

From AI Alerts to Accountable Decisions: A Governance Framework for Regulatory Compliance

Monisade Oluwagbemigun

Business Administration, Indiana Wesleyan University

DOI: <https://doi.org/10.47772/IJRISS.2026.1014MG0179>

Received: 31 August 2026; Accepted: 5 September 2026; Published: 16 September 2026

ABSTRACT

Artificial intelligence (AI) is increasingly used to manage regulatory and ethical compliance obligations. This paper examines AI's role in regulatory compliance with particular attention to human oversight, accountability, transparency, employee competency, and organizational governance. It builds on existing scholarship on AI governance, regulatory technology, compliance risk identification, human oversight, and organizational AI readiness. It argues that increased reliance on AI can create an accountability gap when organizations lack effective human oversight and clearly defined responsibility. The paper also incorporates findings from a recent practitioner survey the author conducted. The survey findings reveal that human oversight, AI accuracy, and reliability are the top challenges to AI's use for compliance. Respondents also identified privacy and data security, employee knowledge and training, unclear processes, and integration with existing systems as significant concerns.

Building on existing literature and the survey findings, the paper proposes the STAGE framework (Scan, Triage, Assess, Govern, and Evaluate) as a practical approach to maintaining human judgment and organizational accountability when integrating AI into regulatory compliance. STAGE does not treat AI as an independent decision-maker. Instead, it positions AI as a support tool that requires constant human verification and clear escalation paths. The framework focuses on whether organizations can use AI to identify risks while keeping qualified people responsible for interpreting alerts, making decisions, documenting actions, and correcting weaknesses.

Keywords, regulatory compliance, AI governance, human oversight, compliance risk, corporate governance.

INTRODUCTION

Artificial intelligence is gradually changing how organizations manage regulatory and compliance obligations. Advanced AI systems have now replaced tasks that once required extensive manual review. These systems can analyze large datasets, detect anomalies, summarize complex regulatory requirements, and help employees review complex information. The shift is particularly important for organizations operating in highly regulated environments, where the volume and complexity of regulatory requirements can make traditional compliance processes difficult to manage. However, the issue is not simply whether AI can perform these tasks. It is also whether organizations have reliable processes for interpreting AI outputs and converting them into accountable compliance action.

Who is responsible when the technology is wrong?

An AI system may flag a transaction as suspicious. It may identify potentially noncompliant language in a policy or recommend that a matter be escalated. However, an alert is not necessarily a violation, and a recommendation is not necessarily a legally correct conclusion. Someone must still determine what the information means. Someone must also determine whether further investigation is necessary and what action to take.

This distinction is becoming increasingly important as regulatory frameworks place greater emphasis on human oversight and organizational accountability. The National Institute of Standards and Technology (NIST) identifies accountability and transparency, validity and reliability, explainability, privacy, security, and fairness as important characteristics of trustworthy AI (Tabassi, 2023). The OECD AI Principles similarly call for human agency and oversight, transparency, explainability, robustness, security, and accountability throughout the AI lifecycle (OECD, 2023). The European Union has taken a more specific approach. Article 14 of the EU AI Act requires high-risk AI systems to be designed so that humans can effectively oversee them (Regulation [EU] 2024/1689, 2024). The provision contemplates oversight that is proportionate to the risk and level of autonomy of the system.

The literature suggests, however, that simply assigning a human to oversee an AI system does not necessarily produce effective oversight. Human oversight can be difficult to evaluate because its effectiveness depends on the technology, the people performing the oversight, and the organizational context (Langer et al., 2026). The discussion therefore needs to move beyond whether a human is technically present to whether that person can identify errors, challenge AI outputs, and intervene when necessary. This paper examines AI as part of a broader organizational compliance process. It asks how organizations can integrate AI into regulatory compliance while maintaining meaningful human oversight, accountability, and organizational responsibility. To address this question, the paper combines existing literature with practitioner survey findings and proposes the STAGE framework as a practical approach to maintaining human judgment and organizational accountability.

