Cloud Security Governance Guidelines

Research Proposal · August 2022

DOI: 10.13140/RG.2.2.30839.50080/3

4 authors:

Joshua Amah
Lamar University
4 PUBLICATIONS **44** CITATIONS
SEE PROFILE

Nneoma A. Okoroafor
6 PUBLICATIONS **55** CITATIONS
SEE PROFILE

Joseph Mart
Austin Peay State University
15 PUBLICATIONS **107** CITATIONS
SEE PROFILE

Amos Oyetoro
Austin Peay State University
9 PUBLICATIONS **66** CITATIONS
SEE PROFILE

Cloud Security Governance Guidelines

Ugochukwu Amah [ORCID 1]***, Nneoma Okoroafor*** [ORCID 2]***, Joseph Mart*** [ORCID 3]***, Amos Oyetoro*** [ORCID 4]

[1]*Department of Computer Science, Lamar University, Beaumont, United States*
[2]*Department of Computer Science, Prairie View A&M, Texas, United States*
[3]*Department of Mathematics and Computer Science, Austin Peay State University, Clarksville, TN, United States*
[4]*Department of Computer Science, Austin Peay State University, Clarksville, TN, United States*

Email address*: ugochukwujoshua55@gmail.com (Ugochukwu Amah) okoroafornneoma@gmail.com (Nneoma Okoroafor), martjo.expert@gmail.com (Joseph Mart), oyetoro.amos@gmail.com (Amos Oyetoro),*

To cite this article*: Amah, J., Okoroafor, N., Mart, J., Oyetoro, A. (2022). Cloud Security Governance Guidelines.*

10.13140/RG.2.2.30839.50080/3.

Abstract:

Cloud computing is a widely adopted technology that offers many benefits, including cost-effectiveness, scalability, and flexibility. However, the use of cloud computing also poses significant challenges related to data security and privacy. Cloud security governance is a critical component of managing these challenges. This research paper aims to provide an in-depth analysis of cloud security governance, its importance, challenges, and best practices for implementation.

Study findings indicate that cloud security governance is critical in protecting organizational assets and reputation, especially in regulated industries. The study results also highlight the importance of proactive risk management, employee training, and continuous monitoring as essential elements of cloud security governance.

This research paper offers practical insights and recommendations for organizations seeking to improve their cloud security governance practices. This article emphasizes the importance of effective cloud security governance. It provides a valuable framework for developing tailored security policies and procedures that align with the unique requirements of the cloud environment.

Keywords*: Cloud Security, Security Governance, NIST, Amazon Web Services, Microsoft Azure, Google Cloud*

Introduction

In recent years, cloud computing has become an increasingly popular technology for businesses and organizations of all sizes. Cloud computing provides many benefits, including scalability, cost-effectiveness, and flexibility. However, with the benefits come challenges, especially regarding data security and privacy. Cloud security governance is crucial in managing these challenges [1].

Cloud security governance is the set of policies, processes, and procedures used to manage and mitigate the risks associated with cloud computing. These risks include data breaches, unauthorized access, service disruptions, and compliance violations. Effective cloud security governance helps organizations identify and manage these risks, protecting their assets and reputation [6,9,13].

The importance of cloud security governance has increased in recent years as more organizations move their data and applications to the cloud. This shift has increased the complexity of managing data security and compliance, especially in regulated industries such as finance and healthcare. Cloud security governance is

critical in ensuring organizations meet the regulatory requirements for data protection, privacy, and compliance [2].

Despite the critical importance of cloud security governance, many organizations struggle to implement effective practices. The complex and constantly evolving nature of cloud computing requires organizations to be proactive in their approach to security governance. Organizations must understand the risks associated with cloud computing and develop effective strategies for mitigating those risks [5].

This research paper aims to provide an overview of cloud security governance, its importance, challenges, and best practices for implementation. The paper will review the existing literature on cloud security governance, including the various frameworks, models, and best practices.

The paper will use a qualitative research approach, including a literature review and a case study. The report will conclude with a summary of the essential findings and recommendations for future work.

Overall, this research paper aims to contribute to the ongoing discussions around cloud security governance and provide practical insights for organizations looking to improve their security governance practices in the cloud [3].

