

Article

From Risk Management to Accountability: Security, Compliance, and Governance in AI-Enabled and Cloud-Driven Ecosystems

Muslima Jahan Diba^{1*}

*Department of Accounting, LeBow college of business, Drexel University Philadelphia,
Pennsylvania, United States*
muslimajahan1997@gmail.com

Abstract: The rapid adoption of artificial intelligence (AI) and cloud computing is transforming organizational operations while introducing increasingly complex challenges in security, regulatory compliance, risk management, and accountability. Traditional risk management approaches, which primarily emphasize identifying and mitigating threats, are often insufficient for dynamic, distributed, and interconnected AI-enabled and cloud-driven environments. This review examines the transition from conventional risk management toward an integrated governance approach that connects security, compliance, and accountability across the technology lifecycle. Particular attention is given to the shared responsibility model, where fragmented ownership among cloud providers, technology vendors, and organizational stakeholders can create significant accountability gaps. The review further examines how common controls, clearly defined responsibilities, risk-based requirements, continuous monitoring, governance metrics, and operational evidence can strengthen organizational oversight. Accountability artifacts and traceability mechanisms are also considered for their ability to connect data, decisions, controls, system activities, and responsible parties across complex technology environments. Key challenges include regulatory complexity, evolving AI models, third-party dependencies, fragmented ownership, evidence management, and excessive governance burdens. The analysis indicates that effective governance depends not on isolated technical controls but on coordinated structures that integrate security, compliance, and accountability. A lifecycle-based, evidence-driven governance model can improve transparency, operational resilience, regulatory assurance, and responsible management of AI and cloud technologies. These findings highlight the importance of continuous assurance, measurable thresholds, third-party oversight, and clearly assigned accountability for managing evolving technological risks.

Keywords: AI governance; Cloud security; Regulatory compliance; Risk management; Accountability.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

1. Introduction

Artificial intelligence (AI) has become an integral part of the digital infrastructure, along with cloud computing and distributed digital infrastructure, which have reshaped the way organizations manage information, provide services, and make operational decisions. From automating decisions and forecasting trends to detecting fraud and safeguarding cyber networks, resource allocation and customer interactions, AI-powered systems are taking the lead in a variety of tasks [1].

Simultaneously, cloud driven architectures offer scalable computing, storage, application service and interconnected systems and environments that enable such systems to function across organizational and geographic boundaries. While these technologies offer significant potential for efficiency and innovation, they do bring some challenges in terms of security, compliance, and governance that are not easily solved with traditional risk management [2]. The expansion of AI and cloud ecosystems has changed the nature of organizational risk. The traditional risk management processes are mainly concerned with the identification, estimation, and reduction of the threats by adopting controls. However, in AI-enabled environments, risks can manifest from data quality, model drift, lack of model explainability, biased outputs, unauthorized use of data, and interactions between the automated systems and humans [3]. In cloud environments, shared infrastructure, third party dependency, data flows, distributed data, identity management, configuration issues and ever-evolving service architectures compound the complexity. This means risk is not a technical/operational problem anymore. It is becoming more and more about accountability, regulatory responsibility, transparency and organisational oversight. Security is also one of the core pillars of this dynamic landscape, as the reliance of AI and cloud systems on significant data sharing and interwoven digital services makes it essential to have robust security measures in place [4]. Confidentiality, integrity and availability of data can be compromised through unauthorized access, data breaches, adversarial attacks, insecure application programming interfaces, model manipulation, and cloud misconfigurations. For effective protection, this has to be combined with integrating security controls with identity and access management, encryption, monitoring, vulnerability management, incident response, and resilience mechanisms [5]. However, the use of technical safeguards does not automatically ensure an organization is fulfilling legal, ethical and regulatory requirements. Compliance adds to the complexity. New privacy, cybersecurity, data protection, financial services, and AI regulations are pushing companies to show how their digital systems are designed, operated, monitored, and controlled. The complexities of managing AI and cloud environments in multiple markets are exacerbated by the fact that there are differences between jurisdictions and regulatory systems. Governance structures out of which these responsibilities are coordinated [6]. Effective governance defines roles, the rights to make decisions, accountability processes, policies, risk ownership, audit processes and oversight processes. In AI enabled and cloud driven ecosystems, the framework for governance should also incorporate considerations for model lifecycle management, data stewardship, third party risk, explainability, human oversight, continuous monitoring and incident accountability [7]. It addresses the interaction of technological risk to regulatory requirements and organizational responsibility, and looks at the shortcomings of the fragmented control strategies. Special focus is placed on AI's related risks, cloud security, regulatory alignment, governance structures, accountability mechanisms, resilience, and continuous assurance. Interlinking these dimensions, a wider framework for responsible digital risk management can be created, which shows how security measures limit exposure, compliance creates obligations, governance assigns responsibility and accountability provides a framework to show that AI and cloud systems are controlled, transparent and meet organizational and regulatory requirements [8].

