ISSN: 2182-2069 / E-ISSN: 2182-2077

Data-driven Security Assessments for Predicting Information Security Maturity Levels

Alva Hendi Muhammad[1*], Hanafi[2], Kumara Ari Yuana[3], Bahrun Ghozali[4], and Ruby Haris[5]

[1*]Assistant Professor, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia. alva@amikom.ac.id, https://orcid.org/0000-0003-1970-3139

[2]Assistant Professor, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia. hanafi@amikom.ac.id, https://orcid.org/0000-0002-8592-7678

[3] Assistant Professor, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia. kumara@amikom.ac.id, https://orcid.org/0000-0003-4864-8693

[4]Lecturer, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia. oza@amikom.ac.id, https://orcid.org/0009-0000-3121-4229

[5]Master Student, Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia. ruby.haris@students.amikom.ac.id, https://orcid.org/0009-0002-7454-4118

Received: March 08, 2025; Revised: April 15, 2025; Accepted: May 14, 2025; Published: May 30, 2025

Abstract

This study investigates the use of machine learning to improve Information Security Risk Assessment (ISRA), with a particular emphasis on the KAMI framework, which is adapted from ISO 27001. It compares the performance of conventional machine learning algorithms, such as Logistic Regression, Random Forest, Decision Tree, and Support Vector Machine, with advanced boosting methods, including CatBoost, Gradient Boosting, LightGBM, and XGBoost. Findings reveal that boosting models outperform traditional classifiers, with CatBoost achieving the highest accuracy (98.45%) and balanced evaluation metrics, demonstrating strong capabilities in managing complex and imbalanced datasets. The integration of machine learning into the KAMI framework effectively addresses key cybersecurity challenges, including the analysis of unstructured data and the expansion of assessment coverage. This research highlights the practical benefits for organizations and technology providers by showing how ML-powered tools can streamline risk assessments, enhance strategic decision-making, and strengthen cybersecurity resilience. By aligning with global standards and utilizing AI, the study contributes to the advancement of efficient and scalable ISRA methodologies, paving the way for future innovation at the intersection of machine learning and cybersecurity.

Keywords: Information Security, Risk Assessment, Classification, Boosting Algorithms, KAMI Framework.

Journal of Interner Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 906-925.
DOI: *10.58346/JISIS.2025.I2.060*

*Corresponding author: Assistant Professor, School of Postgraduate, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia.

1 Introduction

In an increasingly digitalized global economy, organizations must prioritize their security posture to protect sensitive data and information (Admass et al., 2024; Saeed et al., 2023). Protecting data not only maintains client trust but also ensures that activities continue uninterrupted. Meanwhile, the cybersecurity threats continue to evolve in both complexity and scale. This condition sometimes makes it difficult for businesses to avoid possible threats. Thus, companies must adopt robust security measures to defend against these advanced threats (Gourisetti et al., 2020; Magesa & Mshana, 2023). Establishing a suitable Information Security Management System (ISMS) can assist organizations in protecting their assets. This approach enables them to identify vulnerabilities in their diverse systems (Bettaieb et al., 2020; Schmitz et al., 2021). An effective information security management policy can assist staff in preventing cyber threats (Armenia et al., 2021; Muhammad et al., 2023). ISMS encompasses the critical function of security assessment that enables organizations to identify risks and accurately ensure their effective management (AL-Dosari & Fetais, 2023; Wangen et al., 2018). Through systematic assessments, organizations can determine whether their risk mitigation measures are functioning as intended.

Furthermore, traditional security assessments enable the identification of gaps in policy enforcement and the detection of security controls that may be obsolete or no longer effective. Security assessments offer a new way to evaluate the current condition of organizational security. These assessments also create important opportunities for continuous improvement. Security assessments support organizations in adapting their security measures over time (Aliyu et al., 2020; Wangen et al., 2018). Organizations can improve their security practices by carrying out assessments regularly. Regular assessments help organizations to remain flexible and responsive to new cyber threats (Deshmukh & Menon 2025). In practice, security assessments often rely on manual evaluation methods, which depend on the subjective judgment of experts. However, this approach may lead to inconsistencies in the results. Different outcomes may occur because each expert may have a different perspective. The diverse expertise levels can also affect the assessment results (Wangen et al., 2018). Moreover, this approach is time-consuming, costly, and counterproductive regarding security controls (Cheimonidis & Rantos, 2023).

On the contrary, the development of Artificial intelligence (AI) and machine learning (ML) for security assessments has been in the advanced stage. AI and ML are able to analyse complex datasets and discover patterns that are difficult to obtain through traditional methods (Asadov 2018; Raimundo & Rosário, 2021). AI can also deliver straightforward recommendations for future security actions by evaluating activities and the relationships of existing security controls (Schmitz & Pape, 2020; Mehra & Iyer 2021). Machine learning can also improve organizational risk management by employing data from security evaluations (Cremer & Strbac, 2021; Clavijo-López et al., 2024). Among others, ensemble learning are more reliable than single model for classification tasks (Konstantinov & Utkin, 2021; Shaukat et al., 2020; Sunarto et al., 2023; Zahedifard et al., 2015). Ensemble ML models allow organizations to predict security plans with lower bias. For instance, (Bettaieb et al., 2020) proposed automated decision-making assistance to determine security controls for a system in a specific context. This is achieved by sifting through many security controls and deciding which ones have impacted the security requirements of the given system. Ensemble meta-classifier techniques can also enhance the accuracy of vulnerability assessments by harmonizing different vulnerability reports and security indicators (Jiang & Atif, 2021). However, the lack of universal ML solutions for measuring information security maturity levels makes choosing an appropriate model challenging. An improper ML technique could introduce significant security risks and impede sound decision-making.

This study tackles the difficulty of selecting an effective machine learning model capable of accurately estimating and predicting organizations' security maturity levels. While machine learning applications in cybersecurity risk assessment are increasingly common, our research uniquely contributes by explicitly integrating advanced boosting algorithms (particularly CatBoost and LightGBM) with the nationally adopted KAMI framework. To our knowledge, prior studies have not comprehensively evaluated such algorithms within the structured context of national cybersecurity standards, mainly focusing on the Indonesian governmental context, thereby addressing a critical gap in both methodological rigor and practical applicability. To bridge this gap, this study adopted data-driven analysis in cybersecurity, which is the process of making security decisions for an organization based on real-world data (Alqurashi & Ahmad, 2024; Schneeberger & Lemaître, 2023).). It entails gathering and processing data to detect, assess, and mitigate risks and threats. Data-driven cybersecurity can help organizations create a proactive strategy to protect their data and applications (Johora et al., 2024).

We introduce a dataset by collecting data from the target population using a generated questionnaire to achieve the research's goal. The questionnaire is designed from an information security assessment framework named KAMI Index, a nationally recognized security maturity index in Indonesia (Badan Siber dan Sandi Negara, 2024). The KAMI index has been used as a comprehensive tool for assessing the organization's security maturity level, especially in government agencies of Indonesia. This framework encompasses a wide range of attributes, capturing both qualitative and quantitative aspects of organizational security practices. This study is the first to translate the qualitative assessments of the KAMI framework into structured numerical features. Hence, the structured dataset was developed and pre-processed to discover how the defining factors contribute to the target variable.