LITERATURE REVIEW

From Traditional Compliance to AI-Assisted Compliance

Traditional compliance systems rely on policies, internal controls, periodic assessments, audits, reporting requirements, and human review. These mechanisms remain important, but the increasing volume of organizational data has created pressure for more continuous and technology-enabled approaches.

Scholars argue that traditional Control Self-Assessments (CSAs), which often rely on periodic reviews and subjective assessments, can struggle to identify emerging compliance risks (Ogedengbe et al., 2023). Their research proposes integrating data-driven CSAs with machine learning, real-time analytics, behavioral analysis, and surveillance models to support more proactive risk identification. Their findings are relevant because they demonstrate one of AI's strongest potential contributions to compliance, which is early identification of risk (Ogedengbe et al., 2023).

However, AI's ability to identify large potential risks creates a second problem. Once an AI system expands the number and speed of compliance alerts, organizations need people and processes capable of evaluating those alerts. The more organizations rely on AI to identify potential problems, the more important human judgment, data governance, cross-functional collaboration, and organizational capability become.

AI Governance Must Become Part of Organizational Governance

AI governance cannot operate as a completely separate function. Scholars describe organizational AI governance as a governance area that must interact with existing corporate, IT, and data governance structures (Mäntymäki et al., 2022). AI creates risks that cross traditional organizational boundaries. Other scholars argue that organizations need practical governance structures that can translate principles such as fairness, transparency, and accountability into actual organizational processes (Agarwal, 2023). Organizations do not simply adopt AI. They adopt AI alongside new responsibilities, new workflows, risks, and expectations for employees.

Organizational Readiness and Employee Competency

Technology cannot produce sustainable compliance improvements if employees do not know how to use or evaluate it. Successful organizational AI implementation depends on organizational readiness, workflow

integration, data quality, governance, change management, and AI-related competencies (Onnen, 2026). Technical capability alone does not guarantee organizational value. AI adoption further creates contradictions that organizations must be ready to address. They include autonomy versus human oversight, efficiency versus trust, and innovation speed versus governance stability (Lawrence, 2026). Organizations that treat AI as a plug-and-play efficiency tool may create operational fragility, while organizations that redesign workflows and governance around human-AI collaboration are better positioned to achieve sustainable benefits.

Human Oversight is More Than Having a Human in the Loop

One of the most important issues in AI compliance is the difference between formal human oversight and meaningful human oversight. A person can technically review an AI output without exercising meaningful independent judgment. Scholars explain that effective oversight requires more than a checklist (Langer et al., 2026). It depends on the oversight personnel, the technology, and the operational environment. The EU AI Act similarly requires officials to understand the system's capabilities and limitations, interpret its output, recognize the risk of automation bias, and intervene when necessary (Regulation [EU] 2024/1689, 2024). Other scholars provide a practical extension of this principle. Their policy-prototyping work on Article 14 of the EU AI Act recommends clear allocation of human-oversight responsibilities, identification of designated actors, appropriate AI literacy, tailored instructions, and information about the system's risks and intended use (Ooms et al., 2025)

Accountability and Traceability

Accountability becomes even more complicated when AI performs part of the professional's interpretive work (Salomão de Oliveira, 2026). When an algorithm identifies or reports a regulatory violation, traditional compliance doctrines may not clearly establish whether responsibility belongs to the deploying organization, system designer, supervising officer, or other actors. Organizations therefore need traceability between AI output and an accountable human or institutional decision-maker.

The United States approach to AI governance also illustrates the need for accountability and traceability. NIST's Artificial Intelligence Risk Management Framework (AI RMF 1.0) provides organizations with a voluntary framework for identifying and managing AI risks. It encourages organizations to consider trustworthiness throughout the design, development, use, and evaluation of AI systems (Tabassi, 2023). In Illinois, the Artificial Intelligence Video Interview Act requires employers that use AI to analyze applicants' video interviews to notify them and obtain their consent before AI use (820 ILCS 42/5). This requirement illustrates that organizations still need clear procedures for determining how AI is used, who reviews its output, when human intervention is required, and how decisions are documented.

