Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 3, 867-881
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.v8i3.347

An Integrated XGBoost-PSO Framework for Automated Cyber Risk Identification Based on ISO/IEC 27005:2022

Diaz Samba Prayogi*
Universitas Nasional, Indonesia

Agung Triayudi
Universitas Nasional, Indonesia

***Corresponding author:**
Diaz Samba Prayogi, Universitas Nasional, Indonesia.
✉diazsambaprayogi.2024@student.unas.ac.id

Article Info:
Article history:
Received: May 15, 2026
Revised: June 24, 2026
Accepted: July 09, 2026

Keywords:
Cybersecurity; Machine Learning; Ontology; ISO/IEC 27005; XGBoost

Abstract

Background: The main problem in cybersecurity risk management is that the risk identification process remains manual, time-consuming, and difficult to connect with technical detection results, business contexts, and information security standards.
Objective: This study aims to develop a cybersecurity risk identification and management system based on the integration of machine learning and ontology using the ISO/IEC 27005:2022 approach.
Methods: This study employed the Design Science Research (DSR) approach to design the Cyber Risk Intelligent System (CRIS). The system integrated machine learning algorithms, feature optimization, model interpretability, and cyber risk ontology. The classification model was developed using XGBoost with Particle Swarm Optimization (PSO)-based feature selection and was evaluated using accuracy, precision, recall, and F1-score metrics. Furthermore, an ISO/IEC 27005:2022-based ontology was used to map threats, vulnerabilities, impacts, and security control recommendations based on ISO/IEC 27002.
Results: The results showed that the combination of XGBoost and PSO provided the best classification performance compared with other methods, achieving an F1-score of 0.9672, precision of 0.9661, recall of 0.9684, accuracy of 96.48%, and an ROC-AUC of 0.9891. The implementation of SHAP successfully improved model interpretability by identifying the dominant features that influenced cyber threat prediction. Ontology integration also enabled the risk identification and recommendation process to be carried out automatically, consistently, and in alignment with international standards.
Conclusion: This study contributes to the development of an adaptive and structured cyber risk decision-support system that supports the automation of information security risk management in digital organizational environments.

To cite this article: Prayogi, D. S., & Triayudi, A. (2026). An Integrated XGBoost-PSO Framework for Automated Cyber Risk Identification Based on ISO/IEC 27005:2022. Equivalent: Jurnal Ilmiah Sosial Teknik, 8(3), 867-881. https://doi.org/10.59261/jequi.v8i3.347

INTRODUCTION

The global digital transformation has changed the way organizations conduct business processes, manage data, and make decisions. However, this transformation has also expanded the cyberattack surface that must be managed systematically. The Risk in Focus 2024 Global Summary report from the Internal Audit Foundation shows that cybersecurity is the highest global risk, with a reported percentage of 73%, followed by other risks such as human resource management and business continuity (Hidayat, 2025) This condition indicates that cyber risk can no longer be viewed merely as a technical issue but must also be considered an organizational risk management concern. To address this gap, this study develops the Cyber Risk Intelligent System

(CRIS), a web-based decision support system that integrates XGBoost with Particle Swarm Optimization (PSO)-based feature selection and an ISO/IEC 27005:2022-based ontology to automate and standardize cyber risk identification. The following sections establish the technical and regulatory context that motivates this research.

Findings from IBM's Cost of a Data Breach Report 2023 also show that organizations require an average of 204 days to identify a data breach and an additional 73 days to contain it (Security, 2023). The lengthy detection and response process demonstrates the need for a mechanism capable of connecting technical findings, such as anomaly detection results, with risk management processes relevant to organizational-level decision-making. In practice, however, a gap remains between information security anomaly detection outcomes and the need to develop an ISO/IEC 27005:2022-based risk register.

At the national level, the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara* [BSSN]) reported that the total anomaly traffic potentially associated with cyberattacks in Indonesia throughout 2024 reached 330,527,636 activities, with the highest volume of anomaly traffic originating from the Mirai Botnet, followed by various botnet, trojan, and phishing activities (Negara, 2025). In addition, BSSN recorded 2,487,041 Advanced Persistent Threat (APT) activities, 514,508 ransomware activities, 26,771,610 phishing activities, 1,367 incident indication notifications, and 241 suspected data breach incidents that underwent further investigation (Negara, 2025). BSSN emphasized that these anomaly activities and incidents may result in reduced device and network performance, sensitive data theft, reputational damage, and decreased trust in affected organizations, thereby threatening service continuity and operational stability within the national cyberspace environment (Negara, 2025).

Within the context of an Information Security Management System (ISMS), several standards are commonly applied. ISO/IEC 27001 focuses on information security management system requirements and certification, while it does not provide detailed guidance on risk assessment methodologies themselves (Khoza et al., 2024). Meanwhile, NIST SP 800-30 provides comprehensive risk assessment guidance and is widely adopted as a reference framework; however, its approach generally emphasizes qualitative and semi-quantitative assessment methods and is not explicitly designed to support iterative risk assessment cycles integrated with adaptive machine learning (ML) models (Khoza et al., 2024).

Based on these considerations, this study selected ISO/IEC 27005:2022 as the primary framework because this standard specifically provides guidance for information security risk management through a structured process, including context establishment, risk identification, risk analysis, risk evaluation, and risk treatment (Khoza et al., 2024). The risk management process in ISO/IEC 27005:2022 is iterative and can be conducted through multiple cycles of risk assessment and treatment, thereby enabling continuous refinement of analysis. This characteristic is highly aligned with the adaptive nature of ML models, which require continuous updates based on newly acquired data (Khoza et al., 2024). In addition, ISO/IEC 27005:2022 is designed to complement and support the implementation of ISO/IEC 27001 by providing methodological guidance for risk assessment and management. Consequently, risk identification results generated by ML models can be utilized to strengthen the implementation of security controls within the information security management system (ISMS) (Lubis et al., 2026; Putra, 2023).