1. Literature Review:

Cloud computing is a rapidly growing field that offers many benefits, including cost savings, flexibility, scalability, and accessibility. However, it also presents many challenges, particularly around security governance. Cloud security governance is a complex and multifaceted issue that requires a comprehensive and holistic approach to ensure the security, privacy, and compliance of cloud-based applications and services. To address these challenges, many researchers and practitioners have developed models, frameworks, and best practices to help organizations manage their cloud security risks and protect sensitive data and information [6].

One of the key concepts in cloud security governance is the shared responsibility model, which defines the respective roles and responsibilities of cloud providers and

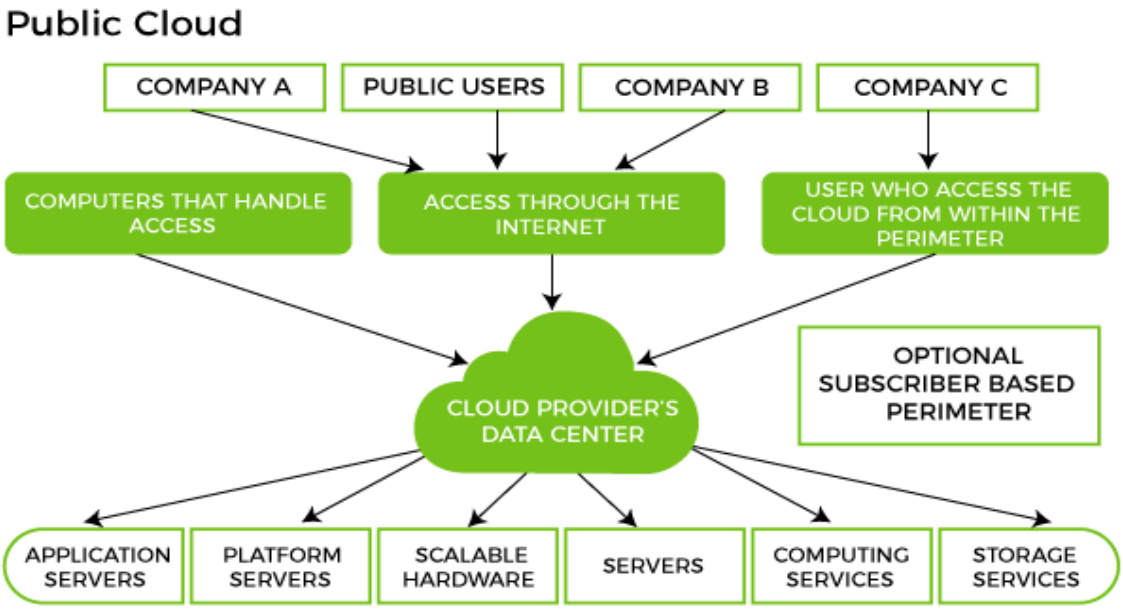

Figure 1 Cloud deployment model

customers in ensuring the security of the cloud environment. According to this model, cloud providers are responsible for securing the underlying infrastructure and services, while customers are responsible for securing their data, applications, and configurations. This model has been widely adopted by major cloud providers, such as Amazon Web Services, Microsoft Azure, and Google Cloud Platform, and is

considered a best practice in cloud security governance [4].

Another important concept in cloud security governance is the risk management framework, which provides a systematic and structured approach to identifying, assessing, and mitigating cloud security risks. The National Institute of Standards and Technology (NIST) has developed a comprehensive risk management framework for cloud computing, which includes five key steps: *categorization, selection, implementation, assessment, and authorization*. Government agencies and private organizations have widely used this framework to assess and manage cloud security risks [8].

Several models and frameworks have been proposed to address specific aspects of cloud security governance. For example, the Cloud Security Alliance (CSA) has developed a Cloud Controls Matrix (CCM) that provides a set of controls and guidelines for cloud security governance, including data governance, identity and access management, and compliance management. The CSA has also developed a Consensus Assessment Initiative Questionnaire (CAIQ) that helps organizations assess the security posture of cloud providers and services [12].

