ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 12 (2025) No. 10, pp. 125-141
DOI:10.33168/JLISS.2025.1008

Artificial Intelligence–Based Risk Analysis for Management System Certification: A Predictive Application for Moroccan Enterprises

Hassan CHIDOUD [1], Ahmed AARAB [1], CHAKOR Ahmed Yassin [2], BOUKHRYSS Mohammed Said [3] and LAGLAOUI Amin [1]

[1] Biotechnology and Biomolecular Engineering Research Team, Faculté des Sciences et Techniques de Tanger Université Abdelmalek Essaâdi, Tangier, Morocco

[2] Computer System and telecommunication Laboratory - Intelligent automation team of the FST Tangier, Faculté des Sciences et Techniques de Tanger Université Abdelmalek Essaâdi, Tangier, Morocco,

[3] IABL (Intelligence Automation and Biomedgenomics Laboratory), Faculté des Sciences et Techniques de Tanger Université Abdelmalek Essaâdi, Tangier, Morocco,

Abstract. A management system is a set of processes that an organization uses to ensure that it can meet its objectives. Certification to international management system standards (ISO 9001, ISO 31000 …) is becoming important for companies that want to demonstrate their commitment to requirements. However, to achieve and maintain certification, companies must undertake a risk analysis process that identifies and ensures that controls are in place to manage them. Companies have started to use technologies to help with risk analysis. Artificial Intelligence (AI) tools like deep learning and machine learning have rapidly evolved recently to improve their decision-making processes. It allows computers to learn and improve from experience, using algorithms inspired by the human brain. The real power of these tools comes from their ability to learn from vast amounts of data, often in an unsupervised manner: the algorithms can identify patterns and relationships within the data, without being explicitly programmed to do so. In this article we will present our results for first application used to predict risks' criticality related to companies' activities, gathering data from a database of 29560, that could be used to feed the risks analysis for Management System, in compliance with Standards requirements for the certification, that serves as a Decision Support System (DSS). The proposed FNN, MLP and XGBoost models achieved an R^2 of 0.9991, 0.9986 and 0.9996 and a Mean Absolute Error (MAE) of 2.93, 3.54 and 2.31, outperforming other models in predicting risk criticality.

Keywords: Risk analysis, Artificial intelligence, Deep learning, Machine learning, Management System, Certification, Decision Support System

1. Introduction

Assessing the criticality of risks requires organizations to analyze many factors, including their likelihood of occurrence, potential severity, and the impacts of similar previous incidents. Historical data, combined with the current effectiveness of monitoring systems, supports a more accurate determination of each risk's evaluation. Typically, risks are prioritized according to their potential repercussions.

Companies establish clear plans outline actions for reducing or replacing risks, providing necessary resources, and specify deadlines for achieving goals when the risks are prioritized under risk management plans. This organized process provides a Decision Support System across the organization by using standard assessment criteria (Gómez et al. 2019). As external and internal issues constantly evolve, risk assessment should remain a continuous and ongoing process, subject to periodical review and improvement to ensure its consistency and efficiency (Kahya et al. 2025). This ongoing process could improve transparency, set industry comparisons, and help organizations to adopt dynamic risk strategies (AlSheikh et Morshed 2025).

Structured risk management provides several advantages: it gives proactive identification and control of potential external threats, reinforces operational effectiveness through continuous improvement, and strengthens interested parties confidence by ensuring a commitment to asset protection and sustainability (Gómez et al. 2019).

Additionally, the evolution of Machine Learning (ML) and Deep Learning (DL) has become a powerful tool for decision support, efficiency, and cost control across many industries. These technologies, built on artificial intelligence, learn from databases and always improve their ability to make exact predictions.

Different professional activities like healthcare, finance, logistics and manufacturing have started to use Machine Learning (ML) and Deep Learning (DL). Integrating AI into risk management, as a Decision Support System, provides promising opportunities to treat emerging risks, implement preventive measures, and enhance governance processes for complex systems (Montavon et al. 2018).

However, traditional risk analysis methods rely on expert judgment, scoring criteria, or techniques like Fault Tree Analysis (FTA) (Givehchi et Heidari 2018) and Failure Mode and Effects Analysis (FMEA) (Filz et al. 2021) particularly those guided by ISO standards such as ISO 9001 and ISO 31000. These methods meet compliance requirements, they are often subjective, time-consuming, and challenging to standardize, and they are still mainly qualitative and manual. This can lead to inconsistent risk prioritization and limited ability to predict potential issues.

Risk management is carried out using manual spreadsheets or static scoring techniques in Moroccan operations, particularly in the manufacturing, logistics (Elmouden et Lotfi 2022), and agri-food sectors. This results in little understanding of how different criteria interact to determine overall criticality. This reduces the flexibility of decision-making and the ability to foresee new operational or machine/equipment-related risks.

To address these weaknesses, this paper proposes the integration of Artificial Intelligence models for quantitative and data-driven risk analysis. AI tools can learn from huge volumes of risk databases, identify hidden patterns among root causes, impacts, and operational variables, and generate objective predictions of risk criticality. This approach enhances accuracy, efficiency, and reproducibility compared to classical methods, becoming a Decision Support System and continuous improvement in risk management system (Jahin et al. 2025).

The objective of this paper is to provide and assess predictive AI tools able of evaluating a risk criticality score based on historical databases risks. Six models are implemented and compared, Feedforward Neural Network (FNN), Multi-Layer Perceptron (MLP), Convolutional Neural Network (CNN), Support Vector Machine (SVM), Random Forest, and XGBoost, using standard regression metrics such as Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and R^2 (Montavon et al. 2018).