Despite the proliferation of ML applications in cybersecurity, no prior study has attempted to operationalize and model the KAMI framework. This presents a critical gap, as KAMI remains widely used by Indonesian institutions but lacks automated, predictive tools to support decision-making. We explore how boosting algorithms such as Gradient Boosting, Adaptive Boosting, Categorical Boosting, Extreme Gradient Boosting (XGBoost), and LightGBM can effectively classify and predict an organization's security maturity level based on KAMI-based inputs. We also investigate the relative performance of these models, providing a comparative evaluation to determine the most suitable technique for this domain. Thus, our study aims to offer the following list of contributions:

1. Develop comprehensive questionnaires and systematically gather data in a manner that supports rigorous data-driven analysis, thereby generating meaningful and actionable insights. This approach ensures that the collected information is both relevant and conducive to uncovering significant patterns and trends.
2. Conduct thorough experimental analyses using actual datasets, thereby demonstrating and validating the proposed model's performance, reliability, and applicability in practical scenarios. This ensures that the model's effectiveness is proven in real-world conditions, enhancing its credibility and utility.
3. Propose a boosting ensemble learning model for prediction that fully exploits the strengths of multiple machine learning algorithms, including Gradient Boosting, Categorical Boosting, Adaptive Boosting, Extreme Gradient Boosting, and LightGBM. This integrative approach aims to improve prediction accuracy and model robustness by combining the diverse capabilities of each algorithm.

This work is organized in the following flow: Section 2 discusses relevant studies. Section 3 thoroughly explains the research methodology and defines the workflow by breaking it into separate modules. Section 4 provides an in-depth performance analysis, proves the study's effectiveness, and displays the experimental results. Section 5 discusses the findings and implications. Section 6 concludes the paper.

2 Literature Review

Information security issues have evolved from a technical perspective to a systemic approach, involving policies, processes, people, and controls. ISMS helps organizations protect their information assets holistically, based on the principles of Confidentiality, Integrity, and Availability (CIA), and ensure that information is not disclosed or made available unless authorized (Makhija, 2021). According to ISO/IEC 27001, ISMS consists of a set of policies, procedures, and controls aimed at detecting, managing, and reducing information security risks (Junaid, 2023). ISO 27001 outlines the requirements for planning, implementing, operating, and continuously improving an ISMS (Haufe et al., 2016). Among various security frameworks, such as NIST CSF, COBIT, and PCI DSS, ISO 27001 is one of the most widely adopted standards (Alrehili & Alhazmi, 2024). As shown in Figure 1, ISO 27001/2's position in the upper-right quadrant signifies its role as a robust and adaptable framework, providing comprehensive guidelines for information security management (Forge, 2024).

Integrating ISO 27001 with other standards can enhance system effectiveness and streamline implementation processes. (Barafort et al., 2019) propose a process reference and assessment model that integrates ISO 33004's risk management with ISO 27001. This strategy may enhance risk management while facilitating ongoing improvements regarding quality, project management, IT services, and also information security. Similarly, (Al Faruq et al., 2020) illustrate that integrating Information Security Management Systems (ISMS) with the IT service management framework ITIL v3 can decrease costs by optimizing deployment and harmonizing procedural processes. By establishing an ISMS customized to its own context, a business can formulate a resilient security framework that complies with ISO 27001 criteria while improving additional security operations.

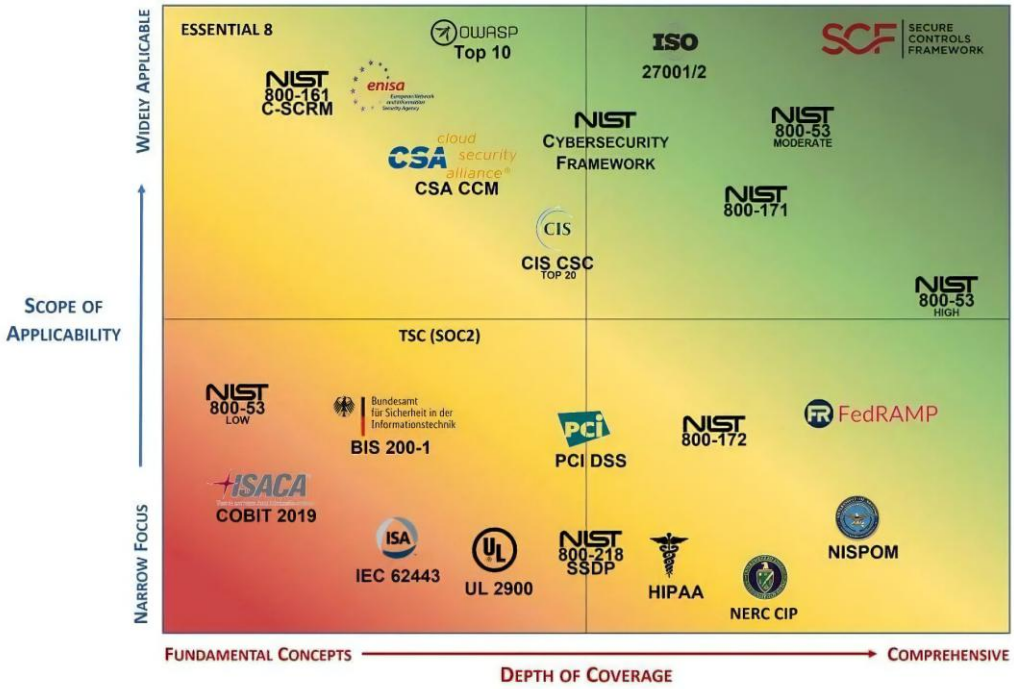

Figure 1: Cybersecurity Framework Heatmap (Forge, 2024)

For ISMS, a compliance model based on value is mandatory. It often includes user engagement and input during the design and deployment of security controls (Makhija, 2021). ISMS includes risk assessments, security audits, and continuous monitoring (Alrehili & Alhazmi, 2024). Risk assessments

is critical to determine potential risks and exposures that can compromise information assets. By detecting risk earlier, organizations can allocate time to evaluate the likelihood and also the impact of various security incidents and prioritize their security efforts effectively (Rosado et al., 2024; Szczepaniuk et al., 2020). Security audits, both internal and external, serve to prove the implementation and effectiveness of security controls. This will also ensure the alignment between established policies and standards (Bozkus Kahyaoglu & Caliyurt, 2018; Steinbart et al., 2018). In the end, continuous monitoring allows real-time insights into the security environment so that organizations can maintain the detection and response to emerging threats (Culot et al., 2021; Makhija, 2021). Through these ISMS practices, the organization can consistently improve its security posture, promoting a proactive risk management culture within the organization.

Even if adopting ISMS allows organizations to assess and strengthen their ability to protect their critical assets over time, organizations must establish a method to measure their current security posture. Thus, some standards provide a systematic way to evaluate the current state of security practices while allowing organizations to grow. For example, The Capability Maturity Model Integration (CMMI) has a level where organizations could incrementally improve their operations and security-related capabilities (Paulk et al., 2021). Similarly, the Information Security Maturity Model (ISMM) allows explicit measurement of information security operations (including aspects of governance, risk, and compliance). It also assesses the effectiveness and efficiency in critical areas, including governance and response (Pfleeger & Pfleeger, 2022). As demonstrated by Alharkan and Ibraheem (2023), maturity models enhance security outcomes by providing benchmarks and executable steps for organizations.

The ISMS have also been influenced by the rapidly expanding domain of data analytics and machine learning. The research conducted by Zhang et al. (2022) demonstrates how technologies, such as machine learning, produce more precise and adaptable security maturity evaluations. Nonetheless, certain limits persist despite these developments. For example, the model and condition are contingent upon the industry, complicating the assessment of security postures, especially on qualitative variables (Smith & Doe, 2021). Consequently, despite these drawbacks, there remains a necessity for ongoing research to address these while developing the fields of AI and machine learning in response to the shifting threat landscape.