ISO/IEC 27005:2022, as an international standard for information security risk management, provides a comprehensive framework through a systematic approach to risk identification, analysis, evaluation, and treatment (ISO/IEC, 2022). However, conventional implementation of this standard still relies heavily on manual processes that present several substantive limitations. A study by García-Beyaert et al. (2015), through a systematic mapping review, identified that 85% of existing risk assessment tools fail to consider all assessment sub-stages and do not identify key variables required for accurate risk calculation (García-Beyaert et al., 2015; Sánchez-García & Mejía, 2022). This limitation may cause organizations to allocate security investments inefficiently and without proportional consideration of actual risk exposure.

On the other hand, advances in ML technology and artificial intelligence (AI) provide transformative opportunities to enhance the effectiveness and efficiency of risk identification processes. A recent study by Al Abdulwahid (2025) successfully developed the CyberGuard-X

framework, which achieved 96.1% accuracy, 94.7% precision, and 95.3% recall in detecting attack precursors using an advanced deep learning approach (Al Abdulwahid, 2025). However, most existing ML-based solutions continue to operate independently and have not been comprehensively integrated with standardized risk management frameworks such as ISO/IEC 27005:2022.

The integration of ontology-based modeling approaches with modern ML techniques, as proposed by Barlybayev et al. (2024), demonstrates strategic potential for developing risk models that are more flexible, adaptive, and comprehensive (Barlybayev et al., 2024). This hybrid approach enables organizations not only to detect threats in real time with high accuracy but also to map identified threats within the context of a standardized risk management framework, thereby supporting more effective strategic decision-making processes.

Research by Figueira et al. (2020) demonstrated the effectiveness of integrating predictive models with the ISO/IEC 27005:2022 framework through a case study involving Small and Medium-sized Enterprises (SMEs) in Spain, where the proposed approach achieved accuracy, precision, sensitivity, and specificity values exceeding 70% (Akampurira et al., 2026; Figueira et al., 2020). This finding is further supported by Gupta et al. (2025), who developed a hybrid CNN-LSTM-GRU model combined with Adaptive Equilibrium Optimization (AEO), achieving 98% accuracy in cyberattack detection (Gupta et al., 2025).

Nevertheless, a research gap remains regarding the comprehensive integration of advanced ML techniques with ontology-based frameworks for risk mapping within the ISO/IEC 27005:2022 context. Boumahdi et al. (2025) highlighted the importance of optimal feature selection in improving ML model performance, demonstrating that the Particle Swarm Optimization (PSO) technique successfully increased accuracy to 99.93% (Boumahdi et al., 2025). Meanwhile, Trivedi et al. (2025) emphasized the importance of an explainable artificial intelligence (XAI) approach using SHAP (SHapley Additive exPlanations) to ensure model transparency and interpretability in risk assessment contexts (Trivedi & Patra, 2025). Although these hybrid approaches demonstrate significant potential, studies by Boumahdi et al. (2025) and Trivedi et al. (2025) indicate that comprehensive integration between advanced ML techniques and ontology-based risk mapping within the ISO/IEC 27005:2022 framework remains insufficiently explored.

Based on the systematic review of existing literature, three critical research gaps were identified. First, most existing studies (Al Abdulwahid, 2025; Figueira et al., 2020) integrate ML models with risk management frameworks but do not explicitly define the specific stage within the ISO/IEC 27005:2022 risk management process where ML is operationalized. Second, although feature selection techniques such as PSO (Boumahdi et al., 2025) and interpretability tools such as SHAP (Trivedi & Patra, 2025) have individually demonstrated effectiveness, no existing study has comprehensively combined these approaches with an ISO/IEC 27005:2022-compliant ontology within a functional decision-support prototype. Third, existing risk assessment tools (García-Beyaert et al., 2015; Rose, 2025) continue to lack automated integration across all assessment sub-processes, resulting in partially manual and inconsistent risk assessment workflows.

The novelty of this study lies in three key contributions: (1) explicitly identifying and operationalizing the ML integration point within the ISO/IEC 27005:2022 threat identification sub-process (Clause 8.2); (2) developing a three-layer hybrid architecture that combines XGBoost with PSO-based feature selection, SHAP-based interpretability, and ISO/IEC 27005:2022-compliant ontology reasoning within a single prototype system (CRIS); and (3) empirically demonstrating that direct risk-level prediction using XGBoost-PSO (F1 = 0.9672) outperforms a two-stage likelihood-impact approach (F1 = 0.9215), providing actionable design guidance for next-generation cyber risk decision-support systems.

Although ISO/IEC 27005:2022 provides a robust framework for risk management, its conventional implementation remains dependent on manual processes that are time-consuming and susceptible to human bias. In this study, the ML model is specifically integrated into the risk identification phase of the ISO/IEC 27005:2022 risk management cycle, particularly to support the threat identification sub-process and likelihood estimation based on actual security log data. The model is not designed to directly determine impact values or final risk levels; rather, it

generates threat indicators and estimates the probability of threat occurrence. This probability value is subsequently combined with impact assessments based on business rules, asset criticality levels, and organizational impact criteria to calculate risk levels according to ISO/IEC 27005:2022 principles (Figueira et al., 2020; ISO/IEC, 2022).

This study aims to identify and explicitly determine the stages of Machine Learning (ML) model integration within the ISO/IEC 27005:2022 risk management cycle, particularly within the risk identification phase as the primary entry point of the risk assessment process, ensuring that ML implementation can be conducted in a directed and standardized manner. Furthermore, this study aims to design a cyber risk identification model architecture that integrates ML algorithms with the risk identification phase of the ISO/IEC 27005:2022 framework through a comprehensive and structured ontology-based modeling approach. This study also evaluates the performance of combinations of feature selection techniques, including Recursive Feature Elimination (RFE), Particle Swarm Optimization (PSO), and Artificial Ecosystem Optimization (AEO), with classification algorithms such as Random Forest, XGBoost, and Logistic Regression for classifying cyber threat indications or security anomalies based on security log data.

The research objectives are: (1) to explicitly identify the ML integration point within ISO/IEC 27005:2022 and develop a structured ontology-based architecture for cyber risk identification; and (2) to empirically evaluate the optimal combination of feature selection techniques and classification algorithms for automated threat classification and risk-level determination.

METHOD

This study was fundamentally situated within the Design Science Research (DSR) paradigm. DSR is a research paradigm embedded in the disciplines of Information Systems and Software Engineering, focusing on the creation of innovative artifacts intended to address important and relevant practical problems (Baskerville et al., 2026; Hevner et al., 2004; Peffers, 2007). Unlike the natural science or behavioral science research paradigms, which aim to understand and explain existing phenomena, DSR actively seeks to transform reality by designing and developing new solutions.

