Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 11| 2025

Research Article **Received:** 01-10-2025| **Accepted:** 23-10-2025 | **Published:** 07-11-2025

AI-Augmented Risk Scoring in ITSM Workflows for Proactive Compliance Monitoring

Rashmi Bharathan

University of Madras, Chennai, Tamil Nadu, India

Abstract: Enterprises are increasingly reliant on detailed IT Service Management (ITSM), which is becoming more difficult to sustain in accordance with the demands of safety and regulations. Traditional ITSM risk assessments are not oriented toward the proactive identification of threats. This paper introduces a novel AI-driven risk scoring framework within IT Service Management (ITSM) workflows, designed to enable real-time compliance monitoring and proactive risk mitigation**.** The proposed approach enhances transparency, predictive capability, and audit readiness, representing a significant step toward autonomous compliance in regulated enterprises.

Keywords: AI-Augmented Risk Scoring**;** ITSM Workflows**;** Proactive Compliance**;** Regulatory Monitoring**;** IT Risk Automation.

INTRODUCTION

In today's digital enterprises, compliance monitoring is no longer done periodically and reactively, but on a continuous and active basis. The companies are not only required to satisfy the demands of the industry, like GDPR, HIPAA, and ISO 27001, but also demonstrate that they can forecast and prevent all the risks prior to their occurrence. The core of this evolution is the IT Service Management (ITSM), which is the rational approach to managing the IT services and aligning them with the business objectives. Nevertheless, traditional ITSM procedures often lack the agility and intelligence needed for proactive compliance, especially in cases in which the risk scoring mechanism is based on static or manually-tuned metrics (Michalk, W. *et al.*, 2010; Mohammadi Koushki, N. *et al.*, 2025) There is an opportunity for change in this sphere because of the increased use of AI technologies. The AI-enhanced risk scoring comes with dynamically self-learning capabilities that constantly assess the behavior of the system, patterns of incidents, and contextual variables in order to identify the risk levels. The intelligent evaluation enables ITSM solutions to provide service ticket precedence, automate the scaling up, and discover conformity violations in real-time. These properties are essential in a large distributed setting where the IT resources, users, and vulnerabilities are dynamic (Hamlen, K. W. *et al.*, 2012; Ravichandran, N. *et al.*, 2020)

Moreover, the regulators are encouraging high-level analytics and automation to be applied in compliance programs as well (Surana, 2021). The tools that are controlled by AI not only accelerate the process of non-compliant behavior identification, but also make the logs accountable and understandable, including providing the report in real-time. Introducing AI into the ITSM processes, then, may lead to the reduction of the gap between the IT process under operation and the management of compliance as a strategy (Fray, I. E. *et al.*, 2012; Ashish, N., & Sharavan, R. 2024)

UNDERSTANDING ITSM AND ITS ROLE IN COMPLIANCE

IT Service Management (ITSM) can be defined as those policies, procedures, and tools through which organizations plan, deliver, operate, and control IT services. ITIL-type frameworks provide a standard practice, and the organization should apply it to manage the service requests, incidents, problems, and changes effectively. Compliance monitoring is a crucial component of these workflows, particularly due to the sheer volume of user data, access policies, and infrastructure changes that can harm security and regulatory positions that ITSM systems handle (Battula, V. 2023; Rusman, A. *et al.*, 2022)

The ITSM compliance is not merely associated with documentation and audit trail, but also involves ensuring that system configuration and access provision, and service action are uniform with the requirements of a given regulation. As an example, access control policies created by compliance regulations should check a ticket that gives high privileges to a user. Mostly, the ITSM platforms perform the vulnerability tests, document the time of incident recovery, and provide compliance measures to the governance groups (Oladosu, S. A. *et al.*, 2022; Ahmed, M. *et al.*, 2012)

