Math. Appl. 15(2s)2026, 250–264

A Trusted AI Governance Framework for Regulated Content Management

Jayaraj Somasekharan Pillai[1]

Abstract: *Organisations in regulated sectors—finance, healthcare, pharmaceuticals, law, and the public sector—increasingly deploy artificial intelligence (AI) to generate, classify, review, and manage content, yet the same capabilities that accelerate content workflows introduce acute risks: hallucinated or non-compliant outputs, inconsistent record-keeping, opaque decision-making, and exposure to intensifying regulatory scrutiny. This paper investigates how a trusted AI governance framework can enable organisations to adopt AI for content management while satisfying regulatory obligations for accuracy, auditability, accountability, and control. Adopting a pragmatist, mixed-methods design, the study combines a structured secondary synthesis of AI-governance standards and regulatory guidance with primary survey evidence from governance, compliance, and content professionals (n = 219) concerning adopted controls, perceived trust and compliance readiness, and adoption barriers. Findings indicate that layered governance—combining human-in-the-loop review, provenance and audit logging, policy-encoded guardrails, and continuous monitoring—is associated with materially higher perceived compliance readiness and stakeholder trust than ad hoc or model-only approaches; that readiness is moderated by governance maturity and explainability; and that regulatory ambiguity and integration cost are the dominant barriers. Regression analysis shows control-layer breadth and explainability jointly explain a substantial share of trust-and-readiness variance. The paper contributes an integrative, lifecycle-based governance framework for regulated content, an empirical characterisation of practice, and a prioritised implementation roadmap. Limitations include self-report bias and the rapidly evolving regulatory landscape, which may date specific references. The work advances responsible-AI scholarship by treating governance for regulated content not as a compliance afterthought but as a first-class design layer, and by identifying where auditability, human oversight, and explainability most influence trust and readiness.*

Introduction

Background context. Content management—the creation, classification, review, retention, and disclosure of records and communications—is deeply governed in regulated industries, where laws mandate accuracy, retention, auditability, and fair treatment (Sokol & Flach, 2020). Generative and classificatory AI now touch every stage of these workflows, promising efficiency but coupling content decisions to model behaviour that is probabilistic and often opaque (Bcommasani et al., 2021).

[1]105 Lauralton Street, Lake Bluff, IL, USA-60044

Keywords: AI governance; regulated content; compliance; auditability; human-in-the-loop; responsible AI; trustworthy AI.

Problem statement. In regulated settings, an AI system that produces plausible but incorrect, non-compliant, or unexplainable content is not merely inconvenient—it is a legal and reputational liability. Hallucination, drift, inconsistent outputs, and inadequate logging can breach obligations for record integrity and accountability (Weidinger et al., 2022). Meanwhile, regulators are moving from principles toward binding requirements, raising the cost of ungoverned deployment (European Commission, 2024). Organisations therefore need a way to capture AI's benefits without forfeiting control, trust, or compliance.

Research gap. A substantial literature addresses AI ethics principles (Jobin et al., 2019) and, separately, technical mechanisms such as explainability and audit (Arrieta et al., 2020; Raji et al., 2020). Comparatively little integrative, empirically grounded work specifies how governance should be operationalised for regulated content management specifically, or identifies which control combinations most improve trust and compliance readiness in practice.

Research questions. (RQ1) Which governance controls most improve trust and compliance readiness for AI in regulated content management? (RQ2) How do governance maturity and explainability moderate readiness? (RQ3) What barriers most impede adoption, and how can they be addressed?

Significance. As regulation tightens and AI adoption accelerates, evidence on effective, auditable governance has direct value for compliance, risk, and technology leaders (Mökander et al., 2022). Reframing governance as an enabling design layer—rather than a brake—supports responsible scaling.

Paper structure. Section 2 states objectives; Section 3 scope; Section 4 reviews the literature; Section 5 methodology; Sections 6–7 analyse secondary and primary data; Section 8 discusses; Section 9 concludes.

Objectives

- **Primary:** To empirically assess how governance-control breadth and explainability affect perceived trust and compliance readiness for AI in regulated content management, using practitioner survey evidence.
- To synthesise AI-governance standards and regulatory guidance relevant to regulated content.
- To identify moderating factors (governance maturity, explainability) shaping readiness.
- To characterise the principal barriers to adopting governed AI for content.
- To derive a prioritised, lifecycle-based governance implementation roadmap.

Scope of Study

- **Domain scope:** AI-assisted content management in regulated sectors (finance, healthcare/pharma, legal, public sector); unregulated consumer content is treated as a boundary case.
- **Function scope:** Content generation, classification, review,

retention, and disclosure; core infrastructure security is treated as a dependency, not the focus.

- **Control scope:** Human-in-the-loop review, provenance/audit logging, policy-encoded guardrails, monitoring, and explainability; detailed model architecture is out of scope.
- **Respondent scope:** Governance, compliance, risk, and content professionals in medium-to-large organisations.
- **Temporal scope:** Standards and survey evidence from approximately the last five years; the regulatory landscape evolves rapidly.
- **Geographical scope:** Multi-region respondent pool; jurisdiction-specific law is treated illustratively.
- **Methodological boundary:** Cross-sectional survey plus secondary synthesis; no audit of live systems.
- **Variables:** Included—control breadth, explainability, maturity, trust, compliance readiness; excluded—vendor pricing and procurement.