These insights demonstrate the relationship between security assessments and maturity models within a developed ISMS. Security assessment provides data that maturity models can utilize to assess an organization's performance and identify areas for improvement. Meanwhile, maturity models serve as a strategic roadmap, guiding enterprises in enhancing security assessment processes. The dynamic interaction guarantees that security operations stay agile while enabling enterprises to maintain a robust defence in a shifting environment (Johnson & Lee, 2022). In conclusion, organizations should apply a holistic approach to information security through a combination of an assessment approach and a maturity model approach.

3 Research Methodology

The research methodology and the structured workflow are illustrated in Figure 2. The data-driven methodology, as illustrated in Figure 2, shows that our data-driven analysis adopts an ensemble learning framework. It consists of two main stages: Data Collection and Ensemble learning. In the Data Collection phase, the reliability of the questionnaires was tested by constructing and validating the instrument based on expert judgment. Then, the pre-processing phase enables raw data to enhance its quality prior to the application of Ensemble Learning. The feature selection is then used to find out the

most important attributes. The dataset is then split between training and testing for model training and testing. The next step is hyperparameter optimization to maximize the performance of the models, and the training data is fed into an ensemble engine. We then test the integrated ensemble model on the remaining test data to evaluate the performance. The results are then analysed to highlight the remaining possibilities for improvement of the predictive output.

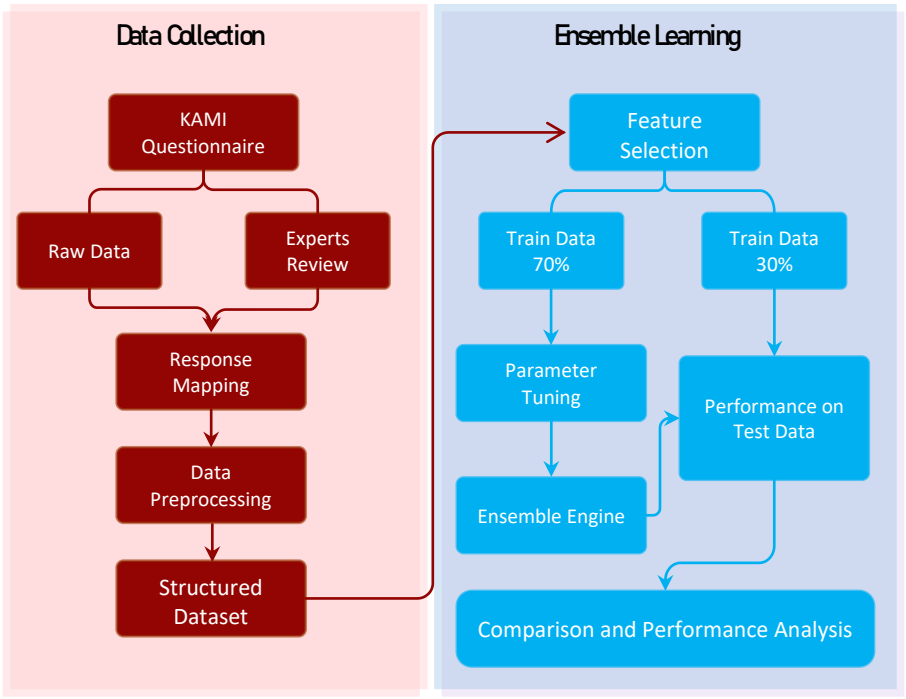

Figure 2: Overall research methodology

Transformation of the KAMI Framework into a Structured Dataset

The integration of the KAMI framework with machine learning involves transforming qualitative responses from questionnaires into quantitative input features suitable for predictive models. At the outset, we collaborated with domain experts in cybersecurity and governance to design a customized questionnaire aligned with the KAMI version 5, developed by Indonesia's National Cyber and Crypto Agency (Muhammad et al., 2025). Their expertise was instrumental in ensuring the validity and contextual relevance of the questions across organizational types and sectors. The KAMI Index is designed to assess the maturity of information security practices within organizations. It evaluates six primary domains: Information Security Governance, Risk Management, Information Security Framework, Asset Management, Technology and Security Operations, and Personal Data Protection, with an optional seventh domain called Supplement. Each domain is assessed across five maturity levels, from Level I (Initial) to Level V (Optimizing), based on criteria that capture the implementation, consistency, and effectiveness of security controls. The primary domain and its definition are included in Table 1, together with the components of the domain and the total number of questions applicable to each domain.

Table 1: The domain of the KAMI framework

Domain	Domain Description	Subdomains/Components	#Questions
1. Governance	Provides overall direction, leadership, and oversight for	1.1. Structure & Responsibilities	22
		1.2. Competence & Capacity	

	information security across the organization.	1.3. Integration & Coordination	
		1.4. Strategic Decision-Making	
		1.5. Compliance & Performance Monitoring	
		1.6. Legal Compliance & Incident Handling	
2.Risk Management	Focuses on identifying, assessing, and mitigating risks associated with information security in a structured and documented manner.	1.7. Risk Management Program & Framework	16
		1.8. Roles & Responsibilities	
		1.9. Risk Assessment & Identification	
		1.10.Risk Treatment & Mitigation	
		1.11.Monitoring & Evaluation	
		1.12.Strategic Integration	
3.Security Framework	Involves the development, implementation, and management of information security policies, procedures, and technical controls to protect IT assets.	1.13.Policy and Documentation Management	32
		1.14.Incident & Exception Handling	
		1.15.Technical Operations & Project Security	
		1.16.Threat Intelligence & Response	
		1.17.Business Continuity & Disaster Recovery	
		1.18.Security Strategy & Program Management	
4.Asset Management	Covers the comprehensive management of IT assets including inventory, classification, configuration, backup, and both physical and cloud security controls.	1.19.Asset Inventory & Classification	53
		1.20.Configuration & Change Management	
		1.21.Policy & User Conduct Controls	
		1.22.Incident & Backup Management	
		1.23.Physical Security Management	
		1.24.Cloud Security & Data Privacy Controls	
5. Technology & Information Security	Focuses on technical measures and controls to protect networks, systems, applications, and data from cyber threats.	1.25.Network & Infrastructure Security	35
		1.26.Configuration & System Management	
		1.27.Logging & Monitoring	
		1.28.Encryption & Key Management	
		1.29.Access & Authentication Controls	
		1.30.Malware & Endpoint Security	
		1.31.Secure Development & SDLC	
6. Personal Data Protection	Focuses on ensuring that personal data is managed and protected in compliance with	1.32.Data Identification & Documentation	16
		1.33.Data Flow Mapping & Process Documentation	

	legal requirements, while maintaining data subject rights.	1.34.Policy & Governance	
		1.35.Risk Assessment & Mitigation	
		1.36.Data Subject Rights & Consent	
		1.37.Data Lifecycle Management	

The questionnaire applies a structured scoring scheme using four standardized responses: Not Implemented, In Planning, Partially Implemented, and Fully Implemented. Each response is assigned a numerical score that varies by domain and level to reflect the domain's criticality and contribution to overall security maturity. The most common encoding schemes used are (0, 1, 2, 3), (0, 2, 4, 6), or (0, 3, 6, 9), depending on the domain weight and intended granularity. This transformation enables the conversion of qualitative judgments into quantifiable variables suitable for machine learning input. Each question, once encoded, becomes an independent feature in a structured dataset. These datasets serve as the foundation for training classification models, such as those based on ensemble learning algorithms. Figure 3 illustrates the transformation from expert-validated questionnaire formulation and response scoring to dataset structuring.

