NextGen Scientific Publication
American International Journal of Computer Science and Technology
Volume 7 Issue 2, Pg. No. 167-176, AIJCST-V7I2P113, 2025
https://doi.org/10.63282/3117-5481/AIJCST-V7I2P113

Original Article

AI-Based Risk/Compliance Decision Framework

***Lalitha Reddy Badam**

Independent Researcher, University of New Haven, USA.

Abstract:

The growing regulatory demands, the ambiguity in the field of operation, the safety of the information and networksecurity challenges have led to the emergence of the dynamic and intelligent risk and compliance management measures. The more conservative traditional risk assessment frameworks tend to utilize fixed rules, manual reviews and fragmented data, constraining their capability to discern arising risks and aid in timely compliance decisions. The hypothesis is the study has a risk/compliance decision structure based on models of artificial intelligence, predictive analytics, mapping of regulatory rules, and risk-prioritization to improve the way organizations make decisions. The framework includes data collecting and standardization, risk detection, AI-powered risk classification, compliance requisites mapping, decision recommendation, and ongoing monitoring. The pattern of the risk, the occurrence of anomalies and the estimation of the potential compliance deviation are identified using machine learning methods and the compliance with the relevant regulatory requirements, as well as the organizational policies, is maintained by rule-based validation. Human-in-the-loop mechanism is implemented in an attempt to enhance transparency, accountability as well as expert view in high impact choices. Conceptual evaluation of the framework is done based on such aspects as risk detecting capabilities, and consistency in decision making, regulatory traceability, adaptability and explainability. The suggested methodology offers a systemized background of incorporating smart risk assessment and compliance governance, which will allow the organization to put more emphasis on the mitigation activities, streamline the effort of manual assessment, and enhance audit preparedness. This study adds a flexible decision-support architecture to organizations aiming at proactive and transparent, risk, and compliance management based on data.

Keywords:

Artificial Intelligence, Risk Assessment, Compliance Management, Predictive Analytics, Machine Learning, Explainable Ai, Decision Support Systems.

Article History:

Received: 15.02.2025

Revised: 14.03.2025

Accepted: 26.03.2025

Published: 03.04.2025

1. Introduction

The growing adoption of artificial intelligence (AI) in decision-making in organizations has altered how institutions risk recognize, conduct compliance requirements, and distribute resources. With the help of AI-centric systems, it will become possible to handle large volumes of structured and unstructured data, uncover complex patterns, estimate the potential risks, and aid decision-making in the financial sector, healthcare, cybersecurity, government, and enterprise management. However, along with the growing usage of algorithmic decision-making, accountability, transparency, fairness, data protection, and compliance with regulations are also raised. That is to say, businesses must possess formalized solutions to effect an amalgamation of AI-based risk analysis, compliance, and justified decision-making. These methods are particularly established within an operational regulatory environment where the decisions should be relative to the risks that they identify and must be explainable, auditable and consistent to the legal stipulations that apply.

Copyright by the Author(s). This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-NC-ND 4.0) License (https://creativecommons.org/licenses/by-sa/4.0/)

Risk-based regulation is a conceptual basis important in setting up such decision processes. Unlike imposing the same controls on all activities, risk-based systems center on regulation focus (on the seriousness, likelihood and the impact of the failure of the result). Nevertheless, to make effective practices, the numeric risk scores are not involved. According to the correct plan of control, roles of the organization, and system of decision review, categories of risks should be associated with corresponding measures to be provided. The studies of risk-based regulation emphasise the need to be responsive and the difficulties of regulatory practice which is insufficient to deal with substantial risks [2]. The considerations above can be applied to AI-powered compliance because the automated suggestions should reflect the dynamic risk factors rather than be decided on the predetermined limits or set of fixed-rule regulations.

The other aspect that would be considered is the relationship between the risk evaluation and the governance capability. Risk-based governance operates under a wide range of institutional and regulatory environments, and, therefore, giving it constant priority is always hard in an environment where stakeholders have different perceptions of risks or they all cannot cope with them competently using monitoring and control mechanisms [3]. Such challenges may be compounded in AI-enriched environments by incomplete data, uncertainty in the model, the difference in operating conditions and complication of relationships between regulatory requirements. It would also mean that a decision model must encompass computational assessment of decision models that ensure accountability, facilitates upsizing and immediate reevaluation. This integration could help organizations to distinguish between normal compliance violations and those which indeed are real threats that require immediate response.