2. Method

To conduct a comprehensive synthesis of governance, security, and compliance mechanisms within AI-enabled and cloud-driven ecosystems, this review adopts an integrative literature review methodology. This approach enables the synthesis of emerging theoretical concepts, practical frameworks, and regulatory developments across cross-disciplinary domains.

Search Strategy and Source Selection

A systematic search was conducted across prominent academic databases and institutional repositories, including IEEE Xplore, ACM Digital Library, Web of Science, ScienceDirect, and official publications from standards organizations (e.g., ISO/IEC, NIST). Keywords and Boolean operators

utilized in the search string included: ("AI governance" OR "Artificial Intelligence governance") AND ("Cloud security" OR "Cloud ecosystems") AND ("Regulatory compliance" OR "Compliance frameworks") AND ("Accountability" OR "Shared responsibility model").

Inclusion and Exclusion Criteria

- **Inclusion Criteria:**

1. Peer-reviewed journal articles, conference proceedings, and recognized international standards (e.g., ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, EU AI Act) published between 2018 and 2026.
2. Literature directly examining the intersection of cloud security, AI model governance, accountability artifacts, or regulatory alignment.

- **Exclusion Criteria:**

1. Articles focusing solely on technical hardware specifications without governance or security implications.
2. Non-peer-reviewed opinion pieces or literature lacking clear methodologies or framework references.

Data Extraction and Analytical Synthesis

Selected studies were analyzed using thematic synthesis. Extracted data points were categorized into core structural dimensions:

1. The transition from traditional risk management to continuous accountability orientations.
2. Mapping of security and compliance standards (Table 2).
3. Evaluation of AI lifecycle metrics, operational thresholds, and traceability mechanisms.

3. Results

The analytical synthesis of the literature reveals critical transitions in how organizations approach risk, governance, and compliance within complex AI and cloud environments.

1. Paradigm Shift from Risk Assessment to Continuous Accountability

The comparative analysis indicates a fundamental shift in operational paradigms (Table 1):

- **Unit of Analysis:** Transitioned from evaluating isolated technical assets, threats, and vulnerabilities toward auditing decisions, outcomes, and full chains of custody.
- **Assurance Timing:** Evolved from periodic annual attestations to real-time continuous monitoring against predefined risk thresholds.
- **Evidence and Ownership:** Moved away from static policy questionnaires toward dynamic, versioned operational evidence (e.g., execution logs, test results, and data provenance links) assigned to specific control owners.

2. Harmonization of Regulatory and Technical Frameworks

The evaluation of primary international standards highlights both complementary capabilities and limitations in establishing organizational accountability (Table 2):

- Information security standards like **ISO/IEC 27001** and **NIST CSF 2.0** provide robust foundational management systems and governance functions, but often lack explicit controls tailored to AI-specific behaviors (e.g., model drift, prompt injection, data poisoning).
- Frameworks such as the **NIST AI RMF 1.0** and **ISO/IEC 42001** effectively bridge this gap by defining auditable lifecycle oversight (Govern, Map, Measure, Manage).
- Hard law regulations, including the **EU AI Act**, **GDPR**, and **DORA**, mandate structured traceability artifacts, third-party vendor registers, post-market monitoring, and strict human-in-the-loop oversight mechanisms.

3. Operationalization through Governance Metrics and Traceability

The results demonstrate that bridging the accountability gap in shared responsibility models requires two primary technical enablers:

- 1. **Quantitative Thresholds:** Establishing measurable metrics—such as unpatched critical vulnerabilities, unauthorized access attempts, prediction error rates, and model drift indicators—enables automated triggers for control escalation or system suspension.
- 2. **Accountability Artifacts:** Multi-layered digital ecosystems depend on end-to-end traceability (Figure 1 & Figure 2). Documenting data provenance, pipeline configurations, model versions, and human overrides creates an immutable audit trail necessary for regulatory compliance and post-incident investigation.