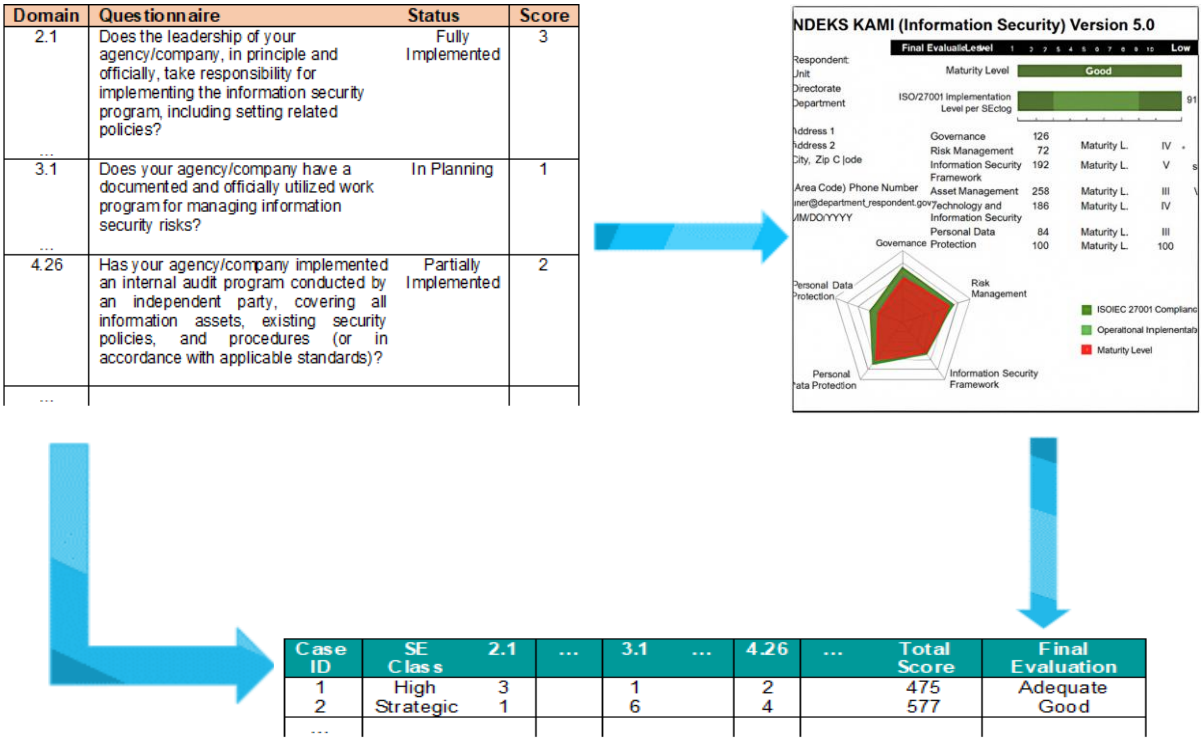

Figure 3: Transforming questionnaire into dataset

The dataset contains attributes that represent various questions, while the responses to these questions serve as the primary data values or records within the dataset. Data has been collected individually from organizations that are required to participate in annual security audits and stored in these datasets. Due to an insufficient amount of data, we combined the original dataset with generated data. The final dataset includes 190 distinct features. The first two features indicate the level of an organization's dependence on electronic systems. The remaining 174 features are based on different questions from six domains, with the last 13 features representing the values and levels associated with each domain. The final column of the dataset is the output column, which reflects the overall security posture based on

organizational responses. This output can be classified as Not Adequate, Basic Framework Fulfilment, Adequate, or Good. These outputs are interpretable and actionable, enabling decision-makers to identify weak domains and prioritize resource allocation and intervention strategies based on predicted maturity gaps.

Data Collection and Preprocessing

The correlation between security assessments and maturity models is fundamental to a successful ISMS. Security evaluations provide the information necessary to guide maturity models, allowing organizations to identify areas for enhancement. In turn, maturity models offer a structured framework to assist organizations in strategically improving their security practices based on evaluation outcomes. This dynamic interaction ensures that security assessments remain focused while adaptable. The main reasons for questionnaire development were confirming and evaluating several security assessment factors. The questionnaire was designed to gather data on the main security maturity models as recognized by the Indonesian government agency.

Our study developed a customized questionnaire after reviewing key security assessment factors and maturity model indicators, particularly those adopted by Indonesian government agencies. The questionnaire was designed to capture organizational practices across multiple information security domains. Since no publicly available dataset existed to support this purpose, we constructed a private dataset specifically for this study. The initial data collection involved several respondents and was conducted through three main channels: extracting public records from government assessments, directly collecting data from private institutions, and distributing the questionnaire through an online form to reach additional participants. These responses were used to construct the foundation of our dataset.

Because we have a limited number of original samples, some of the samples were artificially produced to increase the quantity of samples. The generation was undertaken by randomly creating a new set of literals according to previously generated patterns and placed within the initial responses. This was done to control the size of the data structure while trying to obtain acceptable coverage of the describable attributes across the dataset. The result is a dataset comprising 5,167 instances with four class labels, which are: Adequate (3,477 instances), Basic Framework Fulfilment (972 instances), Not Adequate (598 instances), and Good (121 instances). Because of this imbalance, we accordingly applied a Random Undersampling on the preprocessing step to reduce the bias of the majority class and provide a balance in the training of our machine-learning models. The method achieved a more unbiased learning performance and a reduced classification bias while preserving the patterns extracted from the raw data (Yang et al., 2024). The final dataset contains 190 variables, including one target column and 189 entities. Each of the questionnaires was converted into an attribute by identifying the implementation level for several security controls through responses in numbers (e.g., ‘1’, ‘2’, ‘3’, ‘4’, ‘6’ and ‘9’). Additional columns were calculated that represented the maturity level for each security dimension; in turn, the resulting “Final Results” classification field indicated the security maturity level of one’s organization. The final dataset is private for institutional reasons at the time of this research. It will be publicly available post-publication to allow reproducibility and further research on ISRA using machine learning.

Ensemble Boosting Classifiers

This paper presents a comprehensive analysis of information security maturity prediction by considering them with traditional classifiers and advanced ensemble methods. We compared the performance with

Logistic Regression (LR), support vector machine (SVM), decision tree (DT), and random forest (RF) as the classical models for comparison. LR and SVM were selected because they are straightforward algorithms and suitable candidates for building classification baselines. DT and RF were chosen due to their ability to interpret and handle high-dimensional security data whilst maintaining the interpretability for complex multivariate problems (Prova, N. N. I, 2025).

Additionally, we showed that applying advanced boosting techniques can be advantageous. The advanced ensemble boosting algorithms were chosen specifically because of their superior performance on datasets with properties such as high dimensionality, categorical features, and class imbalance, as referred in (Khan, 2024). These conditions are frequently encountered in security risk assessments. Boosting classifiers are ensemble techniques that combine weak learners to create a strong predictive model. The core premise of boosting is to iteratively train each successive model to emphasize the cases where prior models were misclassified, hence gradually improving overall accuracy. Unlike the bagging ensemble method, which trains many models in parallel and aggregates their predictions, boosting concentrates on difficult-to-predict examples to reduce bias and variance. Consequently, this adaptive technique allows boosting algorithms to perform better on complex datasets. Boosting classifiers are primarily valuable for applications where high predicted accuracy and the capacity to handle complex patterns are required. Moreover, separating the dataset into training and testing subsets is essential before using machine learning classifiers. The dataset used in this study is divided into training and evaluation portions in a 70:30 ratio. To train the data, we utilized four different boosting algorithms: Gradient Boosting (GB), Category Boosting (CatBoost), Adaptive Boosting (ADA), Extreme Gradient Boosting (XGB), and LightGBM.

