Information Technology Governance in Cloud Computing: A Framework of Risk Management and Compliance

Ifeanyi Amuche Ilochonwu
Campbellsville University, Campbellsville University, School of Business, Economics and Technology, Louisville, Kentucky, USA

Abstract: Despite the amazing benefits cloud computing has brought organizations, it comes at the cost of new challenges. Cloud computing has changed the way organizations manage their technology. However, with these changes come challenges such as cloud governance and compliance because of the multitenancy, cross-border data flows, and changing regulations that come with a cloud environment. This paper evaluates current IT governance frameworks like COBIT, ITIL, and ISO/IEC 27001/2. Then, highlight the gaps in these frameworks that don't address cloud-specific risks. To address these cloud-specific risks, there is a need for new governance frameworks that improve the risk management and compliance of cloud environments. A new framework was proposed after thoroughly reviewing existing models and methodologies like STRIDE, GDPR, and ITIL. This proposed framework integrates AI and machine learning to detect threats and manage risks in real-time. Unifying fragmented governance approaches offers a scalable and flexible solution capable of adapting to different cloud setups. Beyond the already numerous advantages of this new framework, it also provides a practical means for Organizations with complex regulations across multiple regions to better comply with international standards. This framework provides an effective, clear, and structured way for organizations to manage their security and compliance in the cloud.

Keywords: IT governance, cloud computing, risk management, compliance, cybersecurity

INTRODUCTION

The large-scale integration of cloud computing worldwide has driven the rapid evolution of information technology (IT) management. Cloud services have changed how organizations manage their IT resources, offering scalability, flexibility, and cost-efficiency [1][2]. As more businesses change from traditional on-premises data centers to cloud-based solutions, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), cloud computing models have become the core of modern operations [1][3]. Despite its benefits, Cloud Computing comes with significant governance, risk, and compliance (GRC) challenges due to the decentralized nature of the cloud infrastructures. Maintaining data confidentiality, integrity, and availability in cloud environments is becoming increasingly complex, and organizations must strive to cope with evolving regulations that require strict data protection across multiple jurisdictions [1]. Hence, a robust GRC framework is needed in cloud computing.

IT governance in cloud environments involves developing policies, access controls, and accountability mechanisms to maintain systems and processes [1]. Risk management strategies must also adjust to address emerging threats such as data breaches, service outages, and new cyber threats. There is also a need for organizations to address complex compliance regulations, like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA). These regulations impose a strict requirement on the handling of personal data [2][4]. Although there have been some significant advancements in cloud technologies, there are still some issues in terms of security and privacy. Several pieces of literature highlight these current vulnerabilities and the need for privacy management and adopting adaptive solutions to protect sensitive data [4][5]. To make things worse, cloud computing keeps evolving rapidly, continuously introducing new risks and attack vectors.

This paper proposes a comprehensive framework for IT governance in cloud computing to combat the highlighted challenges. It emphasizes integrating risk management and compliance strategies through a detailed view of existing regulatory frameworks and technological solutions. This Research aims to provide valuable insights into the best practices and emerging

trends for effective GRC strategies in cloud environments [3]. The proposed framework provides a practical guide for organizations to improve their governance, mitigate cloud-specific risks, and ensure compliance in the cloud. Cloud integration continues to grow, but significant gaps must be in managing governance, risk, and compliance effectively. Most of the foundational frameworks, like COBIT, ITIL, and ISO/IEC 27001/2, often need to be revised when applied to cloud environments' dynamic and complex nature. There is a need to address major challenges like multitenancy, cross-border data flows, and shifting regulatory environment. Traditional risk management methods also require more agility to respond with better initiative to new upcoming clod-specific threats such as data breaches and service interruptions.

This paper addresses the gaps highlighted in the current frameworks by proposing an integrated governance framework tailored to cloud environments. The framework proposed in this paper improves traditional GRC models by modifying them and including adaptive risk management strategies that leverage AI and machine learning for proactive and automated threat detection and compliance. This upgraded approach ensures that organizations can maintain robust governance, reduce risks, and follow complex regulatory requirements in our increasingly cloud-dependent world.

LITERATURE REVIEW

IT governance has become a very important aspect of cloud computing, especially as more and more organizations rely on cloud services ([6]). It is necessary to have effective governance frameworks for managing risks and ensuring compliance with important standards and policies. Understanding security vulnerabilities, service delivery models, and the known risks of cloud computing is essential when establishing strong governance. This literature review analyzes existing research in cloud computing frameworks to propose a more extensive framework for risk management and compliance in cloud governance. Organizations gain a lot from the services rendered by cloud computing, but they are also faced with new governance challenges, especially compliance and security risks [7]. This review was conducted systematically, focusing on key concepts related to cloud security, service models, and risk management. The sources referenced in this review were chosen based on their relevance to IT governance in cloud environments and their contributions to cloud computing-related risks and compliance challenges.