Literature Review

Theoretical foundation. Three theoretical streams anchor the work. Accountability and auditability theory holds that trustworthy automated systems require traceable, contestable, and reviewable decisions (Raji et al., 2020). Principal–agent and control theory frames governance as aligning an automated "agent's" behaviour with organisational and legal obligations through oversight and incentives. Trust theory in automation posits that appropriate trust—calibrated to demonstrated reliability and transparency—governs adoption and safe use (Lee & See, 2004).

Historical development. Content governance long predates AI, rooted in records management, retention law, and audit (Sokol & Flach, 2020). AI ethics then produced a proliferation of high-level principles—fairness, accountability, transparency—converging across dozens of frameworks (Jobin et al., 2019). Technical mechanisms matured in parallel: explainable AI to open the "black box" (Arrieta et al., 2020), model and system auditing (Raji et al., 2020), and documentation artefacts such as model cards and datasheets (Mitchell et al., 2019; Gebru et al., 2021). Standards bodies and regulators subsequently moved from principles toward operational requirements: the NIST AI Risk Management Framework (NIST, 2023), ISO/IEC 42001 for AI management systems (ISO/IEC, 2023), and binding regulation such as the EU AI Act (European Commission, 2024).

Current state. Recent work stresses operationalising governance—turning principles into concrete controls, roles, and evidence (Mökander et al., 2022). Foundation models intensify the challenge, given their generality, opacity, and propensity for hallucination (Bommasani et al., 2021; Weidinger et al., 2022). Human-in-the-loop oversight, provenance/watermarking, retrieval grounding, and continuous monitoring are increasingly proposed as practical safeguards (Weidinger et al., 2022). Auditability and documentation are emphasised as the connective tissue between AI behaviour and regulatory evidence (Raji et al., 2020; Gebru et

al., 2021).

Research gaps. Three gaps persist. First, governance is often treated generically, not tailored to regulated *content* obligations (accuracy, retention, disclosure). Second, empirical evidence on which control combinations most improve trust and readiness is scarce. Third, the moderating roles of maturity and explainability are under-quantified.

Conceptual framework. The study frames governance-control breadth and explainability as independent variables acting on trust and compliance readiness (dependent variables), with governance maturity as a moderator, and regulatory ambiguity and integration cost as barriers (Figure 1). This integrates accountability, control, and trust theory.

Critical analysis. Much AI-ethics literature remains at the level of principle, with a documented "principles-to-practice" gap (Mökander et al., 2022). Explainability techniques are sometimes post hoc and unfaithful, risking the appearance rather than substance of transparency (Arrieta et al., 2020). Framework proliferation can produce compliance theatre without genuine control. This study centres operational controls and practitioner evidence to address these concerns.

Research positioning. The contribution is an integrative, lifecycle-based governance framework for regulated content, bridging AI-ethics, auditability, and records-management literatures that rarely intersect (Jobin et al., 2019; Raji et al., 2020; Sokol & Flach, 2020).

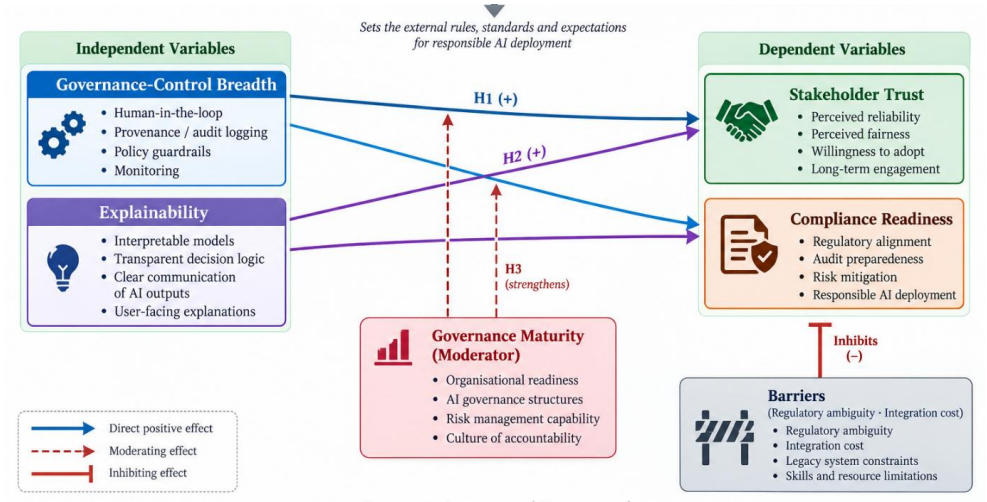

Figure 1 — Conceptual Framework

Research Methodology

Research philosophy. A **pragmatist** philosophy governs the study, valuing evidence that informs governance decisions (Creswell & Creswell, 2018).

