AI-Based Compliance Policy Recommender

Aditya A Ranaware[1], Nandkumar A Kaldhone[2], Sahil N Shinde[3], and Pranjal D Sahane[4]
[5]Prof. Saba Chaugule
[1,2,3,4]*Student, Department of Computer Engineering, P. K. Technical Campus, Pune*
[5]*Professor Department of Computer Engineering, P. K. Technical Campus, Pune*

***Abstract*— In the current digital landscape, organizations are required to implement structured information security policies to protect sensitive data and comply with international standards such as ISO 27001. However, developing these policies manually is a complex, time-consuming process that requires domain expertise and a deep understanding of regulatory frameworks. Many small and medium-sized organizations struggle to create and maintain proper compliance documentation due to a lack of resources and technical knowledge.**

This paper presents an AI-Based ISO 27001 Compliance Policy Generation System that automates the creation of information security policies based on organizational inputs. The system collects key details such as industry type, system environment, data storage methods, and sensitivity level, and dynamically maps them to relevant ISO 27001 controls. A structured policy engine is designed using predefined rule-based logic and control mappings to generate context-aware and standardized policy documents.

The proposed system is implemented using a Flask-based backend, a MySQL database for data management, and a responsive web interface for user interaction. It also includes automated PDF generation for producing professionally formatted policy documents. By reducing manual effort and ensuring consistency with ISO standards, the system improves compliance readiness and simplifies the policy creation process.

The results demonstrate that the system can generate accurate, structured, and industry-relevant policy documents dynamically, making it a practical solution for organizations seeking efficient and reliable compliance management.

Index Terms*— *Artificial Intelligence (AI), ISO 27001, Information Security Policy, Compliance Automation, Policy Generation System, Information Security Management System (ISMS), Rule-Based System, Data Security.

I. INTRODUCTION

In the modern digital era, organizations across various industries generate and manage large volumes of sensitive data, making information security a critical concern. To protect this data and ensure regulatory compliance, organizations are required to implement structured policies aligned with international standards such as ISO/IEC 27001. These policies define the necessary controls and practices required to maintain the confidentiality, integrity, and availability of information. However, developing such policies manually is a complex and resource-intensive process that requires domain expertise, technical knowledge, and continuous monitoring of evolving standards.

Traditional approaches to compliance management rely heavily on manual documentation, expert consultation, and interpretation of lengthy regulatory texts. This process is time-consuming, error-prone, and often inconsistent, particularly for small and medium-sized enterprises that lack dedicated compliance teams. As regulatory requirements continue to evolve across industries, there is a growing need for an automated and intelligent system that can simplify policy creation while ensuring adherence to established standards.

To address these challenges, this paper presents an AI-Based ISO 27001 Compliance Policy Generation System that automates the creation of information security policies based on organizational inputs. The system collects key parameters such as industry type, system environment, data storage methods, and sensitivity level, and dynamically maps them to relevant ISO 27001 controls. Unlike traditional recommendation systems, the proposed solution generates complete and structured policy documents using a rule-based policy engine, ensuring consistency and alignment with compliance requirements.

The system is developed using a Flask-based backend, a MySQL database for managing user and company data, and a web-based interface for user interaction. It also integrates automated PDF generation to produce professional and ready-to-use

policy documents. By reducing manual effort and providing context-aware policy generation, the system enhances compliance readiness and offers a practical solution for organizations aiming to implement effective information security management practices.

II. LITERATURE REVIEW

Researchers have increasingly explored the application of Artificial Intelligence (AI) and Natural Language Processing (NLP) in automating compliance management and policy analysis. Early studies focused on transforming complex regulatory documents into structured and machine-readable formats to simplify interpretation and reduce manual effort. In [1], an automated regulatory document analysis model was proposed using NLP techniques to extract key obligations and compliance clauses from large policy documents. This approach helped reduce human errors and enabled efficient handling of regulatory requirements.

Further advancements in this domain introduced machine learning-based classification techniques for compliance identification. In [2], a compliance management framework was developed using algorithms such as Support Vector Machine (SVM) and TF-IDF feature extraction to classify organizations under relevant regulatory standards based on their operational characteristics. Similarly, research presented in [3] utilized semantic similarity and ontology-based models to map business activities to compliance requirements, improving the accuracy of policy relevance identification.