Brandis et al. (2019) developed a framework addressing the compliance challenges in cloud environments concerning the decentralization of services [8]. They hammered the impact of structured compliance management in reducing regulatory violations. However, they relied on data from just two organizations, limiting their findings' scope. Although their framework properly covers the balance between cloud adoption and regulatory compliance, clarifying and further exploring if it applies across diverse environments is necessary. In 2019, Bounagui et al. emphasized the fragmentation of governance frameworks like COBIT, ITIL, and ISO/IEC 27001/2 [9]. They proposed a unified approach for managing cloud risks, which aligns with broader governance goals in cloud computing. However, practical applications of integrated frameworks across various cloud models still need to be developed. Their approach to fragmentation raised concerns about the effectiveness of existing frameworks in providing comprehensive governance solutions for cloud environments. Faizi and Rahman (2019) highlighted the challenges faced in aligning IT governance with business objectives in cloud settings [10]. Just like Bounagui et al., they mentioned similar concerns about fragmentation in governance but only offered theoretical solutions [9]. There needs to be more real-world implementation strategies and a need for practical and not just theoretical frameworks.

Apeh et al. conducted a study exploring cloud environments' risks, such as data security, vendor management, and legal compliance, in 2023 [1]. They spoke about the need for the current Governance, Risk, and Compliance (GRC) frameworks to adapt to these risks' evolving nature adequately. Stein et al. (2020) also emphasized the necessity of constantly adapting governance strategies, especially for sectors like Certified Public Accountant (CPA) firms [11]. Their focus on audit processes narrowed the relevance of the contribution to wider organizational governance. It raised even more concerns about the need for frameworks covering different aspects of cloud governance. In 2020, Tissir et al. broached a new perspective focusing on Cybersecurity and how standards like ISO and NIST are difficult to apply in cloud-specific contexts [12]. They pointed out the urgent need for custom-made security frameworks, the same concern raised in 2023 by Oladoyinbo et al., who also highlighted the need for continuously adapting security evaluations to combat the fast-evolving digital threats [13]. Although both of these research papers highlight the need for adaptive cybersecurity

frameworks, they still need to provide practical means of achieving this adaptability, leaving instead a gap in implementation that organizations must navigate.

In 2021, Ullah et al. proposed a multilayered risk management framework for smart city governance based on the Technology-Organization-Environment (TOE) model [2]. Although this research did not focus solely on Cloud computing, it presented an approach for managing distributed risks relevant to cloud ecosystems and offers a basic approach for managing risk in complex environments. Sadly, the TOE model approach to cloud governance remains unexplored. This paper intends to address this gap by creating a refined and adaptive version of the TOE model framework specifically for cloud risk management. The categorization of risks in this research paper provides a good starting point, but tailoring these approaches to cloud governance will require further research.

All the literature reviewed signifies a need for a comprehensive, adaptive, and integrated framework for cloud computing IT governance, risk management, and compliance. Key gaps identified include the need for unified governance models [9], adaptive GRC strategies ([1]), and tailored cybersecurity frameworks [12]. This Research aims to address these gaps by developing a holistic governance framework that combines existing IT models and adjusts to the ever-changing structure of cloud computing. This study will combine theoretical and practical applications to develop more effective and resilient governance strategies that organizations can use to navigate the different aspects of the cloud environment.

METHODOLOGY

This research uses the systematic literature review (SLR) to evaluate current IT governance, risk management, and compliance frameworks in cloud computing environments. The decision to use the SLR model is based on its ability to provide a detailed overview of the existing body of knowledge, following established guidelines for conducting literature reviews, as recommended by previous studies [14]. Peer-reviewed journals, industry reports, and case studies, among others, provide relevant secondary data, focusing on sources that cover governance frameworks, risk management strategies, and compliance measures within cloud computing. The review information creates a governance model that combines best practices while addressing the identified gaps. The search process involves using specific keywords to identify relevant literature to the research. Following the approach of Alouffi et al. (2021), keywords like "IT governance in the cloud," "cloud risk management," "cloud compliance frameworks," and "cloud security challenges" are used [5]. Boolean operators (“AND” and” OR”) are used to add synonyms and alternate phrases to ensure a more detailed search. Major research data sources include academic databases like Google Scholar, Science Direct, and IEEE Xplore. Tools like MyBib or Endnote are used to manage references and eliminate duplicates.

Papers are included if they meet the following conditions:

- Published between 2019 and 2024 to ensure relevance to current trends and technologies in cloud computing.
- Written in English and peer-reviewed.
- Focus on IT governance, cloud computing, risk management, or compliance models.

Papers are only included if they are relevant to or unrelated to governance in cloud environments or solely focused on the Technical (non-organizational) aspects of cloud computing. This step ensures the relevance of the data collected [14].

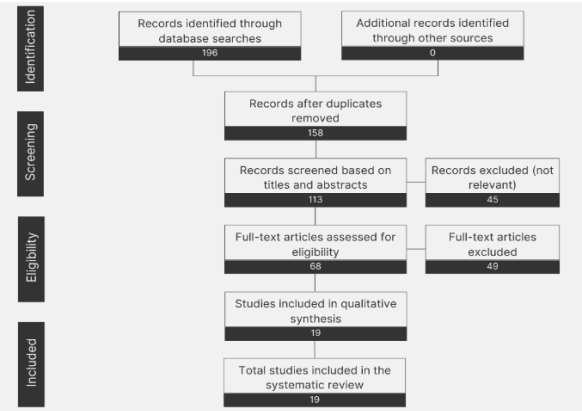

Figure 1: PRISMA Chart

A checklist-based quality assessment ([5]) ascertains that the research data included in this study is methodologically sound. Every paper is assessed based on its standards, clarity of contributions, and relevance to risk management and cloud governance. Papers meeting the predefined threshold score are kept for continued analysis. The method used for data extraction involves categorizing findings based on the research questions. The approach used by Heidari and Jafari Navimipour (2021) is used for extracting both

qualitative and quantitative data [15]. Qualitative data includes descriptions of governance frameworks, while quantitative data includes metrics related to compliance failures or risk incidents. The extracted data is collated using a narrative approach to identify common factors and gaps in existing research. This enables comparison of the multiple governance frameworks and their applicability to cloud environments.