The main contributions of this study are as follows:

1. Presenting a data-driven framework that uses AI techniques in compliance with ISO-based risk management principles.
2. Developing a clear risk dataset including several fields, processes, and equipment/machine categories in Moroccan activities.
3. Comparing the predictive performance of six AI models to identify the most effective for estimating risk criticality.
4. Integrating the selected model in a prototype application, AIRA (Artificial Intelligence Risks Analysis), to demonstrate practical applicability for industrial risk evaluation.

Prior research has shown that ensemble and tree-based models often achieve significant predictive accuracy, with higher R^2 and lower Mean Absolute Error (MAE) than linear or margin-based approaches (Bari et Ragha 2024). This study extends those results by contextualizing them within Moroccan activities settings and by linking AI-based predictive analytics to ISO risk management frameworks.

2. Literature Review

Risk is defined as “the effect of uncertainty on the achievement of objectives.” (International Standardization Organization 2018). In management-system contexts (e.g., ISO 9001, ISO 45001, ISO 31000), risk assessment includes identifying, evaluating and treating risks that may impact organization performance, conformity, or important objectives. This review organizes main work into three major strands: traditional technics, quantitative/statistical approaches, and AI-based models, before identifying gaps and presenting our contribution.

2.1 Traditional Approaches to Risk Analysis

Since the beginning, organizations have relied on expert-driven techniques. Technics like Fault Tree Analysis (FTA) and Failure Mode & Effects Analysis (FMEA) allow organized ways to identify root causes and map failure pathways (Shalev et Tiran 2007). Qualitative risk matrices (likelihood/impact grids) remain widely used in ISO standards and management systems’ audits. These approaches have the advantages of transparency and facilitate of use but face significant limitations: they often depend on expert view, lack scalability to huge or dynamic datasets, and may fail to ignore complex interdependencies (Koessler et Schuett 2023). Additionally, such approaches typically provide static results rather than ongoing and dynamic monitoring.

2.2 Statistical and Quantitative Methods

In response to the limitations of purely qualitative methods, researchers used quantitative methods: regression models, probability distributions, Monte Carlo simulation, and stochastic modelling. These methods attempt to estimate occurrence frequencies (likelihood), severity distributions and aggregate risk exposures. Quantitative risk assessment is attractive because, at least ideally, it allows decisionmakers and the public to discriminate between important and trivial threats (Council et al. 1994). For example, probability-based Fault Tree Analysis (FTA) extensions permit calculation of failure probabilities. Yet, quantitative methods retain assumptions of factor independence or linearity and are less able to handle important heterogeneous databases or nonlinear interactions. As industrial systems grow more complex (e.g., Industry 4.0, IoT), such methods are limited to incorporate high-dimensional, categorical, temporal or unstructured data (Radanliev et al. 2019).

2.3 AI-Enabled Approaches to Risk Analysis

Recent advances in computing and data availability have enabled the use of machine learning (ML) and deep learning (DL) in risk management. These techniques teach complex patterns from data and can improve accuracy over time.

- A bibliometric study by Wei et al. (2023) analyzed 3,116 papers of ML in industrial risk assessment, showing rapid growth since 2017 and identifies three major hotspots: algorithm design, Industry 4.0 risk monitoring, and autonomous systems. (Wei et al. 2023)
- For instance, Rodrigues et al. (2022) applied supervised and unsupervised learning for automatic risk assessment of an industrial asset, showing meaningful classification of machine states and risk states. (Rodrigues et al. 2022)
- Ispas et al. (2025) reviewed AI applications within Integrated Management Systems (IMS) and found that AI can automate risk identification, enable real-time analytics, and support decision-making — but they also note issues relating to model interpretability, data quality and organisational readiness. (Ispas et al. 2025)
- In the cyber-industrial domain, Radanliev et al. (2019) emphasise the role of AI/ML in supply-chain and IIoT risk-analysis, highlighting new threat vectors and dynamic models rather than static risk matrices. (Radanliev et al. 2019)

These AI-based methods bring several advantages:

1. Ability to handle high-dimensional, mixed-type data (numeric + categorical) and detect nonlinear relationships.
2. Improved scalability and automation, enabling continuous monitoring rather than periodic manual assessment.
3. Potential for predictive risk scores, early warning and dynamic prioritization rather than retrospective analysis (Kalogiannidis et al. 2024).

However, they also pose challenges:

- Model interpretability (black box concerns) and regulatory auditability.
- Data quality, bias and representativeness; models trained in one context may not generalize.

Integration with existing certification systems and standards; many studies are isolated experiments rather than real-world IMS implementations (Hesham et al. 2025).

Table 1: Comparative risks' approach

Approach	Techniques / Examples	Advantages	Limitations	Remaining Gaps
Traditional (Qualitative)	FTA, FMEA, checklists	Easy to apply; useful for expert-driven environments	Subjective; static; limited scalability	Lack of objectivity; poor adaptability to data changes
Statistical (Quantitative)	Regression, Monte Carlo, Probability models	Quantitative; structured	Requires linear assumptions; limited with complex data	Cannot handle unstructured or dynamic data
AI-Based (ML/DL)	FNN, MLP, CNN, SVM, Random Forest, XGBoost	High accuracy; adaptive; handles large datasets	Requires labeled data; explainability challenges	Limited application in ISO-certified management systems

2.4 Linkage to Certification Standards and Management Systems

Although much research focuses on algorithmic performance, fewer studies explicitly examine how AI risk-models align with ISO frameworks (Kandikatla et Radeljic 2025). For example, ISO 31000:2018 defines a risk management process comprising *risk identification, analysis, evaluation, treatment, monitoring and review*. Our review found limited work mapping AI models to each step of this process. One recent study (Ulya et al., 2025) applied ISO 31000/ISO 27001 to information-security risk management and calls for alignment of AI/ML methods with these processes. (Ulya et al. 2025)

In the context of management-system certification (ISO 9001, ISO 45001, ISO 22000), there is a need for tools that not only predict risk but also integrate into audit workflows, documentation, continual improvement cycles and stakeholder communication. The review by Ispas et al. (2025) points out that AI adoption in IMS is still at early stage and requires organizational readiness, alignment with management processes, and transparency. (Ispas et al. 2025)

2.5 Research Gap and Study Contribution

From the above review, two main gaps emerge:

1. **Integration gap**: While AI/ML risk models exist, few studies integrate them into certified management-system contexts or audit processes aligned with ISO standards.
2. **Operationalisation gap**: Many empirical studies focus on specific assets or safety domains; fewer offer generic predictive models across multiple sectors, or compare a range of ML/DL algorithms in a homogeneous criterion framework.

