International Journal of Management Information Systems and Data Science,2024;1(1):31-40

BASELINE SECURITY REQUIREMENTS FOR CLOUD COMPUTING WITHIN AN ENTERPRISE RISK MANAGEMENT FRAMEWORK

Md Rasel Ul Alam[1]; Asif Shohel[2]; Mahmudul Alam[3];

[1]PhD Candidate, School of Computer and Information Sciences, University of the Cumberlands, Kentucky, USA.

[2]Graduate Student, Master of Science in Information Technology Management, Grand Canyon University, Phoenix, USA

[3]PhD Candidate, School of Computer and Information Sciences, University of the Cumberlands, Kentucky, USA

Keywords

Cloud Computing

Enterprise Risk Management (ERM)

Baseline Security Requirements

Compliance and Governance

Risk Assessment

ABSTRACT

This paper examines integrating baseline security requirements within an Enterprise Risk Management (ERM) framework, specifically focusing on cloud computing environments. As organizations increasingly migrate their operations to the cloud, the necessity for a robust security posture that aligns with comprehensive risk management practices has never been more critical. Through a systematic review of existing literature and analysis of case studies, this study identifies key strategies for implementing security measures that address the unique risks posed by cloud computing. The findings highlight the importance of continuous risk assessment, compliance and governance standards adherence, and resilient incident response and business continuity plans. The research further explores the dynamic relationship between cloud service models (IaaS et al.) and ERM strategies, offering insights into best practices for mitigating risks while capitalizing on the cloud's scalability and flexibility. The paper concludes with recommendations for organizations seeking to enhance their security and risk management practices in cloud environments, emphasizing the need for an integrated approach that supports business objectives and drives technological innovation.

1 Heading

Cloud computing has fundamentally transformed the technological landscape for enterprises by offering unparalleled scalability, flexibility, and cost efficiency, enabling on-demand access to shared computing resources (Dzombeta, Stantchev, Colomo-Palacios, Brandis, & Haufe, 2014). The adoption of service delivery models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) allows organizations varied levels of control over their cloud environments, thus catering to diverse needs

(Iqbal et al., 2016). However, transitioning from traditional on-premises systems to the cloud introduces significant security challenges, including new vulnerabilities, shared responsibility models, and compliance issues that necessitate a structured approach to risk management (Khalil, Khreishah, & Azeem, 2014). Enterprise Risk Management (ERM) provides a holistic framework that enables businesses to systematically identify, analyze, assess, and address risks across interconnected domains, thereby supporting the integration of ERM principles with cloud computing strategies to enhance security measures (Ryan, 2013). This paper emphasizes the importance of implementing stringent baseline security requirements—such as access control, data encryption, vulnerability management, and logging mechanisms—as fundamental to securing cloud environments. These measures ensure the protection of sensitive assets and underpin the integrity and availability of data and systems within the cloud (Bappy & Ahmed, 2023). By embedding these security controls from the outset and throughout the development lifecycle, organizations can adopt a secure-by-design approach, enabling proactive risk mitigation and aligning with ERM frameworks to foster a comprehensive and strategic stance on cloud security.

Cloud computing has revolutionized the information technology landscape, offering a new paradigm that significantly changes how organizations and individuals utilize computing resources. Defined by Sehgal and Bhatt (2018) as a model enabling ubiquitous, convenient, on-demand access to a shared pool of configurable computing resources, cloud computing excels in providing scalability, flexibility, and cost-efficiency, marking a departure from traditional on-premises IT infrastructures to a service-oriented approach. This shift allows for the rapid provisioning and release of resources with minimal management effort, ensuring broad network access across various client platforms, from mobile devices to desktop workstations (Singh, Jeong, & Park, 2016). At its core, cloud computing is characterized by key features such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service, all of which create an adaptable and efficient IT environment (Somani, Gaur, Sanghi, Conti, & Buyya, 2017). Within this framework, cloud computing encompasses several service models designed to meet diverse IT needs: Infrastructure as a Service (IaaS) offers virtualized computing resources over the Internet, Platform as a Service (PaaS) provides tools for application development without the complexities of hardware management, and Software as a Service (SaaS) delivers software applications online on a subscription basis, eliminating the need for in-depth software and hardware management (Subramanian & Jeyaraj, 2018). These models are supported by various deployment strategies, including public clouds managed by third-party providers, private clouds for exclusive organizational use, and hybrid clouds that combine the benefits of public and private clouds (Xu, 2012). Cloud computing facilitates digital transformation for enterprises through these models and deployment strategies (Zhang et al., 2017). It fosters innovation in business models and technology infrastructures, representing a significant advancement in the management and consumption of technological resources in today's digital era.