Learning from Broader Regulatory Compliance Research

Research on broader regulatory compliance also supports this concern. Research on corporate reporting obligations under Nigeria's Climate Change Act 2021 found that regulatory ambiguity, limited technical capacity, inadequate awareness, institutional overlap, and weak governance structures could weaken formal regulatory requirements (Oluwagbemigun, 2025). These findings provide a useful comparative lesson for AI-supported compliance. Sophisticated technology does not eliminate the need for clear responsibilities, capable personnel, reliable processes, and governance. Similarly, research on enforcement and incentives found that technology, incentives, and voluntary compliance mechanisms work best when supported by credible enforcement, verification, and transparent reporting (Oluwagbemigun, 2024).

Research Gap

Existing literature provides a foundation for understanding AI-assisted compliance and emphasizes the importance of AI governance, risk management, organizational readiness, and meaningful human oversight. However, these concepts are often discussed as governance principles rather than as a sequence of organizational actions following an AI-generated compliance alert. This study proposes the STAGE

framework, which brings these principles together into a process-oriented framework. Scan reflects continuous risk identification. Triage reflects risk prioritization. Assess reflects meaningful human oversight and independent review. Govern connects compliance findings to decision authority, escalation, and accountability, and Evaluate creates a feedback mechanism for assessing both AI performance and organizational responses. In this way, the framework translates established governance principles into an operational compliance process. The framework is therefore positioned as a process-oriented governance model rather than a replacement for existing AI risk-management or governance frameworks.

Theoretical Contribution and Practical Implications

The primary theoretical contribution of this study is its process-oriented approach to AI-supported regulatory compliance. Existing AI governance and risk-management frameworks provide organizations with principles for identifying and managing AI-related risks, while research on human oversight emphasizes the importance of meaningful human intervention. STAGE connects these perspectives by focusing on the organizational process that follows the identification of a potential compliance issue. Rather than treating human oversight as a general governance requirement, STAGE specifies how human involvement can operate through sequential stages of prioritization, assessment, decision-making, escalation, documentation, and evaluation. The framework therefore provides a bridge between AI governance principles and the operational responsibilities of compliance functions.

The STAGE framework provides organizations with a practical structure for managing AI-generated compliance alerts without transferring final responsibility to technology. Organizations can use the framework to establish procedures for prioritizing alerts, identify employees responsible for reviewing AI outputs, define escalation requirements, document compliance decisions, and evaluate the accuracy and effectiveness of AI-supported processes. The framework also highlights the need for employee training and clear decision authority, which are particularly relevant given that human oversight and employee knowledge were among the most frequently identified challenges in the practitioner survey. STAGE can therefore serve as a starting point for developing internal AI compliance procedures while allowing organizations to adapt the process to their regulatory requirements, organizational structure, and level of AI adoption.

METHODOLOGY

To supplement the literature, I conducted an anonymous practitioner survey titled “AI and Regulatory Compliance: A Practitioner Survey.” The survey was designed to gather preliminary perspectives from professionals working in compliance, legal/regulatory affairs, AI/data/technology governance, and related organizational functions. The survey focused on four areas: current organizational use of AI in compliance and risk-related activities; how organizations respond when AI identifies a potential compliance issue; whether organizations have defined human-review procedures; and the challenges organizations face when using AI for compliance.

The analysis was primarily descriptive. Responses were summarized using counts and percentages, and the open-ended responses were reviewed for recurring themes. Inferential statistical testing was not used because the sample size and non-probability design would not support reliable generalization. The anonymized survey dataset was made publicly available through Zenodo, supporting transparency and allowing the reported findings to be examined alongside the underlying data (Oluwagbemigun, 2026).

The survey used a voluntary, non-probability practitioner sample rather than a statistically representative sample. The target population was professionals with experience or exposure to compliance, legal/regulatory affairs, AI/data/technology governance, and related organizational functions. The final analytic dataset contained 20 responses. Because the sample was small and not randomly selected, the study does not attempt to estimate population parameters or establish statistically generalizable relationships.