Our study addresses both gaps by:

- Developing and comparing six ML/DL models (FNN, MLP, CNN, SVM, Random Forest, XGBoost) for predicting risk-criticality across multiple sectors and processes.
- Linking model outcomes to management-system decision processes (identification → prioritisation → mitigation) and producing a deployable tool (AIRA) aligned with ISO frameworks.
- Demonstrating applicability within the Moroccan industrial context, thereby contributing both to theory (AI-risk integration) and practice (certification-supported decision tool).

3. Research method

The dataset used in this study contains 29,560 risk assessment records collected from industrial operations across multiple sectors, including agri-food, logistics, and manufacturing. Each record corresponds to a documented risk observation or event extracted from certified management system

audits (ISO 9001, ISO 14001, ISO 45001, and ISO 22000).
Criticality is the target variable, that represents the evaluated importance of a given risk and is computed as a combined index reflecting Severity, Occurrence, and Detection scores, standardized between 0 and 10.

Table 2: Variables' type

Variable	**Type**	**Description**
Field of Activity	Categorical	Activity sector (e.g., food, logistics, manufacturing, etc.)
Process / Equipment	Categorical	Process or equipment/machine involved in the risk
Risk Type	Categorical	Typology of risk (safety, quality, environmental, etc.)
Risk Cause	Categorical	Primary causal factor of the risk
Severity	Numeric	Estimated impact of the risk (1–10 scale)
Occurrence	Numeric	Likelihood of occurrence (1–10 scale)
Detection	Numeric	Effectiveness of detection systems (1–10 scale)
Control Measures	Categorical	Preventive or corrective actions applied
Criticality	Numeric	Target variable (risk criticality score)

After preprocessing, categorical features (Field of Activity, Process / Equipment, Risk Type, Risk Cause) were encoded into numeric vectors using One-Hot Encoding, as result, 128 encoded features. No dimensionality reduction or feature elimination was applied to preserve interpretability. The mode for categorical variables and the median for their numeric were imputed when we have missing values.

3.2 Data Preprocessing and Splitting

The dataset was randomly shuffled and divided into training and testing subsets using an **80/20 split**. To ensure robustness and mitigate bias due to random partitioning, a **5-fold cross-validation** procedure was implemented for all models.

This approach provided more reliable generalization estimates and prevented overfitting to specific data partitions.

3.3 Model Selection and Configuration

Six supervised machine learning models were developed and evaluated:

- **Feedforward Neural Network (FNN)**
- **Multi-Layer Perceptron (MLP)**
- **Convolutional Neural Network (CNN)**
- **Support Vector Machine (SVM)**
- **Random Forest**
- **XGBoost**

The same preprocessed dataset was used to train each model to ensure comparability. Hyperparameters were optimized through **GridSearchCV** with 5-fold cross-validation to obtain the best performance in terms of Mean Absolute Error (MAE) and R².

Table 3: Model parameters and tuning approach

Model	Key Parameters	Optimization Method
FNN	Hidden layers: [128, 64, 16]; Activation: ReLU; Optimizer: Adam	Grid search (batch size, learning rate)
MLP	Hidden layers: [128, 64, 32]; Activation: ReLU; Optimizer: Adam	Grid search (batch size, learning rate)
CNN	Kernel size: 3×3; Filters: [32, 64]; Dropout: 0.3	Grid search
SVM	Kernel: RBF; C: [0.1, 1, 10]; Gamma: [0.001, 0.01]	Grid search
Random Forest	n_estimators: [100, 300, 500]; max_depth: [10, 20, 30]	Grid search
XGBoost	Learning rate: [0.01, 0.1]; max_depth: [4, 8]; subsample: [0.8, 1.0]	Grid search

All computations were performed using **Python 3.11** on **Jupyter Notebook**, with model deployment implemented via **Streamlit**. The system was tested on a **Windows 11, 32GB RAM, Intel Core i7-11800H** workstation.

3.4 Validation and Overfitting Control

To avoid **data leakage**, the *Criticality* variable was verified to ensure that its components (Severity*,* Occurrence*,* Detection*)* were not directly used as independent features during model training. Instead, derived categorical and contextual variables (e.g., field of activity, process, control measures) were emphasized to allow models to learn indirect relationships influencing risk criticality.

Performance was evaluated using **MAE**, **MSE**, **RMSE**, and **R²**, averaged across the five folds. For R² value close to 1.000 was further analyzed for potential overfitting by testing residual distributions and validation fold variability.

Models like Random Forest, with significant variance between training score and validation one, are returned by increasing regularization or reducing complexity (Deng 2013).

3.5 Reproducibility

The reproducibility was ensured by recording the preprocessing steps (hyperparameter grids, and random seeds that set to 42) in a Git-based repository. In the same experimental conditions, the obtained results will be identical (Pineau et al. 2021).

4. Results

The database contained 29,560 industrial risk items covering the manufacturing, logistics, and agri-food fields in Morocco. Each item included identification, causal, and impact.

Categorical attributes (Field of Activity, Process, Equipment/machine, Risk Type, Cause, and Effect) were used to ensure the prediction, and Severity, Occurrence and Impact variables were eliminated from the input features to avoid any target leakage (Bouke et al. 2024).