In addition, intelligent risk assessment systems have been explored to enhance compliance monitoring. In [4], deep learning techniques were applied to analyze organizational data and identify potential compliance risks, providing automated recommendations for mitigation. More recent work in [5] demonstrated the use of advanced NLP models such as BERT to extract compliance entities and relationships from regulatory documents, achieving higher precision compared to traditional methods.

While these studies highlight the effectiveness of AI and NLP in compliance automation, most existing systems are primarily focused on policy classification, document analysis, or recommendation of regulatory frameworks. They do not provide a complete solution for generating structured compliance policies tailored to specific organizational needs.

The initial concept of this work was presented in a previously published study, which focused on recommending compliance policies using AI-based techniques. Building upon this foundation, the current system extends the approach by introducing a dynamic policy generation mechanism aligned with ISO/IEC 27001 standards. Unlike earlier methods, the proposed system not only identifies relevant controls but also generates complete, structured policy documents based on user inputs. This enhancement bridges the gap between compliance recommendation and practical policy implementation, providing a more comprehensive and usable solution for organizations.

III. PROPOSED METHODOLOGY

The proposed AI-Based ISO 27001 Compliance Policy Generation System is designed to automate the creation of structured information security policies based on organizational inputs. Unlike traditional compliance systems that only recommend regulatory frameworks, the proposed solution focuses on generating complete and context-aware policy documents aligned with ISO/IEC 27001 standards. The system combines rule-based logic with predefined control mappings to ensure accurate and consistent policy generation.

A. System Overview

The system accepts key organizational inputs such as company name, industry type, system environment, data storage methods, and sensitivity level of the data handled. These inputs are processed by the policy engine, which dynamically maps them to relevant ISO 27001 controls. Based on this mapping, the system generates structured policy content, ensuring that each policy aligns with standard compliance requirements. The generated output is presented in a professional document format and can be exported as a PDF.

B. Policy Engine and Control Mapping

The core component of the system is a rule-based policy engine designed using a structured JSON format. The engine contains predefined mappings between organizational attributes and ISO 27001 controls. For example, organizations handling

sensitive data are mapped to stricter access control and data protection policies, while cloud-based systems are associated with network security and operational controls. This approach ensures that the generated policies are relevant, accurate, and aligned with industry standards.

C. Input Processing and Customization

The system supports both automatic and user-defined inputs. Based on the selected industry, default system type, storage method, and sensitivity level are automatically determined. Additionally, users are provided with customization options to override these values, allowing greater flexibility and control over policy generation. This hybrid approach ensures both ease of use and adaptability to specific organizational needs.

D. System Architecture

The architecture of the system consists of three main layers:

1. Frontend Layer: A user-friendly interface developed using HTML, CSS, and Bootstrap, providing forms and dashboards for user interaction.
2. Backend Layer: A Flask-based application responsible for processing inputs, executing the policy engine, and managing system logic.
3. Database Layer: A MySQL database used to store user data, company information, and generated policy records.

These layers interact through well-defined modules, ensuring modularity, scalability, and efficient data flow within the system.

E. Workflow

The overall workflow of the system is as follows:

1. User Authentication: The user registers or logs into the system.
2. Input Submission: The user enters company details and system-related inputs.
3. Data Processing: The system evaluates inputs and applies rule-based logic for control mapping.
4. Policy Generation: The policy engine generates structured policy content aligned with ISO 27001 controls.
5. Output and Export: The generated policy is displayed on the dashboard and can be downloaded as a PDF document.

This methodology ensures that the system delivers accurate, dynamic, and standardized policy documents while minimizing manual effort and reducing the complexity of compliance management.

IV. ISMS COMPLIANCE BRIEFING

An Information Security Management System (ISMS) is a systematic framework used to manage and protect an organization's sensitive information. It consists of a set of policies, procedures, and controls designed to ensure the confidentiality, integrity, and availability (CIA) of data. ISMS provides a structured approach for identifying security risks, implementing appropriate safeguards, and continuously improving security practices within an organization.

ISO/IEC 27001 is the internationally recognized standard for establishing, implementing, maintaining, and improving an ISMS. It defines a comprehensive set of security controls that organizations must follow to protect information assets and maintain compliance with regulatory requirements. The standard adopts a risk-based approach, allowing organizations to identify potential threats, assess vulnerabilities, and apply suitable controls to mitigate risks effectively.