The questionnaire was developed from recurring issues identified in the literature reviewed in this study, particularly AI-assisted compliance risk identification, human oversight, accountability, employee

competency, privacy and data security, and organizational governance. The questions were designed to examine both current organizational practices and practitioner perceptions of the challenges associated with AI-supported regulatory compliance. The structured questions addressed organizational use of AI for compliance and risk-related activities, organizational responses to AI-identified compliance issues, human-review procedures, and implementation challenges. The questionnaire also included an open-ended question that allowed respondents to identify improvements they believed organizations should make to use AI more effectively for compliance.

The final analytic dataset included 20 respondents from a range of professional functions. AI/data/technology governance represented the largest group (30%), followed by legal/regulatory affairs (15%) and compliance/regulatory compliance (15%). Other respondents worked in corporate governance (10%), project management (5%), human resources (5%), business information security (5%), risk management (5%), cloud and AI (5%), and internal audit (5%). The range of roles provided perspectives from both technical and governance-oriented functions. However, the voluntary and non-probability nature of the sample limits the representativeness of the respondent group and does not support generalization to the broader population of compliance and governance professionals.

For questions that allowed respondents to select more than one response, each selection was treated independently when calculating percentages. As a result, the percentages for these questions do not sum to 100%. The analysis was intended to identify patterns in practitioner responses rather than establish statistically significant relationships.

FINDINGS

Among the 20 respondents, 60% reported that their organizations currently use AI for compliance or risk-related activities, while 15% reported that their organizations are currently testing or considering AI. Regarding specific AI compliance use, 45% of respondents reported that their organizations use AI for compliance risk identification, 30% of respondents reported that their organizations currently use AI for compliance reporting, 25% reported AI audit/testing, 35% reported regulatory monitoring AI use, 40% reported policy and documentation monitoring, while 25% reported investigations. 15% reported that their organizations didn't use AI, while 5% reported that their organizations were at the forefront of AI use.

Another significant finding concerns human oversight. When asked what happens after AI identifies a potential compliance issue, 30% of respondents reported that their organizations have a formal escalation process, 25% reported that another designated person reviews the issue, and 20% reported that a compliance or legal professional reviews it. Ten percent reported that their organizations had no clearly defined process, while 15% did not know what process applied. No respondent reported that potential compliance issues were automatically acted upon.

The survey also examined whether organizations have clear rules on how their staff review AI-supported compliance decisions. 10 respondents (50%) reported that their organization had clearly defined rules. 5 respondents (25%) indicated that their organization's rules were informal. Three (15%) indicated that rules were being developed. One (5%) respondent indicated that there were no clear rules, while one (5%) respondent did not know.

The challenges respondents identified further reinforce the need for clear organizational governance. Human oversight and accuracy and reliability were the most frequently identified challenges, with 12 respondents (60%) selecting each. Eleven respondents (55%) identified privacy and data security, and 11 (55%) identified employee knowledge or training. Five respondents (25%) selected accountability, four (20%) identified a lack of a clear process, five (25%) identified integration with existing systems, and two (10%) identified explainability. These findings are consistent with the literature's emphasis on human oversight, organizational readiness, and accountable AI use.

The survey also asked respondents what organizations should improve to use AI more effectively for compliance. Responses emphasized employee training and clearly defined human-review processes.

Respondents also suggested stronger organizational control over AI, context-specific AI tools, accurate organizational data, and stronger data security. One respondent specifically suggested establishing an enterprise AI environment to strengthen data security and accountability. Although the findings are based on a small number of participants, they provide useful practitioner perspectives that reinforce concerns identified in the literature.

