

## **AI compliance framework for cyber insurance**

Chetan Prakash Ratnawat

*Department of Cyber Security*

*Jiwaji University*

*Gwalior 474011*

*Madhya Pradesh*

*India*

*and*

*Capgemini Inc.*

*Pune 411027*

*Maharashtra*

*India*

---

### **Abstract**

AI systems are increasingly playing a pivotal role in the operation of cyber insurance products, from risk assessment to underwriting and claims handling. However, in the field of cyber insurance regulatory compliance is done mainly through disconnected, passive and manual controls which are mainly slow in adapting to changing cyber threats and new regulatory requirements. The message of this paper is the growing disconnect between the AI-driven cyber insurance workflows and the traditional compliance framework. It offers an AI Compliance framework that seamlessly connects with regulatory intelligence, cybersecurity risk scoring, underwriting, and claims management & governance in a very straightforward way.

The framework builds on the ongoing discussions on AI governance, RegTech and cyber insurance and provides a blueprint for regulators to be resilient in an extremely volatile and volatile cyber risk landscape.

---

**Subject Classification (2020):** 90B60, 90B50, 62P25.

**Keywords:** AI compliance, Cyber insurance, RegTech, AI governance, Explainable AI, Regulatory automation.

---

E-mail: [Chetanpr7110@gmail.com](mailto:Chetanpr7110@gmail.com)

## I. Introduction

The cyber insurance market has matured to best financial tool to manage and transfer cyber risk, particularly during the era of significant cyberattacks, ransomware, and data leakage. The insurers to the sectors that are very dependent on a digital future need to attend to the internet of threats very closely, but also be mindful of the dynamic and evolving regulatory landscapes [1].

Cyber risk, unlike traditional insurance, is a non-linear process, a constant changing game and is heavily driven by real-time factors and behaviour. Now the authorities are targeting the companies that are responsible for regulating the tech and they want transparency, explainability and accountability. Going forward, compliance will not be considered as a layer of external supervision as it will have to become a part and parcel of the AI-based insurance process.

This paper puts forward the idea that compliance-by-design is a must for the feasible functioning of cyber insurance. Insurers must not see compliance just as a regulatory approval needed at the end or audit process; they should rather have the regulatory intelligence built into the AI systems that will decide on cyber risk evaluation, policy issuance, and claims settlement.

## II. Background and Related Work

### A. AI and Cyber Insurance Risk Governance

Recent literature indicates that AI-based ecosystem models are increasingly replacing traditional questionnaire-based methods for cyber-risk assessment due to improved accuracy, but they also create challenges related to model transparency and regulatory accountability [2]. Recent Taru Publications research further supports the relevance of AI-enabled risk assessment in insurance operations [3]. RegTech research shows that AI and machine learning can automate compliance monitoring, reporting, and enforcement, while NLP converts complex regulations into machine-readable rules and rule-based engines enable continuous compliance checks across enterprise systems.

### B. Explainable AI and Ethical Governance

The new IEEE research shows that governance-aware AI systems must be more than simply a governance oversight mechanism—they must be embedded within the day-to-day decision-making processes, with

explain ability, accountability, and regulatory traceability connected to this process [4], [5], [6].

### C. Framework Differentiation

The proposed RegTech framework differs from conventional approaches that treat regulatory reporting, compliance monitoring, and rule interpretation as separate functions. Instead, it integrates compliance logic directly into AI-based cyber-insurance processes, including risk scoring, underwriting, and claims validation. This compliance-by-design approach ensures continuous regulatory traceability, explainability, and audit readiness throughout the decision-making process rather than adding compliance only at the final supervision stage [7]. Table 1 summarizes the comparative compliance-integration characteristics of the discussed governance approaches.