Real-world applications support the proposed framework through case studies that simulate its implementation. For example, a fictional case study of a financial services company using a hybrid cloud model portrays the framework's usability. Automating security threat monitoring using machine learning and artificial intelligence tools will help companies improve their risk management capabilities while ensuring compliance with SLAs with third-party providers. This simulation demonstrates the practical efficiency of the framework, providing insights into its real-world use. This research recognizes that there might be possible limitations around data availability and the evolving nature of cloud governance. Although the SLR focuses on peer-reviewed literature, the progressive nature of regulations in cloud computing might render some frameworks outdated. However, this is addressed using a similar technique to Alouffi et al. (2021), which involves identifying trends that show signs of future directions for governance models [5]. The methodology employed in this study combines the methods of Rodrigues et al. (2019), Alouffi et al. (2021), and Qasem et al. (2019) to provide a structured framework for reviewing IT governance in cloud computing [3][5][14]. This research aims to propose an innovative framework for cloud governance that combines the findings of multiple sources and addresses the unique risks and compliance challenges of cloud environments.

Proposed Framework for IT Governance in Cloud Computing

The proposed framework is designed to enhance IT governance in cloud computing by focusing on four critical components: adaptability, risk management, compliance, and vendor oversight. Drawing from established models like COBIT and STRIDE, it introduces innovative concepts, including AI and machine learning (ML) for proactive risk management and real-time governance.

Diagram of Framework for Case Study Application

Here is a visual representation of the proposed framework, displaying the interaction between adaptability, risk management, compliance, and vendor oversight. AI and ML are integrated into all layers for real-time governance.

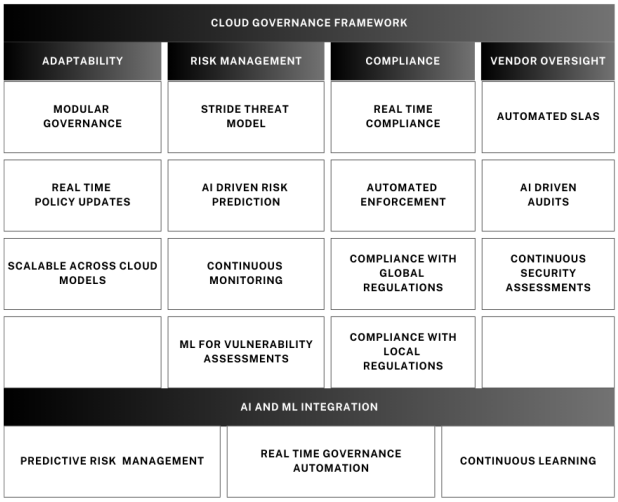

Figure 2: The Proposed Framework (Source: Self-Adapted)

Risk Management

Effective risk management in cloud environments requires regular evaluation of potential threats. The different cloud computing deployment models (private, community, public, and hybrid) have unique risk profiles. Private clouds are expensive and require many resources but provide stronger security controls [4]. Public clouds, on the other hand, although affordable and scalable, do not offer strong security controls, and this translates to a higher risk of data breaches and compliance violations.

Hybrid models combine the best features of the public and private cloud deployment models, but they require clear governance to manage data exposure risks and compliance across numerous environments. Governance frameworks must address these deployment-specific risks to ensure operational efficiency and security.

Building on Abdulsalam and Hedabou (2021), this framework uses the STRIDE model for threat identification and modeling across public, private, and hybrid cloud environments [4]. This model identifies security vulnerabilities, potential data breaches, and compliance risks, making it essential for handling cloud-specific risks. Further risk management is achieved using the multilayered risk management approach from Ullah et al. (2021), which categorizes risks at various levels: technology, organization, and

environment, yielding custom governance strategies [2]. For instance, public clouds may need more data protection and threat detection processes than private clouds.

This framework is centered on continuous vulnerability assessments, cross-environment risk modeling, and real-time threat detection. These processes ensure that emerging threats are addressed before they cause harm. Brandis et al. (2019) highlighted the complex nature of distributed services and the need for risk models to adapt to cloud-specific contexts and prioritize continuous monitoring and mitigation of emerging threats [8].

Threat		Security Property Violated
Spoofing	→	Authentication
Tampering	→	Integrity
Repudiation	→	Non-repudiation
Information Disclosure	→	Confidentiality
Denial of Service	→	Availability
Elevation of Privilege	→	Authorization

Figure 3: The STRIDE Threat Model diagram [16]

Compliance

Each region has a different cloud regulatory standard, and compliance is the most difficult aspect of cloud governance. Compliance is very important in cloud computing, especially given the dynamic nature of cloud environments. Abdulsalam and Hedabou (2021) emphasized the need for more traditional security measures, such as encryption, to address compliance needs properly [4]. Compliance in cloud computing involves regulatory frameworks like GDPR, HIPAA, and industry standards (ISO/IEC 27001), and they demand continuous monitoring of data privacy, access management, and security controls. For a governance framework to be termed efficient or effective, it must have mechanisms to ensure compliance in static and dynamic environments.