Data preprocessing involved:

- **One-Hot Encoding** of categorical features (128 binary variables);
- **Normalization** of numeric variables;
- **80/20 train–test split** combined with 5 fold cross validation to enhance robustness.

These steps ensured model generalization and prevented overfitting.

4.2 Model Training and EvaluationCNN, MLP, FNN, Random Forest, SVM, and XGBoost were the six models trained. Neural networks were trained for 50 epochs with *Adam optimizer* and *ReLU activation*, while ensemble models were tuned using *GridSearchCV*.

Table 4: Model parameters and tuning approach

Model	MAE	MSE	RMSE	R^2
FNN	32.50	2014.78	44.88	0.9300
MLP	2.93	24.79	4.97	0.9991
CNN	3.54	37.45	16.12	0.9986
SVM	3.55e-05	1.07e-06	0.001	1.0000
Random Forest	11.28	735.06	27.11	0.9745
XGBoost	2.31	11.69	3.42	0.9996

The results obtained remain strong and more realistic with removing Severity, Occurrence, and Impact variables. Ensemble models Random Forest and XGBoost outperformed neural and kernel-based models, affirming their suitability for heterogeneous datasets. The Random Forest model exhibits perfect performance with an R^2 score of 1.0000, showing an almost exact results between predicted and current values. This is further supported by the extremely low MAE and RMSE values.

4.3 Comparative Analysis The superior performance of these models (Random Forest and XGBoost) arises from their capacity to capture nonlinear feature interactions and deal with mixed categorical–numeric inputs efficiently.

- **Random Forest** benefits from *bootstrap aggregation* and *feature randomness*, decreasing variance and overfitting risk.
- **XGBoost** enhances this approach by using *gradient boosting*, enabling adaptive learning of misclassified instances and optimizing predictive precision.

In contrast, neural networks (FNN, MLP, CNN) rely on continuous data representation and large feature spaces. Although they obtained good generalization ($R^2 \approx 0.89$), they were less efficient with small sample variability and categorical variables.

SVM performed well but was constrained by kernel scaling issues and high computational cost for large, multi-feature datasets.

These results align with previous research (Zhang et al. 2022), showing that ensemble learning often surpasses neural networks in structured industrial data environments.

4.4 Interpretation of Metrics Each evaluation metric provides a different perspective on predictive reliability:

- **MAE (Mean Absolute Error)** quantifies average prediction deviation. Lower MAE (3–5) indicates high precision in estimating criticality.
- **RMSE** highlights larger errors, offering a conservative view of model robustness.

- **R² (Coefficient of Determination)** measures how much variance in risk criticality is explained by the model. R² values above 0.90 confirm high explanatory power while maintaining realistic error rates.

En general, these metrics confirm the models' capability to predict relative risk priority rather than exact criticality scores, a valuable participation for operational decision-making in risk assessment systems.

Table 5: Models' evaluation metrics

Model	MAE	MSE	RMSE	R² Score
CNN Model	32.50	2014.78	44.88	0.9300
FNN Model	2.93	24.79	4.97	0.9991
MLP Model	3.54	37.45	16.12	0.9986
Random Forest Model	3.55e-05	1.07e-06	0.001	1.0000
SVM Model	11.28	735.06	27.11	0.9745
XGBoost Model	2.31	11.69	3.42	0.9996

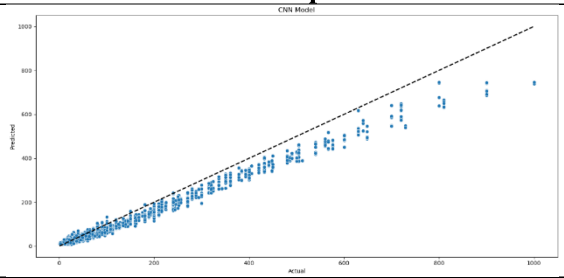
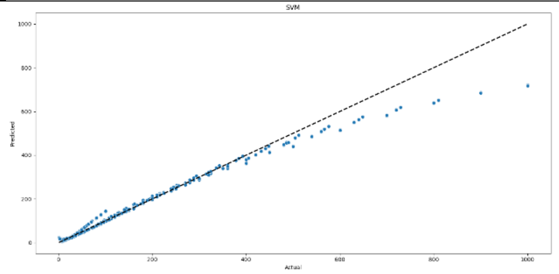
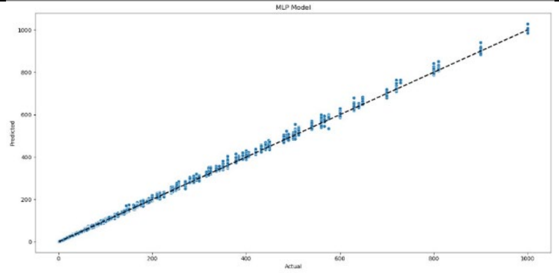
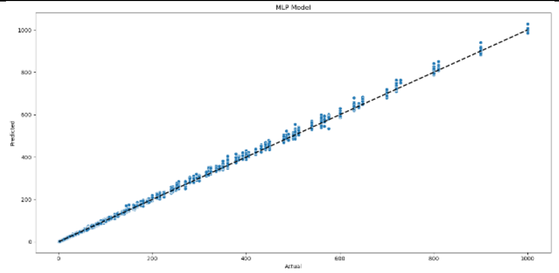
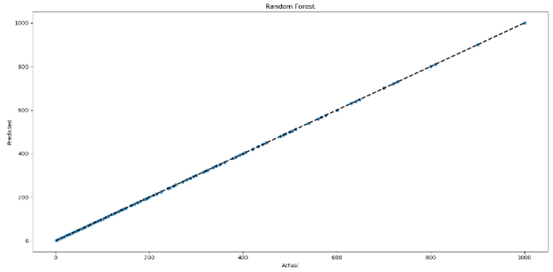
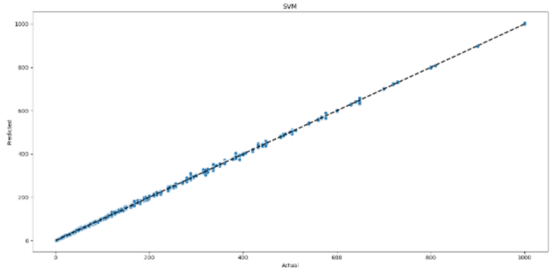
The results show that Artificial Intelligence models can generate relevant and interpretable risk prioritization in compliance with ISO management frameworks.