Enterprise Risk Management (ERM) has become a pivotal strategic framework for organizations focused on identifying, assessing, prioritizing, and managing risks affecting their operations, financial health, and overarching goals (Ittner & Oyon, 2019) . Jankensgård (2019) highlighted that ERM surpasses traditional risk management by weaving risk management practices into every facet of an organization's processes and culture, promoting a holistic approach that embeds risk considerations within strategic decision-making. This allows for an effective balance between risks and opportunities and establishes a structured methodology for risk aggregation and communication at various organizational levels, thereby cultivating a risk-aware culture (Metwally & Diab, 2021). For ERM to be effectively implemented, an organization must gain a deep understanding of its internal and external environments, ensuring that risk management strategies align with business aims and comply with regulatory standards (Muralidhar, 2010). This alignment is essential in today's global business milieu, marked by swift technological changes, shifting regulatory frameworks,

and new threats. Guidelines set forth by frameworks like those from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) advocate for a proactive and consistent approach to risk management, reflective of an organization's appetite for risk. With increasing organizations acknowledging the significance of a comprehensive and integrated approach to managing risk, ERM has emerged as a vital mechanism for boosting organizational resilience, ensuring sustainability, and bolstering long-term success (Stoel, Ballou, & Heitger, 2017). By strategically applying ERM principles, organizations are equipped to navigate risks effectively and seize opportunities, thus establishing a competitive edge in their industries.

Figure 1: Integrating Cloud Computing and Enterprise Risk Management

Concept	Explanation	Integration for Robust Cloud Security
Cloud Computing	Characterized by scalability, flexibility, cost-efficiency, and resource pooling. Includes IaaS, PaaS, and SaaS service models.	▪ Evaluate security and privacy implications of public, private, and hybrid cloud models. ▪ Scrutinize SLAs, data security provisions, shared responsibility clauses, and incident response plans. ▪ Address data security, network protection, access management, and application security within the shared responsibility model.
Enterprise Risk Management (ERM)	A holistic framework for identifying, assessing, prioritizing, and managing strategic, operational, financial, and technology risks.	▪ Identify cloud-related risks, including data breaches, compromised credentials, vendor failure, regulatory non-compliance, and technology obsolescence. ▪ Analyze the impact and likelihood of identified risks, considering business objectives, data sensitivity, and regulatory requirements. ▪ Establish clear roles and responsibilities for cloud security decision-making, risk reporting, and policy development within the ERM framework.
Baseline Security Requirements	Foundational security controls for cloud applications, databases, systems, networks, and information processing.	▪ Protect data at rest and in transit with robust encryption algorithms and management ▪ Implement IAM solutions with least privilege principles and strong authentication, potentially including multi-factor authentication. ▪ Continuously scan and remediate vulnerabilities in applications, systems, and network configurations. ▪ Enable comprehensive monitoring for anomaly detection, investigations, and compliance. ▪ Test and update plans for systems and data within the cloud environment.