***Corresponding Author:** Rashmi Bharathan

DOI- https://doi.org/10.5281/zenodo.17691553

The reactive risk management model limits traditional ITSM systems as its metrics are exercised manually in terms of asset criticality, previous incidents, or user roles that are not readily applicable to the rapidly evolving threats. These outdated approaches to doing things often fail to focus on the key context- abnormal user behavior, evolving asset exposure, or emerging external threats- and active, real-time compliance oversight is more of a challenge. As complexity and the amount of data in IT settings continue to grow, human analysts are struggling to detect early warning signs within a time frame. This loophole means that AI-based solutions will be able to crunch large quantities of data, learn by patterns, and, in effect, identify anomalies, and this is why the conventional risk scoring employed in ITSM is inherently limited (Mendes, T., & Carvalho, L. 2023)

RISK SCORING MECHANISMS

The conventional scoring of risks in ITSM is usually rule-oriented and depends on hardened thresholds and pre-determined circumstances. Such guidelines usually consider the value of assets, the seriousness of the incident, the level of access by the user, and the impact on business to attain a numerical score for a ticket or event. This score can then be used to run prioritization, resource allocation, or escalation paths. Although this approach offers a foundation of operational risk management, the approach is not as flexible and smart as current compliance requirements need (Pesic, M. *et al.*, 2009; Liang, Z. 2025)

The main problem with the use of static risk scoring is that it lacks the capacity to consider contextual and temporal factors. As an example, a system patch request made during standard working hours would have little risk. When the same request is initiated when an attack campaign is known or when the request is initiated by a suspicious IP address, though, the risk profile can change considerably. Conventional systems cannot perform these disparities in real-time as they lack the ability to unite with third-party threat intelligence, behavioral analytics, or anomaly detection engines (Ethan, M. 2025; Tran, H. *et al.*, 2012). The other weakness is that scoring rules are manually maintained, and this becomes very cumbersome as the IT environments expand. Rules might be old-fashioned, redundant, or conflicting, and result in false positives or risks unnoticed. Also, human biases usually affect the formulation of such rules, which makes them even less effective in objective compliance evaluation. Moreover, the conventional risk scoring lacks continuous learning. After establishing a rule, very little performance is appraised or optimized depending on the results. This is where the feedback loop is absent, and as such, it cannot be scaled to fit new threats or varying compliance needs and evolving IT architectures. This rigidity is a huge liability in regulated industries in which the price of non-compliance is steep (Savaş, S., & Karataş, S. 2022)

AI-AUGMENTED RISK SCORING: FRAMEWORK AND CAPABILITIES

Building on the limitations of traditional models, AI-enhanced systems offer flexibility, contextual awareness, and continuous learning. The AI-based risk scoring models are based on machine learning (ML), natural language processing (NLP), and statistical clues; the dynamic score of risk of events in IT services, tickets, and user actions is generated by the AI-based systems compared to the rule-based systems. These models are able to consume large amounts of both structured and unstructured data, identify structures that count, and refresh risk measures on a real-time basis according to previous trends and incoming threat information (Singh, B. 2025; Muntala, P. S. R. P. 2024; Surana, 2025)

The main design of the AI-based risk scoring system in ITSM is linked with data ingestion, contextual data analysis, and machine learning to provide proactive risk management. These feature engineering layers are, in turn, driven with different sources of data such as logs, tickets, vulnerability scanners, user actions, and third-party threat reporting to define relations between anomalies, system exposure, and configuration changes in addition to generating context-based risk assessment inputs (Gupta, R. *et al.*, 2008). ML engine predicts risk using past events of occurrences and outlier detection to give dynamically changing risk profiles based on supervised/unsupervised/reinforcement learning (Chalamala, S. R. *et al.*, 2020). The model also undergoes constant evolution based on the feedback loops as tickets are fixed, and explainability is used to support IT managers and auditors and aid in the regulatory compliance (Fritz-Morgenthal, S. *et al.*, 2022). Through APIs, the AI model integrates with ITSM platforms such as ServiceNow, BMC Remedy, or Jira Service Management to make ITSM a proactive, context-sensitive risk management framework rather than

Publisher: SARC Publisher

an active service hub. Dynamic prioritization of the tickets, automated incident response procedures, and escalation of the high-priority incidents can be achieved (Hasan, M., & Faruq, M. O. 2025).