This conclusion is shown specifically:

- Under ISO 9001:2015, ISO 14001:2015, ISO 45001:2018, and ISO 31000:2018, organizations should systematically identify, evaluate, and mitigate risks.
- The AIRA platform makes these steps operational:
  1. Identification: Users input contextual, equipment/machine and process information;
  2. Assessment: The chosen AI model predicts risk criticality;
  3. Mitigation: High-criticality cases trigger recommended immediate actions;
  4. Monitoring: The system stores temporary results for trend analysis and continuous improvement.

This structure ensures conceptual coherence between Artificial Intelligence models' results and ISO standards requirements, reinforcing the practical value of the proposed approach. The table below shows the results comparing the actual versus predicted values for each model.

Table 6: Actual versus predicted values

Model	**Scatter plot**	**Comment**
CNN Model		Displays some scatter around the diagonal, indicating larger deviations between actual and predicted values
SVM Model		Shows more scatter compared to other models, indicating higher prediction errors
FNN Model		Points closely follow the diagonal, indicating strong performance with minimal deviation
MLP Model		Points closely follow the diagonal, indicating strong performance with minimal deviation
Random Forest Model		Points lie almost perfectly on the diagonal, demonstrating near-perfect predictions
XGBoost Model		Points lie almost perfectly on the diagonal, demonstrating near-perfect predictions

As shown in the comparative study between different AI models, the appropriate models to use for forward analysis and application are:

- **Feedforward Neural Networks (FNN);**
- **Multilayer Perceptron (MLP)**;
- **XGBoost**.

These models show the optimal metrics that could be used to well predict the risks' criticality.

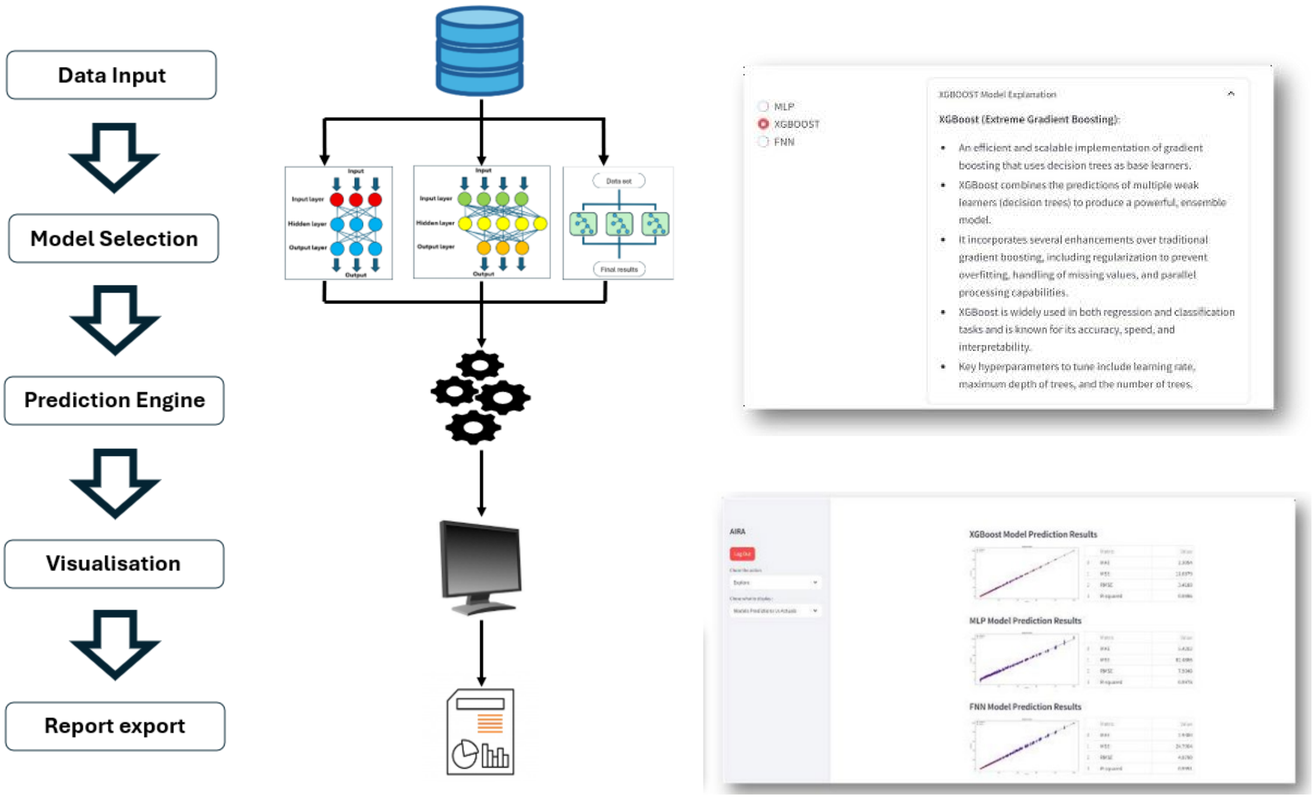
4.6 Discussion: Analytical and Managerial InsightsThe paper's findings have several important implications:

1. **Predictive Efficiency**: Ensemble AI models' superior accuracy highlights their potential as Decision Support System in risk analysis, particularly for data-driven auditing and process control prioritization.
2. **Operational Relevance**: The capacity to predict risk criticality automatically can reduce manual evaluation time by up to 60%, improving the effectiveness of ISO certification audits.
3. **Cost and Compliance**: By identifying high-risk process, equipment/machine proactively, AIRA application can help organizations optimize resource allocation, reduce audit nonconformities, and enhance audit readiness.
4. **Scalability for Moroccan Companies**: The approach addresses limitations of traditional, qualitative risk evaluation methods that are often subjective, inconsistent, and slow. AI models offer replicability, traceability, and integration with digital compliance management system.