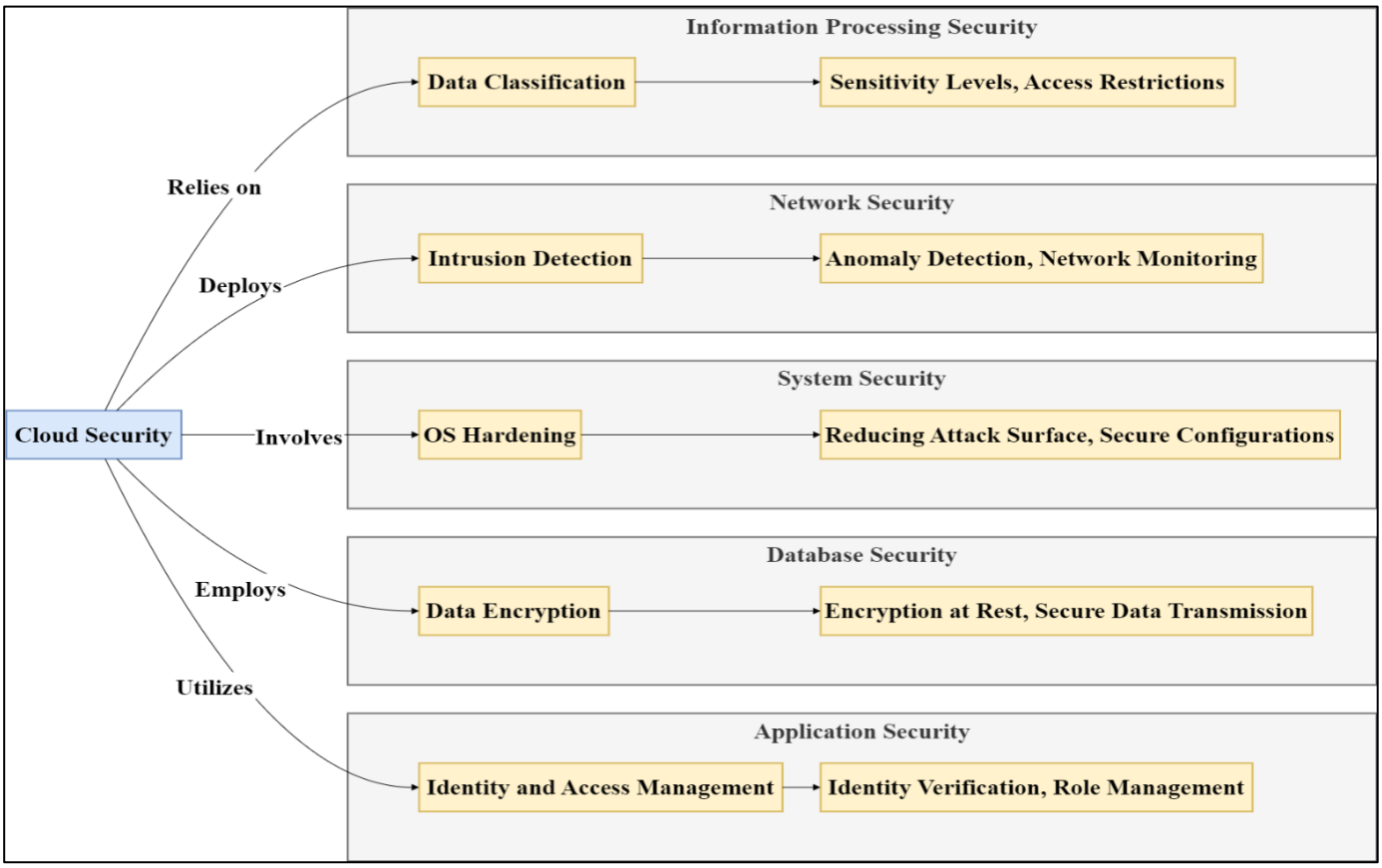
2 Literature Review

2.1 Security Requirements for Cloud Applications

In the domain of cloud computing, the sanctity of application security is heavily reliant on robust Identity and Access Management (IAM) frameworks and the strategic deployment of Multi-factor Authentication (MFA). These practices are paramount for regulating access to cloud resources, with IAM meticulously tailoring access rights congruent with user roles and MFA adding an extra layer of security through methods such as verification codes or biometric data, significantly

mitigating the risk of unauthorized access (Tounsi & Rais, 2018; Wu & Moon, 2017; Zhang et al., 2017). Complementarily, security measures are integrated into the Software Development Life Cycle (SDLC) from the outset, incorporating threat modeling, regular code reviews, and secure coding practices to preclude security flaws and adopt a proactive posture toward potential vulnerabilities (Subashini & Kavitha, 2011). Additionally, within the database and system domains, stringent access controls such as Role-Based Access Control (RBAC) and data encryption are pivotal for risk mitigation and data integrity preservation. This is augmented by data masking and tokenization to protect non-production environments, alongside auditing and logging activities that contribute to anomaly detection (Singh et al., 2016).