Analysis and Implications

The survey findings largely reinforce the concerns identified in existing literature. The survey does not suggest that organizations are simply struggling to adopt AI. Instead, it points to a more practical challenge. The finding that 60% of respondents reported current AI use for compliance or risk-related activities shows that AI-assisted compliance is already part of the working environment for many of the respondents. Human oversight and AI accuracy were the most frequently identified challenges. This suggests that organizations still need clear procedures, adequate training, and sufficient authority to review and challenge AI-generated results.

Also, not all respondents reported formal oversight procedures. Although half reported that their organizations had clearly defined rules for human review, others described their procedures as informal or still being developed. This finding supports the distinction between formal and meaningful oversight. A human reviewer may not have the training, knowledge, information, or authority needed to exercise independent judgment on AI results. Organizations therefore need to determine who is responsible for reviewing AI outputs, what training those individuals require, when escalation is mandatory, how decisions are documented, and how the organization will evaluate the system over time.

This is particularly important because AI can create a false sense of security. An automated system may produce hundreds of alerts, dashboards, risk scores, or compliance reports. Sophisticated output does not necessarily mean effective compliance. Earlier research on enforcement and incentives makes a similar point. Formal compliance measures can produce misleading results when they are not accompanied by verification and meaningful enforcement (Oluwagbemigun, 2024).

AI creates the same possibility. An organization may report a high percentage of “compliance alerts reviewed” while still failing to address the underlying risks. The more meaningful measure is whether the organization identifies relevant risks, responds appropriately, documents its decisions, and reduces future compliance failures. This is why STAGE focuses on the entire process rather than the AI system alone.

The Stage Framework

The literature and practitioner findings identify a consistent implementation problem. Organizations can use AI to increase the speed and scope of compliance monitoring, but detection alone does not produce effective compliance. Organizations also need a reliable process for deciding what an alert means, who should review it, when it should be escalated, how the decision should be documented, and how the organization should learn from the outcome. To address this gap, this paper proposes the STAGE framework: Scan, Triage, Assess, Govern, and Evaluate to answer the question: What should happen after AI identifies a potential compliance issue?

S — Scan

T — Triage

A — Assess

G — Govern

E — Evaluate

Scan

Organizations can use AI to scan organizational information for potential compliance risks, including policies, contracts, transactions, regulatory updates, reports, communications, audit information, and other relevant data. The purpose of this stage is to expand the organization's ability to identify potential risks, not to make final compliance decisions. This builds on research suggesting that data-driven surveillance can move organizations from periodic and reactive compliance toward more continuous risk identification (Ogedengbe et al., 2023).

Triage

Not every AI alert deserves the same response. Once an AI system identifies a potential compliance issue, the organization needs clear rules for determining which issues require immediate attention and which can be addressed later. A designated and qualified reviewer should rank alerts based on the seriousness of the potential violation, urgency, organizational exposure, and potential harm to employees or stakeholders. For example, if an AI system identifies several potential compliance issues, the compliance team may need to prioritize an issue involving a possible federal violation over an internal policy concern. Triage helps organizations focus limited review capacity on significant issues and avoid unnecessary escalation.

Assess

This stage involves reviewing an issue after it has been prioritized. A qualified human reviewer should assess the flagged issue rather than simply accept the AI's conclusion. The reviewer should examine the underlying data, applicable laws and policies, the AI output, and the circumstances surrounding the potential violation. The reviewer should also consider why the AI identified the issue and whether the system misunderstood the information or data. For example, if AI identifies language in a contract as potentially inconsistent with a regulatory requirement, the reviewer should examine the applicable legal requirement, understand the purpose of the provision, and determine whether further action is necessary.

A reviewer should be able to question, reject, or override an AI recommendation. This is important because employees may place too much confidence in an automated result simply because it appears technologically sophisticated. Reviewers must therefore exercise independent judgment rather than simply approve AI results. This stage also allows the organization to identify weaknesses in the AI system. If reviewers repeatedly find that alerts or conclusions are based on poor data quality or misunderstood information, the organization should document the pattern and address it. This can help determine whether the system requires adjustment and what level of reliance is appropriate.

