch are two of the most popular frameworks, there are other options available, including:

- Keras: ahigh-level API that can be used on top of TensorFlow or Theano;
- scikit-learn: a Python library for ML that includes a variety of algorithms and tools;
- JAX: a Python library for accelerating ML research, combining the flexibility of NumPy with the power of automatic differentiation.

In addition to open-source frameworks, proprietary ML platforms are also available. Examples of proprietary platforms include:

- Amazon SageMaker: a fully managed platform from Amazon Web Services;
- Azure Machine Learning: a cloud-based platform from Microsoft; and
- Google Cloud AI Platform: a platform from Google for building and deploying AI applications.

9.1.2 Integrated development environment (IDE)

An IDE can be valuable for writing, debugging and visualizing code efficiently in many AI/ML development scenarios. Tools like Jupyter Notebook, PyCharm or Visual Studio Code often provide an interactive and user-friendly environment for developing AI/ML models, allowing for rapid experimentation and prototyping. These are well-suited for projects requiring iterative development, such as model prototyping, data analysis and visualization in research and development settings. IDEs are not always essential, and their necessity depends on the specific project requirements, developer preferences and available resources. In some cases, simpler IDE or cloud-based solutions may be more appropriate, especially for quick scripts, resource-constrained environments, or when working with legacy systems

Specifications:
- IDE: Jupyter Notebook, PyCharm Professional or Visual Studio Code with AI/ML extensions;
- simpler IDE: Thonny, Geany;
- cloud-Based Solutions: Google Colab, Replit;
- integration with version control and cloud storage for collaboration.

9.1.3 Version control

Collaborative AI/ML projects where multiple team members work on codebases, such as developing and maintaining Customs analytics systems or collaborative research projects, require version control systems. This enables collaborative development, tracking changes in code and maintaining integrity across versions. Integration with IDEs allows seamless code management and collaboration among multiple developers.

Specifications:
- Git support with integration into the IDE;
- centralized repositories (e.g. GitHub, GitLab, Bitbucket) for team collaboration.

9.2 Automation tools and frameworks

9.2.1 Orchestration tools

Orchestration tools like Apache Airflow, Prefect or Luigi automate the workflow of ML pipelines, ensuring efficient management of tasks such as data preprocessing, model training and evaluation. These are needed for projects that involve complex, multi-step pipelines, such as data pipeline automation for Customs data processing or automated model retraining systems.

Specifications:
- support Apache Airflow (v2.x+), Prefect or Luigi;
- integration with cloud and on-premises data sources.

9.2.2 Continuous integration and continuous deployment (CI/CD) pipelines

AI/ML projects requiring frequent updates and deployment, such as continuous improvement of predictive models for Customs risk management, require CI/CD tools that enable automated testing, deployment and monitoring of ML models. This ensures rapid and reliable updates of models in production environments.

Specifications:

- CI/CD integration with Jenkins, GitHub Actions or GitLab CI;
- automated testing frameworks (e.g. pytest, TensorFlow Model Analysis);
- pre-built templates and configurations.

9.2.3 Template library

Projects aiming to accelerate AI/ML development for tasks like trade data analysis or document classification can benefit significantly from pre-built templates - which are essentially a library of reusable code for common AI/ML tasks, which help to reduce development time. These templates can cover data preprocessing, feature engineering, model training and evaluation.

Specifications:
- cover a wide range of AI/ML tasks, including classification (e.g. document classification), regression (e.g. trade data analysis), natural language processing, computer vision, time series analysis;
- provide for IDE Integration;
- enable quick customization and adaptation of templates to specific project requirements
- repository of templates for various tasks (e.g. data preprocessing, model training).

9.2.4 Configuration management

Configuration management ensures the automated provisioning,[29] monitoring and management of infrastructure resources, maintaining consistency, reliability and scalability across different environments. It enables uniform deployment environments, such as deploying AI/ML models across multiple Customs offices. Customs administrations can efficiently manage infrastructure changes, reduce deployment errors and maintain compliance with regulatory requirements.

Specifications:
- support for leading configuration management tools and industry-standard tools for automated deployment and infrastructure management;
- pre-configured scripts for setting up AI/ML models, APIs, databases and networking in both development and production environments;
- supports hybrid deployments/integration with cloud platforms and on-premises infrastructure
- compatibility with tools like Prometheus, Grafana and ELK Stack for tracking infrastructure performance and security compliance;
- support for containerized environments: enables Docker and Kubernetes orchestration for scalable and efficient AI model deployment;
- self-healing mechanisms: implements automated recovery from failures, ensuring high availability of critical AI-driven Customs applications.

9.3 Data management and governance

9.3.1 Data lake

Projects involving large-scale data analytics, such as predictive modelling for trade volumes or fraud detection in Customs operations, require a data lake that serves as a centralized repository for storing and managing diverse data sources, facilitating seamless access and integration of structured and unstructured data, crucial for comprehensive ML models.

Specifications:
- scalable data lake infrastructure (e.g. Hadoop, AWS S3 Data Lake);

[29] Automated provisioning is the self-configuring of infrastructure and resources programmatically.

- support for diverse data types (e.g. JSON, Parquet, CSV).

9.3.2 Data governance framework

Projects handling sensitive data, such as personal information in Customs declarations or trade compliance data, necessitate a data governance framework ensuring data security, privacy and compliance with regulations. It includes policies and processes to manage data integrity throughout the AI/ML lifecycle.

Specifications:
- data governance tools (e.g. Apache Atlas, Collibra);
- compliance with relevant data privacy regulations.

9.3.3 Data quality tools

Projects requiring high-quality data input, such as anomaly detection systems and ML models for Customs valuation, require data quality tools which provide functionalities for cleaning, validation and standardization of data to maintain high data integrity and accuracy, which is critical for reliable AI/ML model performance.

Specifications:
- data quality tools (e.g. Talend, Informatica);
- automated data validation and cleansing processes.

9.4 Model development and training

9.4.1 Experimentation tools

Interactive tools facilitate experimentation, rapid prototyping and iterative model development, allowing data scientists to explore different models and parameters quickly. These are best suited for research and development projects, such as developing new algorithms for Customs fraud detection or optimizing existing models for better performance.

Specifications:
- Jupyter Notebook (v6.x+), RStudio Server;
- support for GPU acceleration in notebooks.

9.4.2 Hyperparameter tuning

Projects requiring model optimization, such as improving the accuracy of predictive models for Customs revenue estimation, also require automated hyperparameter tuning techniques to help enhance model performance by efficiently finding the best parameters for ML algorithms.

Specifications:
- hyperparameter tuning libraries (e.g. Optuna, Hyperopt, Scikit-learn's GridSearchCV);
- integration with distributed training frameworks.

9.4.3 Distributed training

Projects involving large-scale datasets, such as image recognition for Customs inspections or natural language processing for document analysis, need to use distributed training frameworks which enable scaling of model training across multiple GPUs or clusters, significantly reducing training time for large datasets.

Specifications:
- support for Horovod, TensorFlow's distributed strategy;
- multi-GPU and multi-node training capabilities.

9.5 Platform architecture and infrastructure

9.5.1 Deployment options

Each deployment option has its ideal use case depending on the nature of the AI/ML project. On-premises deployment is best for projects requiring stringent control over sensitive data. Cloud deployment is suited for large-scale data analysis and projects needing flexible scaling. A hybrid cloud architecture offers a balance, combining on-premises control with cloud scalability, making it suitable for complex projects like real-time anomaly detection. Utilizing government cloud platforms is crucial when compliance with government security and data sovereignty regulations is necessary.

9.5.2 On-premises deployment

On-premises deployment involves setting up and managing all computing resources, storage and software within the organization's data centres. This option provides full control over hardware, data and security measures, which is crucial for projects that involve highly sensitive data or strict regulatory compliance.

On-premises deployment is best suited for AI/ML projects that involve processing sensitive Customs data, such as fraud detection, threat assessment and sensitive document processing, where data sovereignty and compliance with strict security regulations are paramount.

Specifications:

- dedicated data centre with high-performance servers (minimum 16-core CPUs, 256 GB RAM, multi-GPU support);
- local and network storage solutions (e.g. 2 TB NVMe SSDs, 10 TB NAS);
- high-speed networking (e.g. Infiniband, 10/40/100 Gbps Ethernet);
- robust security infrastructure (e.g. firewalls, VPNs, IAM).

9.5.3 Cloud deployment

Cloud deployment uses services provided by external cloud platforms like AWS, Azure or Google Cloud Platform (GCP). This option offers scalability and flexibility, allowing the organization to quickly adjust computing resources based on demand. It is ideal for projects that require large-scale data processing, rapid experimentation or collaboration across multiple locations.

Cloud deployment is best suited for AI/ML projects that involve large-scale data analysis, such as predictive analytics or ML model training on large datasets. Cloud deployment is particularly beneficial for projects requiring flexibility in scaling resources or those involving non-sensitive data.