Furthermore, to ensure data recoverability and operational continuity, the implementation of comprehensive backup and disaster recovery plans stands as an essential element, particularly in response to unexpected incidents that could otherwise disrupt business processes (Saevanee, Clarke, Furnell, & Biscione, 2015; Subramanian & Jeyaraj, 2018). System security is further fortified through practices like operating system hardening and endpoint protection, while network security measures such as network segmentation and intrusion detection are deployed to strengthen defenses against potential cyber threats (Al Bashar, Taher, Islam, & Ahmed, 2024). Information processing security, the pinnacle of this architecture, relies heavily on data classification to establish sensitivity levels and implement access restrictions, thereby preserving the confidentiality and integrity of the data, a necessity in cloud environments (Rahaman & Bari, 2024). These multilayered security measures construct a comprehensive framework that is not only crucial for the protection of cloud environments against evolving threats but also exemplifies the integrated security approach essential across all levels of applications, databases, systems, network infrastructure, and information processing. Such an approach is integral to an Enterprise Risk Management (ERM) framework, ensuring that organizations can adeptly manage the array of risks inherent in cloud computing and align their security



strategy with their broader business objectives (See Figure 2).

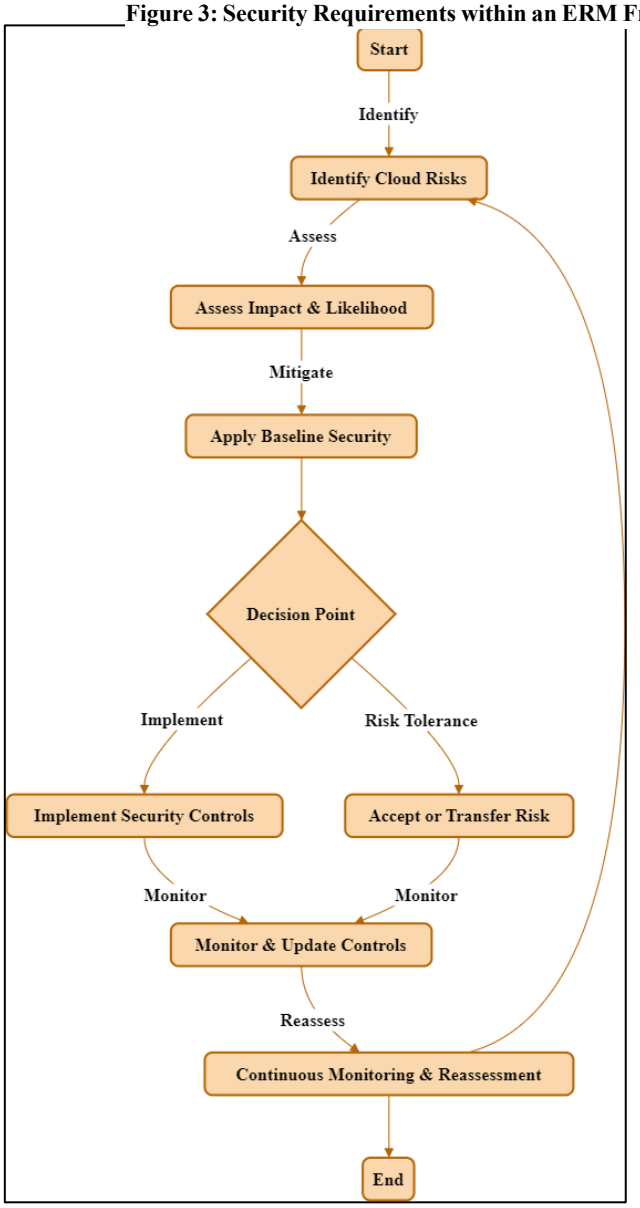
Figure 2: Overview of Cloud Security

2.2 Security Requirements within an ERM Framework

Integrating cloud security into an enterprise risk management (ERM) framework begins with a thorough identification of risks associated with cloud adoption, necessitating a detailed mapping of the organization's business processes and assets to the chosen cloud deployment models, including public, private, and hybrid. This crucial first step, informed by the shared responsibility model of cloud services, lays the foundation for understanding the specific risks of cloud environments (Ryan, 2013; Subramanian & Jeyaraj, 2018). The process extends to a meticulous analysis of regulatory requirements, vendor contracts, and industry-specific threat intelligence, enabling a bespoke risk identification process that reflects the unique context of the organization. This preparatory phase sets the stage for the subsequent critical step of risk assessment (Subashini & Kavitha, 2011).