Shared Responsibility and the Accountability Gap in Cloud Driven Ecosystems

The impact of cloud computing has truly shifted the burden of responsibility for information security, data protection and operational resilience. Cloud driven ecosystems are a departure from traditional on premises environments where organizations have direct control over physical infrastructure, networks, applications and data, and instead distribute control between cloud service providers, customers, software vendors, managed service providers and others [9]. Shared responsibility is a typical form of this distribution. In this approach, the cloud services provider typically handles security and availability of the underlying infrastructure, with the customer handling security and usage, identity management, access controls, application configuration, data protection, and so on [10]. The allocation of the precise service is variable based on the service model, contractual agreements and provider architecture. The shared responsibility model can enhance security by enabling specialised providers to run infrastructure at a capacity that might be hard for individual providers to reach. Providers can deploy all their physical security, infrastructure monitoring, redundancy, vulnerability management and incident response capabilities (Table 1). Transfer of operational responsibility does not mean the same thing as transfer of organizational accountability, however. An organization can be very dependent on the infrastructure security of the cloud provider yet largely responsible for the information that it processes inside the environment [11]. This separation also leaves a space for accountability if there is poor delineation of responsibilities or if organizations assume that providing security services involves them in meeting the security provider's governance requirements. The accountability gap is even more critical in multi cloud and hybrid environments. The data can be transferred to multiple cloud services, applications, geographical regions, and third party platforms, making it challenging to create a full chain of responsibility. Infrastructure can be from one provider, software from another vendor, identity services from a third service provider, and AI components provided via an external application programming interface [12]. After an incident happens, it can be hard to identify who was responsible for controlling the problem component, who was supposed to notice the problem, and who was supposed to report it or take action to fix it. Though there may be a shared ownership of responsibility, the overall responsibility for the business outcome rests with the business.

Table 1. From risk management to accountability: shifts in governance orientation

Dimension	Risk management orientation	Accountability orientation	References
Unit of analysis	Assets, threats, and vulnerabilities	Decisions, outcomes, and the chain of custody behind them	[6], [2]
Assurance timing	Periodic assessment and annual attestation	Continuous monitoring against defined thresholds	[14], [6]
Ownership	Departmental and often implied	Named owner for each control, with an escalation path	[11], [3]
Evidence	Policies, questionnaires, and certificates	Logs, versioned records, test results, and traceability links	[5], [15]

Third parties	Contractual assurance at onboarding	Continuous vendor oversight and exit planning	[12], [13]
Failure response	Treat, tolerate, transfer, or terminate the risk	Investigate, remediate, report, and change the control	[16], [15]

Integrating Security, Compliance, and Governance Frameworks

With growing interdependence of AI systems, cloud infrastructure, data platforms, and distributed applications, keeping fragmented control frameworks under check has become quite an ordeal. In the past, security, compliance, and governance were managed in different policies, teams and assessment procedures. Security teams are tasked with securing systems and information, compliance teams are responsible for meeting regulatory and contractual obligations, and governance teams are responsible for setting organizational authority and accountability [13]. While every function is specific to a particular requirement, fully separating the functions can result in duplicated controls, inconsistent risk assessments, lack of clarity of ownership, and mismatches between documented requirements and operational practices. It is therefore necessary to establish an integrated framework between technical controls and regulatory obligations as well as to organisational decision making. The identity, access management, encryption and network security controls, vulnerability management controls, secure development controls, logging and monitoring controls, incident response controls and business continuity controls lessen exposure to cyber threats and operational disruptions (Table 2) [14]. These controls need to be implemented in the infrastructure, applications, interfaces, data repositories, and third party services in distributed cloud architectures. Identity based security is especially important, when users, applications, workloads and services are spread across a number of environments. Therefore, identifying, privileging, device and access requests can be more effectively controlled through continuous verification of identities, privileges, devices, and access requests. Governance sets the rights to make decisions, who takes risk and what happens when things go wrong, who watches, what happens if they do, who is held accountable, and how (Figure 1) [15]. The alignment of information technology processes with organisational goals can be achieved with the support of ITIL and COBIT frameworks; the management of information security and risk with the support of ISO based management systems. These frameworks should not be applied in the form of a list of requirements. They are more meaningful if they relate to overlapping controls and responsibilities that span multiple frameworks, such as where a single operational control can meet multiple security, compliance and governance goals.