A methodological challenge is also encompassed within measuring risk. The Risk assessment is a protracted methodology towards the uncertain event, the potential outcome and the information available to estimating the probability of occurrence. An evaluation of risk can be expressed numerically so that it can be compared and prioritized, but only one amount may conceal drastic differences in a circumstance with numerically equivalent scores [5]. On the same note, risk management is a wider aspect that includes the identification, assessment, treatment, monitoring and communication as opposed to calculating the exposure [4]. In the case of AI-based compliance decision-making, such distinction is vital since a model-based score needs to inform the organizational reaction, not to decide it automatically. It should be based on uncertainty and context and regulatory importance, and contingency of the possible impact of inaccurate classifications.

Whereas a single decision structure, which is a requirement, unites predictive analytics, interpretation of compliance, risk prioritization, and actionable controls, organizations might not connect predictive analytics, compliance interpretation, risk prioritization, and actionable controls with a single decision structure. Patterns can be identified and approximate exposure can be determined by risk models, compliance systems can trace organizational activities to pertinent needs, but none of these are likely to work as standalone mechanisms. This disaggregation can lead to the unreliable measures, time-consuming response, and inability to trace and justify the reason behind prescribing a particular course of action. An organized AI-based risk and compliance decision strategy is thus necessary to relate analytical results to the regulatory requirements, the decision criteria as well as responsible oversight.

In this paper, an integrated framework will be suggested which is a combination of risk identification with the assistance of AI, risk classification, compliance mapping, prioritization of decisions, and human control. The model is designed to be applied in context sensitive test, explicable suggestions, trace decisions and constant monitoring. It also underscores the reality of the fact that AI can be used as a decision-support rather than a rigid and unresponsive provider of professional judgment. It will also make organizations more consistent, transparent, and accountable in their decision making by establishing associations between risk estimations and compliance requirements and proportional response planning. The value addition is an architectural decision-coherent system, based on which the knowledge created by AI can be translated into written down, auditable, and risk-conscious compliance provisions.

2. Related Work

The analysis of the AI-supported risk and compliance decision-making relies on the classical principles of risk management, numerical analysis, law responsiveness, and significance to regulations. Ufert [1] discussed the regulation of AI within framework of fundamental rights and described how regulation of data protection can be applied to the AI issues. This line of thought contends that it is imperative to make sure that the decision made by AI does not contradict the legal protection and rights of individuals. In a researched study by Black and Baldwin [2], the questions regarding the matters of the risk-based regulatory framework were

considered, and the deficiencies in the solutions poorly prioritizing or performing against major risks were identified. Their work provides the foundations of development of decision mechanism which drags right regulatory response to the right risk classification.

Rothstein, Borraz and Huber [3] investigated the disparities in the risk-based governance in the European context and exposed the applicability of institutional settings in determining the regulatory practices. They have a relevant impact on AI-based compliance frameworks as risk assessment cannot be taken out of governance duties, organizational capabilities, and regulatory context. To a greater extent, Dionne [4] analyzed the history, definitions and criticisms of the management of risk making it a much broader managerial area, and not a very measurable challenge. This information adds to the interconnected infrastructure in which the predicting AI is connected to risk treatment, monitoring and decision accountability.

Another valuable basis is quantitative risk assessment. Kaplan and Garrick [5] discussed the quantitative definition of risk which establishes a conceptual point of articulation of uncertain situations and outcomes. These representations can guide AI-based risk scoring and prioritization but the numerical estimates might not represent all the dimensions of uncertainty that are important. Ni, Chen and Chen [6] evaluated variants to risk matrix approach, and this aided in systematic approaches to the comparison and classification of risks. The techniques can apply to decision-support systems that require to transform the outputs of the models into intelligible risk types and potential courses of action.

French, Bedford and Atherton [7] investigated decision making of ALARP as a multi attribute utility theory and cost-benefit analysis. Through their work, we can see how risk-related choices can be made by considering various criteria as opposed to the reliance of just one measure. For their part, Ale, Hartford and Slater [8] explored the interaction between ALARP and cost-benefit analysis with consideration given to the fact that it is crucial to trade such strategies in a normal case of decision making. These types of views in the context of the AI-based compliance management mean that the recommendations should take into account the proportions of interventions, non-compliance impact, and resources necessary to minimize the threat detection activities.