The assessment phase delves into evaluating the impact and likelihood of the identified risks, with a keen focus on the potential financial, operational, reputational, and compliance-related repercussions of each risk factor. The likelihood of risks materializing is systematically assessed using historical data, threat modeling, and analysis of industry trends, thereby providing a data-driven foundation for risk prioritization (Saevanee et al., 2015). This evaluation is integral to deciding whether to mitigate, accept, or transfer risks, guiding organizations in choosing the most appropriate strategy for each identified risk. In some cases, the transfer of risk through insurance or other financial instruments may be an apt choice, especially when mitigation is not feasible or cost-effective. This decision-making process, rooted in the organization's risk appetite and strategic objectives, underpins the development of a robust cloud security strategy within the ERM framework.

Figure 3: Security Requirements within an ERM Framework



The core of a successful cloud security strategy within an ERM framework is the implementation of baseline security requirements, tailored to the organization's risk profile and the sensitivity of the data and systems involved. Incorporating essential security measures such as encryption, access controls, vulnerability management, and secure network architecture establishes a fortified defense against threats. This is complemented by extensive monitoring to ensure ongoing vigilance (Kaur & Singh, 2015). Regular review and updating of security

controls are paramount to address the dynamic nature of cloud security threats and align with best practices. Furthermore, continuous monitoring and periodic risk reassessment, characterized by diligent logging and analysis of security events, enable organizations to remain agile and responsive to emerging threats and changes within the cloud ecosystem. This active and adaptive approach to risk management is essential for maintaining an organization's risk posture that is congruent with its evolving strategic objectives, thereby ensuring the long-term success and security of its cloud-based operations (Butun, Erol-Kantarci, Kantarci, & Song, 2016; Fernandes, Soares, Gomes, Freire, & Inácio, 2013).

2.3 Integration into an Enterprise Risk Management Framework

Integrating baseline security requirements into an Enterprise Risk Management (ERM) framework is a strategic necessity for managing cloud computing risks effectively, emphasizing the importance of a robust risk assessment process as a core element (Sehgal & Bhatt, 2018). This involves continuous evaluation to identify, evaluate, and prioritize risks against the backdrop of business objectives and operations, coupled with regular monitoring of cloud resources to detect emerging threats and vulnerabilities, ensuring that mitigation strategies align with cloud environments' dynamic nature. Compliance and governance stand as another critical pillar, highlighting the need for adherence to complex legal, regulatory, and industry standards to protect sensitive information and ensure data privacy, with frameworks like the GDPR, HIPAA, and ISO 27001 setting the benchmark for security measures and underscoring the role of a strong governance structure in enforcing security policies and fostering a culture of compliance (Sangeetha, 2013). Additionally, developing and rigorously testing incident response and business continuity plans are indispensable, offering predefined protocols for managing security incidents efficiently and ensuring minimal operational disruption, thus safeguarding against financial and reputational damage (Subashini & Kavitha, 2011). These plans facilitate swift recovery post-incident and ensure that critical business functions remain unhampered, underlining the importance of regular updates and tests to address gaps and adapt to evolving threats. These integrated components fortify an organization's ability to manage cloud security complexities effectively, enabling sustained operations and resilience in the face of potential disruptions.

3 Methodology

This study adopts a qualitative case study methodology to investigate the integration of cloud security practices within the Enterprise Risk Management (ERM) frameworks across organizations. It also focuses on a diverse set of companies, such as TechWave Inc., HealthNet Solutions, and Global Finance Group, to explore varied industry approaches. The research involves collecting data through interviews with IT professionals, risk managers, and executives, alongside the examination of organizational documents like security policies and risk assessments. Through thematic analysis, this study also codes and categorizes the data into emergent themes, compare across cases to discern patterns and variations in cloud security and risk management strategies.

4 Findings

The findings from the qualitative study reveal several themes regarding the integration of cloud security within Enterprise Risk Management (ERM) frameworks, as derived from interviews with participants from companies like TechWave Inc., HealthNet Solutions, and Global Finance Group.

Theme 1: Risk Identification and Cloud Architecture Understanding

The first theme that emerges is the depth of understanding of cloud architecture and its inherent risks. Participants from TechWave Inc. highlight that their initial step in risk management involves a comprehensive identification of risks associated with cloud architecture—focusing on data flow, access points, and potential breach areas within their cloud deployments. This process goes beyond surface-level vulnerabilities and dives into the architectural intricacies of cloud services, which are often unique to the organization's chosen cloud model, be it

public, private, or hybrid. The insights reveal that a nuanced understanding of cloud architecture fosters a more targeted and effective ERM strategy.