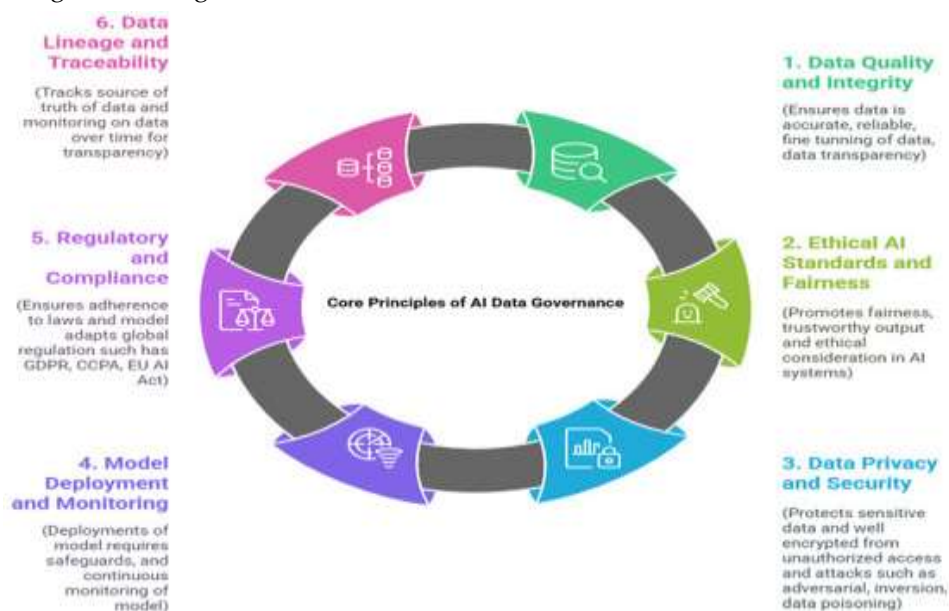


Figure 1. The Importance of AI Data Governance in Large Language Models [39]

Table 2. Principal standards and regulatory instruments and their contribution to accountability.

Instrument	Primary focus	Contribution to accountability	Limitation	References
ISO/IEC 27001	Information security management system	Formal risk treatment, defined responsibilities, internal audit, and management review	Scope is set by the organization, so AI specific risks may fall outside it	[17]
NIST Cybersecurity Framework 2.0	Outcome based cybersecurity risk management	Govern function ties security to strategy, roles, and oversight	Voluntary, and does not prescribe evidence formats	[7]
NIST AI Risk Management Framework	Trustworthy AI risk management across the lifecycle	Govern, Map, Measure, and Manage functions that link context to action	Voluntary, and needs adaptation to sector and system	[6]
ISO/IEC 42001	AI management system	Auditable cycle of policy, roles, impact assessment, and improvement	Certifies the management system, not the behavior of each model	[18]
EU AI Act	Legal obligations for high risk AI	Mandatory documentation, logging, human oversight, and post market monitoring	Phased application and evolving guidance	[8]
GDPR	Personal data protection	Duty to demonstrate compliance and to assess impact where risk is high	Not designed to govern model behavior beyond personal data	[9]
DORA	Operational resilience of financial entities	Third party registers, incident reporting, and exit planning	Sector specific	[13]

Governance Metrics, Thresholds, and Operational Evidence

Measurable evidence is essential for effective governance as it allows the security performance, compliance status, operational resilience and risk exposure to be evaluated. Policies and governance frameworks set expectations; the effectiveness of policies can only be demonstrated through more than just documentation. In the AI enabled and cloud driven ecosystem, governance needs to be backed by measurable indicators, defined thresholds, ongoing monitoring, and evidence of operations [16]. These mechanisms can be used to see if the organization's existing controls are operating as designed, and if there are new risks that need to be addressed. Governance metrics should be directly linked to organizational goals and known risks. Standard security metrics can involve the number of vulnerabilities that have not been resolved, violations involving privileged access, security incidents, patching performance, failures in authentication and the mean time to detect and respond to incidents [17]. For cloud environments, there are more configurations to monitor, services to keep available, backups to check integrity, data that should be exposed and checked, identity permissions that should be monitored, and third party dependencies to watch. These measures serve as a quantitative measure of the control environment and enable changes in risk exposure to be identified over time. One of the reasons thresholds are important is that they can only be useful once acceptable levels of performance have been established beforehand. A threshold may identify a point at which a condition needs to be explored, escalated, remediated or managed [18]. For instance, a company could set thresholds for high-risk vulnerabilities, for too many

privileged accounts, for extended outages of services, for missing security controls, for outstanding compliance issues, or for outstanding findings. Thresholds should not be set at random but on a risk basis. Depending on the type of data involved and the nature of the AI application, a low risk operational deviation can be corrected routinely, while a control failure with sensitive data or a critical AI application must be escalated immediately [19]. Some governance metrics are added to the traditional cybersecurity metrics for AI systems. Evidence of the ability of an AI system to continue functioning within approved conditions is provided by model performance, prediction errors, data quality, drift, abnormal input patterns, explainability measures, human override frequency and monitoring coverage. Depending on the system purpose and risk, the appropriate metrics are determined. A model for low impact automation can have a different set of monitoring requirements than one that's involved in financial, employment, healthcare, etc. decisions that have consequences [20]. The criteria for acceptance should thus be described in measurable terms in advance of deployment and monitored during the lifespan of the model. Finally, governance maturity is about the potential for measurable information to enable accountable decisions. Metrics are used to gain visibility, thresholds define conditions for action and operational evidence shows that the control/operational responsibilities are actually in place and working [21]. These should run alongside, not just be part of periodic audits, in AI-enabled and cloud-driven ecosystems. An evidence based approach enhances transparency, allows for intervention at an earlier stage of the risks, and provides a defensible record of implemented and monitored security, compliance and governance decisions.