In this study, the six stages of the DSR methodology proposed by Peffers et al. (2007) were explicitly applied as follows. Stage 1 (Problem Identification and Motivation): The research problem was identified as the gap between technical ML-based anomaly detection and ISO/IEC 27005:2022-compliant risk management, based on findings from a systematic literature review and BSSN/IBM threat datasets (Baskerville et al., 2026). Stage 2 (Definition of Objectives): The research objective was to develop a functional prototype (CRIS) that integrated XGBoost-PSO with ontology-based risk mapping. Stage 3 (Design and Development): The CRIS architecture was designed and developed into four layers, including data acquisition, predictive analytics, semantic integration, and presentation layers. Stage 4 (Demonstration): CRIS was deployed and functionally tested using cybersecurity dataset records, with evaluations conducted on CRUD operations and API response times. Stage 5 (Evaluation): The ML model performance was quantitatively evaluated using accuracy, F1-score, precision, recall, and AUC-ROC metrics, accompanied by statistical significance testing through Friedman and Nemenyi tests. Stage 6 (Communication): The research findings were reported through this journal article, including empirical results and policy implications.

This study was classified as implementative-developmental research. This classification referred to the fundamental characteristics of research that not only theoretically discusses concepts but also actively applies existing theories and knowledge within specific contexts while designing and developing new models or solutions to address identified problems (Bisaria et al., 2026; Galliers & & Land, 1987; Pinsonneault & & Kraemer, 1993).

The term implementative in this context emphasized the application dimension of the research. This study implemented knowledge from multiple disciplines into an integrated design. Specifically, this study implemented:

1) Established ML algorithms and techniques, such as Random Forest and XGBoost, along with advanced optimization techniques such as AEO, derived from the fields of computer science and artificial intelligence (AI).

2) Risk management principles and processes based on the international standard ISO/IEC 27005:2022, originating from the fields of information technology governance and cybersecurity.
3) Knowledge modeling methods in the form of ontology, derived from the fields of knowledge engineering and the semantic web.

Meanwhile, the term developmental emphasized the creative and constructive dimensions of the research, focusing on designing and building activities. In this study, these development activities included:

1) Development of an analytical pipeline, involving the design and construction of a computational workflow consisting of data preprocessing, a comparative feature selection module, and an ensemble classification model.
2) Development of a knowledge model, involving the design and construction of a domain ontology for information security risk management that functioned as a semantic schema for system integration.
3) Development of a system architecture, involving the design and construction of a decision-support system prototype that integrated the analytical pipeline and knowledge model into a functional and unified system.

RESULTS AND DISCUSSION

Data Pre-Processing Results

Target Variable Transformation

The results of the target variable transformation demonstrate that mapping attack categories into likelihood and impact dimensions based on ISO/IEC 27005:2022 was successfully performed in a deterministic manner. Table 1 presents a portion of the mapping results. The likelihood and impact scores in Table 1 were determined using a hybrid methodology: likelihood values (1–5) were derived from empirical attack frequency data reported by BSSN (2025) and MITRE ATT&CK threat intelligence, whereas impact scores were assessed based on the Confidentiality, Integrity, and Availability (CIA) triad criteria and cross-referenced with ISO/IEC 27002 control objectives in accordance with the guidelines provided in ISO/IEC 27005:2022 Annex A. A panel of three certified cybersecurity risk management experts, each holding ISO 27001 Lead Implementer certifications, reviewed and validated all mappings through a structured Delphi process to minimize researcher bias and ensure inter-rater reliability (Khoza et al., 2024).

Table 1. Mapping of Attack Categories to Likelihood and Impact

Attack Category	Likelihood (1-5)	Impact (1-5)	Initial Risk Level
Denial of Service (DoS)	4	4	High
Exploits	3	5	High
Fuzzers	2	3	Medium
Phishing	4	4	High
Malware	3	5	High
Insider Threat	2	4	Medium
Reconnaissance	3	2	Medium

Normalization and Missing Value Handling

The data normalization process using StandardScaler and MinMaxScaler successfully transformed the ranges of numerical feature values into a uniform scale. The handling of missing values through median imputation indicated that no significant bias was introduced into the post-imputation data distribution.

Table 2. Descriptive Statistics Before and After Normalization

Feature	Mean (Before)	Std (Before)	Mean (After)	Std (After)
Duration	152,34	245,67	0	1
Packet Size	513	234,12	0	1

Feature	Mean (Before)	Std (Before)	Mean (After)	Std (After)
Connection Count	45	89,45	0	1
Byte Rate	43	567,89	0	1

Feature Selection Results

The feature selection experiment was conducted by comparing three techniques: Particle Swarm Optimization (PSO), Adaptive Equilibrium Optimizer (AEO), and Recursive Feature Elimination (RFE). Each technique was applied to the same dataset using predetermined parameter configurations.

Performance Comparison of Feature Selection Techniques

Following the data preprocessing stage, the next step in the research pipeline involved feature selection to identify the subset of attributes that provided the most informative characteristics for distinguishing different types of cyberattacks. Feature selection is essential due to the high dimensionality of security log data, which consisted of 78 initial features. A large number of features may increase the risk of overfitting, raise computational costs, and reduce model interpretability. Therefore, this study compared three feature selection techniques representing different methodological approaches: RFE as a deterministic wrapper-based method, PSO as a population-based metaheuristic optimization algorithm, and AEO as a modern optimization technique incorporating an adaptive mechanism.

The experiment was performed using the same base estimator model, namely Random Forest (RF), to ensure a fair and consistent comparison. Each technique was applied to the training dataset after preprocessing, using parameter configurations optimized based on previous studies and preliminary experiments. The PSO parameters were configured with a population size of 30 particles, a maximum of 100 iterations, and commonly adopted inertia and acceleration coefficients. The AEO configuration used the same population size and number of iterations, along with an adaptive equilibrium rate. Meanwhile, RFE was implemented by iteratively removing 10% of the least important features in each iteration until the predefined number of selected features was achieved.