In order to further compare the AI-enhanced and traditional risk scoring methods as part of ITSM, the overriding differences in capabilities are determined in the operational, analytical, and compliance dimensions in the following table:

Table 1: Comparison of Traditional vs AI-Augmented Risk Scoring in ITSM Workflows

Feature Category	Traditional Risk Scoring	AI-Augmented Risk Scoring
Data Input Sources	Limited to structured data (e.g., severity, asset value)	Includes structured and unstructured data (e.g., logs, NLP from tickets)
Scoring Logic	Static, rule-based scoring criteria	Dynamic, adaptive models using ML and pattern recognition
Context Awareness	Minimal; often ignores user behavior or environmental changes	High; incorporates user patterns, asset state, and time sensitivity
Learning Capability	None; rules must be manually updated	Self-learning through feedback loops and historical outcomes
Anomaly Detection	Not inherently supported	Built in through unsupervised learning models
Integration with Threat Intelligence	Manual or external processes	Seamlessly integrated for real-time threat context
Auditability & Transparency	Limited; rule traces are often undocumented	Explainable AI models support traceability and compliance
Response Automation	Low; reliant on human escalation	High: supports autonomous ticket prioritization and response
Maintenance Overhead	High; frequent manual rule revisions needed	Lower models evolve automatically with operational data
Scalability	Limited in high-volume environments	Designed to scale across distributed IT environments

ENABLING PROACTIVE COMPLIANCE MONITORING THROUGH AI

AI-augmented risk scoring transforms compliance monitoring from a reactive, periodic process into a continuous, proactive system. Unlike traditional audits that detect issues after the fact, AI evaluates risk indicators in real-time, forecasts potential non-compliance, and triggers corrective actions within ITSM workflows (Grace, A. 2025; G Anand, L. 2025). It automates mapping of IT events to standards like NIST 800-53, ISO 27001, or GDPR, monitors configuration drift (Tran, H. *et al.*, 2012), analyzes unstructured data using NLP, and supports role-based monitoring across jurisdictions (Blessing, E., & Hubert, K. 2024). Integrated dashboards provide real-time visibility, enabling timely remediation, strategic decision-making, and a measurable, resilient compliance posture. Key AI-driven compliance features are summarized in Table 2.

Table 2: Key AI Capabilities in Proactive Compliance Monitoring

Capability	Description	Benefits
Real-time Compliance Monitoring	Continuously evaluates risk indicators and system configurations	Early detection of potential non-compliance, reduced audit burden
Predictive Risk Scoring	Forecasts IT assets at risk based on historical data and vulnerabilities	Enables pre-emptive remediation actions
Automated Framework Mapping	Maps IT events/tickets to standards like NIST 800-53, ISO 27001, GDPR	Immediate identification and escalation of policy violations
Configuration Drift Detection	Compares real-time configurations against policy baselines	Reduces audit failures, maintains system integrity
NLP-Based Analysis	Extracts compliance insights from unstructured data in tickets, logs, and change requests	Improves accuracy in identifying hidden compliance signals
Role-Based	Adjusts risk scoring and enforcement by user	Ensures compliance alignment

Publisher: SARC Publisher

Monitoring	role, business function, or location	across multinational operations
Real-Time Dashboards	Displays continuously updated compliance metrics, alerts, and risk scores	Supports strategic decision-making and resource allocation

IMPLEMENTATION CHALLENGES AND RISKS

While AI-augmented risk scoring enhances proactive compliance monitoring in ITSM, its adoption faces technical, organizational, and ethical challenges. Major obstacles include limited or inconsistent data, unstructured information complicating extraction (Michalk, W. *et al.*, 2010; Mohammadi Koushki, N. *et al.*, 2025) model interpretability and transparency for regulated industries (Hamlen, K. W. *et al.*, 2012; Surana, 2025) integration complexity with platforms like ServiceNow, BMC Remedy, or Jira (Ravichandran, N. *et al.*, 2020)organizational resistance, bias, model drift, privacy concerns, and high implementation costs (Fray, I. E. *et al.*, 2012; Rusman, A. *et al.*, 2022). Despite these challenges, successful deployments demonstrate that AI can be adapted to industry-specific compliance needs, offering valuable operational insights. Table 3 summarizes the key implementation challenges and risks.