- **Gradient Boosting** builds models iteratively by addressing the residual errors of previous models. At its core, GB trains weak learners, such as decision trees, on the negative gradients of the loss function to refine predictions with each iteration (Friedman, 2001). It starts with an initial prediction, often the mean for regression tasks, and sequentially updates the model by adding scaled predictions from weak learners. The formula for Gradient Boosting includes initializing the model (Eq. 1) by minimizing the loss, as shown in Eq. (1):

$$F_0(x) = arg\,min_\theta \sum_{i=1}^{n} L(y_i, \theta) \quad \text{Eq. 1}$$

and updating it iteratively using Eq. (2):

$$F_m(x) = F_{m-1}(x) + \gamma_m h_{m(x)} \quad \text{Eq. 2}$$

where $h_m(x)$ represents the weak learner and γ_m the learning rate.

- **Category Boosting** is a gradient boosting algorithm tailored for categorical data. Unlike other boosting models, it processes categorical variables natively, reducing the need for extensive preprocessing such as one-hot encoding. Its use of ordered boosting mitigates overfitting by avoiding data leakage and incorporates oblivious decision trees for efficient computation (Prokhorenkova et al., 2018). This makes CatBoost particularly effective for datasets with a high proportion of categorical features, as its optimization techniques ensure robust generalization. CatBoost optimizes a loss function $L(y,y^)$ with regularization terms, focusing on categorical variable processing, as shown in Eq. (3):

$$\hat{y} = \sum_{m=1}^{M} \gamma_m h_m(x) \quad \text{Eq. 3}$$

where $h_m(x)$ incorporates transformations of categorical variables.

- **Adaptive Boosting**, focuses on improving the performance of weak classifiers, such as decision stumps, by emphasizing misclassified instances. It assigns weights to data points, increasing the

weights for those misclassified and decreasing them for correctly classified points, iteratively refining the overall model (Hastie et al., n.d.). The error of a weak learner is given in Eq. (4):

$$\in_m = \frac{\sum_{i=1}^{n} \omega_i . 1(y_i \neq h_m(x_i))}{\sum_{i-1}^{n} \omega_i} \quad \text{Eq. 4}$$

and the combined model assigns more influence to better-performing learners using a weight, as shown in Eq. (5):

$$\alpha_m = \frac{1}{2} \ln\left(\frac{1-\epsilon_m}{\epsilon_m}\right) \quad \text{Eq. 5}$$

- **XGBoost** is an advanced implementation of gradient boosting that emphasizes speed, scalability, and accuracy. It incorporates second-order derivatives in its objective function for precise optimization and includes regularization terms such as L1 and L2 penalties to prevent overfitting (Chen & Guestrin, 2016). The objective function is formulated in Eq. (6):

$$\mathcal{L} = \sum_{i-1}^{n} L(y_i, \hat{y}_i) + \sum_{k-1}^{k} \Omega(h_k) \quad \text{Eq. 6}$$

with the regularization term defined in Eq. (7):

$$\Omega(h_k) = \frac{1}{2} \lambda \|\omega_k\|^2 + \|\omega_k\| \quad \text{Eq. 7}$$

represents the regularization that ensures both accuracy and model simplicity. XGBoost's parallelized training and robust regularization make it suitable for large-scale datasets and complex tasks.

- **LightGBM** is another gradient boosting framework that prioritizes computational efficiency and scalability. It introduces histogram-based learning, which reduces the computational complexity of finding split points, and uses a leaf-wise tree growth strategy that improves model accuracy (Ke et al., 2017). LightGBM optimizes a similar objective function to XGBoost, as shown again in Eq. (6), but leverages a histogram-based approximation. The approach reduces the complexity of calculating splits. This approach is particularly advantageous for large datasets with high dimensionality, as it enables faster training and better optimization compared to level-wise tree growth.

4 Experiments and Evaluation

This section presents our experimental approach. We begin by examining the fundamental machine learning models before progressing to an assessment of performance enhancement through boosting techniques.

Machine Learning Models

As mentioned above, we conducted initial experiments with four classifiers (LR, SVM, DT, and RF) to specify a performance baseline that is critical for model selection. Table 2 shows their comparative performance across accuracy, precision, recall, and F1-score. Notably, Logistic Regression delivered balanced results with 88.7% accuracy and 88.6% F1-score. However, its linear assumptions constrain nonlinear pattern recognition. As illustrated in Figure 4, it is positioned as a practical choice when model transparency outranks marginal accuracy gains. The model's slight drop in performance is due to its linearity. However, its low processing overhead and ease of interpretation make it the best method for situations where explainability is more important than small accuracy gains.

Further results on Random Forest (Table 2) reveal an accuracy of 93.3% and an F1 score of 92.5%. Compared to Linear Regression, this improvement highlights the effectiveness of Random Forest when

handling complex and high-dimensional data. The slight difference between precision (91.8%) and recall (93.3%) suggests it can capture all positive instances. This is useful for the risk assessment domain, where missing critical cases can have severe consequences. Furthermore, the Decision Tree demonstrates the highest accuracy with 95.5% and 95.4% in the F1 score. Among all models, the classification results of the Decision Tree reflect its ability to classify instances accurately. While DT excels in interpretability and feature importance analysis, this performance might have overfitting.

Table 2: Comparison results of models

Algorithm	**Accuracy**	**Precision**	**Recall**	**F1 Score**
Logistic Regression	0.8872	0.8852	0.8872	0.8859
Random Forest	0.9329	0.9179	0.9329	0.9250
Decision Tree	0.9549	0.9539	0.9549	0.9543
SVM	0.8801	0.8638	0.8801	0.8692

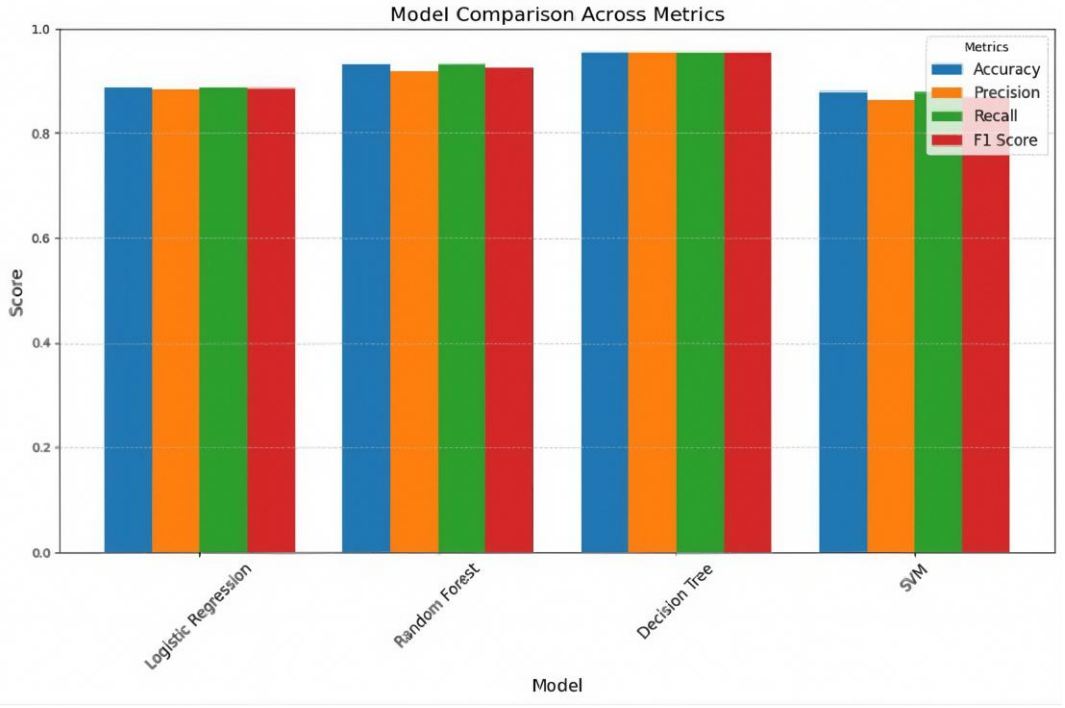

Figure 4: Performance evaluation results

Regression, with an accuracy of 88.0% and an F1 score of 86.9%. However, it lags behind Random Forest and Decision Tree. SVM is practical in datasets with distinctive decision boundaries because it can generate an optimal boundary. However, its relatively lower precision (86.4% vs. recall 88.0%) suggests that it is more prone to false positives. Although SVM is not the best-performing model in this study, its strong theoretical foundation will still be relevant in some fields, especially for smaller datasets or well-defined classes.