Specifications:

- cloud instances (e.g. AWS EC2, Azure VMs) with CPU-optimized (c5.4xlarge) and GPU-optimized (p3.8xlarge, p4d.24xlarge) options;
- scalable cloud storage (e.g. Amazon S3, Azure Blob Storage) starting at 10 TB;
- advanced networking (minimum 1 Gbps);
- cloud-native security services, including encryption, VPNs and IAM.

9.5.4 Hybrid cloud architecture

A hybrid cloud architecture combines on-premises infrastructure with cloud services, offering the flexibility to run workloads both locally and in the cloud. This approach allows seamless data integration and workload migration, balancing control, security and scalability.

Hybrid cloud architecture is best suited for AI/ML projects that require a balance between maintaining control over sensitive data and leveraging cloud resources for scalable processing. This is ideal for

Customs administrations working on projects like real-time anomaly detection, where sensitive data is processed locally, but large-scale model training and data analytics can benefit from cloud resources.

Specifications:
- secure, high-speed connection between on-premises and cloud environments (e.g. VPN, Direct Connect);
- local data centres for sensitive data and cloud resources for scalable processing;
- unified management system for integrated workload orchestration.

9.5.5 Containerization

Containerization involves packaging AI/ML models/applications and their dependencies into a "container". This approach ensures consistency across different environments and seamless transitions between development, testing and deployment, which in turn assists with the rapid deployment of AI/ML projects, enabling faster iteration and testing of models.

Specifications:
- use Docker or similar platforms for packaging AI/ML applications;
- ensure compatibility across on-premises and cloud environments;
- streamlined deployment and portability of containers.

9.5.6 Container orchestration - Kubernetes cluster

Container orchestration, which is the automated process of deploying, scaling and managing containerized applications, plays a significant role in deploying AI applications across various environments, including on-premises, cloud, hybrid and government cloud setups. Orchestration manages and coordinates the various components of an application. This approach allows organizations the flexibility to select the most suitable deployment option based on their specific scalability, security and resource optimization needs.

Customs operations which incur significant workloads, involving complex workflows and large-scale data ingestion, such as declaration processing, HS classification, valuation and risk assessment, etc., would benefit from efficient orchestration.

Kubernetes is a widely used open-source platform for container orchestration. It provides for efficient orchestration of AI/ML workloads in on-premises, cloud or hybrid environments, enabling high availability and resource optimization. Using Kubernetes clusters with GPU support enables parallel processing and optimizes resource usage for AI/ML tasks, ensuring efficient model deployment and scaling. It is best suited for AI/ML projects that require frequent deployment, scaling and management of complex, containerized workloads, such as deploying and maintaining ML models for Customs inspection automation and real-time decision-making systems.

Specifications:
- Kubernetes cluster with GPU support (at least 4 GPUs per node);
- orchestration tools (e.g. Apache Airflow, Argo) for workflow management;
- auto-scaling configuration for dynamic resource management;
- integration with tools like Helm for streamlined deployment and load balancers (e.g. HAProxy, NGINX) for traffic distribution.

9.5.7 Load balancers

Load balancers play a crucial role in Customs operations, for instance in distributing incoming advance cargo information and the house and master manifests and declarations, procedures which require AI/ML-driven processing across AI-powered engines, preventing any single server becoming overwhelmed and causing bottlenecks. By implementing load balancers, Customs administrations can ensure these critical operations, requiring high availability and fault tolerance, remain efficient and reliable, capable of handling large volumes of data and requests, even during peak periods or unexpected surges in trade activity.

Specifications:

- software load balancers (e.g. HAProxy, NGINX) or cloud-native services (e.g. AWS Elastic Load Balancing);
- configuration for automatic traffic distribution to maintain service continuity.

9.5.8 Security

Security is paramount for all Customs systems, particularly when incorporating AI/ML technologies. The use of AI/ML in Customs operations introduces new complexities and potential vulnerabilities that require robust security measures. Added multi-layered security measures are necessary to protect sensitive data and ensure the integrity of AI systems.

Specifications:

- firewalls, VPNs and IAM for secure access;
- data encryption (in transit and at rest);
- compliance with security standards like ISO 27001 and GDPR;
- intrusion detection systems for real-time threat monitoring.

9.6 Compute resources requirements

When starting AI/ML projects, a well-balanced setup should support basic model training, inference[30] and experimentation at an affordable cost.

9.6.1 Central processing units (CPUs)

Central processing units (CPUs) are the backbone of AI/ML workloads, handling core processing tasks. High-performance CPUs provide the necessary computational power for complex These instances provide scalable, cost-effective processing power for operations such as data preprocessing and model inference, and traditional ML algorithm and model training.

Specifications:

- processor type: multi-core x86 or ARM-based CPUs optimized for compute-intensive tasks;
- core count: Typically, 2 to 8 virtual CPUs for basic workloads, with options to scale up for more demanding applications.

Additional features:

- hyper-threading/simultaneous multithreading (SMT): enables better performance for multi-threaded workloads, common in AI/ML tasks;
- cache size: preferably large L3 cache (e.g. 30 MB or higher) to accelerate data access during processing;
- support for Advanced Vector Extensions (AVX) for vector processing, which is beneficial for ML computations.

9.6.2 Memory

Random Access Memory (RAM) is crucial for temporary data storage during processing. A high-capacity RAM setup, such as 256 GB DDR4 or DDR5 ECC (Error-Correcting Code) memory, supports large-scale data processing and intensive model training without performance bottlenecks.

---

[30] Inference in AI/ML is the process of using a trained model to make predictions or decisions on new data, applying learned patterns without retraining the model.

Specifications:

- capacity: minimum of 256 GB RAM (Random Access Memory);
- type: DDR4 or DDR5;
- ECC (Error-Correcting Code): ECC memory is recommended to detect and correct data corruption, ensuring higher reliability and stability for critical AI/ML workloads;
- speed: for DDR4: Typically, 2933 MHz or higher/For DDR5: Typically, 4800 MHz or higher;
- scalability: ensure the server motherboard supports memory expansion (e.g. up to 512 GB or more) to accommodate future scaling needs for more demanding workloads.

9.6.3 Graphics Processing Units (GPUs)

GPUs enable optimized parallel processing, making them essential for ML and AI tasks. For an initial AI/ML project, selecting a cost-effective yet capable GPU is crucial to ensure smooth model development, training and inference without unnecessary expenses. A well-balanced GPU should provide sufficient computing power, memory bandwidth and efficiency for handling entry-level deep learning, computer vision and NLP tasks. For a beginner-friendly AI/ML setup, a GPU with at least 8GB of VRAM and 3,500+ CUDA cores is recommended for a balance of affordability and performance while supporting training, experimentation and inference. As workloads grow, higher-end GPUs can be considered for scaling AI capabilities.

Specifications:

- CUDA cores/Tensor cores[31]: At least 3,500+ CUDA cores for efficient parallel computing. Tensor cores (if available) enhance deep learning acceleration;
- VRAM (GPU memory): 8GB to 12GB to handle moderate batch sizes and model parameters efficiently;
- compute capability: 7.5 or higher for optimal compatibility with modern AI/ML frameworks;
- memory bandwidth: At least 300 GB/s for handling large dataset transfers and tensor computations.

9.6.4 Memory and storage

For an initial AI/ML project, selecting the right memory (RAM) and storage ensures smooth data processing, model training and experimentation without bottlenecks. Non-Volatile Memory Express Solid-State Drives (NVMe SSDs) provide high-speed read/write operations, which are crucial for tasks requiring rapid data access, such as model training and experimentation. They ensure quick access to large volumes of data, reducing training delays.

Specifications:

- memory (RAM) - 16GB RAM (minimum), 32GB recommended for handling larger datasets;
- storage - 1TB NVMe SSD (minimum), recommended for faster data access and model storage.

9.6.5 Network Attached Storage (NAS)/Network File System (NFS)

AI/ML projects in Customs often involve large datasets and require high-speed access for efficient model training and inference. A Network Attached Storage (NAS) or Network File System (NFS) provides centralized, scalable storage that is accessible over a network. To support basic AI/ML workloads, a minimum NAS/NFS setup should support concurrent read/write operations across multiple nodes, ensuring seamless data sharing for AI/ML tasks.

Specifications:

- minimum 10TB scalable storage to accommodate datasets, model checkpoints and logs;

[31] CUDA cores are parallel processors in GPUs that accelerate general computing tasks, while Tensor cores specialise in matrix operations, boosting deep learning performance for AI/ML models.

- Network File System (NFS) v3 or v4 support to enable high-performance read/write operations;
- sequential read/write speed: at least 500MB/s to avoid bottlenecks in model training;
- expandable storage: supports additional drives or cloud integration for future scaling.

9.6.6 Cloud storage

There are two primary types of cloud storage solutions, each suited for different use cases: **cloud object storage** and **cloud block storage**.

Cloud object storage is an optimal solution for storing large, unstructured datasets, including images, videos, logs and AI/ML model artifacts. Accessed via APIs, it is specifically designed for scalability, durability and cost-effectiveness, making it suitable for managing diverse data types and large-scale storage requirements. With high durability and availability, it ensures data integrity and accessibility at scale. Common usage includes storing training datasets, model checkpoints, logs and other unstructured data, making it particularly well-suited for batch processing and offline training workflows.