Accountability Artifacts and Traceability

In an AI enabled and cloud based ecosystem, accountability relies on the ability to prove where the decision was made, what types of controls were used, what was known to make the decision and what measures were used to track the results of the action. While accountability is important, it can only take meaning when the responsibilities it entails can be worked out through a reliable record [22]. Accountability artifacts are then used as documentary and technical evidence for linking governance requirements with operational activities. They serve as a foundation for internal checks and controls, regulatory compliance evaluation, incident analysis, and organizational learning. A special characteristic of cloud environments is the distribution of responsibility over a number of organizational and technical layers, which makes traceability an especially relevant issue [23]. Cloud infrastructure, managed databases, external APIs, identity providers, software libraries and third party applications may all be used in a single service. Relevant evidence may then be spread out in various systems and organizations upon an incident. Centralized asset inventories, dependency records, logging mechanisms and contractual documentation can aid in determining which component was involved and which party was responsible for the control in that component. The outputs of AI systems that can change due to the data, model versions, prompts, configurations, processing pipelines, and deployment environments add extra levels of traceability requirements [24]. Records should thus document relevant phases in the AI lifecycle, such as data provenance, versions of datasets, development of the AI models, results of validation, approvals for deployment, changes to the configuration, results of monitoring, and major interventions. Version control is especially crucial since an application can give different results when it has been updated due to changes in the model, data, prompt structure, or supporting service [25].

Challenges and Governance Practices

Governance of AI enabled and cloud-driven ecosystems is complex due to scale, interdependence, and constant change of modern digital environments. With an active business continuity plan, organizations have to ensure there is a parallel alignment of security controls, regulatory requirements, technological change, third party relationships and accountability mechanisms. Traditional governance models tend to assume fairly stable governance arrangements that have well-defined governance structures [26]. Cloud services and AI applications push the boundaries of these assumptions due to the constant shift in infrastructure, data, applications, and responsibilities. Good governance is thus dependent on adaptive practices that allow governance to

remain effective while not unnecessarily hampering the actions of technology (Figure 2). Another major hurdle is the complexity of regulations. There can be variation between jurisdictions regarding data protection, cyber security, AI application, records retention and third party management. To have good governance practices, there should be constant regulatory monitoring, mapping of regulatory requirements, policy review and reassessment of controls [27]. Regulatory requirements should not be treated as a 'check and check' audit exercise but be built in to the design, procurement, development, deployment and monitoring of the system. Cloud and AI ecosystems often rely on third-party software libraries, application programming interfaces (APIs), infrastructure providers, data sources, and specialized services. Finally, good governance requires balance between control and flexibility. Too many steps could also stifle innovation and foster informal arrangements, while inadequate regulation can leave significant risks uncovered [28]. Organizations can enhance accountability using risk based oversight, well-defined responsibilities, continuous assurance, documented evidence, and structured processes for improvement, and allow AI and cloud technologies to mature in a controlled environment.



Figure 2. Multilayered proposals for addressing the challenges of local AI governance [40]

Discussion

As AI and cloud computing are integrated into business operations, the shift from traditional risk management to holistic security, compliance, and governance has gained even more significance. In the previous sections, it has been shown that the understanding of risk in these environments cannot be grasped in isolation as a technical issue. Technical failures in AI systems, cloud infrastructure, data platforms, applications, and third-party services can have operational, regulatory, financial, and accountability impact on each other [29]. A coordinated approach, where security controls and compliance requirements, organizational responsibilities, measurable performance indicators, and operational evidence are all linked throughout the entire system lifecycle, is the most effective approach to governance. One of the central questions is who bears responsibility for the redistribution of responsibilities of cloud computing. In most traditional information technology infrastructures, organizations had more direct control over physical infrastructure, applications, networks, and data [30]. In the cloud driven environments, these functions are spread across cloud providers, customers, software vendors, managed service providers and other external parties. Shared responsibility model offers a framework for technical responsibility but not overall responsibility. The cloud provider is responsible for providing the underlying infrastructure, the customer is responsible for identity management, data protection, application configuration and the appropriate use of the service [31]. As a result, individual controls can be decentralized, and accountability for results are held within the organization. As cloud architectures become more complex, this difference is more significant. Multi cloud or hybrid