However, the findings should be analyzed with caution. Despite the robust cross-validation and feature correction, dependency between data remains possible since all observations originated from limited industrial databases. Additional research should include cross-sectoral validation and real-time industrial testing to ensure external generalization (Pereira et Thomas 2020).

4.7 Enhanced Visualization and AIRA ArchitectureThe system operates as a web-based platform integrated with a local and confidential database.

Users can choose AI models (FNN, MLP or XGBoost), visualize predicted criticality results, and generate detailed reports for audit documented information.



XGBOOST Model Explanation

XGBoost (Extreme Gradient Boosting):

- An efficient and scalable implementation of gradient boosting that uses decision trees as base learners.
- XGBoost combines the predictions of multiple weak learners (decision trees) to produce a powerful, ensemble model.
- It incorporates several enhancements over traditional gradient boosting, including regularization to prevent overfitting, handling of missing values, and parallel processing capabilities.
- XGBoost is widely used in both regression and classification tasks and is known for its accuracy, speed, and interpretability.
- Key hyperparameters to tune include learning rate, maximum depth of trees, and the number of trees.

Fig.1: Architecture of AIRA

4.8 Summary of Key FindingsEnsemble models (especially XGBoost) provide the most accurate risk predictions.

- Neural models perform well but are less efficient with categorical risk data.
- The removal of target-defining variables corrected artificial accuracy and improved model credibility.
- The AIRA platform operationalizes ISO standards principles through data-driven risk prioritization.
- The approach enhances auditing effectiveness, reduces system management implementation costs, and supports digital transformation of risk management in Moroccan companies.

5. Discussion and Conclusions

This paper explored the use of Artificial Intelligence (AI) models to enhance risk analysis and Decision Support System within ISO management systems (Gueorguiev 2025). the paper has as a goal to ensure the criticality prediction value of risks as a basic component of risk assessment in accordance with ISO standards, by using historical database from processes and equipment/machines. The proposed approach replaces traditional, experience driven evaluations toward data informed, automated, and evidence based practices. Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and statistical risk evaluation often are impacted by subjectivity, limited scalability, and inconsistent documented information, but they remain imperative.

Artificial intelligence models can detect nonlinear interactions between multiple several factors, proposing a more dynamic understanding of risk management (Ajibose et al. 2025). As Shalev and Tiran emphasize, transparent and interpretable AI systems are key to ensuring that data-driven predictions remain auditable and trustworthy an essential requirement for industrial certification processes (Shalev et Tiran 2007).

Multi-Layer Perceptron (MLP), Feedforward Neural Network (FNN), Convolutional Neural Network (CNN), Support Vector Machine (SVM), Random Forest, and XGBoost, were evaluated using K-fold cross validation to avoid overfitting and ensure robustness. Mean Absolute Error (MAE), Mean Squared Error (MSE), Root Mean Squared Error (RMSE), and the Coefficient of Determination (R^2) were included as performance metrics.

Random Forest and XGBoost models' Results show outperformed neural models, owing to their capacity to manage heterogeneous, categorical data and to model nonlinear dependencies effectively. Neural architectures such as FNN and MLP can also give strong and powerful predictions, confirming their potential for more complex risk scenarios when sufficient data are available. The perfect R^2 values (egal to 1.0) observed for Random Forest needs cautious interpretation. These indicate potential data relationships or residual influence from deterministic dependencies within the dataset.

In future iterations, features directly defining the target variable (e.g., Severity, Occurrence, Impact) could be excluded to avoid data leakage and strengthen model validity. This refinement will ensure that predictive performance presents learned relationships rather than mathematical reconstruction.

Overall, the findings demonstrate the importance of choosing the appropriate model based on the specific needs of the task. The results highlight that when some models offer superior accuracy, others provide a balance between performance and computational efficiency. "However, machine learning requires large amounts of data to function properly. Therefore, it can be difficult to control the integrity of datasets, especially in the case of data generated by real-time monitoring systems" (Chakor et al. 2022).

Privacy and security of data are important for models to prevent attacks, are threatened by risks of leaks and model theft. Transparency, real-time supervision and ethical training emerge as vital factors for the responsible action of AI in cybersecurity (González et al. 2024). Rather, capabilities researchers should increasingly focus on the potential benefits from AI, and safety researchers should focus on minimizing any potential tail risks (Hendrycks et Mazeika 2022).

Additionally, robust security measures should be incorporated during the design and development phases, with regular updates to security protocols and vulnerability evaluations to protect against potential threats (Lusiani et Princes 2024).

Moving forward, these insights could lead to the application of AI techniques in similar contexts, with potential for more refinement and optimization to achieve even better results. "An important conclusion is that there is no specific genetic configuration for all data sets. Thus, it will depend on the characteristics of the domain analyzed. This is a reason why it is important to apply a sensitivity analysis, with the objective of selecting the best possible configuration according to the data sets analyzed" (Murillo-Morera et al. 2016).