Specifications:

- starting at a base capacity of 10 TB, cloud object storage offers virtually unlimited scalability, enabling seamless accommodation of growing data volumes.

Cloud block storage, in contrast, provides high-performance, low-latency storage tailored for structured data. It is directly attached to virtual machines (VMs) as virtual hard drives, offering fast and frequent data access essential for applications such as databases, real-time analytics and transactional systems. Designed for speed and efficiency, it supports random read/write operations and can be scaled or adjusted to meet performance demands.

Specifications:

- with a starting capacity of 2 TB per instance, cloud block storage is ideal for latency-sensitive workloads where even minimal delays can impact performance, such as real-time AI inference or database transactions.

The choice between object and block storage depends on the specific requirements of the AI/ML project, including data types, performance needs and access patterns.

9.7 Networking

9.7.1 Network bandwidth

Sufficient network bandwidth is critical for fast data access, remote collaboration and model deployment, particularly in cloud-based or distributed AI/ML environments. A well-optimised infrastructure reduces latency, bottlenecks and performance degradation, especially for data-intensive applications such as deep learning, real-time analytics and large-scale model training.

Specifications:

- high-speed interconnects like Infiniband or 10/40/100 Gbps Ethernet for fast data transfer between servers and storage systems, and distributed training and real-time inference;
- minimum requirement: 1 Gbps network bandwidth to support data transfers, remote development environments and cloud-based processing;
- low latency: ensures smooth interaction with remote AI/ML infrastructure, including data lakes, storage solutions and edge computing devices;
- scalability: the infrastructure should support higher bandwidth (e.g. 10 Gbps or more) as AI/ML workloads scale, particularly for real-time inference and large-scale data ingestion.

9.7.2 Cloud compute resources

The preceding section provides the minimum specifications for on-premises compute resources, which refers to locally hosted hardware and storage within a Customs administration's data centre. This setup ensures full control over data, security and compute resources but requires higher upfront costs and maintenance.

The alternative is cloud compute resources which cater for on-demand computing power, storage and services. The choice between on-premises and cloud-based infrastructure depends on cost, scalability, data security and operational requirements.

Customs administrations can start with scalable cloud compute for AI/ML projects, to minimize upfront costs. Cloud compute instances are virtual machines (VMs) hosted in cloud platforms (AWS, Azure, Google Cloud), offering CPU/GPU configurations for flexible and scalable computing power for varying AI/ML workloads.

Specifications:

- CPU instances: 8 vCPUs, 32GB RAM;
- GPU instances: 4 x NVIDIA V100 GPUs, 64GB GPU memory;
- storage: cloud-based SSD storage;
- networking: high-speed 10GbE+ cloud interconnects for large dataset handling;
- auto-scaling: dynamically adjusts the number of compute instances based on workload demands, ensuring optimal resource utilization and cost efficiency;
- auto-scaling groups to manage instance counts based on demand.

For Customs administrations, a hybrid approach is often ideal - starting with on-premises compute resources for security-sensitive workloads while leveraging cloud AI/ML services for scalable processing and deep learning tasks. This ensures optimal performance, compliance and cost-efficiency, enabling Customs administrations to develop and deploy AI/ML capabilities effectively.

9.8 Machine Learning Operations (MLOps)

Machine Learning Operations (MLOps) refers to the set of practices and tools that enable organizations to build, deploy and maintain ML models in a production environment. MLOps bridges the gap between data scientists and IT operations teams, ensuring that AI models are developed, deployed and managed efficiently and effectively.

9.8.1 Building MLOps capability in a Customs administration

To effectively implement AI/ML initiatives, a Customs administration must not only build the technical infrastructure but also establish robust MLOps capabilities. MLOps (Machine Learning Operations) is a crucial practice that bridges the gap between data science and IT operations, ensuring that ML models can be developed, deployed and managed at scale. This capability ensures that AI/ML models are not only developed and deployed efficiently but also managed, monitored and governed throughout their lifecycle. MLOps brings operational excellence, scalability and compliance to AI/ML initiatives, enabling the Customs administration to harness the full potential of AI/ML technologies while maintaining the highest standards of accuracy, reliability and ethical responsibility.

By implementing MLOps practices, organizations can:

- accelerate AI development and deployment: MLOps streamlines the process of building, testing and deploying AI models, reducing time-to-market;
- improve model performance: MLOps ensures that models are continuously monitored and maintained, optimizing their performance over time;

- enhance reproducibility: MLOps helps establish reproducible workflows, making it easier to replicate and scale AI experiments;
- reduce risks: MLOps helps mitigate risks associated with AI projects, such as data quality issues, model bias and security vulnerabilities.

9.8.2 Steps to build MLOps capability

Developing a robust MLOps capability requires a structured approach to streamline ML model development, deployment, monitoring and governance. The following steps outline key aspects of building a scalable and sustainable MLOps practice:

a. Establish a centralized development environment

A structured development environment ensures efficient collaboration, experimentation and version control.

- Deploy an AI/ML development environment with essential tools, including IDEs, version control systems and ML frameworks.
- Integrate experiment tracking tools for managing model performance and hyperparameter tuning.
- Implement access control policies to manage security in shared workspaces.

b. Automate ML pipelines

Automation improves consistency and accelerates the ML lifecycle.

- Implement continuous integration/continuous deployment (CI/CD) pipelines for seamless model updates and retraining.
- Automate key processes such as data preprocessing, model training, evaluation and deployment.
- Integrate automated testing and validation to ensure reliability before deployment.

c. Develop reusable pipelines and templates

Reusable assets enhance efficiency and standardization.

- Create pre-built ML pipeline templates for common tasks like data transformation, training and inference.
- Implement infrastructure-as-code (IaC) to ensure consistent deployment environments.
- Develop standardized APIs for model inference and system integration.

d. Implement robust data management and governance

Effective data governance ensures data quality, security and compliance.

- Establish a centralized data repository to manage structured and unstructured data.
- Implement data versioning to track dataset changes and ensure reproducibility.
- Enforce data validation and regulatory compliance to align with privacy laws.

e. Enable Scalable Model Training and Experimentation

Scalable training infrastructure optimizes model performance.

- Utilise cloud-based or on-premises compute resources for accelerated model training.
- Automate hyperparameter tuning to enhance efficiency.
- Enable parallel experimentation to optimize model selection.

f. Streamline model deployment and serving

Efficient deployment ensures scalability and reliability.

- Use containerization and orchestration for flexible deployment.
- Implement model serving platforms for optimized inference.
- Conduct A/B testing and shadow deployments to validate new models.

g. Monitor and maintain models in production

Continuous monitoring ensures performance and fairness over time.

- Deploy model monitoring tools to track accuracy, latency and drift.
- Implement drift detection and automated retraining to maintain accuracy.
- Utilise Explainable AI[32] frameworks for transparency in decision-making.

9.9 Data integration tools for integrating AI/ML

To integrate AI/ML solutions with existing systems such as Customs management systems, Single Window platforms, Electronic Cargo Tracking, ERP and HR systems, a Customs administration requires robust data integration tools to facilitate seamless data flow and interoperability between various systems, ensuring that AI/ML models can access, process and deliver actionable insights in real time. These integration tools support various data formats, protocols and real-time processing requirements, providing the necessary infrastructure to enable AI/ML models to leverage data across the Customs ecosystem for enhanced decision-making, automation and operational efficiency. The proposed technical specifications for data integration tools are set out below.

9.9.1 Apache Spark

Apache Spark is a powerful open-source unified analytics engine designed for large-scale data processing. It supports various data integration tasks, including ETL (Extract, Transform, Load), real-time stream processing and advanced analytics, making it an excellent choice for integrating AI/ML models with diverse Customs systems. It is best suited for high-volume, low-latency data integration tasks such as processing large datasets from Customs Management Systems, Single Window platforms, Electronic Cargo Tracking systems, real-time Customs risk analysis and predictive analytics.

Specifications:

- cluster configuration: minimum of 4-node cluster with 16-core CPUs, 64 GB RAM per node;
- storage integration: integration with HDFS, S3, Azure Blob Storage, or local file systems for data storage and retrieval;
- data processing frameworks: support for Spark SQL, Spark Streaming, MLlib (for ML integration) and GraphX (for graph processing);
- security and compliance: integration with Kerberos, end-to-end encryption (SSL/TLS), and access control mechanisms to ensure data privacy and security compliance;
- connector support: pre-built connectors for databases, big data stores and messaging systems;
- real-time processing: support for stream processing with low latency, enabling real-time integration with systems like Electronic Cargo Tracking and Customs monitoring platforms.

9.9.2 Apache NiFi

Apache NiFi (previously Apache Niagara Files) is an open-source data integration tool designed for automating the movement, transformation and management of data between systems. It offers a user-friendly interface for designing data flows and supports real-time data integration, making it ideal for integrating AI/ML models with various Customs systems. This tool is best suited for real-time and batch data integration tasks, including data ingestion from Customs management systems, Single Window platforms and external data sources.