In addition to these models and frameworks, many researchers have proposed innovative approaches to cloud security governance, such as machine learning-based intrusion detection, blockchain-based data protection, and federated identity management. These approaches aim to address specific challenges and opportunities in cloud security governance, such as detecting and responding to advanced threats, ensuring the integrity and confidentiality of data, and managing identities and access across multiple clouds and platforms [1].

Despite the growing body of research on cloud security governance, several challenges and research gaps remain. These include the lack of standardization and interoperability among cloud providers, the difficulty of measuring and quantifying cloud security risks, the limited availability of tools and technologies for cloud security governance, and the need for more user-centered and context-aware approaches to cloud security governance. To address these challenges and advance the field of cloud security governance, further research and collaboration among researchers, practitioners, and policymakers are needed [1,3,18].

2.1 Cloud Computing and Security

Cloud computing is a widely adopted technology that enables organizations to store and access data and applications over the internet rather than on local servers. The technology offers many benefits, including cost-effectiveness, scalability, and flexibility. However, the use of cloud computing also poses significant challenges related to data security and privacy [14].

The main concerns about cloud security include unauthorized access, data breaches, and cyber-attacks. These risks can lead to the loss of sensitive data, damage to organizational reputation, and legal liability. Therefore, effective cloud security governance is critical for protecting corporate assets and reputation, especially in regulated industries [22].

2.2 Cloud Security Governance

Cloud security governance refers to the policies, procedures, and frameworks organizations implement to manage and mitigate cloud security risks effectively. It involves identifying and assessing risks, developing and implementing security controls, and monitoring and reporting security incidents [5,7,12].

Effective cloud security governance requires collaboration between stakeholders, including IT, legal, compliance, and business teams. Organizations must ensure that cloud security governance aligns with their security and risk management strategies and comply with relevant regulations and industry standards [5].

3. Methodology: The methodology used in this research paper is a case study approach. The methodology of cloud security governance typically involves the following steps:

- Identify and assess risks: Organizations should identify and evaluate risks associated with their

cloud-based assets, including data breaches, service outages, and compliance violations.

- Establish policies and procedures: Based on the risks identified, organizations should establish policies and procedures for managing the security and compliance of their cloud-based assets.
- Implement controls: Organizations should implement controls to enforce the policies and procedures established in the previous step. This may include access controls, encryption, monitoring, and other security measures.
- Monitor and measure effectiveness: Organizations should monitor and measure the effectiveness of their cloud security governance program to ensure that it is achieving the desired outcomes.
- Respond to incidents: Organizations should have a plan in place to respond to security incidents and breaches promptly and effectively.
- Continuously improve: Organizations should continuously evaluate and improve their cloud security governance program to address emerging threats and changes in regulatory requirements. [6,13,17].

This methodology allows organizations to establish a comprehensive and effective cloud security governance program that protects their cloud-based assets, data, and services from cyber threats and compliance violations.

4.1 Research Gap:

The central research gap addressed in this study is the limited research on the practical implementation of cloud security governance frameworks, including the Cloud Security Alliance (CSA) Security, Trust, Assurance and Risk (STAR), International Organization for Standardization (ISO) 27001, and National Institute of Standards and Technology (NIST) Cybersecurity Framework. These frameworks provide guidance on cloud security governance, but there is limited research on implementing them effectively in practice. The study also addresses the lack of research for developing user-friendly security policies and procedures tailored to the unique requirements of the cloud environment [12].

4.2 Problem Statement:

The problem addressed in this study is the lack of user-friendly and effective cloud security governance frameworks that align with the unique requirements of the cloud environment. While several frameworks are available, organizations often struggle to implement them effectively, resulting in security gaps and breaches. Additionally, the complexity of the cloud environment can make it challenging to develop security policies and procedures that are user-friendly and effective.

Cloud security governance faces several challenges that organizations need to address to ensure the security and compliance of their cloud-based assets, data, and services. Some of the significant difficulties include [6,8,16].