These results offer meaningful implications for managerial and certification fields. AIRA application provides companies and auditors with the possibility to visualize predicted criticality scores, identify high risk processes, and generate automatic reports aligned with ISO standards and linked with a secure local database. AIRA application was developed as a web platform, under a clear operational flow: Data Input → Model Selection → Prediction Engine → Dashboard Visualization → Report Export.

For Moroccan companies, this application could help prioritize audit focus areas, reduce manual data handling, and support evidence-based Decision Support System. The application represents a step toward system digitalization in compliance management system although its implementation may face challenges related to databases quality, digital infrastructure, and specialized AI expertise.

The paper reinforces the relevance of AI models in professional risk management, advising that data-driven methods can support and enhance ISO-based continuous improvement frameworks. Practically, it demonstrates how AI models can ensure traceability in risk evaluation and contribute to smarter compliance management systems optimizing resource allocation during the system implantation.

In conclusion, FNN, MLP and XGBoost models emerged as the most accurate and stable models for risk criticality prediction, highlighting the potential of ensemble approaches for professional applications.

The study contributes to a practical digital tool and a reproducible framework that links AI technology with ISO standards. Future work should focus on:

1. integrating explainable AI (XAI) models to enhance method transparency and trust;
2. expanding testing to diverse further industrial sectors and real-world datasets; and
3. connecting AIRA application with IoT-based monitoring systems to enable real-time risk evaluation and dynamic certification support.

With these refinements, AI-driven risk evaluation can become an important enabler of smarter, more transparent, and sustainable management systems in Morocco and beyond.

Acknowledgements

This work is part of a project supported by the Hassan II Academy of Sciences and Techniques of Morocco.

References

Ajibose, Kayode, Tobias Adukpo, Seyram Adza, et Jacob Obeng. 2025. « AI-powered Predictive Risk Assessment Models for Preventing Workplace Accidents in the U.S. Mining Industry: Strengthening Safety under MSHA Regulation. » *EPRA International Journal of Environmental Economics, Commerce and Educational Management* 12 (octobre): 2348-814X. https://doi.org/10.36713/epra24263.

AlSheikh, Maha, et Amer Morshed. 2025. « Insurance Adequacy and Supply Chain Resilience: Risk Management Mediation and Complexity Moderation in UAE Firms ». *Journal of Logistics, Informatics and Service Science*, publication en ligne anticipée, septembre 18. https://doi.org/10.33168/JLISS.2025.0615.

Bari, Poonam, et Lata Ragha. 2024. « Machine Learning-Based Extrapolation of Crop Cultivation Cost ». *Inteligencia Artificial* 27 (74): 80-101. https://doi.org/10.4114/intartif.vol27iss74pp80-101.

Bouke, Mohamed Aly, Saleh Ali Zaid, et Azizol Abdullah. 2024. « Implications of Data Leakage in Machine Learning Preprocessing: A Multi-Domain Investigation ». Prépublication, Research Square, juillet 12. https://doi.org/10.21203/rs.3.rs-4579465/v1.

Chakor, Ahmed Yassine, Azmani Monir, et Azmani Abdellah. 2022. « Proposing a Layer to Integrate the Sub-classification of Monitoring Operations Based on AI and Big Data to Improve Efficiency of Information Technology Supervision ». *Appl. Comput. Syst.* 27 (1): 43-54. https://doi.org/10.2478/acss-2022-0005.

Council, National Research, Division on Earth and Life Studies, Board on Environmental Studies and Toxicology, Commission on Life Sciences, et Committee on Risk Assessment of Hazardous Air Pollutants. 1994. *Science and Judgment in Risk Assessment*. National Academies Press.

Deng, Houtao. 2013. « Guided Random Forest in the RRF Package ». arXiv:1306.0237. Prépublication, arXiv, novembre 18. https://doi.org/10.48550/arXiv.1306.0237.

Elmouden, Imane, et Bouchra Lotfi. 2022. « SUPPLY CHAIN RISK MANAGEMENT PROCESS: LITERATURE REVIEW ». *Journal of Operations Management, Optimization and Decision Support* 2 (2): 24-32. https://doi.org/10.34874/IMIST.PRSM/jomods-v2i2.35390.

Filz, Marc-André, Jonas Ernst Bernhard Langner, Christoph Herrmann, et Sebastian Thiede. 2021. « Data-driven failure mode and effect analysis (FMEA) to enhance maintenance planning ». *Computers in Industry* 129 (août): 103451. https://doi.org/10.1016/j.compind.2021.103451.

Givehchi, Saeed, et Alireza Heidari. 2018. « Bayes Networks and Fault Tree Analysis Application in Reliability Estimation (Case Study: Automatic Water Sprinkler System) ». *Environmental Energy and Economic Research* 2 (4): 325-41. https://doi.org/10.22097/eeer.2019.160566.1057.

Gómez, Juan Fco., Pablo Martínez-Galán Fernández, Antonio J. Guillén, et Adolfo Crespo Márquez. 2019. « Risk-Based Criticality for Network Utilities Asset Management ». *IEEE Transactions on Network and Service Management* 16 (2): 755-68. https://doi.org/10.1109/TNSM.2019.2903985.

González, Ariel López, Mailyn Moreno-Espino, Ariadna Claudia Moreno Román, Yahima Hadfeg Fernández, et Nayma Cepero Pérez. 2024. « Ethics in Artificial Intelligence: an Approach to Cybersecurity ». *INTELETICA* 1 (1): 38-54.

Gueorguiev, Tzvetelin. 2025. « An approach to integrate Artificial Intelligence in ISO 9001-based quality management systems ». *Measurement: Sensors* 38 (janvier): 101787. https://doi.org/10.1016/j.measen.2024.101787.