As noted by Brandis et al. (2019) and Tissir et al. (2020), this framework hammers on real-time compliance monitoring and automated processes to meet data protection laws such as GDPR, HIPAA, and others [8][12]. It involves using automated tools to continuously track an organization's compliance status, identify deviations, and enforce corrective measures. These tools also provide intuitive governance strategies that adapt to regulatory changes and ensure compliance without human intervention. For example, suppose a cloud service provider operates in multiple regions. In that case, the framework ensures that all branches comply with their region's specific regulations, such as data sovereignty and encryption standards. The research by Apeh et al. (2023) also highlights the importance of well-rounded Governance, Risk, and Compliance (GRC) strategies, particularly in addressing dynamic cloud environments [1]. Automated tools should be used to continuously track compliance status, identify deviations, and enforce corrective measures.

Figure 4: Major GDPR Implications [17]

Article	Description	Organization	Processes	Systems
1 Territorial scope	**Much broader territorial scope** extends applicability to organizations outside of the EU processing data relating to EU citizens	→	↓	↓
2 Explicit consent	Stricter requirements regarding **explicit consent to the storage and transformation** of data, which has to be **obtained and documented**	↓	→	→
3 Right of access	**Information on controller** and the **stored personal data** has to be granted to the data subject	↓	↑	↑
4 Right to rectification	**Incorrect data** has to be **rectified without undue delay** upon request from the data subject	↓	↑	↑
5 Right to erasure	New requirement to **delete data if it is no longer used** for the purpose it was originally collected or if **consent for the storage of data is revoked**	↓	↑	↑
6 Right to data portability	Individuals have the right to **request copies of personal data in a structured, commonly used and machine-readable format**	↓	↑	↑
7 DP by design and by default	Data protection by design and by default have to be ensured via **developing default privacy protection mechanisms** and by implementing **monitoring processes**	↓	↑	↑
8 Notification requirements	**Data breaches** must be **reported** to the supervisory authority and communicated to the respective data subject(s), posing **potentially severe reputational risks**	↓	↑	→
9 Data protection officers	A data protection officer has to be nominated as dedicated role to **closely monitor internal compliance with the GDPR**	→	→	↓
Sanctions	Non-compliance can result in serious **fines of up to EUR 20 m or 4% of the total worldwide annual turnover**—private enforcement is expected to further increase that impact	OpRisk		↑

↓ Low impact on banks → Medium impact on banks ↑ High impact on banks

Figure 5: Overview of selected GDPR requirements [17]

Vendor Oversight

Vendor oversight is crucial for cloud environments, especially when third-party service providers control key infrastructure components. Drawing from Apeh et al. (2023), this proposed framework includes periodic audits, security assessments, and clear Service-Level Agreements (SLAs) to ensure that vendors adhere to governance and security standards [1]. Cloud service providers and the complexity of cloud ecosystems also impose significant risks. [11]. Data that passes through multiple jurisdictions often comes with additional risks. To combat this, organizations should implement regular vendor performance evaluations and compliance monitoring to ensure continuous adherence to their contract obligations and security policies.

Adaptability

Cloud service models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—each present their form of governance challenges. As highlighted by Faizi and Rahman (2019), governance policies must be tailored to these service models and deployment types (public, private, hybrid) [10]. For instance, IaaS requires infrastructure-level control, while SaaS demands strict data privacy protocols due to its multi-tenancy structure. This framework integrates COBIT, ITIL, and ISO/IEC 27001/2 to offer a unified governance structure across service and deployment models. Bounagui et al. (2019) recommend a unified governance structure to reduce the fragmentation commonly observed in cloud environments [9]. By adopting this framework, organizations can ensure consistent governance across multiple cloud models, reducing gaps and enhancing security.

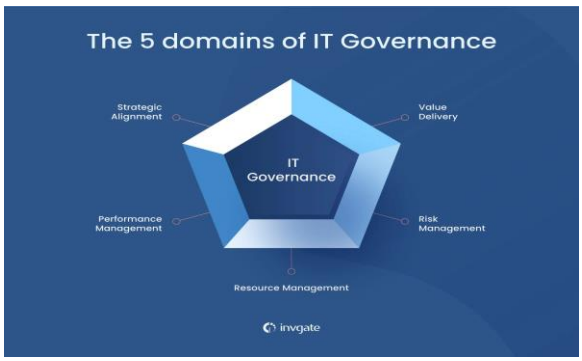

Figure 6: IT Governance Model [18]

AI and Machine Learning for Proactive Risk Management and Real-Time Governance

Integrating Artificial Intelligence (AI) and Machine Learning (ML) into this framework changes how organizations approach governance. AI presents predictive risk insights, while ML improves compliance accuracy, speed, and threat detection over time. This adaptive learning enables real-time governance, preparing organizations for potential threats and regulatory changes. ML models are trained on historical data to detect emerging security vulnerabilities based on usage patterns and environmental changes. These models improve over time, enabling faster identification of risks. AI analyses cloud environments for compliance breaches and governance failures to achieve real-time governance, providing continuous oversight without manual intervention.