- Lack of visibility: Organizations may have limited visibility into their cloud providers' security controls and practices, making it challenging to ensure that their cloud-based assets are secure.
- Compliance complexities: Cloud security governance requires organizations to comply with complex regulations and industry standards that can be challenging to navigate.
- Shared responsibility: Cloud security is a shared responsibility between the cloud provider and the organization, and it can be challenging to determine who is responsible for which aspects of security.
- Complexity of the cloud environment: Cloud environments can be complex, with multiple cloud providers, platforms, and services, making it challenging to manage security and compliance effectively.
- Rapidly evolving threats: Cyber threats constantly change, and organizations must stay updated with the latest security measures to protect their cloud-based assets.
- Limited resources: Organizations may have limited resources, including budget, staff, and expertise, to implement and maintain an effective cloud security governance program [5,9,14].

Organizations must adopt a comprehensive approach to cloud security governance to address these challenges, including continuous monitoring, risk assessment, and compliance management. Additionally, organizations

should invest necessary resources, such as skilled staff and technologies, to implement and maintain an effective cloud security governance program.

4.3 Cloud Security Governance Frameworks

Various frameworks have been developed to guide organizations in implementing effective cloud security governance practices. The most widely adopted frameworks include the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR), the International Organization for Standardization (ISO) 27001, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework [8,12]. The CSA STAR framework provides comprehensive guidelines and best practices for cloud security governance. It includes a self-assessment tool that enables organizations to assess their cloud security governance maturity level and identify areas for improvement. The ISO 27001 standard systematically manages information security risks and includes specific requirements for cloud service providers. The NIST Cybersecurity Framework offers a risk-based approach to cybersecurity governance and provides a common language for stakeholder communication and collaboration [15].

Based on the preceding discussion, it is possible to conclude that developing a conceptual framework is a solution to most organizations' lack of understanding of data governance and how to establish a cloud computing program. This framework would assist a company in understanding how to create an effective cloud data governance program. Many solutions are available for solving data governance problems provided by industries, but to the best of our knowledge, there is no such framework from industry or academia.