Abrahamsen and others [9] applied the concept of ALARP principle to management of safety in the energy generating aspect of the chemical industry. Their work is a sector-specific viewpoint on how to apply principles of risk translation into the practice of management. Baybutt [10] discussed the ALARP principle in terms of process safety and the case is where the structured risk reduction and defensibility of the control decisions are upheld. Jones-Lee and Aven [11] discussed the common understanding of ALARP, as interpretive issues in figuring out when reduction in risk is enough. The contributions can be applied to the sphere of AI-compromised compliance decision-making because the level of risks and intervention groups should bear their grounds and grounds of consistency in interpreting the data and the data interpreting the developed intervention guidelines.

The idea of a relative proportional risk reduction was also contextualized by Hurst et al. [12] who described the principle of ALARP and the thought process. Simpson et al. [13] have suggested a complex climate change risk assessment framework, which demonstrates the necessity to have an approach that deals with interrelated factors and complex causes of uncertainty. Krebs [14] analyzed risk, uncertainty and regulation and noted that uncertain outcomes relate with regulatory decision making. Collectively, these researches uphold the creation of frameworks that can help adopt various risk dimensions, contextual variability, and uncertainty instead of utilizing individual predictive scores.

Design in accountable decision systems is also supported using legal reasoning. Alexy [15] contrasted balancing and subsumption as the structures of the law reasoning setting, which provided a conceptual framework to comprehend the decision-making when there are competing principles and rules. Ufert also articulates the importance of the basic rights in regulating AI [1]. These perspectives make us think that AI-based decision-making regarding compliance cannot be expected to be fully technical, though it must be correlated with the legal principles and the needs of the organization as well.

In total, the literature under analysis builds useful premises in the field of risk management, quantification and estimation, proportionality, and legal justification. However, neither of the above works, individually, elaborates on an integrated AI-based model, that underpins predictive risk recognition, compliance mapping, decision prioritization, explainability, and human control. This provides the reason to develop standardized decision-making structure that relates the analysis results to regulatory standards and prescribed and reasonable organizational actions.

3. AI-Driven Risk–Compliance Intelligence and Decision Orchestration Framework

The proposed framework integrates artificial intelligence, the evaluation of risks, adherence to regulations and responsible decision-making within one organizational framework. Its primary goal is to transform heterogeneous operationally data and regulation demands into form of prioritized, explainable and actionable determinations. The framework is based on risk-based approach in which the intensity of intervention is anchored on the perceived severity, probability as well as the potential effect of risks perceived. It is also humanized in order to ensure automated suggestions can be also interpreted on the context, organizational accountability and legal commitments.

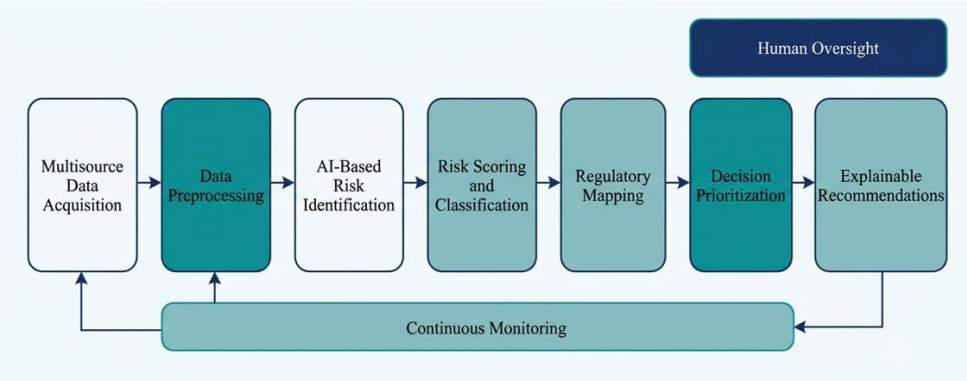


Figure 1. Overall Architecture of the AI-Driven Risk–Compliance Decision Framework

3.1. Multisource Data Acquisition and Contextualization

The framework begins with data acquisition layer that collects information regarding the organizational databases, history of the transactions, database of operational, audit reports, repository of incidents, and policy documents and documents on external regulatory requirements. Information gathered gives the basis of evidence in determining the possible risks and measurement of compliance conditions. Depending on the area of application, these inputs may be pertinent and include access violation, financial aberration, process and incomplete documentation, security incidents and regulatory revision.