In the context of the proposed AI-Based ISO 27001 Compliance Policy Generation System, ISMS plays a crucial role in structuring and validating the generated policies. The system incorporates ISMS principles by mapping organizational inputs—such as industry type, system environment, data storage methods, and data sensitivity—to relevant ISO 27001 controls. These controls form the foundation for generating structured and compliant information security policies.

For example, organizations handling sensitive or confidential data are required to implement stricter access control, data protection, and monitoring mechanisms. Similarly, systems operating in cloud environments require enhanced network security and operational controls. The proposed system dynamically identifies such requirements and integrates them into the generated policy document, ensuring alignment with ISMS standards.

By automating the mapping of organizational inputs to ISO 27001 controls and generating structured policies, the system simplifies the implementation of ISMS practices. It enables organizations to achieve better compliance readiness, reduce manual effort, and maintain consistency in their information security policies.

V. CHALLENGES AND LIMITATIONS

While the proposed AI-Based ISO 27001 Compliance Policy Generation System provides an effective solution for automating policy creation, several challenges and limitations were encountered during its development and implementation.

A. Standard Interpretation Complexity

ISO/IEC 27001 consists of a comprehensive set of controls and guidelines that require proper interpretation to ensure accurate implementation. Translating these standards into structured and rule-based logic for automated policy generation is a challenging task, as it requires careful mapping between organizational inputs and corresponding security controls.

B. Rule-Based System Limitations

The current system utilizes a rule-based policy engine for generating policies. Although this approach ensures consistency and reliability, it may lack the adaptability of advanced AI models. The system depends on predefined mappings, and any missing or incomplete rule definitions can affect the accuracy of generated policies.

C. Limited Domain Customization

While the system supports multiple industries and input variations, it may not fully capture highly specific or niche industry requirements. Certain sectors, such as healthcare or finance, may require additional domain-specific policies that are not fully covered in the current implementation.

D. Evolving Compliance Standards

Information security standards and regulatory frameworks are continuously updated. Maintaining an up-to-date system requires regular updates to the policy engine and control mappings to ensure alignment with the latest ISO standards and compliance requirements.

E. Practical Deployment Constraints

The system is currently developed as a standalone web application. Integrating it with enterprise-level environments, existing compliance tools, or large-scale infrastructure may require additional enhancements in terms of scalability, security, and interoperability.

Despite these limitations, the proposed system demonstrates a practical and efficient approach to automating policy generation and significantly reduces the complexity involved in compliance management.

VI. RESULTS AND DISCUSSION

The proposed AI-Based ISO 27001 Compliance Policy Generation System was implemented and tested using various organizational input scenarios to evaluate its performance and effectiveness. The system was provided with inputs such as industry type, system environment, data storage methods, and data sensitivity levels to generate context-aware policy documents.

The results demonstrate that the system successfully generates structured and comprehensive information security policies aligned with ISO/IEC 27001 standards. The generated documents include well-defined sections such as purpose, scope, definitions, applicable standards, control-based policies, roles and responsibilities, compliance requirements, and review mechanisms. This ensures that the output is not only complete but also follows a standardized and professional format suitable for real-world use.

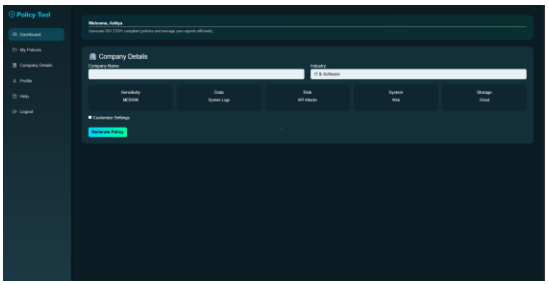
The dynamic nature of the system allows it to adapt policy content based on user inputs. For example, organizations dealing with high-sensitivity data receive stricter access control and monitoring policies, while cloud-based systems include enhanced network security and operational controls. This demonstrates the system's ability to generate context-aware and relevant policies rather than static or generic outputs.

The system also provides a user-friendly dashboard interface where users can input details, view generated policies, and download them as professionally formatted PDF documents. The integration of PDF generation enhances usability by allowing organizations to directly utilize the generated documents for compliance and documentation purposes.