Theme 2: Shared Responsibility Model Clarity

Interviews across all three companies consistently point to the importance of clarity regarding the shared responsibility model in cloud services. HealthNet Solutions reports that delineating the boundaries of vendor versus in-house responsibilities was a pivotal step in their ERM integration. By clearly defining who is responsible for what aspects of cloud security—such as infrastructure management, application-level security, and data governance—they could allocate resources and design controls more effectively. This clear demarcation is integral to establishing accountability and ensuring comprehensive coverage of security measures.

Theme 3: Tailored Risk Mitigation Strategies

Another prominent theme is the customization of risk mitigation strategies. Participants from Global Finance Group emphasize that their approach to mitigating risks is highly tailored to the specific types of data they handle and the regulatory environment they operate within. By incorporating encryption, access controls, and vulnerability management that align with their risk profile and compliance requirements, they can address potential threats proactively. This customization is pivotal in developing a baseline security model that aligns with the organization's specific risk appetite and regulatory landscape.

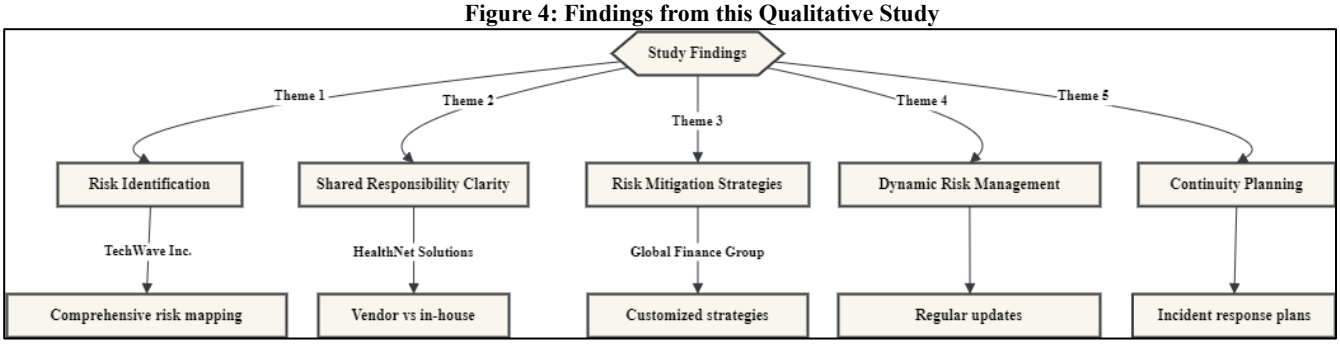
Theme 4: Dynamic Risk Management Processes

Dynamic risk management processes emerge as a critical theme in the study. Regular updates to risk assessments and the agility to adapt to new threats characterize successful ERM frameworks, as noted by TechWave Inc. This dynamism is crucial for cloud environments, where technological and threat landscapes evolve rapidly. The findings indicate that the organizations which periodically reassess their risk profiles and update their security measures accordingly are better positioned to handle the uncertainties of cloud computing.

Theme 5: Continuity Planning and Incident Response

Finally, the significance of robust continuity planning and incident response is a theme that stands out in the findings. Interviewees from HealthNet Solutions and Global Finance Group share that developing and testing incident response and business continuity plans are foundational to their ERM strategies. They stress the need for these plans to be living documents, regularly revisited and updated in line with new insights from continuous monitoring and threat intelligence. This proactive approach to planning ensures that the organization can maintain operations and quickly recover in the event of a security incident, thereby minimizing impact and downtime.

Figure 4: Findings from this Qualitative Study



5 Discussion

The current study's exploration into cloud security integration within Enterprise Risk Management (ERM) frameworks sheds light on how organizations navigate the unique and intricate cloud environment, highlighting an evolution in risk management practices. Research has traditionally emphasized risk identification within IT

infrastructures, but findings from participants at TechWave Inc. illustrate a shift towards a granular understanding of cloud-specific architectures (Akshaya & Ganapathi, 2018). This depth of understanding extends to identifying and managing the risks associated with the elastic and on-demand nature of cloud services (Abbas, Maennel, & Assar, 2017). In contrast to the general IT risk identification in earlier studies, this approach underscores a nuanced appreciation of cloud complexities that significantly influences the effectiveness of an ERM (Butun et al., 2016).