The data is preprocessed, normalized, duplicates are eliminated and the data is evaluated before it is analyzed. The missing information, variation in the format, old records and incompatible observation is spotted as they can also influence subsequent risk estimation. The handling of quite sensitive information follows the necessary data protection guidelines, whereas access controls limit the utilization of secret records. All data objects must be connected (when feasible) to their source, date of acquisition and its organizational environment. This provenance information can assist in traceability and also help the decision-makers to understand the evidences that informed the following recommendations.

3.2. AI-Enabled Risk Identification and Assessment

The second level carries out proper analysis techniques with an aim of identifying the potential risks and estimating their sizes. Machine learning can detect a variation or difference compared to the predictable patterns, detect patterns of repeating incidents, and predict the possibility of bad events impacting based on the information available in the past and the present. The natural language processing can help break down the regulatory requirements and organizational policies into obligations, exceptions, reporting requirements and control statements. There are cases, where predictive models may be combined with rule-based approaches when it comes to situations where there are clear conditions or obligatory requirements that need to be met.

Risk assessment is multidimensional considering the likelihood of occurrence, the likely effects, the regulatory significance, minimum level of exposure to the risk and the uncertainty of the evidence available. These are dimensions that are integrated into a systematized risk profile rather than one outcome of a model to be a wholesome description of risk. In the cases of using numeric scoring, the scheme includes a written guideline, scale, and typical clarification. Risk estimates should also signify relevant constraints, particularly where the incomplete data is involved, the historical trends are unstable or the risk analysis field is different than the training field of the model.

The subsequent assessment pulls the oddity between anomalies discovered, possible hazard, and actual breaches. This differentiation is critical as atypical activity is not always a basis of non-compliance, and a seemingly low predictive performance cannot be used as a solution to a binding regulatory requirement.

3.3. Regulatory Mapping and Compliance Interpretation

The third layer is taken to tie those risks to identification with laws and regulations and internal policies, and with contractual requirements and organizational controls. The regulatory requirements would also be represented as organised compliance statements that would contain the pertinent applicability conditions, activities to be undertaken, units of the organisation that must comply and any available compliance evidence would be contained. The requirements may require to be withdrawn and organized with the aid of natural language processing, yet the enabling of them, which carries a believeable load of the law, must be substantiated by the conditioned compliance staff.

Mapping process bridges the links between all the identified risks and the relevant obligations and controls present. The other is the data-access aberration that could be associated with access-management organizational ideals, confidentiality components, record keeping requirements and reporting of data-breach activities. The framework reflects the status of the implementing control, in part, no supporting evidence, or apparently violated. Such forms of classifications will be differentiable as under-documentation does not necessarily mean that a control does not exist.

In order to limit the possibility of an old requirements regulatory mappings might include version information both the effective dates and the version. Conflicting obligations or where it is unclear that the obligation applies or not, the issue is marked to be reviewed by specialists instead of issuing an unfounded decision. It is by means of this weight which the relationship of analytical discoveries and normative demands of the action of the organization is established.

3.4. Risk Prioritization and Proportionate Decision Logic

The fourth level transforms the mixture of the risk and compliance profiles into prioritized decision advice. The prioritization mechanism considers the approximated probability, worm size, criticality of regulatory issue, and efficiency of regulation and uncertainty and urgency. Cases may be entered into a decision matrix customized with a set of categories of low, medium, high and critical and the corresponding thresholds to be entered and set to the relevant organizational context.

The types are connected with the appropriate response pathways. Cases of less urgency may be made subject to routine control, or to documenting or to regular evaluation. Moderately priority cases may be a trigger of additional data collection, control measures or a recovery plan. The high priority cases may require the advancement of the investigation procedure, the prompt security, as well as the awareness of the given staff. When reviewing an incident linked with credible evidence of serious harm or obligatory reporting, the situation might need an immediate amplification based on the protocol.