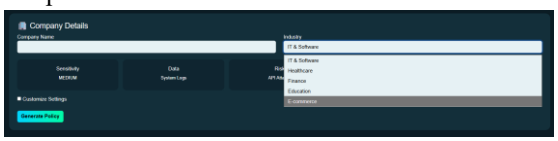
Overall, the results indicate that the system significantly reduces the time and effort required for manual policy creation while maintaining consistency and alignment with ISO standards. The implementation validates the effectiveness of the

rule-based policy engine and highlights its potential as a practical tool for compliance automation in modern organizations.

1. Dashboard



2. Input Form



3. Generated Policy

4. ISO Controls Section

VII. FUTURE WORK

Although the proposed system effectively automates the generation of ISO/IEC 27001 compliant policy documents, there are several opportunities for further enhancement and expansion. Future work can focus on integrating advanced Artificial Intelligence techniques, such as Natural Language Processing (NLP) and machine learning models, to improve the adaptability and intelligence of the policy generation process.

The system can be extended to support additional compliance frameworks such as GDPR, HIPAA, and PCI-DSS, enabling broader applicability across different regulatory environments. Incorporating real-time updates of compliance standards would ensure that the generated policies remain aligned with the latest regulatory requirements.

Another potential improvement is the integration of risk assessment modules, which can analyze organizational vulnerabilities and recommend policies based on risk levels. Additionally, the system can be enhanced by providing an interactive policy editing feature, allowing users to customize and refine generated policies according to specific organizational needs.

The deployment of the system as a scalable cloud-based solution and its integration with enterprise systems can further improve usability and adoption in real-world environments. These enhancements would transform the system into a comprehensive compliance management platform capable of supporting organizations in maintaining continuous regulatory alignment.

VIII. CONCLUSION

The increasing complexity of information security requirements and regulatory standards has created a strong need for automated solutions that can assist organizations in maintaining compliance efficiently. This paper presented an AI-Based ISO 27001 Compliance Policy Generation System that simplifies the process of creating structured and standardized information security policies based on organizational inputs.

The proposed system utilizes a rule-based policy engine combined with ISO 27001 control mapping to generate context-aware and industry-relevant policy documents. By accepting inputs such as industry type, system environment, data storage methods, and sensitivity levels, the system dynamically produces policies that align with established information

security standards. The integration of a user-friendly interface, database management, and automated PDF generation enhances the practicality and usability of the solution.

The results demonstrate that the system significantly reduces the time and effort required for manual policy creation while ensuring consistency, accuracy, and compliance with ISO/IEC 27001 guidelines. The system not only supports organizations in improving their compliance readiness but also provides a structured approach to implementing information security management practices.

In conclusion, the proposed solution highlights the potential of intelligent automation in the domain of compliance management. It serves as a practical and scalable tool that can assist organizations in adopting standardized security policies, thereby contributing to improved data protection and governance in modern digital environments.

ACKNOWLEDGMENT

This research paper would not have been possible without the valuable guidance and encouragement of Prof. Saba Chaugule, whose advice and insights greatly contributed to the completion of this work. We would also like to express our sincere gratitude to all the professors of the Department of Computer Engineering, P. K. Technical Campus, for their continuous support and for providing us the opportunity to work on this research project titled "AI-Driven Control Mapping and Evidence Analyzer." Their motivation and academic environment have been instrumental in shaping our understanding and efforts throughout this study.

REFERENCES

[1] P. K. Sharma and S. Gupta, "Automated Extraction of Regulatory Obligations Using NLP," *IEEE Access*, vol. 8, pp. 124320–124330, 2020.

[2] R. K. Singh and A. Verma, "Machine Learning-Based Compliance Classification System for Data Protection Regulations," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 6, pp. 1589–1597, 2021.

[3] M. S. Ahmed, L. T. Nguyen, and K. Wang, "Ontology-Driven Framework for Policy Mapping in Regulatory Compliance," *IEEE Access*, vol. 9, pp. 102445–102458, 2021.

[4] J. Lee and D. Kim, "Deep Neural Network Approach for Compliance Risk Assessment," *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 85–94, 2022.

[5] S. R. Patel and M. Banerjee, "BERT-Based Framework for Regulatory Policy Extraction and Recommendation," *IEEE Access*, vol. 10, pp. 20351–20363, 2022.

[6] A. A. Ranaware, N. A. Kaldhone, S. N. Shinde, and P. D. Sahane, "AI-Based Compliance Policy Recommender," 2025.