**Table 1**  
**Qualitative Comparison of compliance integration across cyber insurance governance models**

| Approach                    | Continuous Compliance | XAI Integration | Closed-Loop Governance |
|-----------------------------|-----------------------|-----------------|------------------------|
| Manual Compliance Workflows | No                    | No              | No                     |
| Static RegTech Systems      | Partial               | Limited         | No                     |
| Proposed Framework          | Yes                   | Yes             | Yes                    |

## III. Research Gap and Contributions

The study was motivated by a gap between advanced AI adoption and regulatory compliance practices in cyber insurance. While insurers increasingly use machine learning for cyber-risk assessment, policy pricing, and automated claims decisions, compliance still relies on static rules, manual documentation, and retrospective audits. This disconnect creates operational inefficiencies and increases regulatory and reputational risks for insurers [8].

### A. Key Technical Contributions

The proposed framework integrates compliance-aware cyber-risk scoring to jointly assess cybersecurity vulnerabilities, regulatory

sensitivity, and compliance capability [9]. It further introduces a closed-loop compliance feedback architecture connecting AI risk assessment, insurance underwriting, claims management, and regulatory supervision with continuously updated regulations. A regulatory rule-to-AI decision mapping translates regulatory requirements into machine-readable rules linked to AI decisions, while the compliance-first AI lifecycle model embeds compliance considerations throughout AI development and deployment rather than treating them as a final-stage review.

#### *B. Research Objectives and Questions*

The study aims to develop an AI-driven compliance framework for the cyber-insurance industry that enables continuous and adaptive regulatory supervision. Its objectives include implementing compliance-by-design in cyber-insurance processes, applying rule-based evaluation to cyber-risk assessment, underwriting, and claims, examining the role of automated compliance and AI interpretability in governance and transparency, and identifying implementation challenges and requirements for responsible AI deployment. The study therefore investigates how AI can maintain continuous regulatory compliance, the infrastructure required to integrate compliance into insurance workflows, the benefits of AI-enabled governance and compliance readiness, and the ethical, technical, and regulatory challenges associated with implementing such frameworks.

### **IV. Methodology: Conceptual, Exploratory, and Policy-Analytical Approach**

This study adopts a conceptual and exploratory research approach to develop an AI compliance framework for cyber insurance. The research method used in this work is theory-building and architectural modeling, rather than testing of hypotheses or collection of primary data. This research has been based on qualitative secondary data from peer-reviewed academic literature, industry reports, regulatory publications, and case studies. Qualitative thematic coding analysis was applied to the selected sources to uncover the most common patterns in terms of AI adoption, regulatory challenges, governance mechanisms and compliance outcomes [10].

#### *A. Scenario-Based Validation and Benchmarking Methodology*

The notable cyber-insurance scenarios were constructed around the documented regulatory cases and industry benchmarks, including but not

limited to ransomware incidents in SMEs, delayed reporting of breaches, and issues related to regulatory audits. The evaluation benchmarks were developed through expert mapping of framework controls to regulatory expectations, i.e., the compliance standards of the industry, and supervisory principles rather than using empirical datasets. This approach enables a systematic and structured comparison of compliance results respecting the confidentiality constraints that insurance companies impose on their operations.

#### *B. Validation Strategy: Regulatory Alignment and Scenario-Based Evaluation*

The AI compliance framework proposed in this paper is validated using a proxy-based approach based on alignment with regulations, industry standards and evaluation scenarios.

Regulatory alignment is achieved by aligning the various layers of the framework with the supervisory principles highlighted by the NAIC, FCA, and OECD, including traceability, proportionality, auditability, and human oversight in AI-supported decision systems. This alignment underpins not only the regulatory feasibility of the framework, but also the defensibility of its governance [11]. The corresponding regulatory alignment is summarized in Table 2.