Specifications:

- deployment: minimum 4-core CPU, 16 GB RAM per node for small to medium-scale deployments; scalable to multi-node clusters for high-throughput requirements;

[32] Explainable AI (or XAI) refers to techniques that make AI model decisions transparent, interpretable and understandable, helping users trust, audit and comply with regulatory requirements by explaining model predictions and behaviour.

- data flow design: visual interface for designing data flows with support for complex routing, filtering and transformation tasks;
- protocol and format support: integration with diverse data protocols (e.g. HTTP, FTP, MQTT) and formats (e.g. JSON, XML, CSV) to handle data from various Customs and trade systems;
- security: end-to-end encryption (SSL/TLS) for data in transit, role-based access control and integration with LDAP or Kerberos for secure authentication;
- scalability: support for clustering and load balancing to manage large data volumes and ensure high availability;
- real-time processing: capable of real-time data ingestion and processing, making it suitable for applications like real-time cargo tracking and Customs clearance monitoring.

9.10 Data integration with specific systems

9.10.1 Customs management systems and Single Window platforms

Integrating AI/ML models with Customs Management Systems (CMS) and Single Window platforms involves real-time data exchange to facilitate risk analysis, trade compliance and automated decision-making.

Specifications:
- connector support: support for integration with CMS and Single Window APIs (e.g. RESTful APIs, SOAP) for direct data exchange;
- ETL capabilities: ETL processes to extract data from Customs declarations, cargo manifests and other trade documents, transform it for AI/ML model input and load results back into the CMS;
- data transformation: ability to handle various data formats (e.g. UN/EDIFACT, XML, JSON) used in Customs transactions;
- high availability: clustering and failover support to ensure uninterrupted data integration with mission-critical Customs systems.

9.10.2 Electronic Cargo Tracking Systems (ECTS)

Electronic Cargo Tracking Systems (ECTS) provide real-time tracking and monitoring of cargo movement. Integrating these systems with AI/ML models requires handling high-velocity data streams for tasks like predictive analytics and anomaly detection.

Specifications:
- streaming data support: integration with real-time data streams (e.g. Apache Kafka, MQTT) for continuous data ingestion from cargo tracking devices;
- low-latency processing: real-time processing capabilities with latency under 1 second for time-sensitive tasks like route optimization and anomaly detection;
- data aggregation and enrichment: ability to aggregate and enrich tracking data with other sources, such as weather information and historical trade data, to enhance AI/ML model accuracy.

9.10.3 Enterprise Resource Planning (ERP) and Human Resources (HR)

ERP and HR Systems contain valuable data related to internal processes, staff allocation and resource management, which can be integrated with AI/ML models for operational optimization.

Specifications:
- connector integration: pre-built connectors for common ERP and HR systems (e.g. SAP, Oracle, Workday) to facilitate data extraction and integration;
- data privacy: secure handling of sensitive information such as employee records and financial data, including encryption, access control and compliance with data privacy regulations;

- scheduled data sync: support for periodic data synchronization (e.g. daily, weekly) to update AI/ML models with the latest operational and HR data for tasks like workforce optimization and resource allocation;
- testing and fairness testing tools: AI models test tools e.g. MLflow, AI Verify, AI Fairness 360 or Fairlearn for assessing fairness, bias, trustworthiness and ensuring compliance with key ethical standards;
- security and compliance: cybersecurity measures, data encryption, access control and compliance with data protection regulations.

9.10.4 Security and compliance

Data integration tools must ensure secure data exchange between systems, especially when dealing with sensitive Customs, trade and personnel data. Compliance with data privacy regulations and Customs data exchange standards is crucial.

Specifications:
- data encryption: end-to-end encryption (SSL/TLS) for data in transit and at rest;
- access control: role-based access control (RBAC) and integration with existing authentication systems (e.g. LDAP, Kerberos);
- audit and logging: comprehensive logging and auditing capabilities to track data access, transformations and transfers for compliance purposes.

10 Costs

The indicative estimated cost ranges presented in this section are derived using a combination of market research, industry benchmarks[33] and contextual insights, as well as consultations with various industry players[34].

These estimates are based on current open literature. However, they are not to be construed as precise or actual financial costs, as these will vary when factoring in the unique operational needs, existing infrastructure and strategic objectives of the Customs administration. In addition, software licensing fees, support contracts and integration costs can vary significantly based on vendor pricing changes, market demand and negotiation outcomes. Costs may differ based on the geographic location of the Customs administration, including regional pricing variations, availability of local vendors and differences in labour costs. The size and scale of the Customs administration, including the number of users, complexity of operations and extent of required integrations, can lead to variations in actual expenses.

The indicative estimated cost ranges are intended solely for informational and planning purposes.

10.1 AI/ML frameworks

Foundational AI/ML frameworks like TensorFlow, PyTorch and R are open source and freely available. However, effective implementation requires investment in infrastructure, skilled personnel and ongoing operational support, as well as integration with Customs-specific systems. Nonetheless , there may be additional costs associated with the use of these open-source frameworks, such as licensing fees and maintenance/support for databases and visualization tools and specialized libraries for tasks like image recognition in cargo inspection or anomaly detection in trade data.

The estimates cost range are indicated in the following table.

Table 3 - Cost range for AI/ML frameworks

Cost category	Description	Indicative estimated cost range
Software and tools	Open-source frameworks (free),[35] proprietary extensions, enterprise support licences	Open source (community edition) – free Enterprise level -USD 10,000 - USD 100,000 annually
Licensing and compliance	Licensing for additional software	USD 10,000 – USD 100,000 annually

10.2 Integrated development environment (IDE)

As discussed in section 10 of this report, an IDE is crucial for writing, debugging and visualizing code efficiently. Tools like PyCharm require annual licences per user, while others such as Visual Studio Code and Jupyter Notebook are open-source and free; however, enterprise versions or cloud-based services may have associated fees. The estimated cost ranges are indicated in the following table.

[33] Market research references and sources such as: IDC. “Worldwide AI and Generative AI Spending Guide”; Run.ai. “AI cost estimation: Understanding the financial implications”; ProjStream. “The future of cost estimating: Embracing AI and machine learning.” and PhoenixNAP. “HPC server price: Understanding the cost of high-performance computing”.

[34] Industry consultations include Deloitte, Google, Huawei, Nuctech.

[35] Open-source/community versions are typically free but may incur indirect costs for deployment, maintenance and support. Enterprise-level costs can vary widely based on factors such as the scale of deployment, number of users and level of support required.

Table 4 - Cost range for Integrated Development Environment (IDE)

Cost category	Description	Indicative Estimated Cost Range
Software licensing	Open-source licences - Visual Studio Code, Jupyter Notebook	Open source (community edition) – free
	Enterprise level (cloud-based) - Jupyter Enterprise Gateway, Google Colab Pro	USD 10 - USD 50 per user/month
	Enterprise level (licensed) - PyCharm Professional, IntelliJ IDEA Ultimate	USD 200 - USD 700 per user/year

10.3 Version control

Version control systems are essential for collaborative AI/ML projects. The costs involved are for proprietary version control systems or subscription fees for GitHub Enterprise, GitLab Premium, etc.

Table 5 - Cost range for version control

Cost category	Description	Indicative estimated cost Range
Free/open source	Tools such as Git, GitLab Community Edition and Bitbucket Cloud (free tier) provide essential version control functionality with no licensing fees.	Open source (community edition) – free
SaaS/cloud enterprise	Hosted enterprise solutions (e.g. GitHub Enterprise Cloud, GitLab Premium, Bitbucket Premium) that offer advanced collaboration, security and support features.	USD 10 – USD 30 per user per month
Self-hosted enterprise	Enterprise-grade self-hosted solutions (e.g. GitHub Enterprise Server, GitLab Self-Managed) which may require annual licensing fees, infrastructure and maintenance costs.	USD 3,000 – USD 10,000 annually

10.4 Automation, data management and governance

Automation Tools along with Data Management and Governance Frameworks are crucial to enhance operational efficiency, ensure data integrity and maintain compliance with regulatory standards. The estimated costs include software licensing for proprietary solutions, tools and template library.