Table 3: Key Implementation Challenges and Risks in AI-Augmented ITSM Compliance

Challenge	Description	Associated Risks
Data Availability & Quality	Siloed sources, inconsistent metadata, unstructured ticket notes	Reduced reliability, noisy, or biased risk scores
Model Interpretability & Transparency	Black-box AI may not explain risk scoring or escalations	Governance and regulatory compliance risks
ITSM Integration Complexity	AI integration requires APIs, middleware, and data pipelines	Increased cost, time, and technical skill demands
Organizational Resistance	Teams accustomed to rule-based scoring may distrust AI	Slow adoption, lack of buy-in
Bias & Model Drift	Historical biases or changing system behavior	Misleading risk scores, compromised compliance
Privacy & Security	AI ingests sensitive logs, accesses data, and analyzes user behavior	GDPR/HIPAA violations, data breaches
Implementation Costs	Upfront investment in tools, infrastructure, and training	Hesitation to adopt, ROI concerns

USE CASES AND INDUSTRY APPLICATIONS

AI-augmented risk scoring in ITSM workflows is increasingly adopted across industries with complex regulatory and operational demands. In financial services, AI models analyze service tickets, change requests, and incident logs to detect operational risks and compliance anomalies under regulations such as SOX, Basel III, and PCI-DSS, considering contextual factors like transaction timing and access patterns (Oladosu, S. A. *et al.*, 2022; Ahmed, M. *et al.*, 2012). Healthcare organizations leverage AI to monitor access to EHRs, medical devices, and patient data, triggering alerts for unauthorized access and enhancing patient data protection (Mendes, T., & Carvalho, L. 2023; Pesic, M. *et al.*, 2009). In energy and critical infrastructure, AI tracks configuration drift in SCADA systems and assesses field operation risks using sparse but high-value telemetry Liang, Z. 2025; Ethan, M. 2025). Retail and e-commerce sectors employ AI to ensure compliance with GDPR and CCPA, monitor vendor integrations, and secure digital transactions (Tran, H. *et al.*, 2012; Savaş, S., & Karataş, S. 2022). Government and defense organizations use AI to enforce cybersecurity frameworks, audit compliance, and manage high-risk requests for sensitive systems (Singh, B. 2025). Across these sectors, AI enhances ITSM by automating anomaly detection, prioritizing risk responses, and embedding continuous compliance into daily operations, paving the way for predictive analytics, self-healing systems, and adaptive governance.

Publisher: SARC Publisher

Table 4: Industry Use Cases for AI-Augmented Risk Scoring in ITSM

Industry / Sector	AI Applications in ITSM	Key Benefits
Financial Services	Analyze service tickets, change requests, and incident logs; assess contextual factors like transaction timing and access patterns	Early detection of compliance anomalies; faster resolution; reduced regulatory fines
Healthcare	Monitor EHR access, medical device configurations, and patient data transmissions	Proactive alerts for unauthorized access; enhanced patient data protection
Energy & Critical Infrastructure	Track configuration drift in SCADA systems; monitor field operations using sparse telemetry	Identify risky configurations; improve operational safety
Retail & E-Commerce	Ensure GDPR/CCPA compliance; monitor vendor integrations and digital transactions	Reduce data leakage; secure third-party access; maintain operational control
Government & Defense	Score compliance of sensitive systems; enforce cybersecurity frameworks; manage high-risk service requests	Ensure regulatory adherence; block risky operations; strengthen national security posture

FUTURE DIRECTIONS

AI in ITSM processes is changing rapidly, with several emerging trends that have characterized the future of compliance and risk management. Self-healing systems will redefine operational efficiency by not only detecting non-compliance but also executing corrective actions, such as reversing unauthorized configuration changes or automatically generating compliance reports (Muntala, P. S. R. P. 2024; Gupta, R. *et al.*, 2008) The other direction is called federated learning, as the AI models can be trained on distributed data without centralizing sensitive information, enhancing privacy without influencing collaborative risk scoring (Chalamala, S. R. *et al.*, 2020). In addition, explainable AI (XAI) is beginning to receive relevance, as it allows the auditors and regulators to understand how they got their risk score, detect biases, and obtain transparency in automated decision-making (Fritz-Morgenthal, S. *et al.*, 2022).