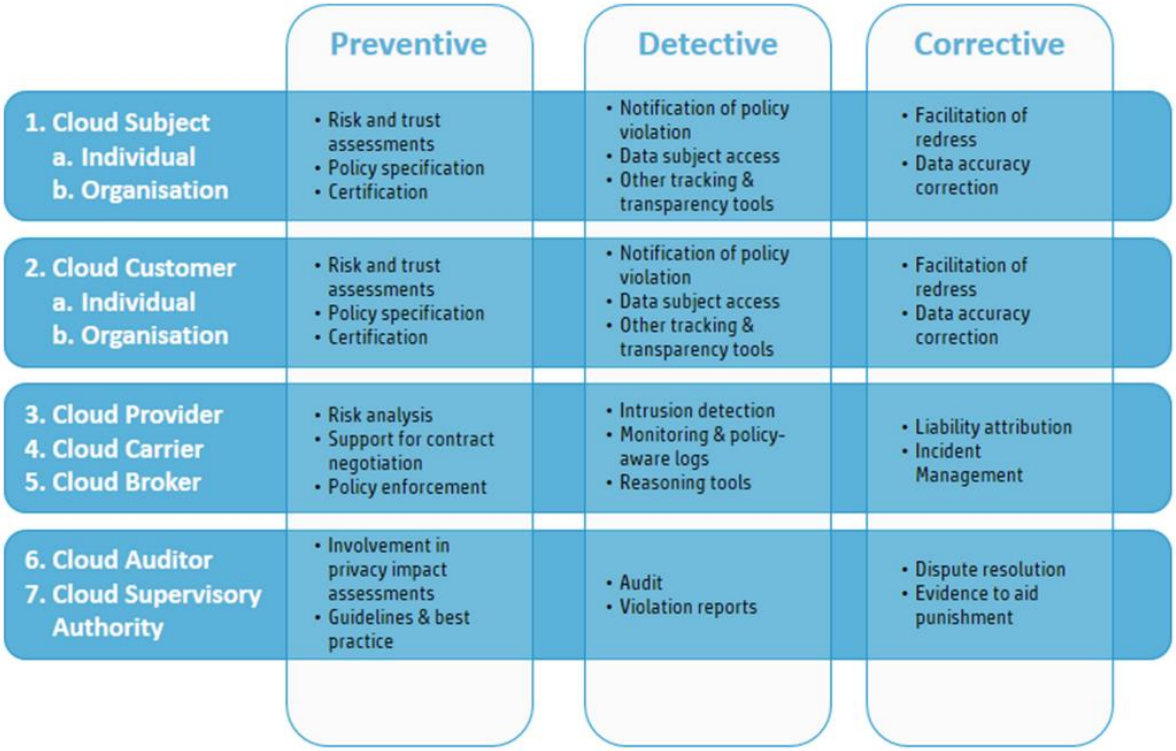

Figure 2 Cloud Security Governance Frameworks

for implementing cloud data governance in the public sector. Because the interactions for data access, processing, and/or updates between the cloud consumer and provider are complex, so is designing a cloud data governance program. To address this complication, the proposed solution is a conceptual framework derived from Analytic Theory [10].

Several key elements are involved in cloud security governance, including:

Governance and operations are two distinct domains within an organization's security framework. The governance domain is concerned with policy and strategy issues, whereas the operations domain is concerned with technical security and implementation. For an organization to maintain adequate protection, critical areas in each discipline must be addressed [10]. The governance domain encompasses various issues, including governance and enterprise risk management, legal issues, compliance and audit management, and information governance. These areas are critical because they ensure that an organization's security policies align with its business objectives and comply with applicable laws and regulations. Effective governance requires a deep understanding of an organization's risks and the ability to make informed decisions about managing those risks. It also involves developing and implementing policies and procedures to guide security-related activities and monitoring and reporting on security-related issues [16,18].

Enterprise risk management is a vital component of the governance domain. It involves identifying, assessing, and managing risks across an organization. Effective risk management requires a comprehensive understanding of an organization's business operations and the potential threats that could impact those operations. It also involves establishing risk tolerance levels and developing risk mitigation strategies [9].

Legal issues are another critical area of the governance domain. Organizations must comply with various laws and regulations related to data privacy, security, and other issues. Failure to comply with these laws can result in significant financial penalties and damage an organization's reputation. Organizations must understand the legal landscape and develop policies and procedures to ensure compliance [4].

Compliance and audit management are also crucial components of the governance domain. Compliance involves ensuring that an organization's policies and procedures are aligned with applicable laws and regulations. Auditing involves evaluating an organization's security controls to ensure they effectively mitigate risks. Effective compliance and audit management require robust policies and procedures and the ability to monitor and report on compliance-related issues [8].

Information governance is another critical area of the governance domain. It involves managing an organization's information assets to ensure they are secure and properly used. Information governance includes policies and procedures related to data classification, retention, disposal, access controls, and data protection measures [2].

The operations domain is concerned with technical security matters and implementation. It encompasses several critical areas, including management plan and business continuity, infrastructure security, virtualization and containers, incident response, notifications, and remediations [9].

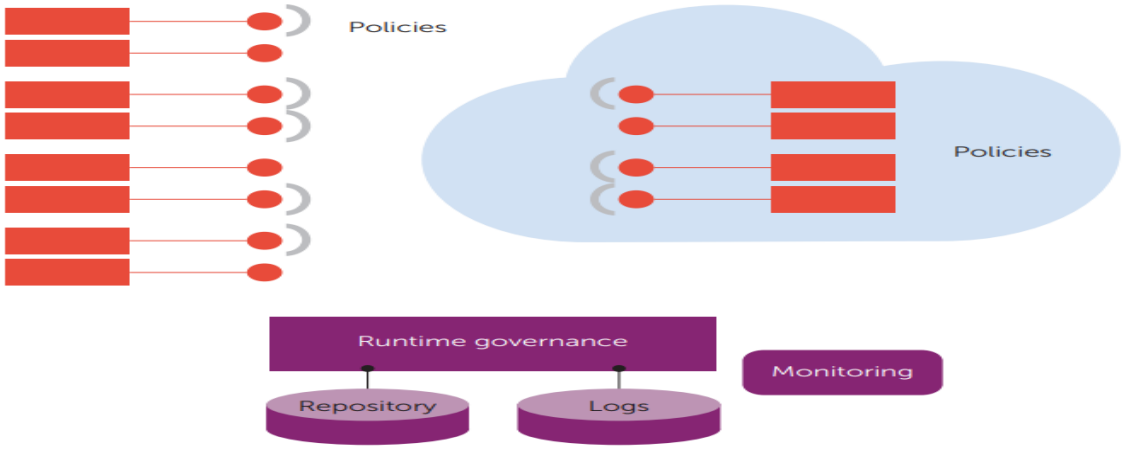

Figure 3 Cloud Infrastructure Security

Management plane and business continuity are critical areas of the operations domain. They ensure an organization's systems and data are available and functional during an outage or other disruption. Practical management and business continuity planning require robust disaster recovery and business continuity programs and the ability to quickly restore systems and data during a disorder [2].