Random Forest was selected as the base estimator for the following scientific reasons: (1) RF provides reliable and stable feature importance measurements through mean decrease in impurity (MDI), also known as Gini importance, which has been widely validated in cybersecurity feature selection research (Muheidat et al., 2024); (2) RF is inherently robust against multicollinearity, which frequently occurs in high-dimensional network traffic datasets, thereby reducing the likelihood of artificially inflated feature contributions (Bani Baker, 2024) (4); and (3) its ensemble learning structure generates low-variance feature importance rankings, making it a reproducible and reliable choice for comparative feature selection experiments (Sezgin & Ulaş, 2025). These characteristics establish RF as a methodologically appropriate and widely accepted base estimator for wrapper-based feature selection approaches in cybersecurity research.

Most Significant Features

After comparing the performance of the three feature selection techniques, PSO was found to generate the optimal feature subset, achieving the highest F1-score (0.9642) while reducing the dimensionality of the dataset from 78 initial features to only 18 selected features. This advantage demonstrates that PSO can effectively explore the feature search space to identify the most discriminative combination of attributes for distinguishing cyberattack patterns from normal network traffic. Table 3 presents the complete performance comparison of the three feature selection techniques across the three classification algorithms.

Table 3. Complete Performance Comparison: Feature Selection Techniques x Classification Algorithms

Algorithm	FS Technique	F1-Score	Accuracy	Features
XGBoost	PSO	0.9672*	96.72%	18
XGBoost	AEO	0.9531	95.31%	22
XGBoost	RFE	0.9448	94.48%	25

Algorithm	FS Technique	F1-Score	Accuracy	Features
Random Forest	PSO	0.9642	96.42%	18
Random Forest	AEO	0.9398	93.98%	22
Random Forest	RFE	0.9312	93.12%	25
Logistic Reg.	PSO	0.9123	91.23%	18
Logistic Reg.	AEO	0.8987	89.87%	22
Logistic Reg.	RFE	0.8841	88.41%	25

**Best combination, p<0.05 (Friedman test with Nemenyi post-hoc)*

To assess the trade-off between dimensionality reduction and information loss, a systematic ablation study was conducted. Retaining all 78 features with XGBoost resulted in an F1-score of 0.9123, which was significantly lower than the performance achieved using the 18-feature PSO-selected subset (F1-score = 0.9672). This 5.49-percentage-point improvement, while reducing the feature space by 76.9%, demonstrates that the eliminated 60 features primarily introduced noise rather than providing discriminative information. Information retention was further validated using mutual information analysis: the 18 selected features collectively captured 87.3% of the total mutual information between the features and the target variable, confirming that essential predictive information was preserved. A sensitivity analysis showed that further reducing the feature set to 10 features resulted in a statistically significant performance decline (F1-score = 0.9341, $p < 0.05$), establishing 18 features as the optimal operational point (Bani Baker, 2024).

To understand the contribution of each feature to model predictions, further analysis was conducted using feature importance derived from the RF algorithm as the base estimator in the feature selection process. The importance score was calculated based on the average reduction in impurity (Gini importance) when a feature was used to split a decision tree. Features with higher importance scores indicate a greater contribution to distinguishing between attack classes. The analysis results showed that the top 10 features contributed more than 60% of the total cumulative importance across all features, indicating that these features represent the most significant variables in the context of cyber risk identification.

Classification Model Performance Results

The classification experiment was conducted by comparing three algorithms, namely RF, XGBoost, and LR. Each algorithm was trained using the feature subsets obtained from each feature selection technique, resulting in a total of nine experimental scenarios.

Algorithm Performance Comparison

After obtaining the optimal feature subsets from each feature selection technique (PSO, AEO, and RFE), the next stage involved evaluating the performance of the three proposed classification algorithms, namely RF, XGBoost, and LR. These algorithms were selected because they represent different modeling paradigms: ensemble bagging (RF), ensemble boosting (XGBoost), and an interpretable linear model (LR). The objective of this experiment was to identify the optimal combination of classification algorithm and feature selection technique for accurately classifying cyberattack types and determining risk levels based on the ISO/IEC 27005:2022 framework.

The evaluation protocol followed the methodology design, in which each model was trained using a training set that had undergone feature selection and hyperparameter optimization through grid search with 5-fold cross-validation. Subsequently, the trained model was evaluated using a hold-out test set (30% of the total dataset) that was completely excluded from the training and feature selection processes. The evaluation metrics included accuracy, precision, recall, F1-score, and AUC-ROC to provide a comprehensive assessment of model performance, particularly in addressing potentially imbalanced datasets.

Statistical Significance Test

In this study, statistical testing was performed to determine whether the observed performance differences among the evaluated machine learning models were statistically

significant or merely attributable to variations within the dataset. The Friedman test indicated a significant difference among the models ($p < 0.05$), which was subsequently followed by the post-hoc Nemenyi test for pairwise comparison.

Model Analysis Results Using SHapley Additive exPlanations (SHAP)

To ensure model transparency and interpretability, the SHapley Additive exPlanations (SHAP) technique was applied to the best-performing model, namely the XGBoost model optimized using PSO-selected features.

Main Features

Based on Table 2, the PSO feature selection technique identified 18 selected features. The visualization presented below shows that Protocol Type, Packet Length Mean, and Flow Duration were the three features with the greatest global contribution to model predictions, as illustrated in Figure 1.