In addition to them, the concept of AI integrated with GRC systems is turning into one of the most significant trends because operational risk scoring is associated with strategic governance and regulatory reporting (Hasan, M., & Faruq, M. O. 2025). Multi-modal AI systems, integrated structured ITSM data, and unstructured, e.g., emails, chat, voice records, and social media solutions are also on the menu at organizations to provide comprehensive information on compliance (Grace, A. 2025). Those systems can detect signs of potential threats that are not even visible to regular surveillance, like abnormal patterns of communication. Put together, these guidelines show the evolution to predictive, adaptive, and transparent ITSM platforms with the ability to anticipate and manage compliance and risk minimization in increasingly complex enterprise environments.

CONCLUSION

The radical change in the process of active compliance monitoring is the implementation of AI-enhanced risk scoring into the processes of ITSM. The traditional rule-based systems struggle to integrate with the growing IT complexity and to respond to challenging regulatory demands, and AI gives the chance to perform dynamic, context-dependent, and predictive risk evaluation.

As machine learning is implemented in the services of ITSM, companies have the opportunity to automatically assess incidents, service tickets, and system changes and identify non-conformant behaviors in advance before they become a violation or a breach. AI makes configuration drift more visible, emphasizes risk-based action, and is able to trace events to regulatory controls and Explanatory AI is transparent and auditable.

The data must be of high quality, the model governance must be powerful, the cross-functional cooperation required, and the change management to address the challenges, including the legacy integration and resistance to the artificial intelligence-oriented decisions. In real-world deployments, there is increased resilience of operations, reduced compliance at scale, as well as continuous assurance. Improved automation and smart governance will be provided even more rigorously in future developments of self-healing compliance systems and AI-driven GRC platforms to ensure that organizations start to look into the future to forecast risk and respond quickly to regulatory developments.

