VerifyWise: A Modular AI Governance Platform for Data-Driven Compliance Management

Mohammad Khalilzadeh
Faculty of Technology and Engineering
Raja University
Ghazvin, Iran
0009-0005-5540-6360

Firouzeh Razavi
Faculty of Technology and Engineering
Raja University
Ghazvin, Iran
f.razavi@raja.ac.ir

Abstract—**The advancing integration of artificial intelligence (AI) into mission-critical domains demands governance frameworks that go beyond static rules and manual auditing. This paper presents VerifyWise, a modular platform engineered for data-driven AI compliance management. Rather than relying on speculative machine learning or fuzzy logic components, VerifyWise focuses on concrete, implemented functionalities: structured risk registers, policy-to-control mapping interfaces, multi-framework compliance tracking, vendor risk assessments, and evidence management. The platform enables comprehensive risk capture and compliance monitoring across multiple governance standards (e.g. EU AI Act, ISO/IEC 42001), providing unified workflows for risk assessment, control implementation, third-party oversight, and audit reporting. By examining the system's architecture, data model, and modules, we demonstrate how a structured, modular approach supports transparency, adaptability, and scalability in AI governance. While advanced analytics modules (e.g. predictive risk scoring) remain future work, the current implementation offers a robust foundation for deploying practical compliance systems aligned with international standards such as ISO/IEC 42001:2023.**

Keywords—AI Governance, Compliance Management, Risk Assessment, Policy Mapping, Data-Driven Analytics, Intelligent Systems

I. INTRODUCTION

The rapid adoption of AI across industrial, financial, healthcare, and governmental domains has intensified the demand for robust mechanisms that ensure accountability, transparency, and compliance with ethical and regulatory frameworks. As AI systems increasingly influence high-stakes decision-making, governing their development, deployment, and operations has become a central concern for policymakers and practitioners. Emerging standards such as the European Union Artificial Intelligence Act (EU AI Act) and the ISO/IEC 42001 AI Management System Standard emphasize the need for structured risk management, continuous monitoring, and auditable documentation throughout the AI lifecycle. However, existing compliance solutions often rely on static, rule-based procedures and ad-hoc manual audits, which limit scalability and adaptability in complex, data-intensive environments.

To address these challenges, the concept of intelligent compliance systems has gained attention, leveraging techniques like machine learning (ML), pattern recognition, and soft computing to automate governance workflows. Such systems are envisioned to identify latent risk patterns, dynamically assess the severity and likelihood of non-compliance, and provide adaptive decision support. These approaches enable organizations to transition from reactive, post-incident auditing to proactive, continuous governance, thereby enhancing trust, efficiency, and resilience across AI-driven infrastructures. However, many purported "intelligent" solutions remain theoretical or only partially implemented in practice.

In this context, we introduce VerifyWise, an open-source AI governance platform that emphasizes truthful, data-driven compliance management over speculative AI automation. VerifyWise automates risk evaluation, policy-to-control mapping, evidence tracking, and vendor oversight through modular services and structured data analytics. Its implementation demonstrates how a well-designed architecture, incorporating risk registers, control mapping, and lifecycle metadata, can support transparent and adaptive governance of AI systems without relying on unproven predictive algorithms. Unlike traditional governance tools, VerifyWise incorporates continuous risk scoring based on defined criteria, an intuitive policy-to-control mapping interface for aligning internal policies with external requirements, and evidence-backed evaluation of compliance outcomes. The primary objectives of this study are threefold:

- **To analyze the current implementation of VerifyWise as a working model of modular AI compliance management.** We describe the platform's architecture and modules as a practical realization of an intelligent governance system (focusing on implemented features rather than hypothetical AI capabilities).