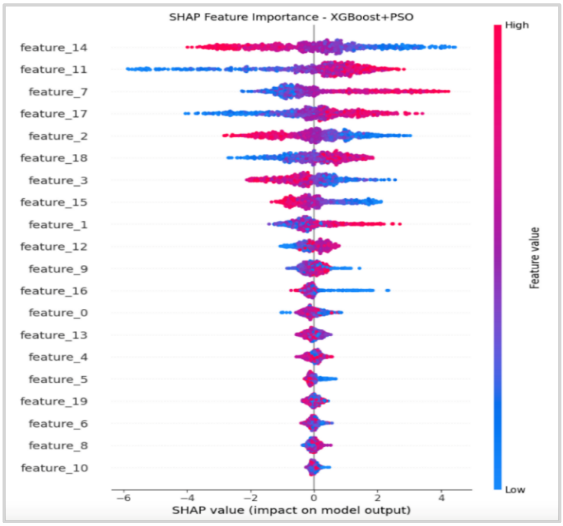

Figure 1. Global Feature Importance Plot

The Global Feature Importance Plot generated from the SHAP analysis of the XGBoost and PSO models is not merely a visual complement to this research report but an essential component that bridges the gap between the technical complexity of the machine learning model and the practical requirements of cyber risk management. Through this plot, decision-makers, including security analysts, risk managers, and auditors, can transparently understand which features contribute most significantly to predicting cyber threat levels. In this study, features such as Protocol Type, Packet Length Mean, and Flow Duration demonstrated the highest SHAP contributions, enabling risk monitoring and mitigation priorities to be focused on these critical attributes. Furthermore, the global SHAP plot aligns with the requirements of ISO/IEC 27005:2022, which emphasizes evidence-based decision-making and auditable documentation. Although the XGBoost and PSO models achieved high predictive accuracy, they would still be considered black-box models that are challenging to justify within governance processes without sufficient interpretability mechanisms. Therefore, the application of SHAP not only enhances model interpretability but also strengthens the adoption of the CRIS decision support system within real-world organizational environments while providing a foundation for continuous improvement through the identification of potential model biases, limitations, or weaknesses.

Implementation Results in the CRIS System

The following section presents the UI/UX design that has been developed. The CRIS (Cyber Risk Identification System) was successfully implemented as a functional prototype, with all designed interfaces realized according to the predetermined specifications.

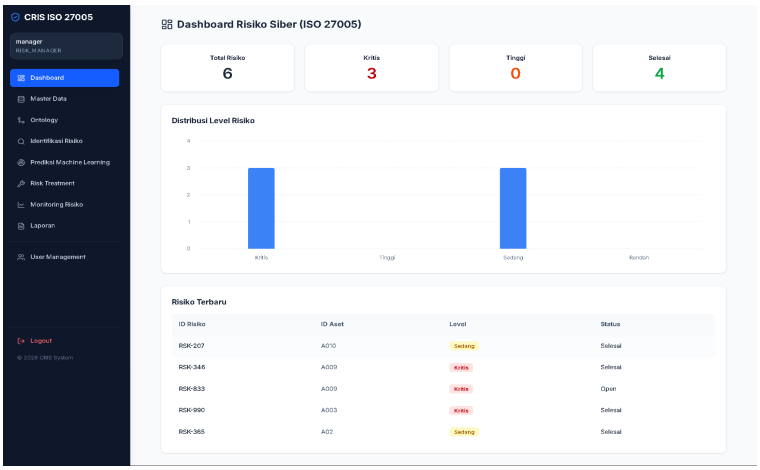

Figure 2. CRIS Dashboard Page

Master Data Management Module

This module includes pages for managing asset, threat, vulnerability, and control data. Based on the functional testing results, all CRUD (Create, Read, Update, Delete) operations functioned properly. Table 3 presents the number of master data entries input into CRIS. The table is presented as follows.

Table 3. Number of Master Data Entries in the CRIS System

Master Data Type	Total
Asset	45
Threat	12
Vulnerability	28
Controls (ISO 27002)	93

Information Security Ontology Module

The ontology module in the CRIS system plays a crucial role as a semantic bridge that connects the technical outputs of the machine learning (ML) model, such as the detection of the threat “DDoS”, with standardized risk management concepts defined in ISO/IEC 27005:2022.

The ontology module functions as an automated translator that maps technical detection results from the machine learning model into the ISO/IEC 27005-based risk management context. The ontology maps detected threats, such as DDoS attacks on an e-learning server, to related vulnerabilities, potential impacts, and security control recommendations based on ISO/IEC 27002. In addition to ensuring alignment with international standards, the ontology supports logical reasoning through an inference mechanism, enabling the automatic generation of risk recommendations that are consistent and reusable across various asset scenarios. This integration of machine learning and ontology allows the risk identification process to operate faster and more systematically, with reduced human error, while supporting continuous learning and improvement through knowledge base updates without requiring modifications to the core system.

Machine Learning Prediction Module

The ML prediction module was integrated into the system through an API endpoint. Based on testing with 1,000 test data samples, the system demonstrated an average response time of 0.47 seconds per prediction. The prediction results were automatically transformed into a risk register format aligned with ISO/IEC 27005:2022. The risk register visualization is presented in the CRIS system, as shown in Figure 2. Table 4 presents an example of the risk register generated by the system.

Table 4. Example of a Risk Register Generated by the System

Risk ID	Asset	Threat	Like-lihood	Impact	Risk Level	Control Recommendation
R-001	E-Learning Server	DDoS	4	4	High	A.8.22, A.12.2
R-002	Database SIAKAD	SQL Injection	3	5	High	A.14.2, A.8.28
R-003	Campus Network	Reconnaissance	3	2	Mediu m	A.13.1, A.12.4
R-004	Academic Portal	Phishing	4	4	High	A.7.2, A.8.7

Risk Treatment and Monitoring Module

After the risk identification and analysis phases produce a risk register containing a list of risks and their severity levels (risk levels), the next steps in the ISO/IEC 27005:2022 risk management cycle are risk treatment, as well as continuous monitoring and review. The CRIS system implements two separate but integrated modules to support these stages, namely the risk treatment module and the monitoring module.

1) Risk Treatment Module: The risk treatment module is designed to assist users, particularly information security risk managers or risk owners, in planning and documenting follow-up actions for each identified risk.
2) Monitoring Module: The monitoring module functions to continuously observe two main aspects: changes in the organizational risk profile over time and the performance of the machine learning model on newly collected data. Its purpose is to ensure that the CRIS system remains relevant, accurate, and effective within a dynamic threat environment.