Despite its strengths, the findings of the assessment have limitations. The performance metrics are, first and foremost, dependent on the behavior of models on the sample of data used, which may not generalize across all situations or tasks. The dataset is highly variable with respect to complexity, feature distribution, class imbalance, noise, and so on, and caters wildly varying from one to the next. We study to alleviate this limitation by adding the boosting models for comparison.

Performance Evaluation Using Boosting Models

Figure 5 illustrates how the boosting models offer a good intuition into their benefits in classification tasks. The boosting model gradually increases the performance of weak learners, tuning predictions by emphasizing instances that have been wrongly predicted. They are, therefore, particularly applicable to intricate and large datasets. The metrics investigated here, i.e., accuracy, precision, recall, and F1 score of each model, theoretically and practically explain the relative strengths and weaknesses of the models.

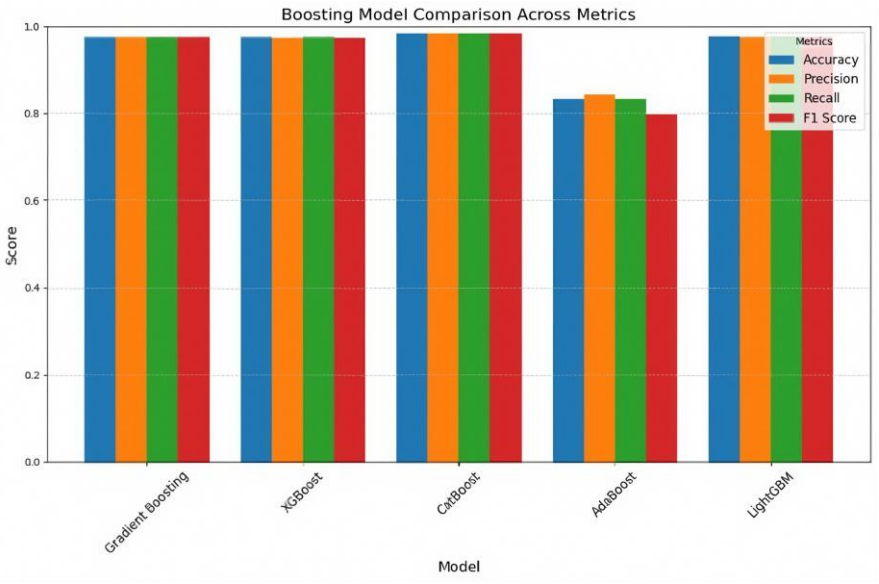

Figure 5: Performance Evaluation of Boosting Algorithms

According to Table 3, CatBoost takes the lead on metrics, surpassing the other models with 98.45% accuracy, 98.44% precision, 98.45% recall, and 98.44% F1 score. These results are as expected since CatBoost can deal with categorical features directly, which means it can reduce the feature engineering process. Also, due to its powerful regularizations and superior gradient optimization, it provides good generalization. This robustness makes CatBoost particularly useful in areas such as cyber security and risk modeling that are characterized by categorical data and imbalanced datasets. At the same time, the Gradient Boosting and LightGBM also reached high accuracy, achieving 97.55% and 97.68%, respectively. In addition, despite the strong capability of Gradient Boosting in iterative refinement, the histogram-based approach by LightGBM contributes to an improvement in computation efficiency, which is well-suited for large-scale datasets. They both have comparable precision, recall, and F1 scores, which are all fairly balanced, and the results are sufficiently reliable to be deployed in real applications. Due to its marginally better accuracy and speed, LightGBM can be used for machine learning techniques in real-time applications.

Table 3: Comparison Results of Boosting Models

Algorithm	Accuracy	Precision	Recall	F1 Score
Gradient Boosting	0.9755	0.9750	0.9755	0.9751
XGBoost	0.9749	0.9738	0.9749	0.9736
CatBoost	0.9845	0.9844	0.9845	0.9844
AdaBoost	0.8337	0.8438	0.8337	0.7977
LightGBM	0.9768	0.9761	0.9768	0.9759

XGBoost, a popular boosting algorithm, also achieved slightly lower accuracy, 97.48%, compared to Gradient Boosting and LightGBM. Nevertheless, the performance is still significantly competitive as the balanced metrics indicate good prediction capability. The parallelizable learning and the strongly regularizing parameters in XGBoost, like the L1 and L2 penalties, make it resilient. However, there may be more computation and tuning involved than LightGBM, making it slightly less efficient in resource-restricted scenes.

On the other hand, the lowest value was obtained by AdaBoost, with an accuracy of 83.37% and an F1 score of 79.77%. These results demonstrate the difficulty of learning in the presence of noise for AdaBoost. Although AdaBoost is favoured due to its simplicity and interpretability for simple tasks, its dependence on weak classifiers might limit its ability to learn complex data spatiotemporal patterns. Thus, AdaBoost is not ideal for high-dimensional or imbalanced data sets.

In cyber security, false positives (FP) and false negatives (FN) have a serious operational impact. A high FP rate could cause resources to unnecessarily be expended on security controls, leading to alert fatigue and inefficiencies. On the other hand, FN cases (i.e., unable to find a security-threat posture) may leave potential serious vulnerabilities not remediated and become a serious threat. Our fine-tuning of boosting models found that CatBoost had relatively low FP and FN rates, which corresponded to its balanced precision (98.44%) and recall (98.45%). Compared to traditional methods such as Logistic Regression or SVM, DNN, like those applied in this paper, yielded much lower false positive rates, which means there was less risk of underestimating the adequate security, thus reducing the possibility of wasting resources.

5 Discussions

Main findings and contributions

As Figure 4 and Tabl 2 illustrate, the comparison of classification algorithms indicates performance differences between Logistic Regression, Random Forest, Decision Tree, and Support Vector Machine. Logistic Regression has stable performances (accuracy: 88.7%, F1 score: 88.6%), which is a reasonable value for linear data, but cannot represent non-linear relations. Although it is less powerful than some of the other models, its simplicity and interpretability make it useful in cases where an economical use of computer power is preferred. SVM was comparable with Logistic Regression (accuracy: 88.0%) but inferior to ensemble models because of false positive sensitivity. This illustrates the pragmatic implication that SVM might not be well suited when type I errors have actual consequences in terms of resources or actions.

The results demonstrate that Random Forest and Decision Tree outperformed Logistic Regression, where Random Forest and Decision Tree obtained accuracy rates of 93.3% and 95.5%, respectively. Its ensemble nature prevents overfitting and allows for good generalization, i.e. valuable in complex, high-dimensional datasets. However, Decision Tree's susceptibility to overfitting may limit its generalizability without appropriate techniques like pruning. In cybersecurity risk assessment contexts, precision and recall trade-offs become highly relevant. For example, a model with high precision but low recall may miss identifying critical vulnerabilities (false negatives), while one with high recall but low precision may generate too many false alarms (false positives). The F1 score provides a harmonic balance between these extremes and is thus a more informative metric when dealing with imbalanced or high-stakes classification tasks.