- **To demonstrate the role of structured data and analytics in identifying governance and risk patterns.** We show how the platform's risk registers and compliance dashboards facilitate visibility into risk distributions and compliance gaps, enabling data-driven insights for decision-makers (e.g. trend analyses of risk levels and control status).
- **To illustrate how VerifyWise's design principles enable interpretability and human oversight in compliance scoring under uncertainty.** We highlight features like rule-based risk level calculation and approval workflows that ensure human experts remain in the loop for qualitative judgments (e.g. assessing "high" vs. "medium" risk with context).

By aligning our analysis with emerging international standards for AI governance, this work contributes to the discourse on adaptive and explainable compliance mechanisms. The proposed approach showcases the potential of VerifyWise's architecture to support scalable, trustworthy AI governance across diverse ecosystems and applications, while remaining grounded in currently available capabilities.

II. Background and Related Work

The integration of AI into high-risk and safety-critical domains has prompted the emergence of AI governance as a formal discipline aimed at ensuring AI systems operate within defined ethical, regulatory, and organizational boundaries. Contemporary frameworks such as the EU AI Act and ISO/IEC 42001:2023 provide baseline requirements for establishing AI management systems, focusing on documentation, risk management, and continuous monitoring. These standards, however, primarily define what organizations should govern, rather than how to operationalize governance efficiently through technology. This gap has motivated development of data-driven compliance systems capable of dynamically interpreting and enforcing requirements in real time.

Recent research in AI governance automation explores computational methods to address this challenge. Early work on governance ontologies and rule-based audit frameworks emphasized symbolic representations and human oversight (e.g. expert-defined rules) but struggled with scalability and ambiguity in complex scenarios. The introduction of machine learning into compliance tooling has been proposed as a paradigm shift from manual documentation to predictive, self-adapting governance. For example, Gasser et al. (2020) and Raji et al. (2022) illustrated how ML models might detect latent risk correlations or compliance anomalies across large datasets. Complementing data-driven approaches, soft computing techniques (fuzzy logic, neuro-fuzzy systems, etc.) have shown promise for handling uncertainty in risk assessments, by translating qualitative judgments (e.g. "medium likelihood") into quantitative reasoning (Zadeh, 1965; Chen et al., 2021). Hybrid frameworks that combine ML and fuzzy inference (e.g. ANFIS) have been explored in academic contexts for risk management and decision support (Hossain et al., 2022; Zhou et al., 2023), aligning with the growing emphasis on explainability in AI governance.

Several practical platforms have also emerged to integrate AI-driven insights into compliance management. Industry solutions like IBM's *Watson OpenScale*, Google's Responsible *AI Toolkit*, and Microsoft's *AI Compliance Manager* incorporate AI-based bias detection or policy mapping, but these tools are largely proprietary and domain-specific. Academic prototypes such as *TrustLens* (Patel et al., 2022) and *AI-RiskMiner* (Jain et al., 2023) have demonstrated data mining and risk prediction techniques (e.g. decision trees, ensemble models) for compliance data[18]. However, these implementations often target narrow use cases and lack the modularity to scale across diverse organizational contexts or to integrate the human interpretability needed in governance processes.

Against this backdrop, VerifyWise is distinct in that it is an **open-source**, **modular**, and **extensible** platform operationalizing AI governance through practical automation rather than purely experimental intelligence. It aims to unify core compliance activities, risk tracking, control implementation, documentation and oversight, within a single system. While inspired by the vision of hybrid intelligence from prior works, VerifyWise's current design emphasizes solid architectural foundations (e.g. layered services, unified data schema, user workflows) over fully autonomous AI. This approach bridges the gap between theoretical governance frameworks and real-world deployment by providing a reproducible system that organizations can adopt and incrementally enhance with intelligent features. In the following sections, we detail the system architecture and functionalities of VerifyWise, highlighting how its design addresses known limitations of earlier solutions (e.g. lack of scalability and interpretability) and aligns with the principles of adaptive, trustworthy AI governance.