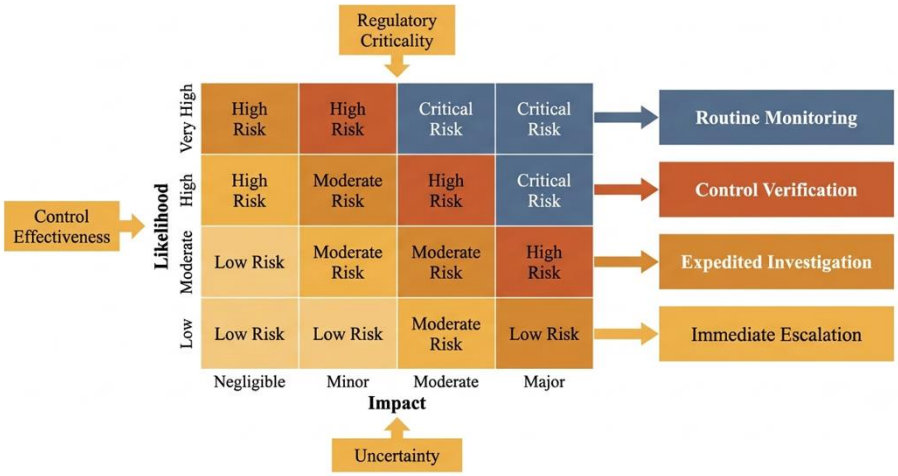


Figure 2. Risk Prioritization and Proportionate Decision Logic

The reasoning behind the choices constitute proportionality which involves the matching of the proposed response proportion to the extreme of the jeopardy and the respective regulative provision. The necessity of law cannot be violated because of low risk score rate offered by a predictive model. Similarly, inaccurate predictions need not always lead to any penalty and insignificance. The framework explaining the factors influencing prioritization and the rationale of proposed response enables an easy review and comparison of cases.

3.5. Explainability, Human Oversight, and Accountability

The fifth layer provides aspects of interpretation of model outputs, reviewing the recommendations and accountability in decision making. Explainability features in order to identify influential input variables, applicable evidences, applicable compliance requirements, and key causes of a risk classification. The system comes with confidence estimates or indications of uncertainty where applicable as well as its recommendations. These explanations should be comprehensible to the users targeted and should not imply what the base model has consented to.

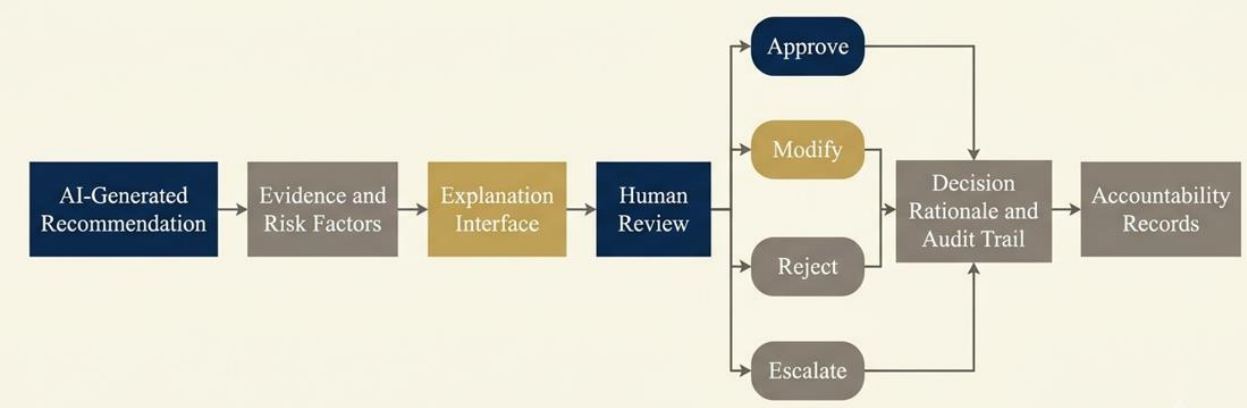


Figure 3. Explainability, Human Oversight, and Auditability Architecture

It includes the aspect of human control as the amount of risk and the sensitivity of the taken decision. Recommendations can be accepted, denied or amended and a reason given by a qualified party and material deviations of automated products should be recorded. Further review is placed on high-impact decisions as compared to the routine monitoring actions. The areas of responsibility are model operation, compliance interpretation and ultimate authorization where the specific organizational roles have their areas of responsibilities.

The framework also keeps a record of the inputs, model versions, risk classification, regulatory mappings, recommendations, reviewer actions and final decisions which are auditable. These records are safeguarded by access controls and data retention policies without the destruction of evidence needed to conduct internal audits and regulation.