environments can include multiple providers, external APIs, managed databases, identity platforms, software services and AI elements. Data may span several systems and locations, and applications may rely on services provided by different organizations. Even though it is a shared responsibility model, there may be an accountability gap when there is no explicit accountability matrix, contractual requirement, escalation process, and ownership structure [32]. With AI, this problem is exacerbated as responsibility is spread throughout the entire AI lifecycle. The behavior of an AI enabled application can be affected by data providers, model developers, cloud infrastructure providers, application developers, system owners and end users. The model output may be unexpected due to training data, model design, deployment configuration, changes in operating environment or due to the misuses [33]. As a result, it is not sufficient to determine the source of the error at a technical level in order to determine accountability. Governance should also define who approved the system, who validated its performance, who monitored it following deployment, and who has the powers to alter and/or halt it. It involves lifecycle based accountability, not just the deployment based responsibility. Conventional cybersecurity controls cannot cope with the new governance demands that AI brings. Security mechanisms can be used to secure an AI system against unauthorized access or malicious manipulation, but they will not answer questions regarding the appropriateness, explainability, reliability or consistency of the system's output with respect to organizational needs [34]. Data provenance, model validation and version control, performance monitoring and human oversight and documentation are thus essential components of AI governance. After deployment, model behavior should be monitored as input data, operating conditions or supporting infrastructure can change over time resulting in changes in model performance. The governance structure should also include conditions for reassessment, retraining, restriction and suspension of a model. These frameworks can be assessed by using governance metrics and thresholds [35]. Policies set expectations, measurable indicators show evidence of whether expectations are being met. For cloud environments, this could be a critical vulnerability that has not been resolved, a violation of privileged access, a configuration deviation, service availability, backup performance, incident response times and compliance findings. Additional model performance, data quality, drift, anomaly, human override, and validation status monitoring of AI systems are also possible [36]. The choice of metrics should be based on the risk of a specific system and not solely on the ease in which they can be measured. One of the key things to remember is that the thresholds are very important because only after a measurement is taken will the need for action be determined. A governance threshold sets a condition that needs to be investigated, escalated, remedied or managed in a governance review. This decreases the amount of subjectivity following an incident has actually happened. Thresholds, however, should be risk based. While a slight deviation in a low impact system might need a routine corrective measure, a similar deviation with sensitive data or a crucial AI application could necessitate immediate action [37]. Therefore, thresholds should be sensitive to the potential consequences, sensitivity and operational importance of the system being monitored. In general, an AI ecosystem and a cloud ecosystem demand a change from traditional risk management to ongoing, evidence-based governance. The goal is not just to identify the risks, but to put in place a means of accountability for the management of the risk throughout the lifecycle of the system. Shared responsibility needs to be accompanied by clear accountability, security and compliance structures need to be linked via common controls, governance metrics need to be linked to risk based thresholds and operational evidence needs to be used for decision making that will be verified [38].

4. Conclusion

AI enabled and cloud driven ecosystems require a governance approach that extends beyond conventional risk management. Shared responsibility must be supported by clear accountability, integrated security and compliance frameworks, measurable governance metrics, defined thresholds, and reliable operational evidence. Traceable accountability artifacts can connect policies and responsible parties across complex technology environments. Continuous monitoring, lifecycle

based AI oversight, third party risk management, and evidence based assurance further strengthen organizational resilience. Effective governance is therefore established not through isolated controls, but through coordinated security, compliance, and accountability practices that enable organizations to manage evolving technological risks while maintaining transparency and regulatory responsibility.

Author Contributions

M.J.D. Conceptualization, literature search and review, methodology, analysis and interpretation of the literature, drafting of the manuscript, critical revision of the manuscript, and final approval of the submitted version.