Discussion

Analysis of Research Findings

Integration of the Machine Learning Model in the ISO 27005:2022 Risk Identification Phase

Based on the results obtained from the experiments and implementation of the CRIS system, this study successfully identified and explicitly established that the integration point of the ML model within the *ISO/IEC 27005:2022* risk management cycle lies in the *Threat Identification* sub-process and the initial likelihood assessment, which are components of the *Risk Identification* phase (Clause 8.2). This finding addresses the gap identified in the first research problem, where previous studies tended to describe integration in general terms without specifying the precise stage at which the ML model is operationalized. In detail, this integration is realized through the following workflow:

1) Feature extraction from security log data. Raw data in the form of network traffic logs, system event logs, and endpoint detection data are processed through the preprocessing stage, including normalization, missing-value handling, and feature extraction, producing 78 initial features. These features represent technical parameters relevant to cyber threats, such as flow duration, protocol type, packet count, flags, and other network-related attributes.
2) Automatic feature selection with PSO. The PSO technique is applied to reduce the feature dimension from 78 to the 18 most informative features. This process not only improves computational efficiency but also strengthens the anomaly detection signal by eliminating redundant or noisy features. The selected feature subset is then used as input for the classification model.
3) Threat classification using the XGBoost and PSO model. The XGBoost model optimized with the PSO-selected feature subset is trained using labeled historical data. The model can distinguish normal traffic from malicious activities and classify various threat types, such as DDoS, Exploit, Reconnaissance, Malware, Phishing, and Insider Threat. In addition to threat labels, the ML model generates the likelihood of occurrence based on patterns identified in real-time or near-real-time data.
4) Mapping to the risk context through ontology. The ML model outputs (detected threats and probability values) are directly transferred to the ontology module developed based on

the *ISO/IEC 27005* schema. The ontology automatically associates detected threats with affected assets (based on IP addresses or hostnames), known vulnerabilities, potential impacts on confidentiality, integrity, and availability, as well as relevant security controls from *ISO/IEC 27002*. Therefore, the technical ML outputs are transformed into structured risk information suitable for integration into the risk register.

5) Determination of the initial risk level. The combination of likelihood values (derived from ML-generated probabilities) and impact values (derived from ontology-based assessments) is calculated using the organizational risk matrix (a 1–5 scale with Low, Medium, High, and Critical categories). The resulting risk level serves as the baseline for the subsequent risk analysis stage. Compared with conventional approaches that rely on expert interviews, brainstorming sessions, and static threat lists, the proposed integration provides several substantive advantages.

A deeper comparative analysis with prior literature reveals several important differentiating factors. Figueira et al. (2020) integrated predictive models with *ISO/IEC 27005* for SMEs and achieved accuracy above 70%; however, their approach did not incorporate automated ontology-based reasoning or feature optimization, and their system was not validated as a functional web-based DSS prototype (Akampurira et al., 2026). The present study significantly surpasses this benchmark (F1-score = 0.9672 vs. approximately 0.70) while additionally providing automated risk register generation and real-time API integration. Compared with Al Abdulwahid (2025), who achieved 96.1% accuracy using deep learning, the CRIS system provides a key complementary advantage: interpretability through SHAP explanations aligned with *ISO/IEC 27005* audit requirements, which deep learning models typically cannot provide without additional post hoc explanation techniques (Trivedi & Patra, 2025). The standard-oriented AI architecture for information security risk management proposed by Chalyi et al. (2026) similarly introduces AI-ISMS integration but does not empirically evaluate feature selection optimization or demonstrate a functional prototype with CRUD-tested modules. CRIS advances this research direction by bridging the gap between theoretical framework alignment and operational deployment. Furthermore, unlike Boumahdi et al. (2025), who achieved 99.93% accuracy using PSO for binary classification, this study applies PSO to a more complex multiclass risk-level classification problem, making the results more directly applicable to real-world risk registers that require fine-grained threat categorization (Bouzaachane et al., 2025; Calviño et al., 2025).

Table 5. Conventional Approach

Aspect	Conventional Approach	CRIS Approach (ML and ISO 27005)
Identification speed	Days to weeks	Seconds to minutes
Threat coverage	Limited to experts' explicit knowledge	Covers invisible patterns in big data
Consistency	Prone to human bias and fatigue	High, because the process is automated and standardized
Predictive capability	Reactive (based on past incidents)	Proactive (detects attack precursors)
Documentation	Manual, often incomplete	Automatic, structured, and auditable

It should be noted that Table 5 represents a conceptual-empirical comparison framework. The speed metrics ("days to weeks" versus "seconds to minutes") are grounded in the documented average breach detection time of 204 days (Security, 2023) for conventional approaches, contrasted with the CRIS system's measured API response time of 0.47 seconds per prediction. The full end-to-end processing time, from log ingestion to risk register generation, was measured at an average of 12.3 seconds in the functional prototype test, representing a reduction of multiple orders of magnitude compared with manual processes. The remaining qualitative comparisons in Table 5 are supported by the experimental findings and the systematic literature review evidence cited therein. This finding also addresses the criticism raised by Sánchez-García et al. (2015), who stated that 85% of risk assessment tools fail to integrate all assessment substages (Sánchez-García

& Mejía, 2023). In the CRIS system, all substages in the risk identification phase, ranging from threat identification using ML, asset identification from the database, and vulnerability identification from the ontology to the initial likelihood and impact assessment, are carried out automatically and in an integrated manner. The iterative integration between the ML model and the risk management cycle enables continuous improvement. Whenever the model detects a new threat that is later confirmed by the security team, the data can be used for model retraining, thereby improving detection capability over time.

This is consistent with the principle of ISO/IEC 27005:2022, which emphasizes that risk management is not a one-time activity but a continuously repeated cycle. Therefore, this study not only successfully establishes the integration point explicitly but also demonstrates through implementation that the integration is technically feasible, provides operational added value, and aligns with international standard frameworks. This contribution provides a foundation for developing the next generation of cyber risk decision-support systems that are more adaptive, efficient, and accountable.

Advantages of the XGBoost and PSO Combination

The experimental results show that the combination of XGBoost and PSO produced the best performance, with an F1-score of 0.9672. This finding is consistent with recent literature reporting the effectiveness of PSO optimization in XGBoost for cyber threat detection. A study conducted by Sheikhi and Kostakos (2024) developed a malicious website detection model using XGBoost optimized with PSO, successfully achieving 98.42% accuracy in binary classification and an F1-score of 0.984 (Sheikhi, 2024). The main advantages of this combination can be explained through several factors, as follows:

1) PSO capability in feature-space exploration: PSO, through its personal best and global best mechanisms, successfully identified a subset of features that was not only individually relevant but also collectively synergistic. A total of 18 selected features from the 78 initial features were able to maintain and even improve the F1-score compared with the use of all features (0.9642 versus 0.9123).
2) XGBoost robustness against overfitting: XGBoost has internal regularization mechanisms, namely L1 and L2 regularization, that help prevent overfitting even when the model is trained on a relatively small feature subset. This is evidenced by the very small performance difference between cross-validation (0.9672) and the hold-out test (0.9648), namely 0.0024.
3) Suitability for cybersecurity data characteristics: Cybersecurity data often contain nonlinear relationships and complex interactions among features. XGBoost, with its boosting approach that builds trees sequentially to correct residuals, is better able to capture this complexity than RF, which relies on independently constructed trees, and LR, which assumes linear relationships.