III. System Architecture and Implementation

System Overview: VerifyWise is implemented as a modular, data-driven AI governance framework designed to facilitate continuous risk assessment, compliance monitoring, and lifecycle traceability across AI projects. The platform's architecture follows a layered, service-oriented design with three principal subsystems: (1) the **Client Interface Layer**, (2) the **Backend Service Layer**, and (3) the **Intelligence & Fairness Layer**. This modular design allows independent scaling of components, technology-agnostic deployment, and integration with external enterprise systems via APIs.

Client Interface Layer: The front-end of VerifyWise is a web-based interface built with React and TypeScript, providing an intuitive environment for structured compliance data management. Through dynamic forms, tables, and dashboards, users can create and edit projects, log risks, define controls, and upload evidence documentation. Dedicated modules in this layer support key governance functions: for example, a **Risk Management** module for entering and reviewing project risk entries, **a Framework/Compliance Tracker** for navigating regulatory requirements (like sections, controls, and sub-controls), and a **Policy Manager** for drafting and managing internal governance policies. Workflow and task-management components allow governance teams to assign ownership, manage approval stages, and track mitigation or review deadlines in real time.

A notable feature of the client layer is the **policy-to-control mapping** interface, which allows users to align internal organizational policies with external regulatory frameworks. This ensures traceability from high-level AI lifecycle phases and policies down to specific risk categories and evidence items, creating a consistent compliance ontology throughout the system. For instance, a user can tag a corporate policy (e.g. "AI Model Validation Procedure") with relevant external requirements (e.g. EU AI Act Article on transparency), and map it to control implementations in projects, thereby maintaining a live link between policy documents and practical compliance controls. This capability is essential for auditability and change management, as it clearly shows how each internal guideline fulfills or relates to regulatory mandates.

Backend Service Layer: The backend of VerifyWise is built with Node.js and Express, exposing a RESTful API that serves as the operational core of the platform. This layer handles all business logic and data persistence for compliance activities. Key services include endpoints for project and asset management, risk register operations, control status updates, vendor assessments, and evidence retrieval. The backend organizes data in a relational database (PostgreSQL), with structured schemas for each core entity, projects, risks, controls, vendors, evidence, etc., enforcing referential integrity and version tracking. Such a unified data model ensures consistency and makes it feasible to query or aggregate compliance information across the organization (for example, generating a summary of all "High" severity risks across all projects, or pulling all evidence files related to a specific control).

The backend layer adopts a modular microservice-inspired architecture: each major functional domain (risk management, vendor management, policy management, etc.) is encapsulated, improving scalability and maintainability. Integration capabilities are built in, for example, VerifyWise provides webhook integration with communication tools like Slack to automate notifications. This means when certain events occur (e.g. a risk entry is flagged as overdue or a control implementation is marked Completed), the system can automatically send alerts to designated channels or personnel. These event-driven automations enable **semi-autonomous compliance operations** (routine follow-ups and reminders are handled by the system) while maintaining human oversight for critical decisions. The backend also maintains an audit log of activities (events such as user modifications, reviews, and approvals), supporting traceability and forensics.

Another important backend function is managing the compliance knowledge base that underpins multi-framework support. VerifyWise comes pre-loaded with data models for major AI governance frameworks (EU AI Act, ISO 42001, ISO 27001). Each framework's requirements (sections, clauses, controls) are represented in the database, allowing the platform to track an organization's compliance status against each item. The system also supports mapping between related controls across frameworks (and the roadmap includes expanding these cross-mappings). By linking evidence documents and risk records to specific regulatory clauses or standards, the backend enables more advanced analysis such as identifying common problem areas or performing gap assessments when new regulations emerge. This structured linkage of data is essential for any future data mining or intelligent analysis modules, providing a rich substrate of labeled governance data (e.g. every risk is tied to a category and maybe a regulation reference).