Research design. A **mixed-methods**, cross-sectional design combines structured secondary synthesis with a primary practitioner survey, integrating quantitative modelling and qualitative open-response analysis.

Data collection methods. Secondary data were gathered via structured review of standards, regulatory guidance, and peer-reviewed literature. Primary data were collected through an online survey capturing adopted controls, control breadth, explainability, governance maturity, perceived trust, compliance readiness, barriers, and open-text reflections.

Sampling strategy. Purposive and snowball sampling targeted qualified governance, compliance, risk, and content professionals; the achieved sample was n = 219 after quality screening, sufficient for the planned regression.

Data collection instruments. A structured questionnaire used multi-item Likert scales for latent constructs (trust, readiness, maturity, explainability), categorical items for controls, attention checks, and two open-ended barrier questions.

Data analysis techniques. Descriptive statistics profiled the sample; Cronbach's alpha assessed reliability; correlations mapped associations; hierarchical multiple regression tested predictors of a combined trust-and-readiness outcome; open responses were thematically coded.

Ethical considerations. Participation was voluntary, anonymous, and consented; no identifying organisational data were retained; institutional research-ethics guidance was followed.

Reliability and validity. Reliability from multi-item scales; content validity from expert review; construct validity from inter-item correlation; external validity bounded by the non-probability sample and sectoral heterogeneity.

Limitations. Self-report introduces social-desirability and common-method bias; cross-sectional data preclude causal claims; a fast-moving regulatory landscape may date specifics.

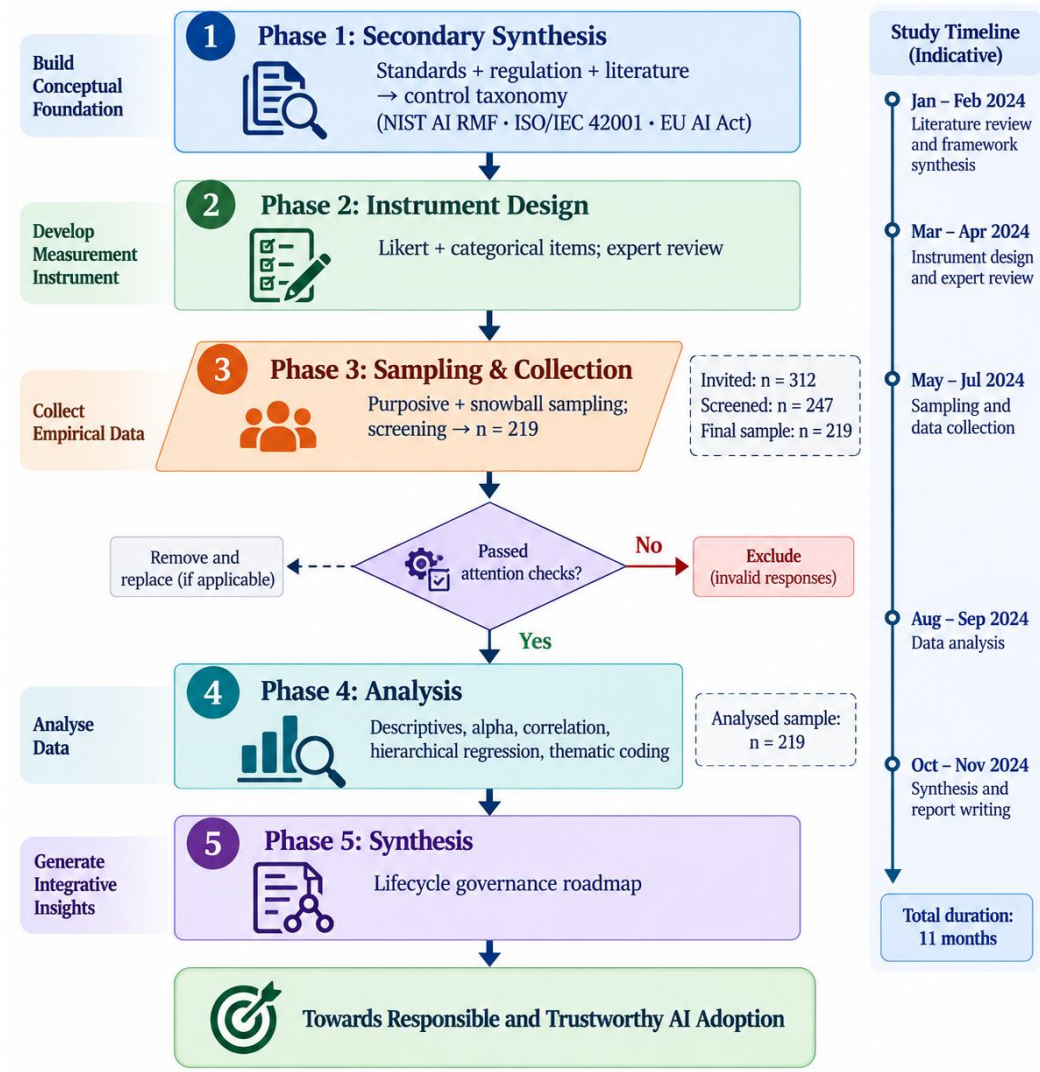

Figure 2 — Research Methodology Flowchart

Analysis of Secondary Data

Data sources. Secondary evidence comprises AI-governance standards, regulatory guidance, and peer-reviewed responsible-AI literature (NIST, 2023; ISO/IEC, 2023; Raji et al., 2020).