**Table 2**  
**Regulatory Alignment of the AI Compliance Framework**

| Regulatory Principle           | NAIC | FCA | OECD | Framework Layer              |
|--------------------------------|------|-----|------|------------------------------|
| Transparency & Explain ability | ✓    | ✓   | ✓    | Explainable AI & Audit Layer |
| Human Oversight                | ✓    | ✓   | ✓    | Governance & Control Layer   |
| Accountability                 | ✓    | ✓   | ✓    | Compliance Feedback Loop     |
| Risk Proportionality           | ✓    | ✓   | ✓    | AI Risk & Underwriting Layer |
| Auditability                   | ✓    | ✓   | ✓    | Compliance Monitoring Layer  |

### **V. Proposed AI Compliance Framework for Cyber Insurance**

This framework is not just another compliance model that is there to assess the incidents after they have occurred, on the contrary, the compliance logic is linked to the AI systems that are usually used for risk assessment, underwriting, claims handling and governance. The main

objective is to ensure consistent compliance with the regulations, but without compromising operational efficiency and decision accuracy.

#### A. Framework Overview

The developed framework consists of four interacting layers comprised of the following

- AI-enabled Cyber Risk and Compliance Assessment
- AI-empowered Underwriting & Policy Management
- AI processing of Claims and incident compliance
- AI Automating compliance and governance supervision

The above-mentioned layers, in combination together, form an ecosystem of adaptive compliance capable of real-time response to regulatory change, cyber threats development and ethical governance enforcement. The four-layer architecture and its interactions are illustrated in Figure 1.

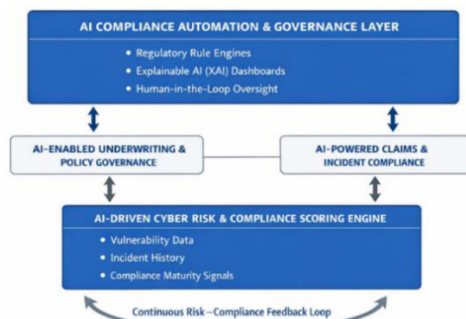


**Figure 1**

**AI Compliance Framework for Cyber Insurance with integrated layers of risk, underwriting, claims, and governance**

#### B. Layer 1: AI-Driven Cyber Risk and Compliance Scoring

In the framework the first layer is the heart of the predictive intelligence. "Combining cybersecurity risk analytics with regulatory importance, to provide compliance-aware risk scores for insured entities [12].

It comes from the governance side and this layer makes sure that compliance issues are considered at the very first stage when making

underwriting and pricing decisions. It allows the insurers to distinguish the technically similar risks on the basis of preparedness for regulation, therefore, the risk selection is done in accordance with the supervisory expectations.

### *C. Layer 2: AI-Enabled Underwriting and Policy Governance*

The second layer of the project included the use of compliance-aware risk intelligence in underwriting and policy management. The AI-based underwriting engines are assigned the rights to policy issuance, coverage structuring, and premium determination deeds automatically through the risk and compliance scoring layer while still functioning under the regulatory restrictions.

If the compliance indicators deteriorate or if the regulations are changed, the system can trigger policy reviews, re-calibration of premium or risk mitigation recommendations [13]. The resulting efficiency and compliance benchmarks are summarized in Table 3.

**Table 3**  
**Underwriting Efficiency and Compliance Performance Benchmarks**

| <b>Metric</b>             | <b>Traditional</b> | <b>AI-Enabled</b> |
|---------------------------|--------------------|-------------------|
| Underwriting Time         | 7–10 days          | 12–24 hrs         |
| Compliance Errors         | High               | Low               |
| Regulatory Review Cycles  | Manual             | Automated         |
| Post-Issue Policy Changes | Frequent           | Minimal           |

This particular stage is employing an AI-based mapping of the rules and reasoning to be able to link the already detected cyber threats with the correct conduct rules, policy clauses, and compliance controls. The purpose of AI here is not to take over the legal judgment but rather to offer consistency, traceability and updateability in the regulatory interpretation across different jurisdictions and hence a support to the legal judgment [14].

### *D. Layer 3: AI-Powered Claims and Incident Compliance*

The strict time frames for breach notification, evidence preservation and data handling heavily regulate cyber insurance claims processing. In building some AI-based claim and incident response workflows, another layer of compliance logic is introduced to address them.