Infrastructure security is another critical area of the operations domain. It protects an organization's network, servers, and other infrastructure components from unauthorized access and other threats. Adequate infrastructure security requires a deep understanding of network architecture and protocols and the ability to implement and manage security controls to protect against threats [17].

Virtualization and containers are also critical areas of the operations domain. They involve implementing and managing virtualized environments and containerization technologies, which can improve efficiency and reduce costs. Practical virtualization and containerization require a deep understanding of the technologies involved and the ability to implement and manage security controls to protect against threats [16].

Incident response, notifications, and remediations are also critical areas of the operations domain. They involve detecting and responding to security incidents, notifying affected parties, and implementing remediation measures to prevent future incidents. Effective incident response requires robust incident response plans and the ability to quickly identify and contain incidents and implement remediation measures [17].

5. Results and Discussion:

The research results in we will recommend ISO 27001:2022 framework for data & asset protection. ISO 27001 is a standard that provides a framework for information security management systems (ISMS) and specifies requirements for establishing, implementing, maintaining, and continuously improving information security.

Regarding a research paper's result and discussion section, ISO 27001 requires that the research findings are presented clearly and concisely, highlighting any significant results, conclusions, and recommendations.

The discussion section should also include a discussion of the limitations of the research, including any potential biases or issues that may have affected the results. This should be followed by a meeting on the implications of the research findings for information security management, including how they may be applied to improve information systems.

In addition to presenting the results and discussing their implications, the paper should also evaluate the effectiveness of the ISMS in place according to the requirements of ISO 27001. This evaluation should include an assessment of the controls that have been implemented to manage information security risks, as well as a review of any incidents or breaches that have occurred and how they were handled.

This research paper will conclude with recommendations for improving the ISMS, based on the findings and evaluation. These recommendations may include modifications to existing controls, additional controls that should be implemented, or changes to policies and procedures.