Intelligence & Fairness Layer: The third layer of the architecture provides analytical capabilities, focusing currently on AI model bias and fairness evaluation. This layer is embodied in a **Bias and Fairness Module**, implemented in Python and accessible via Jupyter notebooks and APIs. The module allows auditors and data scientists to evaluate trained AI models for bias metrics and fairness compliance. For example, using this module, one can run tests on an AI system (such as an NLP model) to measure disparate impact or performance differences across demographic groups, aligning with ethical AI guidelines. The results from these analyses (e.g. bias metrics) can be fed back as evidence into the compliance system, for instance, attaching a bias audit report to a risk item or a control requirement pertaining to fairness. By integrating this module, VerifyWise ensures that **trust and fairness** considerations are built into the governance process (not just security and process compliance). Indeed, fairness assessment is treated as a first-class citizen in the platform's design, reflecting the emphasis on ethical AI principles.

Beyond the bias analysis component, the intelligence layer is designed to be extensible for future data-driven analytics. In its current state, it provides the **foundation** for more advanced risk analytics and intelligent monitoring, though these are in early stages. The architecture anticipates that ML models could be trained on the accumulated compliance data (risks, incidents, control outcomes) to predict potential compliance failures or to prioritize risk mitigation efforts. Similarly, the structure could accommodate a fuzzy logic engine to handle qualitative inputs (e.g. linguistic risk ratings like "medium severity") for more nuanced risk scoring. While these features are not fully implemented, hooks for such capabilities exist in the platform. For example, the system already automatically calculates a risk level from user-provided severity and likelihood inputs using a standardized risk matrix[31], which is a deterministic approximation of what a fuzzy inference system might do. This risk scoring approach ensures consistency and explainability: the combination of Likely + High severity yields a defined outcome (say, High risk), which is transparent to users and based on policy. This emphasis on explainable risk scoring upholds the platform's principle that any "intelligence" in compliance must remain interpretable and accountable to human experts.

In summary, VerifyWise's architecture emphasizes a balance between automation and human governance. The client and backend layers implement **hard-coded, rule-based intelligence**, e.g. risk formulas, workflow rules, notification triggers, that capture best practices in compliance management. The intelligence layer adds a specialized analytical toolkit (currently for fairness checks) and provides a pathway to integrate more sophisticated intelligent system components over time. This layered design ensures that even without full machine learning integration, the platform delivers immediate value through structured data management and partial automation, while remaining future-proof for deeper intelligent features.

Design Principles: The development of VerifyWise has been guided by three key design principles, drawn from international AI governance frameworks and industry best practices:

- **Transparency and Explainability:** All risk scores, compliance statuses, and recommendations produced by the system are derived from traceable rules or documented criteria, ensuring that outputs can be audited and understood by humans. For example, if a project's overall compliance status is 78%, the underlying data (which controls are implemented vs. pending) and calculation method are visible to the user. Likewise, risk levels are computed from clearly defined impact and likelihood ratings, rather than opaque algorithms. This focus on transparency supports accountability and builds user trust in the platform's guidance.

- **Adaptability and Scalability:** The platform's modular, service-oriented architecture allows domain-agnostic deployment and easy integration with enterprise IT environments. VerifyWise is designed to support multiple regulatory frameworks in parallel and can be extended to new ones (e.g. upcoming national AI regulations or industry-specific standards) without a rewrite of core systems. New modules (for instance, integrating an incident management system or a training module) can be added as separate services. This adaptability ensures that the system can scale with an organization's governance needs and evolve as the regulatory landscape changes, a critical requirement given the fast-moving nature of AI policy.
- **Trust and Fairness by Design:** The platform embeds considerations of ethical AI from the ground up, for instance, through the Bias & Fairness Module and the inclusion of fairness-related checkpoints in assessments. Every compliance assessment category (such as AI Ethics in the Assessment Tracker) includes questions on fairness, transparency, and human oversight, emphasizing that technical compliance alone is not sufficient. By integrating tools to measure and document fairness, and by ensuring human experts review qualitative judgments, VerifyWise keeps the compliance process ethically grounded and interpretable. Any future AI-driven features will be subject to the same requirement of producing explainable outputs that align with governance principles.