The layer of transparency thus created would be very helpful in making the case for regulatory compliance during supervisory reviews and post-incident investigation. By making claims processing in line with regulatory requirements the insurers reduce the risk of compliance and increase the efficiency of settlements simultaneously [15], [16].

#### *E. Layer 4: AI Compliance Automation and Governance Layer*

The fourth layer represents the highest level of control and governance in the architecture. It consists of a Regulatory AI Toolkit, including continuously updated compliance rule engines, AI dashboards, and monitoring systems that translate regulations into actionable rules for underwriting, claims, and reporting. Explainable AI (XAI) provides clear reasons behind automated decisions, enabling compliance officers, auditors, and regulators to understand and assess AI-driven outcomes. In addition, human-in-the-loop monitoring ensures that high-impact decisions are reviewed by experts, particularly when they involve significant regulatory or ethical risks.

#### *F. Layer 5: Data Flow and Interconnectivity*

The key factor that determines the performance of AI Compliance Framework is the data flow system that connects all the components of the system. The information can move in both directions, which simplifies risk assessment, operational decisions and the synchronization of regulatory supervision.

The risk to underwriting routes has a direct impact on the decision making process concerning the policies as the scores that take into consideration the compliance issues. It is as if the adjudication and settlement of claims flow under the rendition of policy terms and regulatory mandates. Claims-to-compliance communication enables the risk management layer to identify new regulatory risks and potentially adapt its compliance controls to them [17].

## **VI. Discussion And Implications**

### *A. Operational and Compliance Implications*

The proposed framework offers advantages over siloed compliance models, such as faster reporting, improved audit readiness and decreased operational costs for compliance [18]. Table 4 summarizes the pre- and post-AI compliance integration outcomes.

The AI tools are continuously monitoring the situation, therefore the risk of regulatory infractions after the cyber-attacks is reduced, insurers do not share information with the regulators.

**Table 4**  
**Pre- and Post-AI Compliance Integration Outcomes**

| Indicator             | Before AI  | After AI    |
|-----------------------|------------|-------------|
| Regulatory Readiness  | Low        | High        |
| Compliance Risk       | High       | Reduced     |
| Decision Transparency | Limited    | Explainable |
| Governance Maturity   | Fragmented | Integrated  |

#### *B. Governance and Ethical Implications*

Automated underwriting and claims decisions should remain transparent, understandable, and subject to human oversight, particularly where regulatory compliance and consumer rights are concerned. Without adequate model transparency and controls, AI systems may introduce bias, reduce fairness, and undermine stakeholder trust [19]. Therefore, automated decisions should remain auditable, reviewable, and adaptable to changing regulations. Integrating ethical accountability with technical compliance can strengthen trust among regulators, policyholders, and other stakeholders while promoting responsible AI adoption in insurance.

#### *C. Regulatory and Policy Implications*

Major implementation challenges include legacy system integration, data quality, and interoperability, which can affect the accuracy and compliance of AI models. Fairness and algorithmic bias are also concerns, as historical data may reproduce existing discrimination without proper bias audits and governance controls. Furthermore, differences in regulations across countries and states make it difficult to establish a standardized AI compliance framework for the insurance industry.

## **VII. Conclusion**

The primary aim of this study has been to present the AI Compliance Framework for Cyber Insurance that sees compliance as a continuous, embedded activity instead of a periodic audit exercise. Cyber insurance is an example of an area where compliance-by-design AI should be in charge

because it is always the subject of regulation, automated decision-making and the risk of being hacked. The model developed demonstrates how the use of regulatory reasoning, auditability and controls over governance can be moved to AI-based insurance workflows rather than being applied after the fact.

The framework incorporates regulatory intelligence into the different phases of an insurer's operations including cyber risk assessment, underwriting, claims processing and governance enabling the regulators to be more regulatory ready, transparent and resilient. Hence, the AI governance-first paradigm in cyber insurance offers a foundation for additional empirical investigation and scalable regulatory innovations.

### Acknowledgment

The writer relied mainly on public academic literature, industry reports, and regulatory publications which largely contributed to the conceptual development of the study and were credited the most.