Govern

Once the organization assesses the issue, it must determine the next action. This is where governance converts an AI-generated alert into an accountable organizational decision. Minor issues may be resolved within compliance functions, while serious regulatory concerns may require lawyers, internal auditors, senior management, or other designated authority to review them. Organizations should establish these escalation paths in advance rather than wait until a serious problem occurs.

Governance also requires clear decision accountability. The organization should be able to identify who reviewed the issue, what action was taken, and who made the final decision. These records create a traceable decision trail and allow the organization to explain and defend its response when necessary. This is particularly important when AI-supported decisions affect employees, customers, investigations, or matters with legal or financial consequences. The organization remains responsible for the decisions it makes based on AI outputs.

The survey findings make this stage particularly relevant. Although 50% of respondents reported that their organizations had clearly defined rules for human review, others described their procedures as informal or still being developed. The results suggest that organizations may recognize the importance of human oversight without having fully established the processes needed to implement it. The Govern stage addresses

this gap by requiring organizations to establish clear decision rights, escalation procedures, documentation requirements, and accountability for AI-supported compliance decisions (Ooms et al., 2025).

Evaluate

The final stage is Evaluate. Organizations should not assume that the process worked because an AI system identified the issue and an employee reviewed it. They should evaluate both the AI's performance and the organization's response. Evaluation should consider whether the AI identified the issue correctly, whether it missed information, whether a human reviewer correctly reviewed the AI's output, whether the right person was involved, and whether the final decision was documented properly. The organization should also determine whether its response met legal and regulatory obligations.

Evaluation should also help the organization identify patterns over time. If the AI repeatedly produces inaccurate alerts, misses important risks, or relies on poor-quality data, the organization should investigate the cause. Too many unnecessary alerts can also become a problem because they may make it harder for employees to focus on issues that require attention. Organizations should also evaluate how employees handle AI-generated results. If reviewers have difficulty understanding outputs, fail to document their reasoning, or do not feel authorized to question the AI, the organization may need clearer procedures, additional training, or stronger oversight.

Organizations should consider these 9 questions during evaluation:

- Was the AI alert accurate?
- What information did the AI rely on, and was the information reliable?
- Did the AI miss important information?
- Did the reviewer appropriately challenge the AI output?
- Was the issue escalated to the appropriate person?
- Was the final decision adequately documented?
- Did the organization comply with applicable requirements?
- Did the incident reveal a weakness in the organization's compliance process?
- Does the AI system require adjustment or retraining?

Evaluation is what makes STAGE a continuous process rather than a one-time review. The organization learns from both successful and unsuccessful outcomes and can use those lessons to improve technology, employee training, governance procedures, and compliance controls. In this way, STAGE connects AI-supported detection with an ongoing organizational process of review, accountability, and improvement.

Limitations and Future Research

This study has several limitations. First, the practitioner survey included only 20 respondents and used a voluntary, non-probability sample. The findings therefore cannot be generalized to the broader population of compliance, legal, or technology professionals. The survey is preliminary supporting evidence rather than a statistically representative assessment. Second, the survey analysis is descriptive and based on respondents' reported experiences. Third, the STAGE framework is conceptual and has not yet been empirically validated or tested against established AI governance frameworks. Also, the survey should not be interpreted as empirical validation of the framework itself. Future research should therefore test the framework independently through expert review, organizational case studies, pilot implementation, and larger empirical

samples. Such research could examine whether applying STAGE improves the consistency of compliance decisions, escalation practices, documentation, and ongoing evaluation.

CONCLUSION

AI can strengthen regulatory compliance. It expands an organization's ability to identify risks, analyze information, monitor activity, and assist compliance professionals. However, AI cannot replace organizational accountability. The preliminary practitioner survey provides an important early indication of this challenge. Among the twenty respondents, human oversight and AI accuracy and reliability were the most frequently identified obstacles to effective AI use for regulatory compliance. Privacy, employee training, unclear processes, and system integration were also significant concerns. The findings suggest that organizations are moving toward AI-supported compliance without a fully developed framework for managing human oversight and accountability.