Boosting algorithms, evaluated in Figure 5 and Table 3, significantly enhance classification performance. CatBoost emerged as the top-performing model, achieving an accuracy of 98.45% and near-perfect precision, recall, and F1 scores. Its ability to natively handle categorical data and minimize pre-processing requirements highlights its efficiency for domains like cybersecurity, where such data structures are common. High precision in CatBoost ensures that when a potential security weakness is flagged, it is highly likely to be a real issue, while high recall guarantees that most actual weaknesses are detected. This balance is critical in ISRA contexts, where both missed detections and false alarms can carry significant consequences. Gradient Boosting and LightGBM were similarly very competitive (with accuracies of 97.55% and 97.68%, respectively), but LightGBM was significantly more computationally efficient given its histogram-based learning. As can be seen from the figures, both models achieve a good balance of metrics and can be practically used on a large scale. Although slightly inferior to LightGBM and Gradient Boosting (accuracy: 97.48%), XGBoost showed competitive performance, highlighting its strong regularisation and parallel learning advantages. These results demonstrate that the boosting models not only achieve higher raw accuracy than classical classifiers on the EC2 algorithm but also have better precision-recall trade-offs. Hence, the boosting models are more desirable for such important cybersecurity assessment tasks.

Practical implications

The capability of machine learning keeps its role in cybersecurity relevant for both tech vendors and inside organizations. For technology vendors, the promise of employing machine learning technologies to uncover patterns in text-based evidence opens new possibilities for responding to the changing cybersecurity landscape. It helps them to build better and more adaptive security products. Internal organizations, however, can rely on the increased efficiency of machine learning-based assessment tools, which shorten timelines for decision-making and provide decision-makers with the ability to act on thorough evaluations with confidence.

Furthermore, this study is highly beneficial for information security managers, auditors, and practitioners, who play a key role in protecting critical infrastructure systems and information. Machine learning provides these analysts and specialists with more sophisticated capabilities to analyse large volumes of data effectively, identify possible exploits, and take preventative action. It also grows an appreciation for the dynamics of innovation in organizations and how security measures mature and adjust to a frequently changing threat environment.

The combination of machine learning and the KAMI framework opens new research opportunities in the area of AI and Cybersecurity. Organizations can practically utilize the integrated KAMI-ML model outputs to pinpoint weaknesses in security domains immediately, streamline security budgeting decisions, or prioritize internal audits more effectively. For example, a low predicted maturity level in Technology and Security Operations suggests urgent attention to technological investments or operational training. The study demonstrates the versatility of machine learning in enhancing auditing processes, opening avenues for leveraging AI to protect critical assets more effectively.

While this study focuses on modeling and analyzing scenarios based on the dataset, it does not yet include a live integration or deployment of the model in a real-time ML pipeline. However, this study is necessary to form the basis for developing predictive or decision-support models that, in future work, can assist real-world decision-makers in conducting Information Security Risk Assessments more efficiently. As organizations increasingly adopt AI-driven solutions, information security professionals are poised to harness these advancements, fostering deeper insights and bolstering cybersecurity

practices across industries. This research not only addresses current challenges but also sparks curiosity about the untapped potential of machine learning in advancing the state of information security.

6 Conclusions

This study demonstrates the effectiveness of machine learning in advancing Information Security Risk Assessment (ISRA), particularly in contexts aligned with the KAMI framework. The paper has underlined the importance of a data-driven analysis by evaluating traditional and advanced machine learning algorithms, including boosting techniques. The research highlights the superior performance of models like CatBoost, Gradient Boosting, and LightGBM, which excel in handling complex and imbalanced datasets. The integration of machine learning with globally recognized standards such as KAMI not only enhances the efficiency and accuracy of risk assessments but also addresses persistent challenges like processing unstructured evidence. The practical implications of this research are substantial, benefiting both technology vendors and internal organizations. Machine learning-based tools streamline the assessment process, provide actionable insights, and empower decision-makers to strengthen their cybersecurity strategies. This study sets a strong foundation for future exploration at the intersection of machine learning and cybersecurity, offering a roadmap for leveraging AI to adapt to evolving threats and secure critical systems more effectively.

Acknowledgements

This research was supported by Indonesia's Ministry of Education, Culture, Research, and Technology under Fundamental Research Grant, No: 0609.20/LL5-INT/AL.04/2024, 006/KONTRAK-LPPM/AMIKOM/VI/2024, (dated June, 14th 2024).

References

[1] Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

[2] Al Faruq, B., Herlianto, H. R., Simbolon, S. H., Utama, D. N., & Wibowo, A. (2020). Integration of ITIL V3, ISO 20000 & iso 27001: 2013forit services and security management system. *International Journal*, *9*(3). https://doi.org/10.30534/ijatcse/2020/157932020

[3] AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

[4] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(10), 3660. https://doi.org/10.3390/app10103660

[5] Alqurashi, F., & Ahmad, I. (2024). A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling. *Alexandria Engineering Journal*, *107*, 374-389. https://doi.org/10.1016/j.aej.2024.07.044

[6] Alrehili, A. A., & Alhazmi, O. H. (2024). ISO/IEC 27001 Standard: Analytical and Comparative Overview. In S. Das, S. Saha, C. A. Coello Coello, & J. C. Bansal (Eds.), Advances in Data-Driven Computing and Intelligent Systems. Springer Nature. 143–156. https://doi.org/10.1007/978-981-99-9524-0_12

[7] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

[8] Asadov, B. (2018). The current state of artificial intelligence (AI) and implications for computer technologies. *International Journal of Communication and Computer Technologies (IJCCTS)*, *6*(1), 15-18.

[9] Badan Siber dan Sandi Negara. (2024). *INDEKS KAMI* | www.bssn.go.id. https://www.bssn.go.id/indeks-kami/

[10] Barafort, B., Mesquida, A. L., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, *31*(1), e1984. https://doi.org/10.1002/smr.1984

[11] Bettaieb, S., Shin, S. Y., Sabetzadeh, M., Briand, L. C., Garceau, M., & Meyers, A. (2020). Using machine learning to assist with the selection of security controls during security assessment. *Empirical Software Engineering*, *25*(4), 2550-2582. https://doi.org/10.1007/s10664-020-09814-x

[12] Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial auditing journal*, *33*(4), 360-376. https://doi.org/10.1108/MAJ-02-2018-1804

[13] Cheimonidis, P., & Rantos, K. (2023). Dynamic risk assessment in cybersecurity: A systematic literature review. *Future Internet*, *15*(10), 324. https://doi.org/10.3390/fi15100324

[14] Chen, T., & Guestrin, C. (2016, August). Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining* (pp. 785-794). https://doi.org/10.1145/2939672.2939785

[15] Cremer, J. L., & Strbac, G. (2021). A machine-learning based probabilistic perspective on dynamic security assessment. *International Journal of Electrical Power & Energy Systems*, *128*, 106571. https://doi.org/10.1016/j.ijepes.2020.106571

[16] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*, *33*(7), 76-105. https://doi.org/10.1108/TQM-09-2020-0202

[17] Deshmukh, S., & Menon, A. (2025). Machine Learning in Malware Analysis and Prevention. *In Essentials in Cyber Defence.* 74-89. Periodic Series in Multidisciplinary Studies.

[18] Forge, C. (2024). NIST 800-53 vs ISO 27002 vs NIST CSF vs SCF - ComplianceForge. Governance Risk & Compliance (GRC). https://complianceforge.com/grc/nist-800-53-vs-iso-27002-vs-nist-csf-vs-scf

[19] Friedman, J. H. (2001). Greedy function approximation: a gradient boosting machine. *Annals of statistics*, 1189-1232.