Table 6 - Cost range for automation, data management and governance tools and framework

Component	Description	Indicative estimated cost range
Orchestration tools	Tools like Apache Airflow, Prefect or Luigi.	Open source (community edition) – free Enterprise level -USD 10,000 - USD 100,000 annually
CI/CD pipelines	Open source - Jenkins, GitLab CI/CD, Travis CI Enterprise level - GitLab Enterprise, CircleCI, Azure DevOps	Open source (community edition) – free Enterprise level - USD 20 - USD 200 per user/month
Template library	Open source - scikit-learn, TensorFlow, PyTorch free Enterprise level - IBM Watson, Google Cloud AI, Azure Machine Learning)	Open source (community edition) – free Enterprise level - USD 1,000 - USD 10,000+ per month
Configuration management	Open source - Ansible, Terraform, Chef Enterprise level - Ansible Tower (Red Hat), Terraform Enterprise, Chef Enterprise	Open source (community edition) – free Enterprise level - USD 5,000 - USD 50,000+ per year
Data lake tools	Open source - Apache Hadoop, Apache Spark Enterprise level - Amazon S3, Azure Data Lake Storage, Google Cloud Storage	Open source (community edition) – free (excluding infrastructure costs)

		Enterprise level - USD 0.02 - USD 0.05 per GB/month for storage, additional costs for data processing and analytics
Data governance tools	Open source - Apache Atlas, ODPi Egeria Enterprise level - IBM InfoSphere Information Governance Catalog, Collibra Data Governance, Informatica Axon Data Governance	Open source (community edition) – free (excluding implementation and maintenance costs) Enterprise level - USD 50,000 – USD 200,000 + per year
Data quality tools	Open source - OpenRefine, Great Expectations Enterprise level - Informatica Data Quality, Talend Data Quality, IBM InfoSphere Information Server for Data Quality	Open source (community edition) – free (excluding implementation and maintenance costs) Enterprise level - USD 20,000 - USD 200,000+ per year

10.5 Model development and training

Model development and training components are crucial to develop and maintain efficient ML models. The table below provides estimated costs to plan and budget effectively for experimentation tools, hyperparameter tuning and distributed training frameworks.

Table 7 - Cost range for model development and training

Component	Description	Indicative estimated cost range
Experimentation tools	Open source - Jupyter Notebook (v6.x+), RStudio Enterprise level - RStudio Server Pro, JupyterLab Enterprise	Open source (community edition) – free Enterprise level - USD 5,000 - USD 50,000+ per year
Hyperparameter tuning tools	Open source - Optuna, Hyperopt, Scikit-learn's GridSearchCV Enterprise level - SigOpt, DataRobot AutoML	Open source (community edition) – free Enterprise level - USD 10,000 - USD 100,000+ per year
Distributed training tools	Open source - Horovod, TensorFlow's distributed strategy Enterprise level - managed solutions (e.g. AWS SageMaker, Google Cloud AI Platform)	Open source (community edition) – free Enterprise level - USD 500 - USD 5,000+ per month

10.6 Platform architecture

The cost presented below focuses on software licensing, ongoing support and integration/customization costs for the platform architecture only. These include licences for operating systems (e.g. Windows Server, Linux distributions), virtualization platforms (e.g. VMware vSphere) and security software (e.g. firewalls, VPNs, IAM solutions).

For cloud deployment using cloud service providers like AWS, Azure or Google Cloud to host AI/ML workloads, the costs encompass software licensing for cloud services, ongoing support from cloud providers and integration/customization of cloud environments.

In the case of Hybrid Cloud Architecture, the costs involve licensing for hybrid management tools to manage and integrate hybrid environments, including secure connection tools and unified management software.

For Kubernetes Cluster and containerization deployment, the costs include licensing for enterprise Kubernetes distributions and Containerization platforms like Docker.

Table 8 - Cost range for platform architecture

Component	Description	Indicative estimated cost range
On-premises deployment	Licences for operating systems, virtualization software (e.g. VMware) and security software (e.g. firewalls, VPNs, IAM solutions).	USD 20,000 – USD 80,000 annually
Cloud deployment	Subscription fees for cloud services (e.g. AWS EC2, Azure VMs), software-as-a-service (SaaS) tools and cloud-native security services (e.g. encryption, IAM).	USD 10,000 – USD 80,000 annually
Hybrid cloud architecture	Licences for hybrid management tools (e.g. VMware vSphere with cloud integration), secure connection tools (e.g. VPN, Direct Connect) and unified management software.	USD 15,000 – USD 90,000 annually
Kubernetes cluster	Open source - Vanilla Kubernetes Enterprise level - Red Hat OpenShift, VMware Tanzu	Open source (community edition) – free (excluding infrastructure costs) Enterprise level - USD 5,000 - USD 50,000+ per year per cluster.
Containerization	Open source - Docker Community Edition Enterprise level - Docker Enterprise (now part of Mirantis)	Open source (community edition) – free Enterprise level - USD 15 - USD 24 per user/month

10.7 Compute resources requirements

For a typical Customs administration, the right compute resources setup ensures efficient data processing, accelerated model training and scalable operations essential for tasks such as fraud detection, revenue estimation and cargo inspections.

The compute resources outlined below provide a detailed overview of the essential components, including high-performance computing servers, memory, GPUs and storage solutions. It is important to emphasize that the indicative estimated cost ranges presented are generally dependent on the specific AI/ML development and model training environments. Factors such as the complexity of ML tasks, volume of data, desired scalability and integration with existing systems significantly influence these costs.

Table 9 - Cost range for compute resources requirements

Component	Description	Indicative estimated cost range
High-performance computing (HPC) Servers	High-performance servers equipped with Intel Xeon or AMD EPYC CPUs - CPU Instances: 8 vCPUs, 32GB RAM GPU Instances: 4 x NVIDIA V100 GPUs, 64GB GPU memory	USD 50,000 - USD 80,000 per server
Memory (RAM)	High-capacity RAM - 32GB of high-speed DDR4 or DDR5 ECC memory.	USD 2,000 - USD 3,000 per server
Graphics Processing Units (GPUs)	High-end GPUs (e.g. NVIDIA V100 GPUs, although these may be outdated by 2025, so equivalent modern GPUs are required).	USD 40,000 - USD 60,000 per GPU
Local and network storage	High-speed NVMe SSDs (minimum 2 TB) and scalable NAS/NFS systems (minimum 10 TB) for rapid data access and data sharing across multiple nodes.	USD 5,000 - USD 10,000 per storage setup
Network Attached Storage	Centralized, scalable storage solutions offering high throughput and low latency, supporting concurrent	USD 600 to USD 2000+ per NAS/NFS setup

(NAS)/Network File System (NFS)	read/write operations for seamless data sharing in AI/ML tasks.	
Cloud compute resources	Cloud instances (e.g. AWS EC2, Azure VMs, Google Compute Engine) offer scalable computing power to handle varying workloads. CPU instances like c5.4xlarge are suited for CPU-intensive tasks, while GPU instances like p3.8xlarge or p4d.24xlarge provide multiple GPUs for deep learning and high-performance computing.	USD 10,000 – USD 80,000 annually
Cloud storage services	Scalable cloud object storage (e.g. Amazon S3, Azure Blob Storage, Google Cloud Storage) starting at 10 TB, plus cloud block storage (minimum 2 TB per instance) for high-performance applications.	USD 5,000 – USD 50,000 annually
Auto-scaling services	Auto-scaling services dynamically adjust the number of compute instances based on workload demands, ensuring optimal resource utilization and cost efficiency. Specifications include auto-scaling groups to manage instance counts based on demand.	USD 3,000 – USD 15,000 annually

10.8 Networking

A networking infrastructure is pivotal to ensure fast data transfer, seamless communication between servers and storage systems to support AI/ML initiatives. The networking hardware requirements are generally dependent on the specific AI/ML development and model training environments and therefore indicative estimated cost ranges for networking infrastructure have to be configured to each specific AI/ML environment.

Table 10 - Cost range for networking requirements

Component	Description	Indicative estimated cost range
High-speed interconnects	High-speed interconnects like Infiniband or 10/40/100 Gbps Ethernet are essential for fast data transfer between servers and storage systems, crucial for distributed training and real-time inference.	USD 5,000 – USD 25,000 annually
Network bandwidth	Adequate network bandwidth (minimum of 1 Gbps) is necessary for smooth data transfer and remote access to development environments, minimizing latency in data-intensive operations.	USD 2,000 – USD 10,000 annually

10.9 Cost-effective AI/ML adoption strategies for Customs administrations

While the estimated costs for implementing the minimum technical specifications for AI/ML capacity in Customs administrations may appear substantial, it is important to recognize that there are cost-effective ways to begin the journey towards AI/ML adoption.

Customs administrations can leverage various strategies to incorporate AI/ML capabilities into their operations without immediately investing in extensive in-house infrastructure and development capabilities. These cost-effective AI/ML adoption strategies for Customs administrations offer practical alternatives that allow for a gradual, scalable approach to implementing AI/ML solutions, balancing the need for technological advancement with budgetary constraints.

Customs administrations can explore several alternatives to reduce the costs associated with incorporating AI/ML into their operations without investing heavily in in-house infrastructure and development capabilities:

1. Cloud-based solutions

- Utilise cloud platforms that offer AI/ML services, reducing the need for on-premises infrastructure
- Pay-as-you-go models allow for cost-effective scaling based on actual usage

2. Open-source tools and frameworks
    - Leverage free, community-driven tools like TensorFlow, PyTorch and scikit-learn
    - Benefit from rapid advancements and collaborative problem-solving without licensing costs
3. Collaboration and partnerships
    - Form partnerships with academic institutions or industry experts for knowledge sharing
    - Participate in cross-border collaborations to share resources and expertise
4. Managed MLOps Services
    - Opt for managed MLOps platforms which are cloud-based platforms/services to handle the technical complexities of AI/ML deployment
    - Reduce the need for specialized in-house expertise during the early stages.
5. Gradual implementation
    - Start with small, high-impact projects to demonstrate value before scaling up
    - Implement AI projects incrementally to spread costs over time
6. Pre-built AI solutions
    - Utilise pre-trained models and AI services tailored for specific Customs use cases
    - Adapt existing solutions rather than building from scratch

By exploring the above, Customs administrations can incorporate AI/ML capabilities into their operations more cost-effectively, while still benefiting from the enhanced efficiency and decision-making that these technologies offer.