The proposed framework integrates artificial intelligence (AI) and machine learning (ML) to enhance governance practices, enabling a more reliable approach. As Apeh et al. (2023) highlighted, adopting technological solutions like AI and ML is an innovative way of enhancing governance and risk management in cloud environments [1]. One of the core components of this framework is integrating artificial intelligence (AI) and machine learning (ML) to enhance governance practices.

AI tools can predict potential risks and automate compliance processes, providing a proactive approach to cloud governance. For instance, AI-powered models can detect unusual behavior patterns, alerting organizations to potential security breaches before they escalate. Machine learning enhances this by automating vulnerability assessment and improving risk detection to combat evolving threats. These technologies allow organizations to adapt quickly, making them perfect for the constantly evolving cloud environments.

RESULTS AND DISCUSSIONS

Cloud Security and Governance in Cloud Computing

Governance in cloud computing is closely intertwined with security. Abdulsalam and Hedabou (2021) emphasize that cloud security is managed by privacy-enhancing technologies and policy rules designed to protect data and applications deployed in the cloud [4]. They introduce the STRIDE model to systematically analyze cloud vulnerabilities, helping to identify threat vectors before they materialize. IT governance frameworks must integrate these security considerations to ensure a proactive risk management approach.

The service delivery models—IaaS, PaaS, and SaaS—each present unique governance challenges. IaaS allows users to manage deployed applications while lacking full control over underlying infrastructure, necessitating governance policies ensuring infrastructure resilience and security oversight. In PaaS, user control is limited to applications, requiring additional governance focus on platform management and secure data handling. SaaS, with its multitenancy nature, amplifies risks related to data privacy, requiring robust compliance frameworks to manage cross-border data transfers and user access controls.

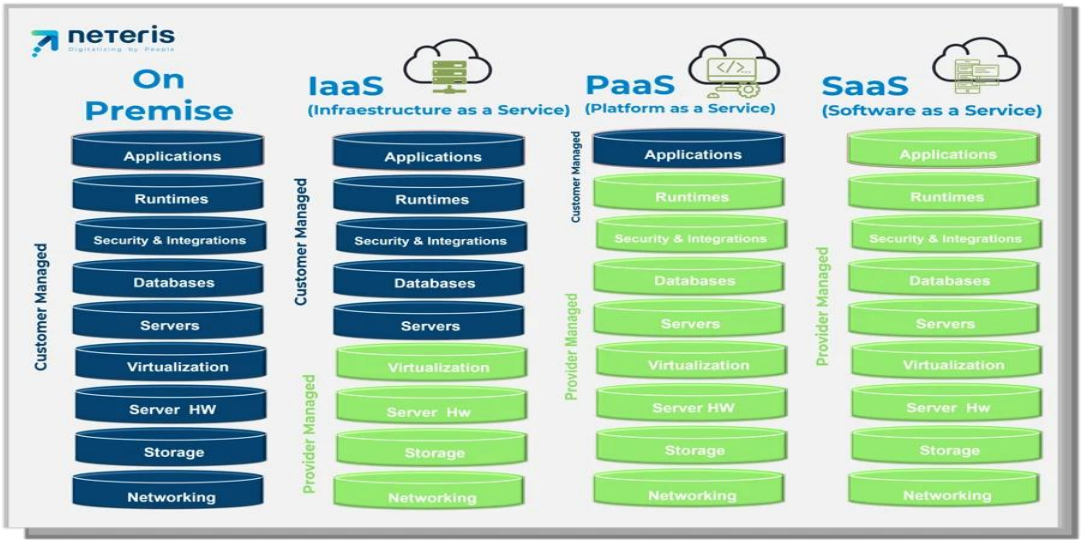

Figure 7: IAAS, PAAS, SAAS [19]

Application of Proposed Framework Using a Fictional Case Study: Financial Services Company

A financial services company adopts a hybrid cloud model to streamline operations while maintaining strict compliance with industry regulations like GDPR and PCI-DSS. With a mix of internal and third-party cloud infrastructure, the company faces significant challenges in managing security, ensuring compliance, and reducing operational complexity. The company implements the proposed IT governance framework to address these issues, focusing on adaptability, risk management, compliance, and vendor oversight with AI and ML integration.

Risk Management

The company uses the STRIDE model to identify threats across its public and private cloud environments to manage risk. By categorizing risks at multiple levels (technology, organizational, and environmental), the company gains a more comprehensive understanding of potential vulnerabilities. Real-time vulnerability assessments and cross-environment risk modeling allow continuous monitoring, ensuring emerging threats are detected and mitigated swiftly. AI-powered risk prediction tools are also integrated, enabling the company to automate risk detection and take proactive measures before threats escalate.

Compliance

The company also improves its compliance processes by implementing AI and machine learning (ML) technologies. These tools continuously monitor the infrastructure for GDPR and PCI-DSS compliance violations, automatically updating governance policies in response to changing regulations. Automated real-time compliance checks reduce the need for manual audits and lower the risk of non-compliance penalties. The ML models, designed for vulnerability assessments, continuously learn from new threats, improving risk detection accuracy.