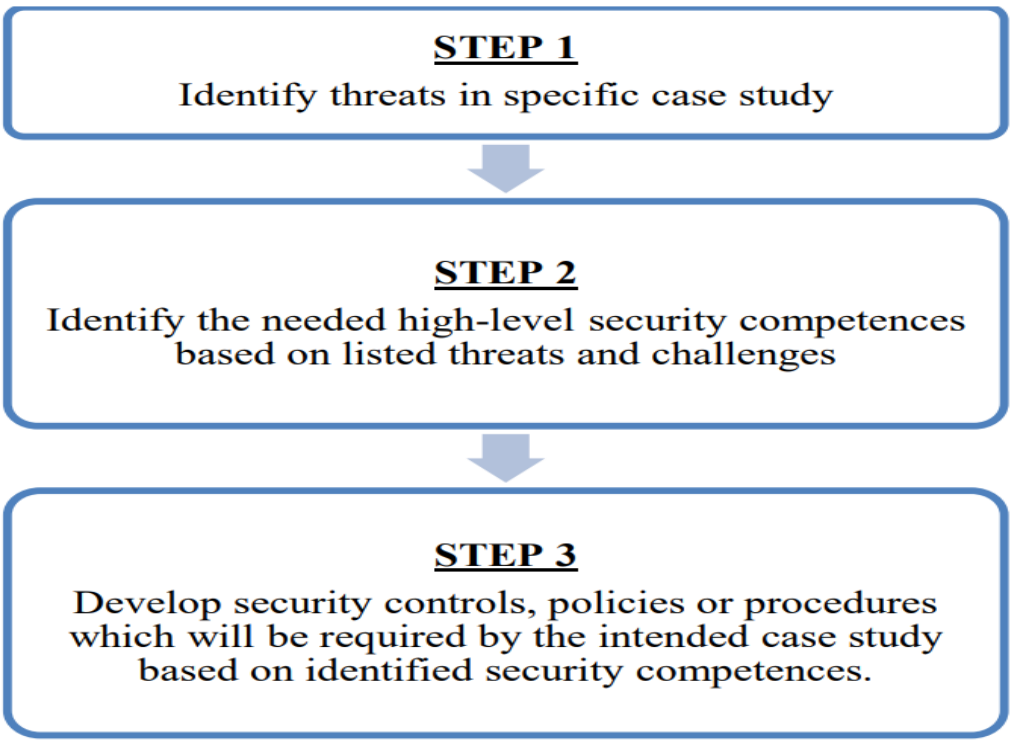

Figure 4 Steps to develop a checklist

Overall, the result and discussion section of a research paper according to ISO 27001 should thoroughly evaluate the ISMS and its effectiveness, along with practical recommendations for improving information security management.

This research provides steps for a new researcher to follow as a guideline when developing a cloud security checklist, assessment, or guideline. The article suggests three steps to follow, which are shown in figure 4 above.

6. Conclusion

Cloud security governance is critical for organizations that use cloud computing services and applications. It requires a comprehensive and holistic approach to identify, assess, and mitigate cloud security risks and ensure the security, privacy, and compliance of cloud-based systems and data. The literature review reveals that various models, frameworks, and best practices have been proposed to address different aspects of cloud security governance, including the shared responsibility model and risk management framework assessment. The methodology of cloud security governance involves identifying and assessing risks, establishing policies and procedures, implementing controls, monitoring and measuring effectiveness, responding to incidents, and continuously improving.

Also, organizations must follow best practices for running workloads in public cloud environments [21]. However, cloud security governance faces significant challenges, such as the lack of visibility, compliance complexities, shared responsibility, the complexity of the cloud environment, rapidly evolving threats, and limited resources.

To address these challenges, organizations must adopt a comprehensive approach to cloud security governance which might adopt the following methodologies. Using Machine learning techniques random forest and neural network to detect cyber attacks [19].

Blockchain-based data protection, and federated identity management, offer promising opportunities to enhance cloud security governance and address specific challenges. However, several challenges and research gaps still need to be addressed, such as the lack of standardization and interoperability among cloud providers, the limited availability of tools and technologies for cloud security governance, and the need for more user-centered and context-aware approaches.

Moreover, organizations must remain vigilant in their cloud security governance efforts, continuously evaluating and improving their programs to stay ahead of emerging threats and regulatory changes. By doing so, they can establish a robust and effective cloud security governance program that protects their cloud-based assets, data, and services from cyber threats and compliance violations and enables them to leverage the full potential of cloud computing.

References

[1] C. I. Forum, "Data governance in the cloud."

[2] Majid Al-Ruithe, Elhadj Benkhelifa and Khawar Hameed "Key Dimensions for Cloud Data Governance"

[3] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J. Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. Proc. ACM Workshop on Cloud Computing Security, Chicago, IL

[4] Rebollo, O., Mellado, D. and Fernández-Medina, E. A systematic review of information security governance frameworks in the cloud computing environment.

[5] the H. I. and M. S. S. (HIMSS) (2015) A ROADMAP TO EFFECTIVE DATA GOVERNANCE: How to Navigate Five Common Obstacles, HIMSS Clinical & Business Intelligence Committee.

[6] Van der, L.M. Measuring Data Governance; Leiden University: Leiden, The Nederland, 2015.

[7] More P, Lingayat M. Survey on Data Sharing in the Cloud Using Distributed Accountability. 2014.

[8] Cloud Security Alliance, "Cloud Data Governance Working Group," 2015.

[9] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Current State of Cloud Computing Adoption – An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA)," Procedia Comput. Sci., vol. 110, pp. 378– 385, 2017.

[10] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A conceptual framework for designing data governance for cloud computing," Procedia Comput. Sci., vol. 94, no. MobiSPC, 2016

[11] Beach T, Rana O, Rezgui Y. Governance Model for Cloud Computing in Building Information Management.pdf. 2015.

[12] Self RJ, Introduction A. Governance Strategies for the Cloud, Big Data and other Technologies in Education. 2014.