Comparison of Feature Selection Techniques

The experimental results in Tables 4.3 and 4.5 provide an empirical basis for conducting an in-depth comparative analysis of the three feature selection techniques tested, namely PSO, AEO, and RFE. Each technique has distinctive characteristics, advantages, and limitations that must be understood contextually to determine its suitability for cyber risk identification applications (Chalyi et al., 2026; Oragwu & Aziz, 2025).

Interpretability through SHAP

The application of SHAP to the XGBoost-PSO model successfully provided the transparency required in the context of risk management. This finding is consistent with Trivedi et al. (2025), who emphasized the need for XAI to ensure stakeholder trust (Trivedi & Patra, 2025). The benefits of SHAP implementation in the CRIS system include the following:

1) The SHAP results show that Protocol Type and Flag Count (SYN) have the highest contributions to DoS attack prediction, which is consistent with cybersecurity expert knowledge.
2) SHAP reveals that Idle Mean, or idle time between connections, has an unexpected contribution to reconnaissance detection, opening opportunities for further research.

3) Every prediction entered into the risk register is accompanied by a SHAP explanation, which can be used as supporting evidence in the information security audit process.

Information Security Policy Recommendations

The results of this study not only provide technical and methodological contributions but also have significant implications for the formulation and refinement of information security policies at both organizational and national levels. These implications are based on empirical findings regarding the most significant features, the superiority of the XGBoost-PSO algorithm, and the effectiveness of ontology in mapping threats to ISO/IEC 27002:2022 controls.

CONCLUSION

Based on the research conducted, several conclusions can be drawn. This study establishes that the integration of the machine learning model is explicitly performed at the Threat Identification stage, which is a subcomponent of the ISO/IEC 27005:2022 Risk Identification process (Clause 8.2). The ML model is designed to automate threat identification by analyzing security log data. The output of the ML model categorizes threats and determines probability values that serve as direct inputs for likelihood determination. The threat identification results generated by the ML model are subsequently contextualized using ontology to produce relevant mappings of assets, vulnerabilities, and controls. Furthermore, this study successfully designed an architecture that integrates the ML model with the ISO/IEC 27005:2022 Risk Identification process through an ontology-based modeling approach. The proposed architecture consists of four layers: the data acquisition layer, which collects and preprocesses security log data; the predictive analytics layer, which executes the XGBoost and PSO models for threat classification; the semantic integration layer, which maps ML outputs to ISO/IEC 27005:2022 concepts; and the presentation layer, which displays the risk register and recommendations through the DSS interface. This study empirically demonstrates that a model that directly predicts risk levels through multiclass classification is more effective than a two-stage approach that separately predicts likelihood and impact.

Future research should address three specific directions for real-world deployment validation. First, the CRIS system should be piloted in a live organizational environment (e.g., a university Security Operations Center [SOC] or financial institution) for a minimum of three months to evaluate operational performance under real network traffic conditions, including concept drift detection sensitivity and false-positive rates in production settings. Second, integration with Security Information and Event Management (SIEM) platforms (e.g., Splunk and IBM QRadar) should be tested to assess API compatibility and the system's ability to operate within established security operations workflows. Third, a user experience study involving certified information security risk managers should be conducted to evaluate the usability and decision-support effectiveness of the CRIS interface, particularly the SHAP (SHapley Additive exPlanations) outputs, in real-world risk governance contexts.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Universitas Nasional for providing academic support, research facilities, and a conducive environment throughout the completion of this study. Appreciation is also extended to researchers, cybersecurity professionals, and relevant stakeholders who contributed valuable insights, knowledge, and resources related to cyber risk identification and information security management.

AUTHOR CONTRIBUTION STATEMENT

Diaz Samba Prayogi contributed to the conceptualization, methodology, data analysis, framework development, and preparation of the original manuscript. Agung Triayudi contributed to supervision, validation, technical guidance, and critical review of the research methodology and manuscript. Both authors collaboratively interpreted the findings, revised the final manuscript, approved the submitted version, and take responsibility for the integrity, accuracy, and accountability of all aspects of the research.

REFERENCES

Akampurira, P., Edozie, E., Sadiq, B. O., & Buhari, M. D. (2026). A Deep Learning-Based User Behavior Analytics Model For Proactive Cyber Threat Detection And Risk Management: A Review. *F1000research*, *15*(674), 674.

Al Abdulwahid, A. (2025). AI-Driven Identification Of Attack Precursors: A Machine Learning Approach To Predictive Cybersecurity. *Computers, Materials & Continua*, *85*(1), 1751–1777. https://doi.org/10.32604/Cmc.2025.066892

Bani, B. Q. (2024). Feature Selection For Iot Botnet Detection Using Equilibrium And Battle Royale Optimization. *Computers & Security*, *147*, 104060. https://doi.org/10.1016/J.Cose.2024.104060

Barlybayev, A., Sharipbay, A., & Shakhmetova, G. (2024). Development Of A Flexible Information Security Risk Model Using Machine Learning Methods And Ontologies. *Applied Sciences*, *14*(21), 9858. https://doi.org/10.3390/App14219858

Baskerville, R., Pries-Heje, J., & Venable, J. R. (2026). Meds: Methodology For Evaluation In Design Science. *European Journal Of Information Systems*, 1–18.

Bisaria, C., Madhubala Kumari, D. S. S., & Patel, B. K. (2026). *Research Methodology: Tools And Techniques*. BR Publications.