3.6. Continuous Monitoring and Adaptive Governance

The final layer will enable continuous monitoring of the risk indicators, the performance of the control and the state of compliance, and the reliability of the model. New issues arise, changes in rules and regulations, new policies and change or deterioration in operations conditions cause re-assessment where necessary. The monitoring of performance can demonstrate variations in the data distributions, discrepancies in the classification, prevalence of false-positive or similarity of the outcomes among the concerned categories. The identification of problems results in the regulation of the models, adjustment of the thresholds, improvements of the data-quality or additional human check-up.

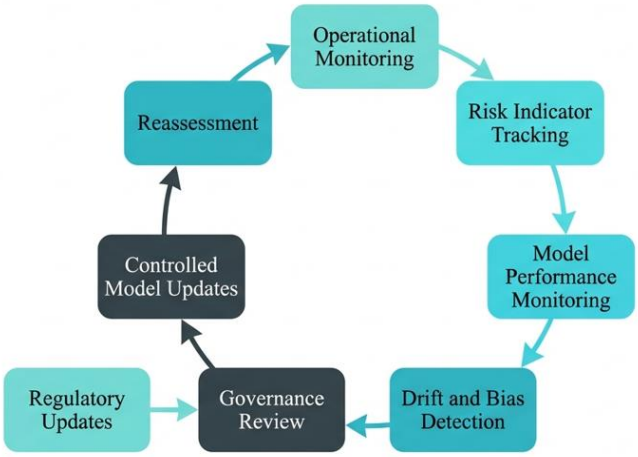


Figure 4. Continuous Monitoring and Adaptive Governance Cycle

The models and decision rules are updated with documented procedures of approval and change management. The framework keeps the historical records intact in a way that the past decisions can be analysed by referring to the information and the rules in place. Investigation, audit and correction give feedback which is used in the next refinement, to be approved.

Overall, the proposed framework offers a traceable decision making pathway that connects with organizational evidence directly, AI-informed risk measurement, regulatory interpretation, appropriate responses, and accountable supervising. Its performance relies on how good the data is, proper selection of models, proper regulatory mapping, well-defined roles and responsibilities and sustained governance. It is a hypothetical choice-centered design, which can be expanded to other domains, but not a claimed outcome of embracing empirical assessment.

4. Framework Appraisal: Governance Alignment, Decision Traceability, and Operational Resilience

The risk-compliance intelligence framework suggested on the basis of AI is assessed on the notion of conceptual analysis of its architectural consistency, regulatory congruency, decision transparency and flexibility. Rather than an experimental analysis, the section looks at how the framework is connected to the main requirements of the risk-sensitive organizational decisions. The appraisal takes into account relationships of its constituent layers and states the conditions which should be satisfied to allow reliable adoption.

4.1. Architectural Coherence and Functional Integration

Its structure builds an integrated process of data capture and risk discovery, data mapping of regulations, decision prioritization and decisions should be controlled by human authority and continued monitoring. The system reduces the conceptual disintegration due to linking the findings of analysis with requirements of compliance and associated organizational responses. It is also hierarchically designed to promote its adoption in a modular format such that organizations can be able to integrate existing monitoring tools they use without necessarily raising their entire infrastructure.

The architectural integrity is based on a regular flow of information between layers. Regulatory mappings should not lose their underlying evidence after being transferred to the prioritization mechanism even as the risk classifications should not lose their underlying evidence. It is also helpful to maintain such relationships which will help to make continuous interpretation and reduce chances of making decisions by isolated model outputs.

4.2. Risk Sensitivity and Regulatory Alignment

Probably one of the most evident benefits of the framework is that it emphasizes the application of proportional decision making. Risk prioritization takes into account the potential impact, probability, regulatory criticality, uncertainty and effectiveness of control. The method is multidimensional in that it encourages differentiated actions as opposed to applying the same intervention to all the anomalies identified.

Mapping results to appropriate requirements and maintaining version control over compliance requirements is more in line with regulatory needs through analytical results. However, the framework alone does not guarantee a legal conformity. The regulations and the need to have mandatory reporting or not may only be discerned through qualified professional judgment based on jurisdiction and whether the regulations are applicable. The automated assessments, therefore, are to be considered as an input to decision support as opposed to a legal conclusion.