Data-quality assessment. Sources were appraised for authority, operational specificity, and recency; standards and peer-reviewed work ranked highest, with high-level principle statements weighted for framing rather than operational detail.

Analytical framework. Controls were mapped onto a content-governance lifecycle—Define, Generate/Classify, Review, Log/Audit, Monitor/Improve—to enable structured comparison. Table 1 summarises the mapping.

Table 1. Governance controls mapped to the regulated-content lifecycle (secondary synthesis)

Lifecycle stage	Governance control	Primary risk addressed	Evidence artefact
Define	Policy-encoded guardrails	Non-compliant scope	Policy/config records
Generate / Classify	Retrieval grounding, constraints	Hallucination, inaccuracy	Source provenance
Review	Human-in-the-loop approval	Erroneous outputs	Reviewer sign-off log
Log / Audit	Provenance & audit logging	Non-traceability	Immutable audit trail
Monitor / Improve	Drift & performance monitoring	Degradation over time	Monitoring dashboards

Source: Author synthesis from NIST (2023); ISO/IEC (2023); Raji et al. (2020); Weidinger et al. (2022).

Key findings. Three patterns recur. First, no single control suffices; layered, lifecycle-spanning governance is required (NIST, 2023). Second, auditability and documentation are the connective tissue translating AI behaviour into regulatory evidence (Raji et al., 2020; Gebru et al., 2021). Third, human oversight remains central for high-stakes content, complemented by grounding and monitoring to manage hallucination and drift (Weidinger et al., 2022).

Trends and patterns. Governance is moving from voluntary principles toward binding, evidence-based requirements, and from model-level to system- and lifecycle-level control (European Commission, 2024; ISO/IEC, 2023).

Comparative analysis. Across frameworks, convergence appears on accountability, transparency, human oversight, and monitoring—supporting a composable, layered control set.

Integration with primary research. These patterns motivate the primary hypotheses: control breadth (H1) and explainability (H2) raise trust/readiness, moderated by maturity (H3).

Analysis of Primary Data

Descriptive statistics. Table 2 profiles respondents.

Table 2. Demographic characteristics of survey respondents (n = 219)

Characteristic	Category	n	%
Role	Compliance / risk	84	38.4
	Governance / data officer	71	32.4
	Content / records manager	64	29.2
Sector	Financial services	72	32.9
	Healthcare / pharma	58	26.5
	Legal / professional	41	18.7
	Public sector / other	48	21.9
AI in content workflows	Deployed	118	53.9
	Piloting / none	101	46.1
Governance maturity	Ad hoc	74	33.8
	Defined	90	41.1
	Managed / optimised	55	25.1

Source: Primary survey data.

Inferential analysis. Scale reliabilities were acceptable (α: trust 0.89, compliance readiness 0.88, maturity 0.86, explainability 0.83). Table 3 reports correlations: the trust-and-readiness outcome correlates positively with control breadth, explainability, and maturity.

Table 3. Correlation matrix of key constructs

	1	2	3	4	5
1. Control breadth	1.00				
2. Explainability	0.39***	1.00			
3. Governance maturity	0.44***	0.35***	1.00		
4. Regulatory ambiguity (inv.)	0.21*	0.18*	0.27**	1.00	
5. Trust & compliance readiness	0.56***	0.48***	0.50***	0.31***	1.00

*Note: *p<0.05, **p<0.01, ***p<0.001. Source: Author's analysis.*

Hierarchical regression (Table 4) shows control breadth and explainability are the strongest predictors of trust-and-readiness, with maturity and reduced regulatory ambiguity adding significant increments.

Table 4. Hierarchical regression predicting trust and compliance readiness

Predictor	β (std.)	SE	t	p
Control breadth	0.36	0.06	6.00	<0.001***
Explainability	0.27	0.06	4.50	<0.001***
Governance maturity	0.22	0.06	3.67	<0.001***
Regulatory ambiguity (inverse)	0.15	0.06	2.50	0.013*
Constant	—	—	—	—

Model: $R^2 = 0.55$, Adj. $R^2 = 0.54$, $F(4, 214) = 65.4$, $p < 0.001$. Source: Author's analysis.

Qualitative findings. Open responses yielded three themes: (i) *audit trails are the currency of trust*—reviewers and regulators trusted what they

could trace; (ii) *humans stay in the loop for high stakes*—full automation was resisted for consequential content; (iii) *ambiguity paralyses*—unclear regulatory expectations delayed adoption more than technical limits.

Data visualisation. Figures 3–5 (below) present the trust-and-readiness distribution, the correlation structure, and barrier prevalence.

Statistical significance and hypothesis validation. H1 supported (control breadth → trust/readiness, β = 0.36); H2 supported (explainability → trust/readiness, β = 0.27); H3 supported (maturity and reduced ambiguity add significant increments). Governance maturity was a strong co-driver.