Vendor Oversight

On the vendor oversight side, the company continuously audits its third-party cloud service providers. The governance framework enforces the company's Service-Level Agreements (SLAs) with vendors, ensuring they meet security, privacy, and regulatory requirements. Any deviations from the SLAs trigger automatic alerts, and corrective actions are taken immediately. The company reduces risks related to outsourcing its infrastructure by ensuring strict vendor accountability.

Adaptability

The framework's modular, adaptable structure ensures that governance policies can scale across the

company's hybrid cloud environment. The framework provides consistent governance practices, whether dealing with private cloud infrastructure for sensitive financial data or public cloud services for customer-facing applications. It integrates COBIT and ISO/IEC 27001/2 standards to offer a unified governance approach, minimizing the fragmentation that often plagues hybrid cloud environments.

RESULT

As a result, the financial services company reduces its operational overhead, enhances risk management, and stays compliant with industry regulations. AI-driven real-time insights into potential risks and compliance violations allow the organization to stay ahead of threats, avoid costly fines, and maintain a secure cloud environment. Through this adaptive, technology-driven framework, the company ensures a resilient, scalable governance structure that aligns with its evolving cloud strategy. By adopting this comprehensive framework, organizations across industries can leverage advanced technologies like AI and machine learning to automate governance processes, ensure compliance, and reduce external risks. The modular nature of the framework ensures that it can scale and adapt to changing business needs and regulatory landscapes, making it a versatile solution for the complexities of cloud computing governance.

By incorporating threat modeling techniques (STRIDE), unified governance frameworks (COBIT, ITIL), and technology-driven solutions (AI, ML), this framework aims to provide a robust, adaptive, and resilient structure for organizations leveraging cloud computing. This model ensures that organizations can manage evolving risks, comply with complex regulatory environments, and maintain secure and efficient operations in the cloud. The literature reviewed, including works from Brandis et al. (2019), Bounagui et al. (2019), Apeh et al. (2023), and others, provided critical insights that shaped this framework [1][8][9]. It explained the importance of integrating established IT governance models, developing adaptive GRC strategies, and leveraging technological tools to enhance governance practices in the cloud.

LIMITATIONS

This paper's proposed framework primarily focuses on widely recognized international standards such as GDPR, ISO/IEC 27001, and NIST. However, it may not comprehensively address regional or industry-specific regulations, particularly in sectors with unique compliance requirements, such as healthcare or finance. This limitation may reduce the generalizability of the framework across various industries and regions. Although the framework emphasizes vendor audits and service-level agreements (SLAs), it does not account for variability in third-party compliance capabilities. Cloud Service Providers (CSPs) often need differing levels of adherence to security and compliance standards, which could affect the framework's effectiveness when applied across multiple vendors or global environments.

While AI and machine learning (ML) are proposed to enhance risk management, these technologies have limitations in predicting emergent, unknown threats. The framework may need to be more effective in addressing novel risks, especially as cyber threats in cloud computing continue to evolve. The reliance on AI and ML for compliance automation and threat detection raises questions about technological readiness. Not all organizations may possess the necessary infrastructure or expertise to implement advanced solutions. This could limit the framework's immediate applicability.

Moreover, the framework has yet to be extensively tested in diverse real-world environments. Most insights are drawn from existing literature and theoretical analysis, meaning practical validation through case studies or pilot programs is limited. This may affect the framework's robustness in various organizational contexts. Lastly, while integrating established models like COBIT, ITIL, and ISO/IEC offers a structured approach, challenges may arise when implementing them cohesively across different cloud architectures and organizational structures. As cloud technologies evolve, such as with the rise of edge computing and serverless architectures, the framework may require further refinement to remain relevant, highlighting areas for future research and practical application.

CONCLUSION AND FUTURE WORKS

This research highlights the need to adapt established frameworks such as COBIT, ITIL, and ISO/IEC 27001/2 to effectively address the unique challenges of cloud governance. While existing risk management and compliance models like STRIDE and the TOE model offer valuable methodologies, they require further refinement to meet the distinct risks posed by cloud ecosystems. The identified gaps in the literature emphasize the necessity for a cohesive approach to governance, risk, and compliance in cloud computing.

Looking ahead, future frameworks will increasingly incorporate artificial intelligence (AI) and machine learning (ML) to predict and manage emerging risks in real time [1]. These technologies will be vital in developing adaptive governance strategies that respond dynamically to evolving regulatory environments. Real-time compliance monitoring tools, especially those applicable across multiple jurisdictions, will likely gain importance [8][11]. Developing unified governance models that integrate existing IT frameworks such as COBIT, ITIL, and ISO will become crucial in managing the fragmented nature of current cloud governance strategies.

Future studies should explore the empirical validation of the proposed framework in various industries to assess its practical applicability. This includes studying the integration of AI and ML in governance practices, identifying potential challenges, and evaluating the effectiveness of these technologies in real-world settings [9]. As cloud technologies evolve, so will the associated security threats. Tailoring cybersecurity frameworks to adapt ISO and NIST standards for cloud-specific environments will be critical for future investigation [12][13]. By addressing these trends and challenges, subsequent research can contribute to developing more robust and adaptable governance frameworks, enabling organizations to manage risks while ensuring compliance with changing regulatory requirements effectively.