4.3. Explainability and Decision Traceability

The explainability layer aids in reviewing by linking recommendations to pertinent evidence, determining factors, risk categories, and requirements. Responsibility is also amplified by documenting the material deviations between the automated recommendations and those recommended by reviewers that plays roles in the process of documenting them. The audit records, in their turn, might assist organizations in using them in order to recreate how a decision is made and whether the arguments were a reflection of a procedure.

However, explanations prove to be only handy when they are comprehensible, informative enough and in agreement with real model behaviour. There should be separation of model generated explanations and confirmed evidence and interpretation of humans. There is also need to have appropriate access controls that protect sensitive operational as well as regulatory information.

4.4. Adaptability and Governance Limitations

Continued tracking ensuring logistics, assists the framework to evolve with the more dynamic regulations, operating conditions as well as new risk patterns. Inventory of models, reconsideration of threshold and reported change-management processes provide cogs of not falling behind time. It is especially important to have human control in situations where there is low data quality, prediction uncertainties or decisions with high legal or organisation costs.

Integration facilities, human skills, regulatory awareness, and administrative funding should be available to achieve the viability of the framework on the job. Implementation is determined by the design, but operational reality would be specified by the comparative testing and stakeholder analysis along with domain-specific validation.

Overall, the review indicates that the framework suggests a unified method of integrating the AI-aided risk assessment and the interpretation of compliance and making responsible decisions. Its major value is its connection to predictive knowledge to explainable, reasonable and reviewed acts of an organization and more so recognizes the necessitation of human decision-making and continuous running administration.

5. From Predictive Intelligence to Accountable Compliance: Discussion

The proposed AI-powered risk-compliance intelligence model suggests that there is the necessity to integrate forecasting analytics, regulation interpretation, and responsibility of organizations in one decision model. Contrary to the paradigm of viewing risk assessment and compliance verification as distinct frameworks, the new framework establishes a continuous system between the process of identifying potential risks, defining the corresponding requirements that need to be met, prioritizing the type of interventions that have to be implemented, and recording of decisions. The conceptual approach in this integration is on the ways that can be implemented to develop consistency and traceability of organizational risk management.

A relevant implication is that AI-generated risk scores are not applicable as a foundation, to take compliance actions. The estimation of risks should be accompanied with regulatory criticality, the quality of evidence, the possible outcomes and the uncertain situation. This especially holds true when the probable risk is minimal and the necessary legal burden exists or where even the predictive information is not adequate to necessitate the automated tests. The framework thus makes AI a decision-support capacity that is supported by human judgment and not as a regulatory interpretation capability.

Other responsible adoption considerations are explainability and auditability. The organizations should have the capability to learn the evidentiary base of recommendations, needs that come with certain risks and the logic of substantial decision-making. Maintaining a record of model versions, regulatory mappings and reviewer and final outcomes can be used to help support internal accountability and regulatory scrutiny. However, documentation cannot guarantee the absence of biases and errors; the quality of the explanations and soundness of the underlying constructs remain a question.

Flexibility is also prioritized in the model through carrying out continuous exercises and guided revisions. The changes in regulations, organization process, and their new risk patterns require a repetitive reassessment of the models and decision criteria. Such flexibility imposes the problems of governance that include data quality and model management, access control, and change management.

Although it has these possible benefits, the framework is still just theoretical and its practical efficacy has not been proven. It would entail sector-based validation, comparison and stakeholder responses to determine its suitability in different organizational contexts. Overall, the framework contributes to a complex approach to the issue of AI-enhanced compliance decisions, in which the risk intelligence is linked to the sufficient response, logical, and commendable governance.

6. Conclusion

The increasing number of control demands, business risk and newly emerged organizational risks demand a complex approach that includes intelligent risk assessment, as well as the transparent and responsible compliance management. The AI-inspired risk/compliance intelligence and decision orchestration framework, which was suggested as a backup of the current research was connected to the collection of multisource data with the help of AI-assisted method of risks detection, regulatory mapping, risk prioritization, generation of explainable recommendations, and monitoring people and ongoing monitoring in the framework of one single structure. The framework leads to a formal progression of transforming various organizational evidences into the proportions, traceable, and workable decisions of compliance.