[13] Cloud Security Alliance. Cloud Data Governance Working Group. https://cloudsecurityalliance.org/group/cloud-data-governance/. Published 2015.

[14] Yale; Wendy., "Is data governance in cloud computing still a mirage or do we have a vision we can trust," vol. 42.1, 2011

[15] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Key dimensions for cloud data governance," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 379–386, 2016.

[16] A. S. Bachelor and I. Technology, "Lewam Woldu Cloud Governance Model and Security Solutions for Cloud Service Providers," no. May, 2013.

[17] Madhuri C., "Cloud Information Accountability Frameworks for Data Sharing \nin Cloud," IOSR J. Comput. Eng., vol. 13.

[18] L. Hunter, "Tools for Cloud Accountability: A4Cloud Tutorial," 2015.

[19] Oyetoro, A., Mart, J., Okoroafor, N., Amah, J., (2022). Using Machine learning Techniques Random Forest and Neural Network to Detect Cyber Attacks. 10.13140/RG.2.2.27484.05763/1.

[20] EY, "Building trust in the cloud," 2014. [20] S. U. Lee, L. Zhu, R. Jeffery, and A. P. Group, "Data Governance for Platform Ecosystems: Critical Factors and the State of Practice.

[21] Mart, J., Oyetoro, A., Amah, J., Okoroafor, N. (2022). Best Practices for Running Workloads in

Public Cloud Environments. 10.13140/RG.2.2.16945.86881/3.

[22] S. Pearson, V. Tountopoulos, D. Catteddu, M. Sudholt, R. Molva, C. Reich, S. Fischer-Hubner, C. Millard, V. Lotz, M. G. Jaatun, R. Leenes, C. Rong, and J. Lopez, "Accountability for cloud and other future Internet services," CloudCom 2012.

Joshua Ugochukwu Amah received his bachelor's degree in Electronics and Computer Engineering from Nnamdi Azikiwe University, Awka, Anambra State, Nigeria, in 2015 and his master's degree in computer science from Lamar University, Beaumont, Texas, in 2022. He has worked for four years in the information technology industry as Cloud Engineer and currently works with one of the top IT firms in the United States. His research interest includes Cybersecurity, Cloud computing, Machine learning, and Artificial intelligence. Joshua is active in different scientific societies, such as Member of the National Society of Professional Engineers, The Nonprofit Technology Enterprise Network, and the National Society of Black Engineers.

Nneoma Okorafor received her master's degree in computer science from Prairie View A&M University, Texas, United States, in 2022 and a bachelor's degree in computer science at Michael Okpara University of Agriculture Umudike, Nigeria. She had four years of experience working in the banking industry in Nigeria as a technical support engineer and software engineer before moving to the United States for her master's program. Her research interests include Machine learning, IoT, Cloud computing, and Cybersecurity.

Joseph Mart obtained his Electrical and Electronic engineering bachelor's degree from the University of Benin, Benin City, Nigeria. He has four years of technical experience across various IT domains. He obtained his master's degree in computer science in 2022 from Austin Peay State University, Clarksville, Tennessee State. Joseph has multiple certifications with giant IT industries such as Amazon Web Services, Cisco, IBM, CompTIA, Juniper Networks, and HarshiCorps Inc. He is an active member of multiple scientific organizations such as IEEE, the National Society of Professional Engineers, the Nonprofit Technology Enterprise Network, and the National Society of Black Engineers. His research interest includes Artificial Intelligence and Machine learning, Cloud Computing, and Cybersecurity IoT.

Amos Oyetoro obtained his M.s in Computer Science from Austin Peay State University, Clarksville, Tennessee, United States. He had his bachelor's degree in computer engineering from Nigeria in 2012. Over the past eight years, Amos has held various positions in the Information Technology industry, from System development to system design and implementation. He has a strong background in Cloud computing and cyber security, Application and system architecture, database design, web application development, and system analysis. He possesses an active member of multiple scientific organizations such as IEEE, the National Society of Professional Engineers, The Nonprofit Technology Enterprise Network, and the National Society of Black Engineers. His primary interest includes Cloud computing, Network and security, Data Analysis and performance, machine learning, Artificial Intelligence, and Information Technologies.