These findings reinforce existing arguments that successful AI implementation depends on organizational readiness, governance, human competency, transparency, and clearly defined responsibilities. The STAGE framework is a practical structure for addressing the implementation gap. By moving organizations through Scan, Triage, Assess, Govern, and Evaluate, the framework connects AI's ability to identify risks with the human judgment and organizational processes necessary to address them. STAGE is proposed as a conceptual framework and requires further validation through expert review, case studies, and larger empirical research. Its central premise is that AI should make compliance stronger, not make accountability disappear.

Ethical Approval

Ethical approval was obtained before conducting the survey involving human participants. All participants were informed of the purpose of the study and participated voluntarily. No personally identifying information was collected, and participants were free to decline participation.

Conflict of Interest

The author declares that there are no financial, professional, or personal conflicts of interest that could have influenced the research, analysis, or conclusions presented in this paper.

Data Availability Statement

The anonymized survey dataset supporting the findings of this study is publicly available through Zenodo at <https://doi.org/10.5281/zenodo.22217897>

REFERENCES

1. Agarwal, L. (2023). Defining organizational AI governance and ethics. SSRN. <https://doi.org/10.2139/ssrn.4553185>
2. Artificial Intelligence Video Interview Act. 820 ILCS 42/5 (2025). <https://www.ilga.gov/documents/legislation/ilcs/documents/082000420K5.htm>
3. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
4. Langer, M., Lazar, V., & Baum, K. (2026). On the complexities of testing for compliance with human oversight requirements in AI regulation. In B. Steffen (Ed.), Bridging the gap between AI and reality: AISola 2025 (pp. 160–169). Springer. https://doi.org/10.1007/978-3-032-07132-3_11
5. Lawrence, C. (2026). The AI implementation paradox: Organizational contradictions and the emergence of the AI-native organization. SSRN. <https://doi.org/10.2139/ssrn.6297038>

6. OECD. (2023). Advancing accountability in AI: Governing and managing risks throughout the lifecycle for trustworthy AI. OECD Digital Economy Papers, No. 349. OECD Publishing. <https://doi.org/10.1787/2448f04b-en>
7. Ogedengbe, A. O., Jejenewa, T. O., Olawale, H. O., Friday, S. C., & Ameyaw, M. N. (2023). Enhancing compliance risk identification through data-driven Control Self-Assessments and surveillance models. *Shodhshauryam, International Scientific Refereed Research Journal*, 6(4), 224–248. <https://doi.org/10.32628/SHISRRJ>
8. Oluwagbemigun, M. (2024). Enforcement vs. incentives: Assessing the EPA's approach to sustainable industrial compliance. SSRN. <https://doi.org/10.2139/ssrn.5687147>
9. Oluwagbemigun, M. (2025). Evaluating corporate reporting obligations under Nigeria's 2021 Climate Change Act: Corporate compliance challenges and strategic measures. *International Journal of Energy and Environmental Research*, 13(1), 13–21. <https://doi.org/10.37745/ijeer.13/vol13n11321>
10. Oluwagbemigun, M. (2026). AI and regulatory compliance: Practitioner survey dataset [Data set]. Zenodo. <https://doi.org/10.5281/zenodo.22217897>
11. Onnen, A. (2026). Success conditions for organizational AI implementations: The role of digital and AI-related competency models. SSRN. <https://doi.org/10.2139/ssrn.6871138>
12. Ooms, W., Cools, L., Gils, T., & Heymans, F. (2025). From policy to practice: Prototyping the EU AI Act's human oversight requirements. SSRN. <http://dx.doi.org/10.2139/ssrn.5196091>
13. Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2(4), 603–609. <https://doi.org/10.1007/s43681-022-00143-x>
14. Salomão de Oliveira, N. (2026). Compliance by algorithm: Regulatory technology, corporate accountability, and the institutional reconstruction of financial governance. SSRN. <https://doi.org/10.2139/ssrn.7159958>
15. Tabassi, E. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>