11 Skills and training

To prepare Customs administrations to leverage AI/ML technologies, they will have to invest in comprehensive training programmes and capacity-building initiatives that equip their workforce with the necessary skills and knowledge. It is essential to prioritize training and capacity building to ensure that both technical and non-technical staff are equipped with the knowledge and skills required for the successful deployment and management of AI/ML technologies.

Training could be prioritized as follows:

- AI/ML fundamentals - provide basic understanding of AI/ML concepts for all staff, focus on practical applications in Customs operations
- Data science and analytics - train technical staff in data preprocessing, analysis and visualization; emphasize Customs-specific data handling and interpretation
- Risk management and predictive analytics - develop skills in using AI for risk assessment and targeting; train staff to interpret AI-generated insights for decision-making
- AI ethics and governance - educate officers working in policy and legal matters on ethical considerations in AI deployment; ensure compliance with data privacy regulations and Customs laws
- AI project management - train managers in overseeing AI/ML projects; focus on integrating AI solutions into existing Customs processes and obtain hands-on experience with AI Tools

Developing in-house expertise is critical for the long-term sustainability of AI/ML projects and for minimizing reliance on external consultants. This development process involves a combination of structured training programmes, collaboration with external experts and hands-on experience with AI/ML tools and techniques.

11.1 Developing data literacy across the organization

Besides technical expertise, Customs administrations need to foster a culture of data literacy across the organization. Data literacy refers to the ability to understand and interpret data, which is essential for both technical and non-technical staff working on AI/ML projects. Customs officers, policymakers and decision-makers should be trained on how to interpret AI/ML-generated insights and apply them in decision-making processes. Understanding data-driven insights allows for better oversight, ensuring that AI/ML models are used effectively to enhance Customs operations.

Some of the suggested activities to build up data literacy include:

11.1.1 Data literacy awareness programmes

Customs administrations can implement awareness programmes that introduce basic data concepts to all staff, including Customs officers, policymakers and administrative personnel. These programmes can cover fundamental concepts like the difference between structured and unstructured data, the role of data in AI/ML models and how data quality affects decision-making. This creates a baseline understanding of how data influences operations.

11.1.2 Workshops on data interpretation

Customs administrations can organize hands-on workshops focused on teaching non-technical staff how to interpret and use data-driven insights. For example, these workshops can cover how to read dashboards, understand risk scores and apply AI-generated risk assessments to make informed decisions during inspections or clearance processes. Practical scenarios involving real Customs data can be used to train staff on applying data insights in everyday operations.

11.1.3 Interactive data dashboards

Providing interactive data dashboards customized to different roles within the Customs administration can empower staff to access and interact with real-time data. For instance, Customs officers could use dashboards to track high-risk shipments, while compliance managers could monitor trends in enforcement actions. Training sessions on how to navigate and extract useful insights from these dashboards would enhance data literacy.

11.2 Strategies for developing AI/ML training and capacity building

11.2.1 Assessing current skill levels and identifying gaps

The first step is to assess the current level of technical expertise within the Customs administration. Understanding the existing capabilities of the workforce will help identify skill gaps in key areas such as data science, ML, data engineering and AI ethics. Customs administrations can then design targeted training programmes to address these gaps, ensuring that their staff have a solid foundation in AI/ML concepts and tools. This includes identifying employees who have the potential to become internal champions for AI/ML initiatives and providing them with advanced training.

11.2.2 Capacity building through cross-departmental collaboration

AI/ML initiatives in Customs administrations require collaboration across various departments, including IT, data management, operations and compliance. Developing cross-departmental teams that work together on AI/ML projects can improve communication and ensure a holistic approach to implementation. These teams should include a mix of domain specialists (e.g. Customs officers), technical experts and data scientists, and ensure that AI/ML solutions align with operational needs and regulatory requirements.

Cross-training programmes, where staff from different departments are introduced to AI/ML concepts and their potential impact on Customs operations, can also foster greater understanding and collaboration. This approach promotes the integration of AI/ML into broader Customs processes, reducing silos and ensuring that AI/ML tools are embedded into everyday workflows.

11.3 Building technical expertise

To develop the necessary technical skills for AI/ML projects, Customs administrations should implement a structured programme that focuses on core AI/ML competencies such as data analysis, model development and the application of algorithmic techniques to real-world Customs operations.

Such training can be done through partnerships with academic institutions, online courses, or in collaboration with AI/ML experts or with other government agencies.

Workshops and boot camps that focus on real-world applications in Customs, such as predicting non-compliance or automating clearance processes, can further strengthen staff's ability to leverage AI/ML in their daily work.

The following are examples of activities and training methods that can help build this expertise:

11.3.1 Partnerships with academic institutions

Customs administrations can collaborate with local or international universities that specialize in data science and AI/ML. These partnerships could offer:

- Certificate programmes in ML or data science for Customs personnel, providing foundational knowledge of AI concepts and algorithms.

- Custom courses tailored specifically for Customs, focusing on AI applications such as trade data analysis, fraud detection and process optimization. Topics should include the use of AI/ML algorithms such as decision trees, random forests and support vector machines, as well as the practical application of these models in Customs operations for risk assessments, fraud detection and process optimization.
- Internships or research collaborations where Customs staff can work with university researchers on AI/ML projects relevant to Customs operations, such as automating document classification for faster clearance processes.

11.3.2 Hands-on training, online courses and certifications

Practical and hands-on training with AI/ML platforms and tools (like Python, R, TensorFlow, etc.) can help build familiarity with the systems needed to develop and deploy AI/ML models. Customs administrations can provide staff with access to popular AI/ML platforms and programming environments, such as:

- Python and libraries like TensorFlow for building ML models.
- R for statistical computing and data analysis.
- TensorFlow for creating deep learning models that could automate complex tasks, such as image recognition in scanned documents.

Due to its popularity and demand, there is no shortage of providers offering specialized AI/ML training for mastering AI/ML tools and software. Customs administrations can encourage staff to complete:

- Online ML courses covering key algorithms like random forests, neural networks and Support Vector Machines (SVMs). These courses often include interactive coding challenges and quizzes that help reinforce learning.
- AI-focused certifications that combine theory and hands-on practice, equipping Customs personnel with practical knowledge of tools like Python, R, TensorFlow, etc. For example, staff could enrol in an online course on predictive modelling for Customs operations, learning how to build models that identify anomalies in trade patterns that indicate potential smuggling activities.

11.3.3 Workshops and boot camps

In-house AI/ML workshops or boot camps can provide intensive, hands-on experience. These activities could be delivered by AI/ML experts or technology vendors and focus on real-world Customs use cases:

- Data analysis boot camps where Customs officers are trained on using Python or R to analyse Customs data, such as identifying trends in Customs declarations or spotting irregularities in trade volumes.
- ML model development workshops that teach staff to build, train and validate AI models using historical Customs data. For example, officers could learn how to develop and validate models that predict the likelihood of non-compliance or duty evasion.

These hands-on sessions provide opportunities to apply AI/ML techniques directly to the datasets that Customs officers work with, ensuring practical and relevant learning.

11.3.4 Hackathons or data challenges

Customs administrations can organize AI/ML hackathons or data challenges where teams of Customs personnel compete to solve specific problems using ML. Examples of challenge topics include:

- Fraud detection models: teams could be tasked with building models that detect unusual trade patterns that may indicate fraudulent declarations or misclassified goods.
- Optimizing clearance times: participants could work on automating the clearance process using predictive algorithms that prioritize low-risk shipments for fast-track processing.

Hackathons encourage collaboration and innovation while allowing staff to gain hands-on experience with AI/ML tools and techniques.

11.4 Establishing new job profiles for AI/ML

The integration of AI/ML into Customs operations requires expertise in areas like ML, data analysis and automation, which are different from traditional Customs roles. The Human Resource (HR) department in Customs administrations would need to establish new job profiles and descriptions for AI/ML to attract, retain and effectively utilize the newly trained staff in this specialized field.

By creating clear and updated job profiles that outline the specific competencies, responsibilities and technical skills required for AI/ML positions, HR can better target, train and recruit the right talent. Additionally, well-defined roles help offer career development opportunities, ensuring that newly trained staff feel valued and see a clear path for growth within the organization, which is essential for retention and the long-term success of AI/ML initiatives in Customs operations.

Some of the new HR profiles and job descriptions are set out below:

11.4.1 AI/ML Specialist

Role overview:

The AI/ML Specialist should ideally be employed in the Customs administration's IT Department, to focus on the technical development and deployment of AI/ML models across different areas of Customs operations.