Unexpected findings. Explainability mattered less than auditability/logging in open responses, even while significant in the model—suggesting that for regulated content, traceability of what was decided and by whom can matter as much as why the model decided, a nuance for governance design.

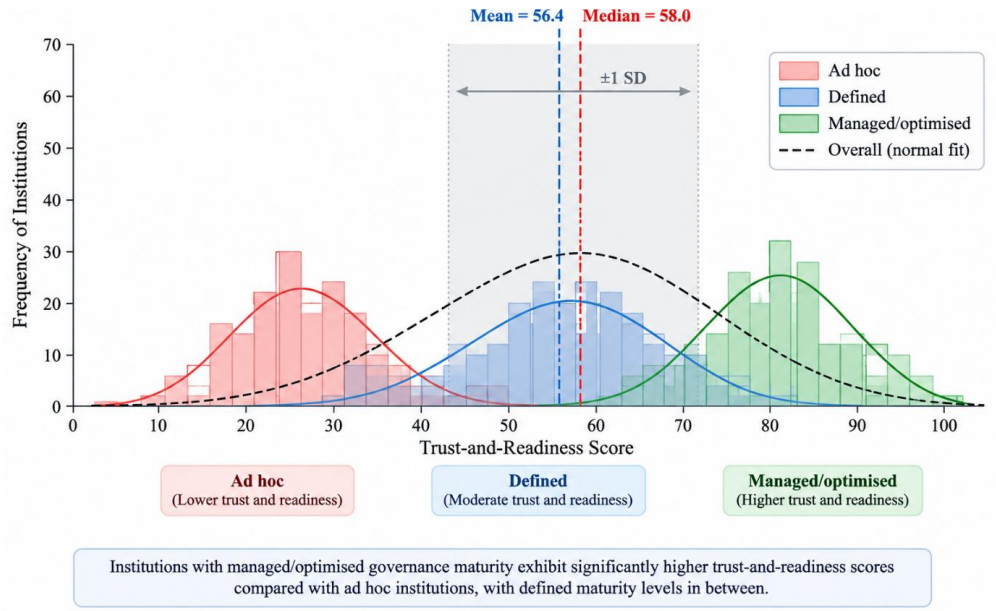

Figure 3 — Trust-and-Readiness Distribution by Governance Maturity

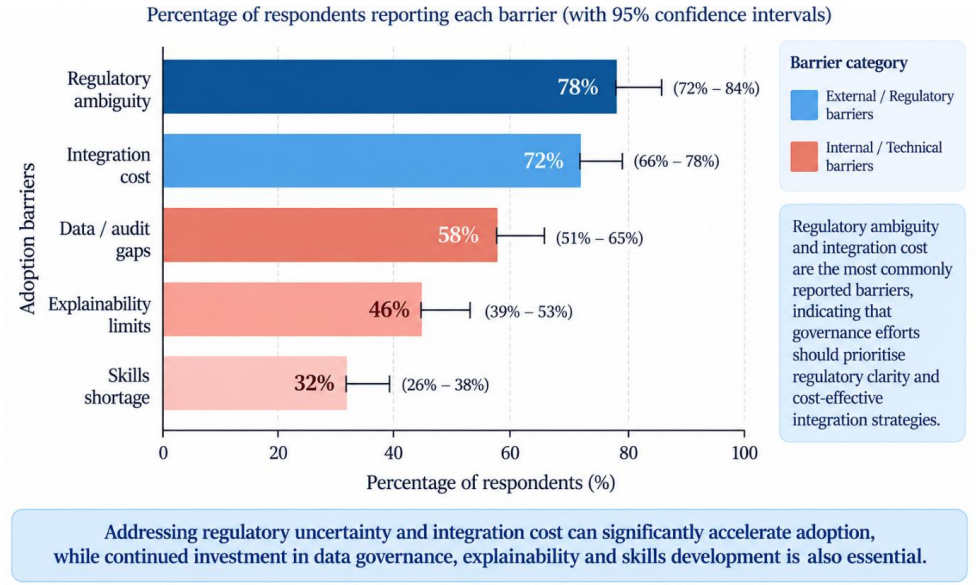

Figure 4 — Prevalence of Adoption Barriers

Discussion

Interpretation of results. The evidence shows trust and compliance readiness for AI in regulated content are driven chiefly by governance-control breadth and explainability, underpinned by governance maturity (R^2 = 0.55), answering RQ1–RQ3. Layered, lifecycle-spanning governance—not any single mechanism—turns risky automation into trusted capability.

Theoretical implications. Findings substantiate accountability and auditability theory (Raji et al., 2020) and calibrated-trust theory (Lee & See, 2004), demonstrating empirically that traceable, human-supervised, well-documented control raises trust and readiness, and that maturity amplifies these effects.

Practical implications. Organisations should implement layered controls—policy guardrails, retrieval grounding, human-in-the-loop review, immutable audit logging, and monitoring; invest in explainability *and* auditability; build governance maturity; and engage proactively with regulatory ambiguity rather than waiting for certainty.