REFERENCES

- [1] O. S. Owolabi, P. C. Uche, N. T. Adeniken, C. Ihejirika, R. B. Islam, and B. J. T. Chhetri, "Ethical implication of artificial intelligence (AI) adoption in financial decision making," *Comput. Inf. Sci.*, vol. 25, p. 49, 2024. doi: 10.5539/cis.v17n1p49.
- [2] A. Schreiber and I. Schreiber, "AI for cyber-security risk: Harnessing AI for automatic generation of company-specific cybersecurity risk profiles," *Inf. Comput. Secur.*, vol. 33, pp. 520–546, 2025. doi: 10.1108/ICS-08-2024-0177.
- [3] A. T. Shama, "AI Governance Challenges in Banking: Model Explainability, Regulatory Compliance, and the Limits of Traditional Risk Management," *Business and Social Sciences*, vol. 3, no. 1, pp. 1–10, 2025. doi: 10.25163/business.3110901.
- [4] V. Capraro *et al.*, "The impact of generative artificial intelligence on socioeconomic inequalities and policy making," *Proc. Natl. Acad. Sci. USA Nexus*, vol. 3, p. pgae191, 2024. doi: 10.2139/ssrn.4666103.
- [5] O. J. Gstrein, N. Haleem, and A. Zwitter, "General-purpose AI regulation and the European Union AI Act," *Internet Policy Rev.*, vol. 13, pp. 1–26, 2024. doi: 10.14763/2024.3.1790.
- [6] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, U.S. Department of Commerce, Gaithersburg, MD, USA, 2023.
- [7] *Information Technology-Artificial Intelligence-Management System*, ISO/IEC Standard 42001:2023, 2023. [Online]. Available: <https://www.iso.org/standard/81230.html>
- [8] M. M. Hossain and A. T. Shama, "GRC Accountability Gap in AI and Cloud Security: Limitations of Automated Compliance and Risk Control Mechanisms," *International Journal on Orange Technologies*, vol. 7, no. 1, pp. 56–63, 2025. doi: 10.31149/ijot.v7i1.5798.
- [9] D. Flonk, M. Jachtenfuchs, and A. Obendiek, "Controlling internet content in the EU: Towards digital sovereignty," *J. Eur. Public Policy*, vol. 31, pp. 2316–2342, 2024. doi: 10.1080/13501763.2024.2309179.
- [10] J. Pohle and T. Thiel, "Digital sovereignty," *Internet Policy Rev.*, vol. 9, pp. 1–19, 2020. doi: 10.14763/2020.4.1532.
- [11] Y. Chen and P. Esmailzadeh, "Generative AI in medical practice: In-depth exploration of privacy and security challenges," *J. Med. Internet Res.*, vol. 26, p. e53008, 2024. doi: 10.2196/53008.
- [12] J. Mökander, J. Morley, M. Taddeo, and L. Floridi, "Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations," *Sci. Eng. Ethics*, vol. 27, p. 44, 2021. doi: 10.1007/s11948-021-00319-4.
- [13] L. Weidinger *et al.*, "Taxonomy of risks posed by language models," in *Proc. 2022 ACM Conf. Fairness, Accountability, and Transparency (FAccT '22)*, New York, NY, USA: ACM, 2022, pp. 214–229. doi: 10.1145/3531146.3533088.
- [14] A. T. Shama, "Evolution of Software-Defined Networking in Enterprise and Service Provider Networks: Opportunities, Challenges, and Future Directions," *Central Asian Journal of Mathematical Theory and Computer Sciences*, vol. 3, no. 7, pp. 75–83, 2022.
- [15] M. H. Chin *et al.*, "Guiding principles to address the impact of algorithm bias on racial and ethnic