### References

- [1] J. Whittlestone, R. Nyrop, A. Alexandrova, K. Dihal, and S. Cave, "Ethical and societal implications of algorithms, data, and artificial intelligence: A roadmap for research," *Nuffield Foundation*, London, U.K. (2019).
- [2] Z. C. Lipton, "The mythos of model interpretability," *Commun. ACM*, vol. 61, no. 10, pp. 36–43 (2018).
- [3] V. Ramisetty and S. S. Saheb, "Leveraging AI for sustainable risk assessment in the insurance industry," *Journal of Information & Optimization Sciences*, vol. 46, no. 8, pp. 2499–2510 (2025), doi: 10.47974/JIOS-2067.
- [4] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning," *Proc. AAAI Workshop on Human Interpretability in Machine Learning*, pp. 1–6 (2017).
- [5] M. Eling and M. Lehmann, "The impact of artificial intelligence on the insurance industry," *Risk Management and Insurance Review*, vol. 21, no. 3, pp. 359–396 (2018).

- [6] J. Brockett and X. Xia, "Big data analytics in insurance risk management," *IEEE Access*, vol. 9, pp. 154812–154826 (2021).
- [7] M. Eling, D. Nuessle, and J. Staubli, "The impact of artificial intelligence along the insurance value chain and on the insurability of risks," *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 47, pp. 205–241 (2022), doi: 10.1057/s41288-020-00201-7.
- [8] R. Böhme, G. Kataria, and J. Grossklags, "Risk analysis of cyber insurance," in *Proc. 13th Int. Conf. Financial Cryptography and Data Security*, pp. 72–89 (2019).
- [9] D. K. Tosh, S. Sengupta, and S. Shetty, "Cyber insurance: Modeling and simulation of cyber risk," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 3, pp. 1835–1848 (2020).
- [10] K. Rieck and P. Laskov, "Machine learning for cyber risk quantification," *IEEE Computer*, vol. 57, no. 4, pp. 44–53 (2024).
- [11] B. Mittelstadt, C. Russell, and S. Wachter, "Explaining explanations in AI," in *Proc. ACM Conf. Fairness, Accountability, and Transparency*, pp. 279–288 (2019).
- [12] J. Kleinberg, S. Mullainathan, and M. Raghavan, "Inherent trade-offs in the fair determination of risk scores," in *Proc. ITCS*, pp. 1–23 (2017).
- [13] A. R. Hevner and S. Chatterjee, "Design science research in information systems," *IEEE Computer*, vol. 56, no. 8, pp. 76–84 (2023).
- [14] R. K. E. Bellamy, K. Dey, M. Hind, S. C. Hoffman, S. Houde, K. Kannan, P. Lohia, J. Martino, S. Mehta, A. Mojsilović, S. Nagar, K. Nate-san Ramamurthy, J. Richards, D. Saha, P. Sattigeri, M. Singh, K. R. Varshney, and Y. Zhang, "AI Fairness 360: An extensible toolkit for detecting and mitigating algorithmic bias," *IBM Journal of Research and Development*, vol. 63, no. 4/5, pp. 4:1–4:15 (2019), doi: 10.1147/JRD.2019.2942287.
- [15] D. Gunning and D. Aha, "DARPA's explainable artificial intelligence program," *IEEE Intelligent Systems*, vol. 34, no. 2, pp. 44–58 (2019).
- [16] A. K. Sharma, N. Babbar, P. Pal, N. K. Verma, and R. K. Saini, "AI-powered framework for real-time dark web monitoring and cyber-security threat detection," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 8, pp. 2955–2966 (2025), doi: 10.47974/JD-MS-2440.

- [17] M. Hind, "Explaining explainable AI," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 84–88 (2019).
- [18] K. R. Varshney, "Trustworthy machine learning and artificial intelligence," *IEEE Security & Privacy*, vol. 17, no. 6, pp. 73–80 (2019).
- [19] C. O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, NY, USA: *Crown Publishing* (2016).

*Received June, 2026*