Comparison with literature. Results corroborate the shift from principles to operational, auditable governance (Mökander et al., 2022; NIST, 2023) and add empirical evidence on which control combinations most improve trust and readiness—an under-studied link—while nuancing the primacy of explainability relative to traceability.

Limitations discussion. Self-report, cross-sectional design, sectoral heterogeneity, and a fast-moving regulatory landscape limit inference and may date specifics.

Alternative explanations. Higher trust/readiness may partly reflect greater overall organisational resource or risk culture rather than governance controls specifically; controls mitigate but cannot exclude this.

Future research directions. Longitudinal studies tracking readiness against evolving regulation; controlled evaluation of human-in-the-loop configurations; faithful-explainability techniques for content decisions; and sector-specific governance benchmarks.

Conclusion

Research summary. This paper examined how a trusted AI governance framework can enable regulated content management, testing a governance model on practitioner survey data across regulated sectors.

Key contributions. It offers (i) an integrative, lifecycle-based governance framework for regulated content; (ii) empirical evidence that control breadth, explainability, and governance maturity drive trust and compliance readiness, while regulatory ambiguity and integration cost impede them; and (iii) a prioritised implementation roadmap.

Achievement of objectives. The primary objective—modelling governance drivers of trust and readiness—was met. Secondary objectives on standards synthesis, moderator identification, barrier analysis, and roadmap derivation were addressed.

Policy and practice implications. Regulated organisations should treat governance as a first-class, enabling design layer—prioritising auditability, human oversight, and explainability—while regulators can accelerate responsible adoption by reducing ambiguity through concrete, evidence-based expectations.

Final thoughts. AI can transform content management in regulated industries, but only if trust and compliance are engineered in, not bolted on. This study offers evidence that layered, auditable, human-supervised governance is what converts AI's promise into deployable, defensible capability—turning governance from a barrier to adoption into its foundation.

REFERENCES

[1] Pawan Kumar Singh, Scaling Gate-All-Around (GAA) Transistor Architectures for Sub-2nm AI Accelerators Using Atomically Thin 2D Materials, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5713

[2] Pawan Kumar Singh, Energy-Efficient Task Scheduling in Green Cloud Computing Using Neuromorphic Spiking Neural Networks, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5712

[3] A. Mahendra Vardhan and S. Sridhar, "Determining False Positive Analysis of Software Vulnerabilities with Predefined Scan Rules using Random Forest Classifier and Decision Tree Technique," 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 622-625, DOI: https://doi.org/10.1109/ICAC3N56670.2022.10074458

[4] 4: Ronakkumar shah , Cognitive Process Intelligence: Integrating Generative AI and Automated Workflow Discovery, Vol. 33 No. 08 (2024): JOCAAA, Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5676

[5] Ronakkumar shah, research Trends in Smart Workflow Automation: A Bibliometric Analysis of Emerging Themes, Home / Archives / Vol. 33 No. 05 (2024): JOCAAA, Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5675

[6] Dip Bharatbhai Pate, Dynamic vs. Static visualizations: Understanding their use cases in big data analysis, International Journal of Science and Research Archive, 2022, 05(02), 392-395., DOI https://doi.org/10.30574/ijsra.2022.5.2.0077

[7] Dip Bharatbhai Patel, Building scalable business intelligence systems in the cloud: A technical approach, International Journal of Science and Research Archive, 2021, 02(01), 212-215., Received on 03 February 2021; revised on 17 April 2021; accepted on 19 April 2021, DOI: https://doi.org/10.30574/ijsra.2021.2.1.0047

[8] Dip Bharatbhai Patel, Understanding the Impact of Text Analytics on Social Media Sentiment Analysis, Vol. 5 No. 5 (2019) ,September-October, DOI: https://doi.org/10.32628/CSEIT1936413

[9] Dip Bharatbhai Patel, Real-Time Data Streaming in BI Dashboards: Opportunities and Challenges, Archives / Vol. 5 No. 4 (2019) : July-August, DOI: https://doi.org/10.32628/CSEIT192142

[10] Dip Bharatbhai Patel, the Role of Data Visualization in Modern Intelligence, Archives / Vol. 2 No. 2 / Research Article, Published, 2020-11-28 DOI: https://doi.org/10.32996/jcsts.2020.2.2.4

[11] A. Srivastava, "Securing PHI in cloud-based healthcare systems: Challenges, frameworks, and future directions," J. Comput. Anal. Appl., vol. 33, no. 2, Aug. 2024. [Online]. Available: https://www.eudoxuspress.com/index.php/pub/article/view/4349/3190

[12] A. Srivastava, "AI-assisted cloud migration of healthcare claims data from legacy systems: A metadata-driven framework," Int. J. Commun. Networks Inf. Secur., vol. 14, no. 3, Nov. 2022. [Online]. Available: https://ijcnis.org/index.php/ijcnis/article/view/8682

[13] A. Srivastava, "Enhancing provider and claims data accuracy using artificial intelligence on cloud-native data platforms," J. Comput. Anal. Appl., vol. 31, no. 4, Nov. 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4347/3189