- disparities in health and health care," *JAMA Netw. Open*, vol. 6, p. e2345050, 2023. doi: 10.1001/jamanetworkopen.2023.45050.
- [16] J. Ayling and A. Chapman, "Putting AI ethics to work: Are the tools fit for purpose?" *AI Soc.*, vol. 8, pp. 405–429, 2022. doi: 10.1007/s43681-021-00084-x.
- [17] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy," *IEEE Access*, vol. 11, pp. 80218–80245, 2023. doi: 10.1109/ACCESS.2023.3300381.
- [18] K. Wach *et al.*, "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT," *Entrep. Bus. Econ. Rev.*, vol. 11, pp. 7–29, 2023. doi: 10.15678/EBER.2023.110201.
- [19] T. S. Afsara and C. Proggo, "Privacy Governance Challenges in AI-Enabled Banking Surveillance Systems: From Compliance to Accountability," *Journal of Knowledge Learning and Science Technology*, vol. 5, no. 2, pp. 131–141, 2026. doi: 10.60087/jklst.vol5.n2.009.
- [20] Y. Zhou, T. Ni, W. B. Lee, and Q. Zhao, "A survey on backdoor threats in large language models (llms): Attacks, defenses, and evaluations," *arXiv*, arXiv:2502.05224, 2025. doi: 10.53941/tai.2025.100003.
- [21] P. O. Shoetan, O. O. Amoo, E. S. Okafor, and O. L. Olorunfemi, "Synthesizing AI's impact on cybersecurity in telecommunications: A conceptual framework," *Comput. Sci. IT Res. J.*, vol. 24, pp. 594–605, 2024. doi: 10.51594/csitrj.v5i3.908.
- [22] Y. Walter, "Embracing the future of artificial intelligence in the classroom: The relevance of AI literacy, prompt engineering, and critical thinking in modern education," *Int. J. Educ. Technol. High. Educ.*, vol. 21, p. 15, 2024. doi: 10.1186/s41239-024-00448-3.
- [23] R. Raman *et al.*, "Navigating artificial general intelligence development: Societal, technological, ethical, and brain-inspired pathways," *Sci. Rep.*, vol. 15, p. 8443, 2025. doi: 10.1038/s41598-025-92190-7.
- [24] H. Liu *et al.*, "Unraveling the mechanics of learning-based demonstration selection for in-context learning," in *Proc. 63rd Annu. Meeting Assoc. Comput. Linguistics (Volume 1: Long Papers)*, Vienna, Austria, 2025, pp. 2623–2641. doi: 10.18653/v1/2025.acl-long.132.
- [25] N. Chukwurah, A. B. Ige, V. I. Adebayo, and O. G. Eyieyien, "Frameworks for effective data governance: Best practices, challenges, and implementation strategies across industries," *Comput. Sci. IT Res. J.*, vol. 5, pp. 1666–1679, 2024. doi: 10.51594/csitrj.v5i7.1351.
- [26] A. T. Shama, "Third-Party Risk Management in API-Driven Ecosystems: Continuous Vendor Security Practices and Emerging Challenges," *American Journal of Technology Advancement*, vol. 1, no. 4, pp. 42–50, 2024. doi: 10.31149/ajta.v1i4.4322.
- [27] S. M. Varnosfaderani and M. Forouzanfar, "The role of AI in hospitals and clinics: Transforming healthcare in the 21st century," *Bioengineering*, vol. 11, p. 337, 2024. doi: 10.3390/bioengineering11040337.
- [28] R. J. Torraco, "Writing integrative literature reviews: Guidelines and examples," *Hum. Resour. Dev. Rev.*, vol. 4, pp. 356–367, 2005. doi: 10.1177/1534484305278283.
- [29] T. Birkstedt, M. Minkinen, A. Tandon, and M. Mäntymäki, "AI governance: Themes, knowledge gaps and future agendas," *Internet Res.*, vol. 33, pp. 133–167, 2023. doi: 10.1108/INTR-01-2022-0042.
- [30] J. Thomas and A. Harden, "Methods for the thematic synthesis of qualitative research in systematic reviews," *BMC Med. Res. Methodol.*, vol. 8, p. 45, 2008. doi: 10.1186/1471-2288-8-45.
- [31] A. T. Shama and A. Biswas, "Cloud Misconfiguration as a Governance Failure in AI-Enabled Healthcare and Finance with Privacy Risk Implications," *International Journal on Economics, Finance and Sustainable Development*, vol. 5, no. 1, pp. 208–214, 2023. doi: 10.31149/ijefsd.v5i1.5799.
- [32] A. Dafoe, *AI Governance: A Research Agenda*, Governance of AI Program, Future of Humanity Institute, University of Oxford, Oxford, UK, 2018. [Online]. Available: <https://cdn.governance.ai/GovAI-Research-Agenda.pdf>
- [33] H. Canton, "Organisation for economic co-operation and development-OECD," in *The Europa Directory*

- of *International Organizations* 2021, Abingdon, UK: Routledge, 2021, pp. 677–687. doi: 10.4324/9781003179900-102.
- [34] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nat. Mach. Intell.*, vol. 1, pp. 389–399, 2019. doi: 10.1038/s42256-019-0088-2.
- [35] S. McLennan *et al.*, "Embedded ethics: A proposal for integrating ethics into the development of medical AI," *BMC Med. Ethics*, vol. 23, p. 6, 2022. doi: 10.1186/s12910-022-00746-3.
- [36] M. Mantymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Defining organizational AI governance," *AI Ethics*, vol. 2, pp. 603–609, 2022. doi: 10.1007/s43681-022-00143-x.
- [37] E. Zaidan and I. Ibrahim, "AI governance in a complex and rapidly changing regulatory landscape: A global perspective," *Humanit. Soc. Sci. Commun.*, vol. 11, p. 511, 2024. doi: 10.1057/s41599-024-03560-x.
- [38] M. M. Hossain and A. T. Shama, "Transition From Monitoring to Observability in Modern Service Assurance Through an Empirical Evaluation of Current Practices," *Innovative: International Multidisciplinary Journal of Applied Technology*, vol. 1, no. 2, pp. 84–93, 2023. doi: 10.51699/8w84ma95.
- [39] P. Hacker, A. Engel, and M. Mauer, "Regulating ChatGPT and other large language AI models: Challenges and prospects," in *Proc. 2023 ACM FAccT Conf.*, New York, NY, USA: ACM, 2023, pp. 1112–1123. doi: 10.1145/3593013.3594067.
- [40] R. Putchakayala and R. Yallavula, "The Intelligent Governance Core: A Multi-Layer AI Framework for Predictive Compliance and Autonomous Digital Analytics," *Int. J. AI BigData Comput. Manag. Stud.*, vol. 6, pp. 171–179, 2025. doi: 10.63282/3050-9416.IJAIBDCMS-V6I1P117.