AI/ML Specialists are to be responsible for designing, developing and implementing AI/ML models to optimize various Customs operations, including risk assessment, fraud detection and trade compliance. This role focuses on leveraging advanced data analytics and ML techniques to support decision-making and enhance efficiency across the Customs administration. AI/ML Specialists will work closely with data engineers, Customs officers and IT professionals to ensure that AI/ML applications align with the organization's strategic objectives.

Key responsibilities:

1. AI/ML model development:
    - Develop, train and deploy ML models for use in Customs operations (e.g. shipment classification, fraud detection, risk assessment).
    - Experiment with different algorithms, such as decision trees, random forests and neural networks, to solve Customs-specific challenges.
    - Fine-tune models to optimize performance, ensuring high accuracy and relevance to operational needs.
2. Data preparation and analysis:
    - Collaborate with the IT data engineering team to prepare, clean and normalize data for AI/ML projects.
    - Analyse large datasets from Customs systems to identify trends, anomalies and potential areas for AI/ML application.
    - Work with structured and unstructured data, including trade data, inspection reports and transaction records.
3. Deployment and maintenance:
    - Oversee the deployment of AI/ML models into production systems, ensuring they are integrated smoothly into the daily operations of Customs.
    - Continuously monitor model performance and accuracy, updating and retraining models as needed to account for new data or operational changes.
4. Cross-departmental collaboration:
    - Liaise with Customs officers, risk management teams and compliance personnel to ensure that AI/ML models align with practical needs and regulatory requirements.

    - Provide training and guidance to non-technical teams on how to use AI/ML-driven insights effectively in decision-making processes.
5. Documentation and reporting:
    - Document model development processes, assumptions and outcomes for internal reporting and auditing purposes.
    - Prepare and present performance reports and data-driven insights to senior management, making recommendations for process improvements.
6. Innovation and research:
    - Stay up to date with the latest advancements in AI/ML technologies and apply innovative techniques to solve Customs-related challenges.
    - Experiment with new models and tools to explore potential new applications of AI/ML in Customs operations.

Key qualifications:

- Education:
    - Bachelor or Master of Data Science, Computer Science, AI, ML, or a related field.
    - Professional certifications in AI/ML, data science, or related areas are an advantage.
- Experience:
    - 3-5 years of experience working with AI/ML models, preferably in a public sector or regulatory environment.
    - Proven experience in developing and deploying ML algorithms such as Support Vector Machines (SVMs), random forests, neural networks, etc.
    - Experience working with AI/ML platforms such as TensorFlow, Scikit-learn or similar tools.
- Technical skills:
    - Proficiency in programming languages such as Python, R or Java.
    - Expertise in data analysis tools and techniques.
    - Experience with cloud-based AI platforms (AWS, Google Cloud, Azure) is a plus.
    - Familiarity with Customs operations, trade regulations or risk assessment frameworks is desirable.

Core competencies:

- Analytical thinking: ability to analyse large datasets, draw meaningful conclusions and develop actionable AI/ML models.
- Problem-solving: ability to approach Customs-related challenges with data-driven solutions and innovative ideas.
- Communication skills: ability to communicate technical AI/ML concepts to non-technical stakeholders.
- Collaboration: ability to work across departments, including with Customs officers, IT teams and compliance officers, ensuring AI/ML models meet operational needs.
- Adaptability: willingness to continuously learn and apply new techniques and technologies in AI/ML.

11.4.2 Data Scientist (Customs Operations)

The Data Scientist should ideally be placed within the Innovation and Research Unit, or the Strategic Planning Unit, focusing on data-driven decision-making.

The Data Scientist's role emphasizes the exploration, analysis and interpretation of data, which supports long-term planning, risk management and operational improvements. They will work closely with departments that rely heavily on data insights for decision-making, such as compliance, policy and inspection teams, ensuring that decisions are based on robust data analysis.

The Data Scientist shall focus on exploring, analysing and interpreting large datasets to extract actionable insights that can improve Customs operations. Unlike the AI/ML Specialist, who is primarily responsible for the development and deployment of ML models, the Data Scientist's role involves generating data-driven insights that inform decision-making and leveraging advanced analytics techniques to optimize processes

Key responsibilities:

1. Data exploration and analysis:
    - Perform in-depth analysis of large datasets, including Customs declarations, trade volumes and inspection results, to identify trends, anomalies and key performance metrics.
    - Use statistical methods to evaluate Customs processes, such as the average clearance times for different types of shipments, or to identify patterns related to trade compliance or fraud.
2. Predictive analytics and statistical modelling:
    - Develop statistical models to forecast trade flows, shipment volumes, or potential risk levels for incoming goods.
    - Use predictive analytics to anticipate Customs bottlenecks, allowing the organization to allocate resources effectively during peak trading periods.
    - Create models to predict changes in trade behaviour due to regulatory shifts, tariffs or global market trends.
3. Data visualization and reporting:
    - Build interactive dashboards and visualizations that help stakeholders quickly understand and act on data insights, such as risk assessment scores, fraud detection trends and clearance time improvements.
    - Generate detailed reports that provide insights into trade patterns, compliance rates and inspection effectiveness, to inform policy-making and strategic planning.
    - Collaborate with senior management and Customs officers to interpret these insights and develop actionable recommendations.
4. Data quality and governance:
    - Work closely with data engineers to ensure that data pipelines and databases are optimized for analytics use, ensuring data quality and integrity.
    - Implement data validation techniques to ensure the accuracy, completeness and reliability of trade data before it is used in analysis or decision-making.
    - Define and monitor data quality metrics, ensuring that Customs operations are driven by accurate and trustworthy data.
5. Collaboration and cross-department support:
    - Collaborate with risk management teams, compliance officers and Customs inspection units to provide data-driven insights that support their operational goals.
    - Work with IT and data engineering teams to ensure data accessibility and to design systems that allow real-time data monitoring for Customs officials.
    - Provide ad-hoc analytical support to different departments, enabling them to use data insights in their day-to-day decision-making processes.
6. Trend and policy analysis:
    - Analyse the impact of new trade agreements, tariffs or regulations on Customs operations and trade volumes, offering insights on how Customs administrations can adapt to these changes.
    - Monitor global trade trends and geopolitical factors, identifying potential risks or opportunities for Customs operations, such as shifts in trade routes or emerging markets.

7. Innovation and research:
    - Stay updated on the latest developments in data science and analytics technologies, including advanced statistical techniques and big data platforms.
    - Explore innovative ways to apply data analytics to emerging challenges in Customs, such as automating compliance checks or improving the accuracy of risk assessments through data-driven approaches.

Key qualifications:

- Education:
    - Bachelor or Master of Data Science, Statistics, Computer Science, Mathematics, Economics, or a related field.
    - Professional certifications in data analytics, statistics or big data are a plus.
- Experience:
    - 3-5 years of experience in data analysis, statistical modelling or data science, preferably in a public sector or trade-related context.
    - Strong background in exploratory data analysis, trend identification and statistical techniques.
    - Experience working with large, complex datasets and designing data visualizations for non-technical stakeholders.
- Technical skills:
    - Proficiency in statistical tools such as R, Python or SAS.
    - Expertise in using data visualization tools like Tableau, Power BI or D3.js to build dashboards and reports.
    - Familiarity with SQL and other database management systems for querying large datasets.
    - Knowledge of cloud-based data platforms (e.g. AWS, Google Cloud) and big data technologies (e.g. Hadoop, Spark) is an advantage.
    - Experience with statistical modelling techniques like regression analysis, clustering and time series analysis.

Core competencies:

- Analytical thinking: ability to analyse complex datasets, discover patterns and make data-driven recommendations.
- Problem-solving: ability to apply statistical and data science techniques to solve real-world challenges in Customs operations.
- Communication: ability to explain data insights and technical concepts clearly to non-technical stakeholders.
- Collaboration: strong teamwork skills, with the ability to work across departments to support data-driven decision-making.
- Attention to detail: high level of accuracy in data analysis, ensuring all insights are grounded in reliable data.

12 Evaluation, success stories and lessons learned

As Customs administrations embark on AI/ML projects, it is essential to establish clear evaluation frameworks and success metrics to ensure these initiatives deliver value and achieve their intended outcomes. Evaluating AI/ML projects involves both quantitative and qualitative assessments, focusing on model performance, operational improvements and alignment with strategic goals.

Success is measured by how well the AI/ML projects meet predefined objectives and contribute to the long-term strategic goals of the organization. Measurement metrics should include improvements in efficiencies, reduction of costs and tangible benefits in Customs operations, which should be monitored through appropriate KPIs in the organizational performance management system.

By continuously monitoring performance and iterating based on feedback, Customs administrations can ensure that AI/ML initiatives deliver sustainable value and drive meaningful improvements in their operations.

12.1 Evaluation

The steps involved in AI/ML project evaluation include:

12.1.1 Defining project objectives

The first step in evaluating AI/ML projects is to clearly define the objectives and expected outcomes. Customs administrations must identify specific goals that the AI/ML initiative is intended to achieve, such as:

- improving the accuracy of fraud detection;
- reducing Customs clearance time;
- increasing revenue through better compliance enforcement.

These objectives serve as the foundation for evaluating the project's performance and success.