IV. Methodology: VerifyWise Compliance Workflow

Instead of relying on unverifiable predictive algorithms, VerifyWise employs a structured methodology to manage AI system compliance. This methodology mirrors established governance processes, enhanced by the platform's automation and data tracking features. The key steps in a typical VerifyWise-driven compliance workflow are as follows:

1. **Framework Setup and Policy Alignment:** The process begins with configuring the relevant governance frameworks and organizational policies in the system. VerifyWise supports multiple standards (e.g. EU AI Act, ISO 42001, ISO 27001) out-of-the-box. Compliance officers select the applicable framework(s) for an AI project, and use the **Policy Manager** to input internal policies or guidelines. Each policy can be tagged or mapped to specific regulatory requirements, establishing traceability between internal rules and external obligations. This ensures the project's compliance efforts are aligned with both company policy and law from the start.
2. **Initial Assessment and Gap Analysis:** Using the **Assessment Tracker** module, the team conducts a structured evaluation of the AI system against the chosen framework. The assessment is organized into categories (e.g. Data Governance, Fairness, Technical Robustness) with predefined questions derived from the framework. Team members answer each question and attach evidence documents as needed (design documents, test results, etc.), all within the platform. The tool provides progress indicators for each section and enforces an approval workflow for completed answers. Upon completion, VerifyWise highlights which requirements are fully met and where gaps exist, giving a baseline compliance score. This step helps identify areas of non-compliance early on.
3. **Risk Register and Analysis:** In parallel with the assessment, the Risk Management module is used to log identified risks. Each risk entry captures details such as a descriptive name, category (e.g. technical, operational, compliance), potential impact, and likelihood. VerifyWise prompts users to quantify the risk's severity and probability with standardized qualitative levels (e.g. Severity: High, Likelihood: Possible). The system then **automatically calculates an overall risk level** by combining these factors according to a risk matrix. For example, a Likely and High severity risk might be categorized as Critical, whereas Unlikely and Medium severity might result in Moderate. This automation provides consistency in risk scoring across the organization. All recorded risks are visible in a project's risk dashboard, which also aggregates summary metrics (total risks, distribution by severity, mitigation status, etc.) to facilitate analysis. Users can easily see, for instance, if most risks cluster in a certain category like Data Privacy, indicating where additional controls or resources may be needed.
4. **Mitigation Planning and Control Implementation:** For each identified risk or compliance gap, appropriate controls or mitigation actions are planned. The Compliance Tracker module comes into play here, listing all required controls (from the selected framework) and their implementation status. Project managers assign each control to an owner and set due dates. The platform supports breaking down controls into more granular sub-controls or tasks if needed, each of which can be marked as Not Started, In Progress, or Done to track implementation progress. As controls are implemented, team members upload or link evidence (policies, configuration files, test reports, etc.) directly to the corresponding control item. VerifyWise's evidence management ensures that every compliance action is backed by verifiable documentation, evidence files are stored and indexed in the Evidence Center, and can be linked to multiple relevant items (e.g. the same document may serve as evidence for both a

risk mitigation and a control requirement). The system maintains version history of evidence and who approved what, creating an audit trail. When a control implementation is completed and documented, it can go through a review workflow: a designated Reviewer/Auditor verifies the evidence and marks the control as verified (or provides feedback for further action). This step-by-step mitigation and control implementation process ensures that identified risks are systematically addressed and that compliance gaps are closed in a controlled manner.