In line with previous research, the importance of clarity around the shared responsibility model is reaffirmed through the experiences of companies such as HealthNet Solutions. The findings highlight a contemporary challenge: the necessity for transparent delineation of security responsibilities between organizations and cloud service providers (CSPs) (Abbas et al., 2017). This clarification is pivotal for effective resource allocation and control design. The current study's participants underscore the critical nature of this clarity, which is essential for establishing accountability and ensuring comprehensive security coverage, suggesting that the model's applicability is becoming increasingly complex as cloud services evolve. Moreover, the study aligns with existing research advocating for tailored risk mitigation strategies, a theme particularly prominent in the practices of the Global Finance Group. These strategies are highly customized to the types of data handled and the regulatory environments in which the organizations operate, responding proactively to potential threats (McShane, Eling, & Nguyen, 2021). This degree of customization, according to current findings, is crucial for the development of baseline security models that reflect an organization's risk appetite and regulatory context. Such alignment emphasizes that risk mitigation in cloud security is not a static process but requires continuous adaptation to the organization's evolving risk landscape.

The findings also indicate that dynamic risk management processes are essential in cloud environments, where technological advancements and threat landscapes are rapidly evolving. Participants from companies like TechWave Inc. report regularly updating risk assessments and modifying security measures, emphasizing a characteristic agility necessary for successful ERM frameworks in cloud computing (Iqbal et al., 2016). This approach, which includes periodic reassessment of risk profiles and security updates, is depicted as an integral component of an adaptive cloud security strategy. Moreover, the present study discusses the significance of continuity planning and incident response as noted by organizations like HealthNet Solutions and Global Finance Group. These plans are not merely procedural documents but are considered living documents, necessitating regular revisions to reflect the insights from continuous monitoring and threat intelligence. Such proactive planning is presented as essential for organizations to maintain operations and recover swiftly in the event of security incidents, ensuring minimal impact on business continuity (Ghafir et al., 2018). The findings suggest that maintaining operational resilience in the face of cloud security incidents is a dynamic and ongoing commitment within contemporary ERM frameworks .

6 Conclusion

The current study provides a comprehensive overview of how modern enterprises integrate cloud security within their Enterprise Risk Management (ERM) frameworks, highlighting a transition from traditional IT risk approaches to those that address the distinctive challenges of cloud computing. It elucidates the necessity for an in-depth understanding of cloud-specific risks, a clear delineation of responsibilities under the shared responsibility model, and the implementation of tailored risk mitigation strategies that align closely with the regulatory context and data sensitivities unique to each organization. Significantly, the findings stress the importance of maintaining dynamic and flexible risk management processes capable of responding to the rapidly changing cloud threat landscape, and the essential nature of proactive continuity planning and incident response that ensures organizational resilience. This study enriches the body of knowledge on cloud ERM by demonstrating the evolving practices that organizations adopt to fortify their defenses against the unique

vulnerabilities presented by cloud environments, thereby offering a nuanced framework for building robust, adaptive, and resilient risk management strategies.

References

Abbas, H., Maennel, O., & Assar, S. (2017). Security and privacy issues in cloud computing. *Annals of Telecommunications, 72*(5), 233-235. doi:10.1007/s12243-017-0578-3

Akshaya, M. S., & Ganapathi, P. (2018). Taxonomy of Security Attacks and Risk Assessment of Cloud Computing. In (Vol. NA, pp. 37-59).

Al Bashar, M., Taher, M. A., Islam, M. K., & Ahmed, H. (2024). The Impact Of Advanced Robotics And Automation On Supply Chain Efficiency In Industrial Manufacturing: A Comparative Analysis Between The Us And Bangladesh. *Global Mainstream Journal of Business, Economics, Development & Project Management, 3*(03), 28-41.

Bappy, M. A., & Ahmed, M. (2023). Assessment Of Data Collection Techniques In Manufacturing And Mechanical Engineering Through Machine Learning Models. *Global Mainstream Journal of Business, Economics, Development & Project Management, 2*(04), 15-26.