Publisher: SARC Publisher

REFERENCES

1. Michalk, W., Blau, B., Stosser, J., & Weinhardt, C. "Risk-based decision support in service value networks." *2010 43rd Hawaii International Conference on System Sciences*. IEEE, 2010.
2. Mohammadi Koushki, N., El-Shekeil, I., & Kant, K. "ConfExp: Root-Cause Analysis of Service Misconfigurations in Enterprise Systems." *Journal of Network and Systems Management* 33.2 (2025): 27.
3. Hamlen, K. W., Kagal, L., & Kantarcioglu, M. "Policy Enforcement Framework for Cloud Data Management." *IEEE Data Eng. Bull.* 35.4 (2012): 39-45.
4. Ravichandran, N., Inaganti, A. C., Muppalaneni, R., & Nersu, S. R. K. "AI-Powered Workflow Optimization in IT Service Management: Enhancing Efficiency and Security." *Artificial Intelligence and Machine Learning Review* 1.3 (2020): 10-26.
5. Fray, I. E., Kurkowski, M., Pejaś, J., & Maćków, W. "A new mathematical model for analytical risk assessment and prediction in IT systems." *Control and Cybernetics* 41.1 (2012): 241-268.
6. Ashish, N., & Sharavan, R. "Advancing DevOps Governance with Compliance-as-Code: Bridging Automation and Regulatory Standards." (2024).
7. Battula, V. "Security compliance in hybrid environments using Tripwire and CyberArk." *International Journal of Research and Analytical Reviews* 10.2 (2023): 788-803.
8. Rusman, A., Nadlifatin, R., & Subriadi, A. P. "Information system audit using COBIT and ITIL framework: literature review." *Sinkron: jurnal dan penelitian teknik informatika* 6.3 (2022): 799-810.
9. Surana, S. "Implementing ERP Systems in Financial Services: A Case Study on Driving Adoption and Ensuring Data Integrity." *Sarcouncil Journal of Economics and Business Management* 4.06 (2025): 1-10
10. Oladosu, S. A., Ige, A. B., Ike, C. C., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. "Revolutionizing data center security: Conceptualizing a unified security framework for hybrid and multi-cloud data centers." *Open Access Research Journal of Science and Technology* 5.2 (2022): 086-076.
11. Ahmed, M., Sharif, L., Kabir, M., & Al-Maimani, M. "Human errors in information security." *International Journal* 1.3 (2012): 82-87.
12. Mendes, T., & Carvalho, L. "Artificial Intelligence for Risk Management and Compliance Monitoring in Healthcare Governance Structures." *Nuvern Applied Science Reviews* 7.12 (2023): 1-12.
13. Pesic, M., Schonenberg, H., & van der Aalst, W. "Declarative workflow." *Modern business process automation: YAWL and its support environment*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. 175-201.
14. Surana, S. "The Efficacy Of Internal Controls And Audit Committees In Mitigating Financial Risk: Perspectives From Indian Corporate Governance." *Journal of International Crisis and Risk Communication Research* (2025): 377–386
15. Liang, Z. "AI-Enhanced Network Intrusion Prevention Systems with Multi-source Data Fusion in Enterprise Management." *Science and Technology of Engineering, Chemistry and Environmental Protection* 1.4 (2025).
16. Ethan, M. "Data Versioning and Drift Detection in Scalable ML Pipelines: Building Trustworthy Real-Time AI Systems." (2025).
17. Tran, H., Zdun, U., Holmes, T. I., Oberortner, E., Mulo, E., & Dustdar, S. "Compliance in service-oriented architectures: A model-driven and view-based approach." *Information and Software Technology* 54.6 (2012): 531-552.
18. Savaş, S., & Karataş, S. "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance." *International Cybersecurity Law Review* 3.1 (2022): 7-34.
19. Singh, B. "Integrating Threat Modeling In Devsecops For Enhanced Application Security." *Available at SSRN 5267976* (2025).
20. Muntala, P. S. R. P. "The Future of Self-Healing ERP Systems: AI-Driven Root Cause Analysis and Remediation." *International Journal of AI, BigData, Computational and Management Studies* 5.2 (2024): 102-116.
21. Gupta, R., Prasad, K. H., & Mohania, M. "Automating ITSM incident management process." *2008 International Conference on Autonomic Computing*. IEEE, (2008).
22. Chalamala, S. R., Kummari, N. K., Singh, A. K., Saibewar, A., & Chalavadi, K. M. "Federated learning to comply with data protection regulations." *CSI Transactions on ICT* 10.1 (2022): 47-60.

Publisher: SARC Publisher

23. Fritz-Morgenthal, S., Hein, B., & Papenbrock, J. "Financial risk management and explainable, trustworthy, responsible AI." *Frontiers in artificial intelligence* 5 (2022): 779799.
24. Surana, S. "The Evolving Role Of The Financial Controller In The Indian Manufacturing Sector: From Accounting Steward To Strategic Business Partner." *Journal of International Crisis and Risk Communication Research* 4.2 (2021): 439–449
25. Hasan, M., & Faruq, M. O. "AI-Augmented Risk Detection in Cybersecurity Compliance: A GRC-Based Evaluation in Healthcare and Financial Systems." *ASRC Procedia: Global Perspectives in Science and Scholarship* 1.01 (2025): 313-342.
26. Grace, A. "Leveraging Natural Language Processing (NLP) for Intelligent Incident Ticket Classification." (2025).
27. G Anand, L. "Reinforcement Learning Models for Adaptive Compliance Strategies." *Reinforcement Learning Models for Adaptive Compliance Strategies (April 28, 2025)* (2025).
28. Blessing, E., & Hubert, K. "Technological Infrastructure and Challenges: Integration challenges in implementing AI solutions in legacy systems." (2024).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Bharathan, R. " AI-Augmented Risk Scoring in ITSM Workflows for Proactive Compliance Monitoring." *Sarcouncil Journal of Engineering and Computer Sciences* 4.11 (2025): pp 183-189.

Publisher: SARC Publisher