5. **Vendor Assessment and Third-Party Risk Management:** Modern AI systems often rely on third-party components or services (such as cloud AI APIs, pretrained models, or data providers). VerifyWise incorporates a **Vendor Management** module to handle these third-party risks. Governance teams catalog all external AI vendors or suppliers in a centralized registry, noting the services they provide and their criticality to the project. For each vendor, an assessment is conducted (similar to the project assessment) focusing on vendor-specific risks: security practices, regulatory compliance, past incidents, etc.. The platform allows assigning a risk level to each vendor (Very Low to Very High) and tracks mitigation plans for vendor-related risks (for example, requiring the vendor to obtain certain certifications or setting up fallback providers). Vendors are associated with the projects they impact, linking vendor risk entries to overall project risk. Regular reviews can be scheduled, the system can remind the organization to re-evaluate a critical vendor quarterly, for instance. This integrated approach to vendor risk ensures that supply chain and third-party dependencies are not overlooked in the compliance program, addressing requirements in regulations (the EU AI Act, for example, mandates oversight of AI providers and suppliers).

6. **Continuous Monitoring and Reporting:** VerifyWise supports ongoing monitoring through both its dashboard visualizations and automated reports. Project dashboards update in real time as team members update risk statuses or control implementations, providing a live view of compliance posture. To communicate status to stakeholders, the **Reporting** module can generate comprehensive audit reports on demand. These reports can cover various perspectives, for example, a **Risk Management Report** summarizes all risks, their ratings, and mitigation progress, whereas a **Compliance Report** details the implementation status of each control and any gaps, and a **Vendor Assessment Report** documents third-party compliance and performance. Reports are customizable and can be output in PDF, Word, or HTML formats for easy sharing. Importantly, because the data is centralized, the reports provide an integrated picture (e.g. linking specific high risks to the controls that mitigate them and the evidence supporting those controls). The platform's event logging means that reports also include an audit trail of actions taken over the period. Continuous monitoring is further supported by features like alerting (email/Slack notifications for approaching deadlines or new high-risk items) and periodic review reminders (for policies, risks, and vendors). Together, these ensure that compliance is not a one-time checkbox activity but an ongoing cycle of assessment, action, and improvement.

Through this structured methodology, VerifyWise facilitates a full lifecycle approach to AI governance. Each step is supported by an implemented feature of the platform, ensuring that what might otherwise be a manual, fragmented process can be executed in a coordinated, efficient manner. Moreover, all the data gathered (risks logged, actions taken, evidence collected) remain available for analysis and future learning, positioning the organization to eventually leverage more advanced intelligent techniques on this data (e.g. to predict where compliance issues are likely to recur, as discussed in future work). For now, the methodology's strength lies in enforcing rigor and consistency, allowing organizations to **operationalize AI compliance with confidence**.

V. Discussion and Future Work

The implementation of VerifyWise offers a practical example of how an AI governance platform can be architected to meet the needs of intelligent risk management using primarily deterministic, well-understood methods. Its structured data capture, modular service design, and integrated workflow automation reflect key governance requirements identified in literature: thorough documentation, traceability of decisions, human oversight, and continuous monitoring. In essence, VerifyWise provides organizations with a compliance nervous system, one that consolidates information from policies, risks, controls, vendors, and evidence into a unified context, making it easier to detect gaps and respond to governance challenges. This unified approach stands in contrast to many existing practices where compliance information is siloed in spreadsheets and emails, thereby demonstrating the value of a dedicated system architecture in AI governance.

For practitioners, the current VerifyWise platform presents a mature foundation for deploying an AI compliance program. Key advantages include its support for multiple regulatory frameworks in one system, transparent risk scoring mechanisms, and a modular architecture that can integrate into enterprise environments (e.g. tying into Slack for alerts, using single sign-on, etc.). Organizations adopting VerifyWise can benefit from improved audit readiness and efficiency, for example, faster compilation of audit evidence and the ability to swiftly map any new regulatory requirement to existing controls using the policy mapping interface. However, practitioners should also approach the platform with realistic expectations. Some of the more "intelligent" capabilities (like ML-based risk prediction or fuzzy logic scoring) are **not yet implemented** and would require additional customization or data science effort. Advanced analytics components will also depend on the organization having sufficient historical data and established processes. Thus, users should focus on leveraging VerifyWise's strengths in **structure and process**

enforcement, while recognizing that predictive insights or autonomous compliance adjustments remain areas for future enhancement. Another consideration for practice is change management: introducing such a system will necessitate training staff, defining new workflows (e.g. how a risk gets approved), and ensuring data quality. Human-in-the-loop oversight is still critical, the platform is a tool to augment, not replace, governance professionals.