Boumahdi, A., Azmi, M., Zegrari, M., Eddermoug, N., & Tazili, S. (2025). Feature Selection In Cybersecurity: A Comparative Study Of Machine Learning Models. *Procedia Computer Science*, *265*, 140–148. https://doi.org/10.1016/J.Procs.2025.07.166

Bouzaachane, K., Guarmah, E. M., & Alnajim, A. M. (2025). Addressing Modern Cybersecurity Challenges: A Hybrid Machine Learning And Deep Learning Approach For Network Intrusion Detection. *Computers, Materials & Continua*, *84*(2), 2391–2410. https://doi.org/10.32604/Cmc.2025.065031

Calviño, B. O., Rodriguez, E., & Costa, J. J. (2025). Enhancing Cybersecurity In Railways: Machine Learning Approaches For Attack Detection. *International Journal Of Critical Infrastructure Protection*, *50*, 100788. https://doi.org/10.1016/J.Ijcip.2025.100788

Chalyi, O., Driaunys, K., & Grigaliūnas, Š. (2026). Standard-Oriented Architecture For AI-Powered Information Security Risk Management. *Electronics*, *15*(6), 1282. https://doi.org/10.3390/Electronics15061282

Figueira, P. T., Bravo, C. L., & & López, J. L. (2020). Improving Information Security Risk Analysis By Including Threat-Occurrence Predictive Models. *Computers & Security*, *88*, 101609. https://doi.org/10.1016/J.Cose.2019.101609

Galliers, R. D., & & Land, F. (1987). Viewpoint: Choosing Appropriate Information Systems Research Methodologies. *Communications Of The ACM*, *30*(11), 901–902. https://doi.org/10.1145/32206.315753

García-Beyaert, S., Bancroft, M. A., Allen, K., & Carriero-Contreras, G. (2015). *Ethics And Standards For The Community Interpreter® - An International Training Tool*. Culture And Language Press.https://Scholar.Google.Com/Scholar?Q=Ethics+And+Standards+For+The+Community+Interpreter®+-+An+International+Training+Tool

Gupta, B. B., Pan, S. H., Gaurav, A., Arya, V., Alhalabi, W., & & Chui, K. (2025). Optimized Hybrid CNN-LSTM-GRU Model For Cyber Attack Detection Using Adaptive Equilibrium Optimization. *Ict Express*. https://doi.org/10.1016/J.Icte.2025.09.006

Hevner, A. R., March, S. T., & Park, J. (2004). Design Science In Information Systems Research. *Mis Quarterly*, *28*(1), 75–105.

Hidayat, D. (2025). Analisis Sistem E-Learning Berbasis Iso 27005:2018 Menggunakan Algoritma Klasifikasi Random Forest Analysis Of An ISO 27005:2018-Based E-Learning System Using The Random Forest Classification Algorithm. *Jurnal Teknologi Dan Informasi (Jati)*, *15*(September), 110–120. https://doi.org/10.34010/Jati.V15i2.16173

ISO/IEC. (2022). *ISO/IEC 27005:2022 Information Security, Cybersecurity And Privacy Protection — Guidance On Managing Information Security Risks (Vol*. International Organization For Standardization. https://www.Iso.Org/Standard/80585.Html

Khoza, D., Ludonga, A., & & Singo, M. (2024). Cyber Risk Management: Frameworks, Strategies, And Case Studies In Cybersecurity. *Zenodo*. https://doi.org/10.5281/Zenodo.17372361

Lubis, M., Luthfi, M. I., Saedudin, R. R., Muttaqin, A. N., & Lubis, A. R. (2026). The Integration Of ISO

27005 And NIST SP 800-30 For Security Operation Center (SOC) Framework Effectiveness In The Non-Bank Financial Industry. *Computers*, *15*(1), 60.

Muheidat, F., Mallouh, M. A., Al-Saleh, O., Al-Khasawneh, O., & & Tawalbeh, L. (2024). Applying AI And Machine Learning To Enhance Automated Cybersecurity And Network Threat Identification. *Procedia Computer Science*, *251*, 287–294. https://doi.org/10.1016/J.Procs.2024.11.112

Negara, B. S. Dan S. (2025). *Lanskap Keamanan Siber Indonesia 2024*.

Oragwu, U., & Aziz, B. (2025). A Machine Learning Approach For Detecting Cybersecurity Vulnerabilities In The Internet Of Medical Things. *Knowledge-Based Systems*, *327*, 114150. https://doi.org/10.1016/J.Knosys.2025.114150

Peffers, K. (2007). A Design Science Research Methodology For Information Systems Research. *Journal Of Management Information Systems*, *24*(3), 45–77.

Pinsonneault, A., & & Kraemer, K. (1993). Survey Research Methodology In Management Information Systems: An Assessment. *Journal Of Management Information Systems*, *10*(2), 75–105. https://doi.org/10.1080/07421222.1993.11518001

Putra, A. P. (2023). Integrated Methodology For Information Security Risk Management Using ISO 27005:2018 And NIST SP 800-30 For Insurance Sector. *International Journal Of Advanced Computer Science And Applications*, *14*(4), 678–687. https://doi.org/10.14569/Ijacsa.2023.0140468

Rose, E. S. (2025). Code Of Ethics For Interpreters: A Comparative Analysis Of Different Professional Standards. *Emily Rose Sophie*.

Sánchez-García, I. D., & Mejía, J. (2022). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, And Validation. *Applied Sciences*, *13*(1), 395. https://doi.org/10.3390/App13010395

Security, I. B. M. (2023). *Cost Of A Data Breach Report 2023*. Ibm.

Sezgin, A., & Ulaş, M. (2025). Multi-Objective Feature Selection For Intrusion Detection Systems: A Comparative Analysis Of Bio-Inspired Optimization Algorithms. *Sensors*, *25*(19), 6099. https://doi.org/10.3390/S25196099

Sheikhi, S. (2024). Safeguarding Cyberspace: Enhancing Malicious Website Detection With Pso Optimized Xgboost And Firefly-Based Feature Selection. *Computers & Security*, *142*, 103885. https://doi.org/10.1016/J.Cose.2024.103885

Trivedi, R., & Patra, S. (2025). Data-Centric Explainable Artificial Intelligence Techniques For Cyber-Attack Detection In Microgrid Networks. *Energy Reports*, *13*, 217–229. https://doi.org/10.1016/J.Egyr.2024.11.075