RECOMMENDATIONS

Organizations should move towards an integrated governance framework that combines COBIT, ITIL, ISO/IEC 27001/2, and GDPR. This unified approach will enhance the efficiency of governance, risk, and compliance management in cloud environments, allowing for cohesive alignment with both operational and regulatory requirements. Incorporating AI and machine learning (ML) into real-time governance strategies is essential for predicting and managing emerging risks. These technologies can improve threat detection, automate compliance monitoring, and facilitate agile responses to evolving security challenges. Organizations should invest in AI-driven tools to enable proactive risk management, particularly in multitenant cloud environments.

Additionally, governance frameworks should be tailored to specific cloud services models such as IaaS, PaaS, and SaaS. For example, SaaS environments face unique multi-tenancy risks requiring robust user access controls and data privacy measures. At the same time, hybrid models require comprehensive policies to ensure security across both public and private clouds. Given the complexity of global regulatory requirements, particularly regarding cross-border data flows, organizations should implement automated compliance tools that continuously monitor and adapt to changing regulations. This will help ensure adherence to frameworks like GDPR, HIPAA, and ISO standards in dynamic cloud environments.

Finally, organizations must ensure their governance frameworks remain adaptable as cloud technologies evolve, including developments in edge computing and serverless architectures. Future research should focus on refining the proposed governance model to address these emerging technologies' risks and compliance needs. By following these recommendations, organizations can achieve more resilient, compliant, and secure cloud operations.

REFERENCES

[1]. A. J. Apeh, A. O. Hassan, O. O. Oyewole, O. G. Fakeyede, P. A. Okeleke, and O. R. Adaramodu, “GRC Strategies in Modern Cloud Infrastructures: A Review of Compliance Challenges,” Computer Science & IT Research Journal, vol. 4, no. 2, pp. 111–125, Nov. 2023, doi: https://doi.org/10.51594/csitrj.v4i2.609.

[2]. F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman, and S. M. E. Sepasgozar, “Risk Management in Sustainable Smart Cities governance: a TOE Framework,” Technological Forecasting and Social Change, vol. 167, no. 1, p. 120743, Jun. 2021, doi: https://doi.org/10.1016/j.techfore.2021.120743 .

[3]. Y. A. M. Qasem, R. Abdullah, Y. Y. Jusoh, R. Atan, and S. Asadi, “Cloud Computing Adoption in Higher Education Institutions: a Systematic Review,” IEEE Access, vol. 7, pp. 63722–63744, 2019, doi: https://doi.org/10.1109/access.2019.2916234.

[4]. Y. S. Abdulsalam and M. Hedabou, “Security and Privacy in Cloud Computing: Technical Review,” Future Internet, vol. 14, no. 1, p. 11, 2021, doi: https://doi.org/10.3390/fi14010011.

[5]. B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, “A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies,” IEEE Access, vol. 9, no. 1, pp. 1–

1, 2021, doi: https://doi.org/10.1109/access.2021.3073203.

[6]. M. Asgarkhani, "The Internet, the Cloud, and Information Technology Governance," International Journal for Applied Information Management, vol. 1, no. 1, Apr. 2021, doi: https://doi.org/10.47738/ijaim.v1i1.5.

[7]. M. Vijverberg, "Management of Cloud Risk Governance: Analyzing Top Risk Topics and a Maturity Model," Studenttheses.uu.nl, 2024, doi: https://studenttheses.uu.nl/handle/20.500.12932/46889.

[8]. K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev, "Governance, Risk, and Compliance in Cloud Scenarios," Applied Sciences, vol. 9, no. 2, p. 320, Jan. 2019, doi: https://doi.org/10.3390/app9020320.

[9]. Y. Bounagui, A. Mezrioui, and H. Hafiddi, "Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models," Computer Standards & Interfaces, vol. 62, pp. 98–118, Feb. 2019, doi: https://doi.org/10.1016/j.csi.2018.09.001.

[10]. S. M. Faizi and S. S. M. Rahman, "Securing Cloud Computing Through IT Governance," SSRN Electronic Journal, 2019, doi: https://doi.org/10.2139/ssrn.3360869.

[11]. M. Stein, V. Campitelli, and S. Mezzio, "Managing the impact of cloud computing.," CPA Journal, vol. 90, no. 6, 2020.

[12]. N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity Management in Cloud computing: Semantic Literature Review and Conceptual Framework Proposal," Journal of Reliable Intelligent Environments, Oct. 2020, doi: https://doi.org/10.1007/s40860-020-00115-0.

[13]. T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. Olaniyi, and O. J. Okunleye, "Evaluating and Establishing Baseline Security Requirements in Cloud Computing: an Enterprise Risk Management Approach," Social Science Research Network, Oct. 25, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4612909 (accessed Sep. 10, 2024).

[14]. H. Rodrigues, F. Almeida, V. Figueiredo, and S. L. Lopes, "Tracking e-learning through Published papers: a Systematic Review," Computers & Education, vol. 136, pp. 87–98, Jul. 2019, doi: https://doi.org/10.1016/j.compedu.2019.03.007.

[15]. A. Heidari and N. Jafari Navimipour, "Service Discovery Mechanisms in Cloud computing: a Comprehensive and Systematic Literature Review," Kybernetes, vol. 51, no. 3, pp. 952–981, Jun. 2021, doi: https://doi.org/10.1108/k-12-2020-0909.