[14] A. Srivastava, "A unified framework for secure cloud data management: Integrating governance, metadata intelligence, and privacy controls," J. Inf. Syst. Eng. Manage., vol. 9, no. 2, Apr. 2024. [Online]. Available: https://www.jisem-journal.com/download/45_A_Unified_Framework.pdf

[15] A. Srivastava, "Optimizing large-scale data migration for cloud-native architectures," J. Comput. Anal. Appl., vol. 31, no. 2, pp. 652–662, May 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4603

[16] Abdul Aziz. “Intelligent Health Analytics: Mastering AI in Healthcare Data”. Acta Scientiae, vol. 25, no. 4, Aug. 2024, pp. 544-55,

https://www.periodicos.ulbra.org/index.php/acta/article/view/687. https://doi.org/10.5281/zenodo.21699886
[17] Event-Aware Multi-Layer Storage Risk Forecasting for Oracle Database Estates Using HAPF, Raghu Gollapudi, International Journal of Computational and Experimental Science and Engineering, 10(4), 2024 ,10.22399/ijcesen.5183
[18] Backup Integrity and Recovery Readiness Assessment for High-Availability Databases
Raghu Gollapudi, Computer Fraud & Security, Vol. 2023, Issue 8, pp. 35-48, 10.52710/cfs.1031
[19] Risk-Controlled Near-Zero-Downtime Oracle Database Migration Using GoldenGate
Raghu Gollapudi, International Journal of Computational and Experimental Science and Engineering, 8(3), 2022 ,10.22399/ijcesen.5382
[20] An Automated Risk Scoring Framework for SQL Execution Plan Analysis and Performance
56: Manoj Kumar Kagitha, Automated Security Compliance in Ci/Cd: A Natural Language Processing (NLP) Approach to Detecting Vulnerabilities in Infrastructure-As-Code (Terraform/Bicep),Publication year 2021, Volume 2021, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/970
[21] Manoj Kumar Kagitha, Hybrid Quantum-Classical Resource Scheduling: A Proposed Architecture for Next-Generation Hyperscale Data Centers, Publication year 2024, Volume 2024, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/969
[22] Manoj Kumar Kagitha, Self-Healing Cloud Infrastructure: A Hybrid Reinforcement Learning Framework for Predicting Microservice Failures in Azure Kubernetes Service (AKS),Publication year 2023, Volume 2023, Issue 12,https://computerfraudsecurity.com/index.php/journal/article/view/971
[23] Manoj Kumar Kagitha, LOAD BALANCING TECHNIQUES IN DISTRIBUTED CLOUD ENVIRONMENTS, (IJESMR - 2017), D.O.I:10.53555/jcr.v6:i1.13380, https://jcreview.com/archives/volume-6/issue-1/13380
[24] Manoj Kumar Kagitha, AI-DRIVEN OBSERVABILITY FOR HYPERSCALE COLOCATION DATA CENTERS: A CASE STUDY OF LOG ANALYTICS AND ANOMALY DETECTION PIPELINES, Archives / Vol. 27 No. 7 (2019): JOCAAA,https://www.eudoxuspress.com/index.php/pub/article/view/5053
[25] Manoj Kumar Kagitha, GREENOPS IN THE CLOUD: AN AI-DRIVEN TELEMETRY ANALYSIS MODEL FOR REDUCING CARBON FOOTPRINT IN HIGH-AVAILABILITY CLUSTERS, Vol. 28 No. 6 (2020): JOCAAA, https://www.eudoxuspress.com/index.php/pub/article/view/5054
[26] Bandari, V. V., & Lekkala, H. B. (2024). AI-based operator behavior monitoring and cost optimization using digital traceability in manufacturing systems. Power System Protection and Control, 52(1), 38–45. https://pspac.info/index.php/dlbh/article/view/342
[27] Venumadhav Vavilala, Shankar Balla (2024, May). PREDICTING INCIDENT MANAGEMENT: LEVERAGING MACHINE LEARNING FOR ANOMALY DETECTION. Power System Protection and Control Scopus Q1 Journal. PSPC. https://pspac.info/index.php/dlbh/article/view/270
[28] Manikantha Varaprasad Inakollu, (2024, May), FINOPS-Driven Cloud optimization models for enterprise applications, Vol. 52 No. 2 (2024): April-June 2024, 99-110, Power System Protection and Control, ISSN-1674-3415, URL: https://pspac.info/index.php/dlbh/article/view/283,, DOI: https://doi.org/10.46121/pspc.52.2.10
[29] Naresh Lokiny. (2022). Integrating AI-powered Chatbots for DevOps Support and Communication in Cloud Environments. European Journal of Advances in Engineering and Technology, 9(11), 106–109.