Hendrycks, Dan, et Mantas Mazeika. 2022. « X-Risk Analysis for AI Research ». arXiv:2206.05862. Prépublication, arXiv, septembre 20. https://doi.org/10.48550/arXiv.2206.05862.

Hesham, Merna, Gihan Hosny, Ehab Mahmoud, et Zekry Ghatas. 2025. « Developing an Integrated Model for Improving Occupational Health and Safety Performance in Some Industries Using Safety Standards ». *Discover Public Health* 22 (1): 338. https://doi.org/10.1186/s12982-025-00714-3.

International Standardization Organization. 2018. *ISO 31000:2018*. https://www.iso.org/standard/65694.html.

Ispas, Lucian, Costel Mironeasa, Traian-Lucian Severin, Delia-Aurora Cerlincă, et Silvia Mironeasa. 2025. « Artificial Intelligence Applications in Risk Management Within Integrated Management Systems: A Review ». *Systems* 13 (11): 967. https://doi.org/10.3390/systems13110967.

Jahin, Md Abrar, Saleh Akram Naife, Anik Kumar Saha, et M. F. Mridha. 2025. « AI in Supply Chain Risk Assessment: A Systematic Literature Review and Bibliometric Analysis ». arXiv:2401.10895. Prépublication, arXiv, février 27. https://doi.org/10.48550/arXiv.2401.10895.

Kahya, Ibrahim, Torsten Huschbeck, et Peter Markovič. 2025. « Predictive Risk Management in the Supply Chain ». In *Developments in Information and Knowledge Management Systems for Business Applications: Volume 8*, édité par Peter Štarchoň, Solomiia Fedushko, et Katarína Gubíniova. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-80935-4_3.

Kalogiannidis, Stavros, Dimitrios Kalfas, Olympia Papaevangelou, et al. 2024. « The Role of Artificial Intelligence Technology in Predictive Risk Assessment for Business Continuity: A Case Study of Greece ». *Risks* 12 (2). https://doi.org/10.3390/risks12020019.

Kandikatla, Laxmiraju, et Branislav Radeljic. 2025. « AI and Human Oversight: A Risk-Based Framework for Alignment ». arXiv:2510.09090. Prépublication, arXiv, octobre 10. https://doi.org/10.48550/arXiv.2510.09090.

Koessler, Leonie, et Jonas Schuett. 2023. « Risk assessment at AGI companies: A review of popular risk assessment techniques from other safety-critical industries ». arXiv:2307.08823. Prépublication, arXiv, juillet 19. https://doi.org/10.48550/arXiv.2307.08823.

Lusiani, Susi, et Elfindah Princes. 2024. « Evaluating the Effectiveness of Mobile JKN Application in Indonesia: A User-Centric Approach Using the ISO 25010 Quality Model ». *Journal of Logistics, Informatics and Service Science* 11 (10). https://doi.org/10.33168/JLISS.2024.1028.

Montavon, Grégoire, Wojciech Samek, et Klaus-Robert Müller. 2018. « Methods for interpreting and understanding deep neural networks ». *Digital Signal Processing* 73 (février): 1-15. https://doi.org/10.1016/j.dsp.2017.10.011.

Murillo-Morera, Juan, Carlos Castro-Herrera, Javier Arroyo, et Rubén Fuentes-Fernández. 2016. « An Automated Defect Prediction Framework using Genetic Algorithms: A Validation of Empirical Studies ». *Inteligencia Artificial* 19 (mai): 114-37. https://doi.org/10.4114/ia.v18i56.1159.

Pereira, Ana, et Carsten Thomas. 2020. « Challenges of Machine Learning Applied to Safety-Critical Cyber-Physical Systems ». *Machine Learning and Knowledge Extraction* 2 (novembre): 579-602. https://doi.org/10.3390/make2040031.

Pineau, Joelle, Philippe Vincent-Lamarre, Koustuv Sinha, et al. 2021. *Improving Reproducibility in Machine Learning Research (A Report from the NeurIPS 2019 Reproducibility Program)*. août 1.

Radanliev, Petar, David Roure, Jason Nurse, Rafael Montalvo, et Pete Burnap. 2019. « Cyber Risk at the Edge: Current and future trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains ». *SSRN Electronic Journal*, publication en ligne anticipée, janvier 1. https://doi.org/10.2139/ssrn.3346528.

Rodrigues, João Antunes, Alexandre Martins, Mateus Mendes, José Torres Farinha, Ricardo J. G. Mateus, et Antonio J. Marques Cardoso. 2022. « Automatic Risk Assessment for an Industrial Asset Using Unsupervised and Supervised Learning ». *Energies* 15 (24): 9387. https://doi.org/10.3390/en15249387.

Shalev, Dan M., et Joseph Tiran. 2007. « Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations ». *Reliability Engineering & System Safety*, Critical Infrastructures, vol. 92 (9): 1231-41. https://doi.org/10.1016/j.ress.2006.05.015.

Ulya, Athiyatul, Annisa Karima, T. Sukma Achriadi Sukiman, Anni Zulfia, et Rafika Rahmawati. 2025. *Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022 | Brilliance: Research of Artificial Intelligence*. octobre 10. https://jurnal.itscience.org/index.php/brilliance/article/view/6564?utm_source=chatgpt.com.

Wei, Ze, Hui Liu, Xuewen Tao, et al. 2023. « Insights into the Application of Machine Learning in Industrial Risk Assessment: A Bibliometric Mapping Analysis ». *2023*. https://www.mdpi.com/2071-1050/15/8/6965?utm_source=chatgpt.com.

Zhang, Yuhao, Kevin McAreavey, et Weiru Liu. 2022. « Developing and Experimenting on Approaches to Explainability in AI Systems »: *Proceedings of the 14th International Conference on Agents and Artificial Intelligence*, 518-27. https://doi.org/10.5220/0010900300003116.