For researchers and system developers, VerifyWise provides a valuable open-source foundation upon which to build intelligent compliance modules. The platform's rich data model (encompassing risk factors, control outcomes, lifecycle metadata, etc.) can enable explorations of pattern recognition and compliance analytics that were previously difficult due to lack of structured data. For instance, researchers could plug in a machine learning service that analyzes the accumulated risk register to find latent clusters or predictors of high-risk projects. The Bias & Fairness Module demonstrates one such extension, focusing on algorithmic fairness, additional analytics modules could be prototyped in a similar manner (e.g. a module for anomaly detection on compliance logs, or NLP-based mapping of legal text to internal controls). By using VerifyWise as a testbed, developers can experiment with ML or fuzzy inference in a controlled, modular fashion, leveraging the fact that the core system keeps the governance workflow intact. This modular extensibility aligns with the conference's emphasis on intelligent systems architecture: it shows how intelligence can be incrementally integrated into an enterprise system without redesigning the whole workflow. In short, VerifyWise can serve as a research platform for governance intelligence, bridging the gap between academic concepts and operational tools.

Despite its contributions, the current system has limitations that point to clear avenues for future work. As of now, the platform lacks publicly documented performance metrics or large-scale validation, so claims regarding its effectiveness and efficiency remain to be empirically substantiated. This reflects a broader industry trend where many organizations believe they have robust AI governance, yet independent audits often uncover gaps. To fully establish trust in VerifyWise (and similar tools), rigorous evaluation in real-world settings is needed. We outline several key directions for future development and research:

- **Empirical Validation and Benchmarking:** A priority is to evaluate VerifyWise in practice. This involves measuring its impact on compliance outcomes (e.g. does using the platform reduce the number of compliance issues or audit findings over time?), as well as user-centric metrics like decision support effectiveness and the effort required for compliance management. Benchmarks against traditional manual methods would help quantify improvements in efficiency or thoroughness. Such validation should also include assessing the platform's usability and the quality of its recommendations or scores, ensuring they align with expert expectations.
- **Real-Time Monitoring and Streamlined Workflows:** Currently, data entry (risks, controls) is done manually or in batch processes. Future enhancements should enable streaming integration, for example, automatically ingesting AI system logs or incident data to update risk levels in real time. This could allow VerifyWise to trigger alerts for compliance drift (akin to real-time signal processing of AI system telemetry). Implementing APIs for continuous monitoring aligns with the notion of moving from periodic audits to continuous compliance oversight. Additionally, improving workflow automation (such as more sophisticated notification rules, or integration with issue trackers for assigning remediation tasks) would further reduce the administrative burden on compliance officers.
- **Expanded Intelligent Analytics:** With more data and experience, the platform can evolve to include the hybrid intelligence components initially envisioned. This includes integrating advanced analytics like anomaly detection (to flag unusual patterns in risk assessments), reinforcement learning to recommend optimal mitigation strategies based on past outcomes, and natural language processing to assist in mapping regulatory text to internal controls. For example, an NLP module could parse new legislation and suggest which existing controls in VerifyWise map to the new requirements, greatly aiding compliance updates. Any such additions should maintain the system's emphasis on explainability, e.g. an anomaly detected should be presented with context as to why it's considered unusual.
- **Cross-Framework Mappings and Scalability:** As the regulatory environment grows, organizations will face overlapping requirements (for instance, an AI system might need to comply with both EU AI Act and a sector-specific standard). A valuable extension would be developing a library of **mapping templates** between frameworks (as mentioned in the roadmap). This would enable the platform to automatically translate a compliance status in one framework into an estimated status in another, highlighting common controls and differences. Technically, this entails scaling the data model to accommodate many-to-many relationships between controls of different frameworks and possibly a rule engine to propagate compliance evidence across them. This feature would significantly streamline compliance for global organizations and further exemplify intelligent system design by making the platform context-aware of multiple rule sets.
- **Enhanced User Experience and Interpretability:** Lastly, improving how information is presented to users will increase the platform's practical impact. This includes richer dashboards (e.g. interactive visualizations of risk trends over time or network graphs linking risks to controls and evidence) and more user-centric reporting (customizable reports for different stakeholders like executives vs. engineers). On the interpretability front, if ML models are introduced, techniques from eXplainable AI (XAI) should be employed so that any risk