Butun, I., Erol-Kantarci, M., Kantarci, B., & Song, H. (2016). Cloud-centric multi-level authentication as a service for secure public safety device networks. *IEEE Communications Magazine, 54*(4), 47-53. doi:10.1109/mcom.2016.7452265

Dzombeta, S., Stantchev, V., Colomo-Palacios, R., Brandis, K., & Haufe, K. (2014). Governance of Cloud Computing Services for the Life Sciences. *IT Professional, 16*(4), 30-37. doi:10.1109/mitp.2014.52

Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2013). Security issues in cloud environments: a survey. *International Journal of Information Security, 13*(2), 113-170. doi:10.1007/s10207-013-0208-7

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., . . . Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986-5002. doi:10.1007/s11227-018-2337-2

Iqbal, S., Kiah, L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K.-K. R. (2016). On cloud security attacks. *Journal of Network and Computer Applications, 74*(NA), 98-120. doi:10.1016/j.jnca.2016.08.016

Ittner, C. D., & Oyon, D. (2019). Risk Ownership, ERM Practices, and the Role of the Finance Function. *Journal of Management Accounting Research, 32*(2), 159-182. doi:10.2308/jmar-52549

Jankensgård, H. (2019). A theory of enterprise risk management. *Corporate Governance: The International Journal of Business in Society, 19*(3), 565-579. doi:10.1108/cg-02-2018-0092

Kaur, M., & Singh, H. (2015). A Review of Cloud Computing Security Issues. *International Journal of Education and Management Engineering, 5*(5), 32-41. doi:10.5815/ijeme.2015.05.04

Khalil, I., Khreishah, A., & Azeem, M. (2014). Cloud Computing Security: A Survey. *Computers, 3*(1), 1-35. doi:10.3390/computers3010001

McShane, M. K., Eling, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review, 24*(1), 93-125. doi:10.1111/rmir.12169

Metwally, A. B. M., & Diab, A. A. Z. (2021). Risk-based management control resistance in a context of institutional complexity: evidence from an emerging economy. *Journal of Accounting & Organizational Change, 17*(3), 416-435. doi:10.1108/jaoc-04-2020-0039

Muralidhar, K. (2010). Enterprise risk management in the Middle East oil industry. *International Journal of Energy Sector Management, 4*(1), 59-86. doi:10.1108/17506221011033107

Rahaman, M., & Bari, M. (2024). Predictive Analytics for Strategic Workforce Planning: A Cross-Industry Perspective from Energy and Telecommunications. *International Journal of Business Diplomacy and Economy*, *3*(2), 14-25.

Ryan, M. (2013). Cloud computing security. *Journal of Systems and Software*, *86*(9), 2263-2268. doi:10.1016/j.jss.2012.12.025

Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. *Computers & Security*, *53*(NA), 234-246. doi:10.1016/j.cose.2015.06.001

Sangeetha, R. (2013). Detection of malicious code in user mode. *2013 International Conference on Information Communication and Embedded Systems (ICICES)*, *NA*(NA), 146-149. doi:10.1109/icices.2013.6508244

Sehgal, N. K., & Bhatt, P. C. P. (2018). *Cloud Computing* (Vol. NA).

Singh, S., Jeong, Y.-S., & Park, J. H. (2016). A survey on cloud computing security. *Journal of Network and Computer Applications*, *75*(75), 200-222. doi:10.1016/j.jnca.2016.09.002

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing. *Computer Communications*, *107*(NA), 30-48. doi:10.1016/j.comcom.2017.03.010

Stoel, M. D., Ballou, B., & Heitger, D. L. (2017). The Impact of Quantitative versus Qualitative Risk Reporting on Risk Professionals' Strategic and Operational Risk Judgments. *Accounting Horizons*, *31*(4), 53-69. doi:10.2308/acch-51777

Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. doi:10.1016/j.jnca.2010.07.006

Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, *71*(NA), 28-42. doi:10.1016/j.compeleceng.2018.06.006

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*(NA), 212-233. doi:10.1016/j.cose.2017.09.001

Wu, M., & Moon, Y. B. (2017). Taxonomy of Cross-Domain Attacks on CyberManufacturing System. *Procedia Computer Science*, *114*(NA), 367-374. doi:10.1016/j.procs.2017.09.050

Xu, X. (2012). From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, *28*(1), 75-86. doi:10.1016/j.rcim.2011.07.002

Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Information Sciences*, *379*(379), 42-61. doi:10.1016/j.ins.2016.04.015