[16]. N. S. Tany, S. Suresh, D. N. Sinha, C. Shinde, C. Stolojescu-Crisan, and R. Khondoker, "Cybersecurity Comparison of Brain-Based Automotive Electrical and Electronic Architectures," Information, vol. 13, no. 11, p. 518, Oct. 2022, doi: https://doi.org/10.3390/info13110518.

[17]. L. Pfannemüller, "General Data Protection Regulation," BankingHub, Jan. 25, 2017. https://www.bankinghub.eu/finance-risk/general-data-protection-regulation (accessed Sep. 18, 2024).

[18]. S. Danby, "IT Governance: Definition, Frameworks, and Best Practices," blog.invgate.com, Mar. 15, 2023. https://blog.invgate.com/it-governance (accessed Sep. 12, 2024).

[19]. Neteris, "Diferencias entre IaaS PaaS SaaS," Neteris.com, Nov. 02, 2017. https://blog.neteris.com/stepforward/servicios-en-la-nube-diferencias-entre-iaas-saas-y-paas (accessed Sep. 18, 2024).

APPENDICES

1. Table I: Quality Assessment Criteria for Selected Papers

S/N	Quality Assessment Questions	Rating Scale
1	Was the research question formulated?	Yes=1, NO=0, Fairly=1
2	Were appropriate academic and industry databases chosen?	Yes=1, NO=0, Fairly=1

3	Were relevant search terms and strategies effectively used?	Yes=1, NO=0, Fairly=1
4	Were inclusion criteria clearly defined?	Yes=1, NO=0, Fairly=1
5	Were exclusion criteria justified?	Yes=1, NO=0, Fairly=1
6	Was a systematic screening process applied?	Yes=1, NO=0, Fairly=1
7	Were studies critically appraised for methodological quality?	Yes=1, NO=0, Fairly=1
8	Was a standardized data extraction protocol used?	Yes=1, NO=0, Fairly=1
9	Was the process documented transparently for reproducibility?	Yes=1, NO=0, Fairly=1
10	Was the PRISMA methodology applied?	Yes=1, NO=0, Fairly=1

Table I: Quality Assessment Criteria (QAC)

- High-Quality Review: 9–10 "Yes" responses
- Moderate-Quality Review: 6–8 "Yes" responses
- Low-Quality Review: 5 or fewer "Yes" responses

2. Table II: Selected papers for the review

S/N	Author	Year	Topic
1	A. J. Apeh, A. O. Hassan, O. O. Oyewole, O. G. Fakeyede, P. A. Okeleke, and O. R. Adaramodu	2023	GRC Strategies In Modern Cloud Infrastructures: A Review Of Compliance Challenges
2	F. Ullah, S. Qayyum, M. J. Thaheem, F. Al-Turjman, and S. M. E. Sepasgozar	2021	Risk Management In Sustainable Smart Cities Governance: A Toe Framework
3	Y. A. M. Qasem, R. Abdullah, Y. Y. Jusoh, R. Atan, and S. Asadi	2019	Cloud Computing Adoption In Higher Education Institutions: A Systematic Review
4	Y. S. Abdulsalam and M. Hedabou	2021	Security And Privacy In Cloud Computing: Technical Review
5	B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz	2021	A Systematic Literature Review On Cloud Computing Security: Threats And Mitigation Strategies
6	M. Asgarkhani	2021	The Internet, The Cloud, And Information Technology Governance
7	M. Vijverberg	2024	Management Of Cloud Risk Governance: Analyzing Top Risk Topics And A Maturity Model
8	K. Brandis, S. Dzombeta, R. Colomo-Palacios, and V. Stantchev	2019	Governance, Risk, And Compliance In Cloud Scenarios
9	Y. Bounagui, A. Mezrioui, and H. Hafiddi	2019	Toward A Unified Framework For Cloud Computing Governance: An Approach For Evaluating And Integrating It Management And Governance Models
10	S. M. Faizi and S. S. M. Rahman	2019	Securing Cloud Computing Through It Governance
11	M. Stein, V. Campitelli, and S. Mezzio	2020	Managing The Impact Of Cloud Computing

12	N. Tissir, S. El Kafhali, and N. Aboutabit	2020	Cybersecurity Management In Cloud Computing: Semantic Literature Review And Conceptual Framework Proposal
13	T. O. Oladoyinbo, O. O. Adebiyi, J. C. Ugonnia, O. Olaniyi, and O. J. Okunleye	2023	Evaluating And Establishing Baseline Security Requirements In Cloud Computing: An Enterprise Risk Management Approach
14	H. Rodrigues, F. Almeida, V. Figueiredo, and S. L. Lopes	2019	Tracking E-Learning Through Published Papers: A Systematic Review
15	A. Heidari and N. Jafari Navimipour	2021	Service Discovery Mechanisms In Cloud Computing: A Comprehensive And Systematic Literature Review
16	N. S. Tany, S. Suresh, D. N. Sinha, C. Shinde, C. Stolojescu-Crisan, and R. Khondoker	2022	Cybersecurity Comparison Of Brain-Based Automotive Electrical And Electronic Architectures
17	L. Pfannemüller	2017	General Data Protection Regulation
18	S. Danby	2023	It Governance: Definition, Frameworks, And Best Practices
19	Neteris	2017	Diferencias Entre Iaas Paas Saas