predictions or recommendations can be traced back to understandable factors. Ensuring the system remains **user-friendly, transparent, and responsive** will determine its success in real-world adoption.

VI. Conclusion

VerifyWise exemplifies a balanced approach to building an "intelligent" compliance system for AI governance, one that prioritizes a solid architectural groundwork and trustworthy data management, while being ready to incorporate advanced analytics as they mature. In its current form, the platform delivers immediate value by unifying disparate governance activities (risk management, policy enforcement, vendor oversight, evidence tracking) into a single, coherent system. This alone addresses a critical pain point in AI governance: the ability to maintain continuous, organized oversight over fast-evolving AI projects. By doing so, VerifyWise helps organizations move toward proactive and preventive governance, in line with emerging standards and ethical expectations.

At the same time, the design of VerifyWise keeps an eye on the future of intelligent systems. Its modular structure and data-centric foundation mean that as algorithms for compliance intelligence become proven, they can be integrated seamlessly into the workflow. Rather than viewing AI and human governance as opposed, VerifyWise demonstrates how they can be complementary: routine tasks and complex data correlations can be handled by machines, while strategic decisions and ethical judgments remain with humans. This synergy reflects the broader vision of intelligent systems in the governance domain, systems that enhance human capabilities and judgment through smart automation, without undermining accountability.

In summary, VerifyWise contributes a practical, extensible architecture for AI compliance management, aligning with the ICSPIS 2025 focus on intelligent and signal-driven system design. It underscores that the path to intelligent AI governance may not lie in one grand algorithmic leap, but in systematically building up our tools, data, and processes. Through continued refinement and validation in real-world contexts, platforms like VerifyWise can evolve into truly intelligent guardians of AI, enabling safe, responsible innovation in the age of autonomous systems.

Acknowledgment

The authors would like to thank the development team at BlueWave Labs and the full group of contributors and developers of VerifyWise, whose dedication and talent have driven the ongoing advancement of the platform. Their commitment to open-source development and collaborative innovation has been instrumental in making this work possible.

References (This is a placeholder for now)

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use "Ref. [3]" or "reference [3]" except at the beginning of a sentence: "Reference [3] was the first ..."

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors' names; do not use "et al.". Papers that have not been published, even if they have been submitted for publication, should be cited as "unpublished" [4]. Papers that have been accepted for publication should be cited as "in press" [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[8] K. Eves and J. Valasek, "Adaptive control for singularly perturbed systems examples," Code Ocean, Aug. 2023. [Online]. Available: https://codeocean.com/capsule/4989235/tree

[9] D. P. Kingma and M. Welling, "Auto-encoding variational Bayes," 2013, arXiv:1312.6114. [Online]. Available: https://arxiv.org/abs/1312.6114

[10] S. Liu, "Wi-Fi Energy Detection Testbed (12MTC)," 2023, gitHub repository. [Online]. Available: https://github.com/liustone99/Wi-Fi-Energy-Detection-Testbed-12MTC

[11] "Treatment episode data set: discharges (TEDS-D): concatenated, 2006 to 2009." U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies, August, 2013, DOI:10.3886/ICPSR30122.v2