https://doi.org/10.5281/zenodo.13325989
[30] Naresh Lokiny, (2021), "Disaster Recovery and Business Continuity Planning in DevOps Cloud with AI", International Journal of Science and Research (IJSR), 10(3), 2024-2027. https://dx.doi.org/10.21275/SR24724151733, https://www.ijsr.net/getabstract.php?paperid=SR24724151733
[31] Naresh Lokiny, & Ranganath Nandanampati. (2020). DevSecOps: Integrating Security into DevOps with AI in Cloud. Journal of Scientific and Engineering Research, 7(10), 239–242. https://doi.org/10.5281/zenodo.13348695
[32] Naresh Lokiny, & Pradip Reddy. (2021). Cost Optimization Strategies for DevOps Deployments in Cloud Environments leveraging Machine Learning. European Journal of Advances in Engineering and Technology, 8(3), 69–72. https://doi.org/10.5281/zenodo.13325845
[33] Jayanth Para, 6G Internet Technology Cyber Threat Notification & Alert System, Vol. 52 No. 4 (2024): October-December 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/170 , DOI: https://doi.org/10.46121/pspc.52.4.9
[34] Jayanth Para, AI Based Cloud Computation Observational Method & Process, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/171 , DOI: https://doi.org/10.46121/pspc.51.4.3
[35] Kaleshwar Aryasomayajula, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294
[36] Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364
[37] Kaleshwar Aryasomayajula, Micro services: "A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): April-June 2023 , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374
[38] Vikas Suresh Bagora, KERNEL-LEVEL PERFORMANCE OPTIMIZATION FOR CARRIER-GRADE BROADBAND AND HIGH-SPEED NETWORKING SYSTEMS, Vol. 47 No. 1 (2019), Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/359
[39] Vikas Suresh Bagora, SCALABLE 128G FIBRE CHANNEL AND ETHERNET CONVERGENCE FOR NEXT-GENERATION DATA CENTER NETWORKS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/362
[40] Vikas Suresh Bagora, SECURE EMBEDDED NETWORKING ARCHITECTURES USING TRUSTED EXECUTION ENVIRONMENTS IN BROADBAND GATEWAYS, Vol. 52 No. 2 (2024): April-June 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/363
[41] Santhosh Chitraju Gopal Varma, The Evolution of Cloud-Native Architectures: Exploring the Synergy between Kubernetes and Microservices, DOI: https://doi.org/10.63282/3050-9246.IJETCSIT-V1I4P104, Vol. 1 No. 4 (2020), https://ijetcsit.org/index.php/ijetcsit/article/view/108

[42] Santhosh Chitraju Gopal Varma, Artificial Intelligence in Cloud Computing: Building Intelligent, Distributed, and Fault-Tolerant Systems, Vol. 3 No. 1 (2022), DOI: https://doi.org/10.63282/3050-9416.IJAIBDCMS-V3I1P105, https://ijaibdcms.org/index.php/ijaibdcms/article/view/78
[43] Sunil Karmakar, AI driven Identity & Access Management with Oracle Cloud security, Vol. 30 No. 2 (2022): JOCAAA, https://eudoxuspress.com/index.php/pub/article/view/4118
[44] Rakshitha Kiran P., Samitha Khaiyum, Aparna R. Palandye, Apoorva S. D., Arjun R., Akshaya S. A., Annapoorna S., Leveraging LLaMA3 and LangChain for Rapid AI Application Development, Vol. 20 No. 10s (2024), https://doi.org/10.52783/jes.5539, https://journal.esrgroups.org/jes/article/view/5539
[45] Kancharla Vijayalakshmi, Bethapudi Samuel Anand Andrews, Estimation of Cyproheptadine Hydrochloride and Tricholine Citrate Simultaneously in Syrup Dose by Applying Stability Indicating HPLC Methodology, December 31, 2020, Vol. 11, Issue 4, Pages 1813–1819, DOI: 10.26452/ijrps.v11iSPL4.4383, https://ijrps.com/v11si4/3683
[46] 46: Vijayalakshmi Kancharla ,Kumar Abbaraju V D N, Andrews B S A, Nagaraju Dasari, Nagu Korupolu, Melphan as Anticancer and New Insights of Drug as Parenteral Dosage form against SARS-CoV-2 by Using Development and Validation , November 18, 2020, Vol. 11, Issue 1, Pages 1437–1446 DOI: 10.26452/ijrps.v11iSPL1.3686, https://ijrps.com/v11si1/2911
[47] GAURAV KUMAR SINHA, Efficient Test-Time Compute Scaling for Resource-Constrained Large Language Models Vol. 32 No. 1 (2024): JOCAAA, DOI: https://doi.org/10.1109/ICAC3N56670.2022.10074458 https://eudoxuspress.com/index.php/pub/article/view/5918
[48] GAURAV KUMAR SINHA , The Impact of Artificial Intelligence on Predictive Quality Assurance in Modern Manufacturing, Vol. 33 No. 05 (2024): JOCAAA, https://doi.org/10.1109/ICAC3N56670.2022.10074458 , https://eudoxuspress.com/index.php/pub/article/view/5919
[49] GAURAV KUMAR SINHA , Hybrid Quantum-Classical Neural Networks for Combinatorial Optimization and Machine Learning, Vol. 33 No. 08 (2024): JOCAAA, DOI: https://doi.org/10.1109/ICAC3N56670.2022.10074458, https://eudoxuspress.com/index.php/pub/article/view/5921