The key worth of the suggested structure is that it integrates the function of forecastable smarts with regulatory deciphering and corporate law. Machine learning and natural language processing can be employed to help identify anomalies, estimate risks, and institutionalize regulatory requirements, and the rule-based validation must be employed to check that it does not conflict with other crucial requirements of the mandatory obligation and internal policies. Uncertainty evaluation, explainability and human review are included and this minimises the reliance of solitary numerical risk ratings and puts emphasis on the significance of expert judgment in the face of consequential risk decisions. In addition, the recording of rationales behind the decision-making, surveillance of regulatory version and audit trail provide an avenue to enhance accountability and audit preparedness.

Adaptability through continuous monitoring, model control and controlled updates with respect to changing regulations and operating conditions are also well highlighted in the framework. Its modular capability offers future possibilities to get adapted in industries, including financial services, healthcare, cybersecurity, and enterprise governance. However, it can be effectively adopted under one condition, namely the valid data; proper selection of model, the proper regulatory mapping, organizational competences, and the well-defined tasks. Proposals made by AI should still be susceptible to apt validation, especially in a decision with legal implications, confidential details, or any other significant implications.

Since it is a theoretical contribution, the proposed framework lays a groundwork of integrated AI-based risk and compliance decision-making as opposed to identifying empirically proven performance. Future research works are expected to examine its applicability on domain specific case-studies, comparative framework analysis, stakeholder analysis and quantitative research of consistency of decisions, explainability of decisions, risk detection and compliance traceability. These studies would aid in setting useful implementation principles and determine constraints in various regulatory frameworks. Lastly, the framework will encourage a governance-oriented structure wherein AI will serve to preempt risks management and transparency, proportionality, the human responsibility, and responsibility of the regulation.

References

[1] Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI? European Papers – A Journal on Law and Integration, 5(2). https://doi.org/10.15166/2499-8249/394

[2] Black, J., & Baldwin, R. (2012). When risk-based regulation aims low: Approaches and challenges. Regulation & Governance, 6(1). https://doi.org/10.1111/j.1748-5991.2011.01124.x

[3] Rothstein, H., Borraz, O., & Huber, M. (2013). Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe. Regulation & Governance, 7(2). https://doi.org/10.1111/j.1748-5991.2012.01153.x

[4] Dionne, G. (2013). Risk management: History, definition, and critique. Risk Management and Insurance Review, 16(2). https://doi.org/10.1111/rmir.12016

[5] Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk Analysis, 1(1). https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

[6] Ni, H., Chen, A., & Chen, N. (2010). Some extensions on risk matrix approach. Safety Science, 48(10). https://doi.org/10.1016/j.ssci.2010.04.005
[7] French, S., Bedford, T., & Atherton, E. (2005). Supporting ALARP decision making by cost benefit analysis and multiattribute utility theory. Journal of Risk Research, 8(3). https://doi.org/10.1080/1366987042000192408
[8] Ale, B. J. M., Hartford, D. N. D., & Slater, D. H. (2015). ALARP and CBA all in the same game. Safety Science, 76. https://doi.org/10.1016/j.ssci.2015.02.012
[9] Abrahamsen, E. B., et al. (2018). Using the ALARP principle for safety management in the energy production sector of chemical industry. Reliability Engineering & System Safety, 169. https://doi.org/10.1016/j.ress.2017.08.014
[10] Baybutt, P. (2014). The ALARP principle in process safety. Process Safety Progress, 33(1). https://doi.org/10.1002/prs.11599
[11] Jones-Lee, M., & Aven, T. (2011). ALARP—What does it really mean? Reliability Engineering & System Safety, 96(8). https://doi.org/10.1016/j.ress.2011.02.006
[12] Hurst, N. W., et al. (2019). A summary of the "ALARP" principle and associated thinking. Journal of Nuclear Science and Technology, 56(2). https://doi.org/10.1080/00223131.2018.1551814
[13] Simpson, N. P., et al. (2021). A framework for complex climate change risk assessment. One Earth, 4(4). https://doi.org/10.1016/j.oneear.2021.03.005
[14] Krebs, H. (2011). Risk, uncertainty and regulation. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 369(1956). https://doi.org/10.1098/rsta.2011.0174
[15] Alexy, R. (2003). On balancing and subsumption: A structural comparison. Ratio Juris, 16(4). https://doi.org/10.1046/j.0952-1917.2003.00244.x
[16] Black, J., & Baldwin, R. (2010). Really responsive risk-based regulation. Law & Policy, 32(2). https://doi.org/10.1111/j.1467-9930.2010.00318.x