[20] Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*, 410-431. https://doi.org/10.1016/j.future.2019.12.018

[21] Haufe, K., Colomo-Palacios, R., Dzombeta, S., & Brandis, K. (2016). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27-47. Scopus. https://doi.org/10.12821/ijispm040402

[22] Jiang, Y., & Atif, Y. (2021). A selective ensemble model for cognitive cybersecurity analysis. *Journal of Network and Computer Applications*, *193*, 103210. https://doi.org/10.1016/j.jnca.2021.103210

[23] Johora, F. T., Khan, M. S. I., Kanon, E., Rony, M. A. T., Zubair, M., & Sarker, I. H. (2024). A data-driven predictive analysis on cyber security threats with key risk factors. https://doi.org/10.48550/arXiv.2404.00068

[24] Junaid, T. S. (2023). *ISO 27001: information security management systems* (Doctoral dissertation, Ph. D. thesis, Unspecified Institution. https://doi. org/10.13140/RG. 2.2. 36267.52005). https://doi.org/10.13140/RG.2.2.36267.52005

[25] Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., ... & Liu, T. Y. (2017). Lightgbm: A highly efficient gradient boosting decision tree. *Advances in neural information processing systems*, *30*.

[26] Konstantinov, A. V., & Utkin, L. V. (2021). Interpretable machine learning with an ensemble of gradient boosting machines. *Knowledge-Based Systems*, *222*, 106993. https://doi.org/10.1016/j.knosys.2021.106993

[27] Magesa, D. M., & Mshana, J. A. (2023). Assessing challenges facing implementation of information security critical success factors: a case of national examination council, Tanzania. *European Journal of Theoretical and Applied Sciences*, *1*(5), 883-897. https://doi.org/10.59324/ejtas.2023.1(5).74

[28] Makhija, A. K. (2021). Information security management systems-evolving landscape and ISO 27001: An empirical study. *Journal of Accounting, Finance, Economics, and Social Sciences*, *6*(1), 9-17. https://doi.org/10.62458/jafess.160224.6(1)9-17

[29] Mehra, A., & Iyer, R. (2021). Improving Cybersecurity Using Artificial Intelligence: Overview, Modeling, Future Directions. *International Academic Journal of Science and Engineering, 8*(2), 11–15. https://doi.org/10.71086/IAJSE/V8I2/IAJSE0810

[30] Muhammad, A. H., Nasiri, A., & Harimurti, A. (2025). Machine learning methods for classification and prediction information security risk assessment. *IAES Int. J. Artif. Intell*, *14*, 457-465. https://doi.org/10.11591/ijai.v14.i1.pp457-465

[31] Muhammad, A. H., Santoso, J. D., & Akbar, A. F. I. (2023). Information security investment prioritization using best-worst method for small and medium enterprises. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(1), 271-280. https://doi.org/10.11591/ijeecs.v31.i1.pp271-280

[32] Prokhorenkova, L., Gusev, G., Vorobev, A., Dorogush, A. V., & Gulin, A. (2018). CatBoost: unbiased boosting with categorical features. *Advances in neural information processing systems*, *31*.

[33] Raimundo, R., & Rosário, A. (2021). The impact of artificial intelligence on data system security: A literature review. *Sensors*, *21*(21), 7029. https://doi.org/10.3390/s21217029

[34] Rosado, D. G., Sánchez, L. E., Varela-Vaca, Á. J., Santos-Olmo, A., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2024). Enabling security risk assessment and management for business process models. *Journal of Information Security and Applications*, *84*, 103829. https://doi.org/10.1016/j.jisa.2024.103829

[35] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

[36] Schmitz, C., & Pape, S. (2020). LiSRA: Lightweight Security Risk Assessment for decision support in information security. *Computers & Security*, *90*, 101656. https://doi.org/10.1016/j.cose.2019.101656

[37] Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security*, *108*, 102306. https://doi.org/10.1016/j.cose.2021.102306

[38] Schneeberger, I., & Lemaître, A. (2023). Supply Chain Excellence: Achieving Peak Performance Through Data-Driven Insights. International Academic Journal of Innovative Research, 10(4), 36–40. https://doi.org/10.71086/IAJIR/V10I4/IAJIR1031

[39] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE access*, *8*, 222310-222354. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3041951

[40] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15-29. https://doi.org/10.1016/j.aos.2018.04.005

[41] Sunarto, A., Kencana, P. N., Munadjat, B., Dewi, I. K., Abidin, A. Z., & Rahim, R. (2023). Application of Boosting Technique with C4. 5 Algorithm to Reduce the Classification Error Rate in Online Shoppers Purchasing Intention. *Journal of Wireless Mobile Networks,*

Ubiquitous Computing, and Dependable Applications, *14*(2), 01-11. https://doi.org/10.58346/JOWUA.2023.I2.001

[42] Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, *90*, 101709. https://doi.org/10.1016/j.cose.2019.101709

[43] Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *International Journal of Information Security*, *17*(6), 681-699. https://doi.org/10.1007/s10207-017-0382-0

[44] Yang, C., Fridgeirsson, E. A., Kors, J. A., Reps, J. M., & Rijnbeek, P. R. (2024). Impact of random oversampling and random undersampling on the performance of prediction models developed using observational health data. *Journal of Big Data, 11*(1), 7. https://doi.org/10.1186/s40537-023-00857-7

[45] Zahedifard, M., Attarzadeh, I., Pazhokhzadeh, H., & Malekzadeh, J. (2015). Prediction of students' performance in high school by data mining classification techniques. *International Academic Journal of Science and Engineering*, *2*(7), 25-33.

[46] Zhu, J., Zou, H., Rosset, S., & Hastie, T. (2009). Multi-class adaboost. *Statistics and its Interface*, *2*(3), 349-360. https://doi.org/10.4310/SII.2009.v2.n3.a8

Authors Biography

Alva Hendi Muhammad received his PhD in Information Technology from the University of Technology Sydney in Australia. He currently works as an Assistant Professor in the Faculty of Computer Science at Universitas Amikom Yogyakarta in Indonesia. He has over 10 years of experience teaching at both the undergraduate and postgraduate levels in an educational institution. His research interests include modeling decision and expert systems, incorporating Artificial Intelligence with Engineering and Educational Technology, and also Information Security.

Hanafi is an Assistant Professor at Universitas Amikom Yogyakarta, with research interests in e-commerce, machine learning, networking, recommender systems, and cybersecurity. He received his PhD in Computer Science from the Universiti Teknikal Malaysia Melaka, with an emphasis on intelligent systems and applied machine learning. His research continually seeks to connect theoretical discoveries to practical applications, particularly in the fields of intelligent informatics and cybersecurity solutions.

Kumara Ari Yuana received his Ph.D. in Computational Fluid Dynamics (CFD) from the Department of Mechanical Engineering at Universitas Gadjah Mada, Indonesia, in 2021. He is currently a lecturer at the Universitas Amikom Yogyakarta. His research interests include computational fluid dynamics, mathematical and statistical modeling, and soft computing. He is actively involved in multidisciplinary research that applies engineering concepts and computational intelligence to complicated challenges in fluid dynamics and system modeling. He is a senior member of the IEEE Indonesia.

Bahrun Ghozali serves as a lecturer in the Computer Engineering Diploma Program at Universitas Amikom Yogyakarta. His areas of expertise include computer networking and cybersecurity. Academically, he holds a Master degree in Informatics and also several professional certifications, such as Certified Network Defender (CND) and Certified Secure Computer User (CSCU) from EC-Council, along with CCNA Routing & Switching and CCNA Security.

Ruby Haris holds a Master degree from Universitas Amikom Yogyakarta, Indonesia. He is interested in the fields of Cybersecurity, Network Analysis, Data Mining, as well as Media and Communication. He works as a civil servant at the Gunung Mas Regency Government, Central Kalimantan Province, and currently serves as the Head of the Department of Communication, Informatics, Encryption, and Statistics. He holds several certifications from the Cisco Networking Academy and is also a Bug Hunter with Cyber Army Indonesia.