12.1.2 Defining performance metrics for the AI/ML models

The long-term sustainability of AI/ML models is crucial. A successful project involves continuous monitoring and updating of the models to ensure they remain relevant, accurate and adaptable to changing trade dynamics and regulatory requirements. To measure the success of AI/ML models, Customs administrations should establish performance metrics that assess the effectiveness of the models in achieving their objectives. These metrics typically include:

- **accuracy:** the percentage of correct predictions or classifications made by the AI/ML model, such as correctly identifying high-risk shipments or non-compliant traders;
- **precision and recall:** in fraud detection or risk assessment, "precision" measures how many of the flagged cases are actually correct (minimizing false positives), while "recall" measures how many true positive cases are identified (minimizing false negatives).
- **false positive/false negative rates:** these metrics are critical in Customs operations, where false positives can lead to unnecessary inspections and delays, while false negatives can result in missed risks or violations.
- **model stability:** model stability is usually measured on the basis of a stability index using techniques like bootstrapping or cross-validation (testing multiple training datasets with slight variations, and measuring performance dispersion and anomalies across datasets).

12.1.3 Impact on organizational performance and strategic alignment

Beyond model performance, Customs administrations should evaluate the broader **operational impact** of AI/ML projects. These projects are successful if they lead to measurable improvements in Customs processes. Key operational metrics include:

- **reduction in clearance times:** one of the main goals of AI/ML projects is to streamline the Customs clearance process. Success can be measured by how much AI/ML solutions reduce the time it takes to clear shipments, especially for low-risk or compliant goods;
- **increase in detection rates for non-compliance:** a successful AI/ML initiative should improve the ability of Customs administrations to detect fraudulent or non-compliant activities, increasing revenue from fines or preventing lost duties;
- **resource optimization:** AI/ML models that accurately predict high-risk shipments or traders enable Customs administrations to allocate resources more effectively, reducing the need for random inspections and focusing attention on higher-priority cases;
- **cost savings:** the deployment of AI/ML solutions should lead to long-term cost savings through process automation, reducing the manual labour required for data entry, inspections and risk assessments.

12.1.4 Measurement of success

Success in AI/ML projects for Customs administrations is measured by their alignment with broader strategic goals, including operational efficiency, risk management, compliance, trade facilitation and security. Evaluating AI/ML contributions to these objectives involves considering the following factors:

- **operational efficiency:** AI/ML should optimize resource allocation, automate processes and reduce processing times and costs. Success is measured by improved clearance times, automation of repetitive tasks and enhanced productivity;
- **trade facilitation:** AI/ML should create a seamless trade environment by expediting Customs clearance, reducing delays and improving supply chain visibility. Success can be measured by increased trade volumes, faster processing and higher trader satisfaction;
- **risk management:** AI/ML should enhance risk assessment by improving the accuracy of fraud detection and anomaly identification. Effectiveness is measured by better targeting of high-risk shipments and passengers while reducing false positives;
- **compliance:** AI/ML should improve adherence to regulations by ensuring accurate classification, valuation and reporting. Success is reflected in higher compliance rates, fewer regulatory breaches and more effective enforcement actions;
- **security:** AI/ML should strengthen border security by enhancing surveillance, detecting illicit goods and preventing smuggling. Effectiveness is evaluated through improved detection rates, stronger monitoring capabilities and better coordination with enforcement agencies.

By assessing these aspects, Customs administrations can gauge the effectiveness of their AI/ML projects in achieving their strategic goals and improving overall performance.

12.1.5 User adoption and satisfaction

A critical measure of success is user adoption and satisfaction. Customs administrations should assess how well Customs officers and other stakeholders are adopting the AI/ML systems and whether they find the tools useful in their day-to-day work. This can be evaluated through:

- **training and ease of use:** measuring how well-trained and comfortable users are with the new AI/ML systems;
- **feedback surveys:** gathering feedback on how AI/ML tools have improved or impacted the workflow for Customs officers, compliance teams and other users.

12.1.6 Cost-benefit analysis

An important measure of success is the return on investment (ROI) for the AI/ML project. Customs administrations should conduct a cost-benefit analysis to assess whether the long-term benefits of the AI/ML system outweigh the costs of development, implementation and maintenance. Success can be measured by the extent to which the system provides:

- **long-term cost savings through reduced manual processing and automation;**
- **revenue gains from better fraud detection, duty collection and compliance enforcement;**
- **efficiency improvements leading to faster Customs clearance time, reduction of inspection due to enhanced risk assessment.**

12.2 Lessons learned

To incorporate "lessons learned" effectively in AI/ML projects, Customs administrations can take several key approaches:

1. **Formalized knowledge sharing platforms:** establish a centralized repository where project teams document challenges, solutions and lessons learned. Regular internal knowledge-sharing sessions, such as workshops and seminars, can help disseminate these insights across departments, ensuring teams are better equipped for future AI/ML initiatives.
2. **Post-implementation reviews:** conduct reviews after project completion to analyse what worked and what did not. These reviews should involve key stakeholders and focus on technical, operational and process-related lessons. Incorporating feedback loops throughout the project lifecycle allows Customs administrations to continuously refine and adapt their strategies.
3. **Training and development programmes:** use lessons learned to update staff training programmes and build in mentorship opportunities, where experienced teams guide emerging adopters. This ensures that staff apply best practices and avoid repeating past mistakes, helping build institutional knowledge around AI/ML.
4. **Cross-agency collaboration:** share lessons with other Customs administrations or relevant agencies to promote collective learning. Through collaborative forums, workshops or conferences, Customs administrations can exchange insights and best practices, helping reduce the digital divide between emerging and advanced adopters.

13 Conclusion: AI/ML as catalysts for transforming Customs administrations

The integration of AI/ML into Customs operations represents a strategic shift in the way Customs administrations manage trade, compliance and enforcement in a complex global environment. This Report has explored the profound implications of AI/ML adoption, covering technological capabilities, legal frameworks, policy considerations, implementation strategies and case studies.

AI/ML technologies offer Customs administrations strategic inflection points, enabling both evolutionary improvements and revolutionary shifts. Evolutionary enhancements focus on streamlining operations, improving risk profiling and automating repetitive tasks. Advanced applications, including generative AI, open doors to revolutionary capabilities, such using LLMs to validate Customs declarations, invoices and certificates of origin in real time, or by combining LLMs with graph neural networks (GNNs), to analyse, visualize and synthesize patterns from shipment data, Customs records and social networks.

One of the key themes emphasized throughout this Report is the importance of a structured and incremental approach to AI/ML adoption. Customs administrations are encouraged to begin with small, high-impact pilot projects focused on specific use cases and achieve quick wins before scaling up to more advanced and integrated systems. One such example used in many Customs administrations, is the use of AI-powered algorithms to improve goods classification and valuation accuracy, reducing Customs processing and cargo clearance times. This phased approach minimizes risks while demonstrating tangible benefits early in the process.

Key to successful implementation is the recognition that AI/ML adoption is not a one-time effort but an iterative process. Customs administrations must continuously monitor performance, update models and integrate insights from pilot projects to refine strategies and enhance outcomes. This requires investment not only in infrastructure and tools but also in governance frameworks that promote flexibility, adaptability and accountability. Additionally, the emphasis on cloud-based solutions and hybrid architectures highlights scalable and cost-effective strategies for implementation, making AI/ML adoption accessible to Customs administrations with varying levels of readiness.

The importance of addressing ethical, legal and regulatory considerations cannot be overstated. As AI systems rely heavily on data, Customs administrations must prioritize data governance frameworks that ensure quality, integrity and compliance with privacy regulations. Establishing safeguards to mitigate bias, ensuring transparency in AI decision-making and implementing human-in-the-loop systems to maintain accountability are critical elements of responsible AI/ML adoption. Furthermore, the report underscores the need for alignment with emerging international AI regulations, promoting consistency and legal compliance across jurisdictions.

The human factor remains central to the success of AI/ML adoption. Building organizational capacity through targeted training programmes and partnerships is crucial for sustaining AI-driven transformations. Developing AI/ML literacy among both technical and non-technical staff, creating specialized roles and promoting collaborative practices enable Customs administrations to harness AI/ML capabilities effectively. Equally important is fostering stakeholder engagement, ensuring open communication and incorporating feedback mechanisms to build trust and drive adoption.

In conclusion, AI/ML technologies present an unprecedented opportunity for Customs administrations to transition into data-driven, agile and intelligent organizations. By leveraging AI/ML, Customs administrations can strengthen their role as facilitators of secure and efficient trade while addressing regulatory and enforcement challenges. However, this transformation demands a balanced approach - one that starts with incremental steps, prioritizes ethical standards and invests in long-term capacity building. With strategic vision and careful planning, Customs administrations can unlock the full potential of AI/ML, ensuring sustainable modernization and global competitiveness in the years ahead.

* * *

*

Contact us:

Smartcustoms@wcoomd.org

Visit our website:

wcoomd.org/SmartCustoms.aspx

World Customs Organization

Rue du Marché 30, B-1210
Brussels, Belgium

#WCOOMD
wcoomd.org