WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cloud Computing Baseline Security Requirements Within an Enterprise Risk Management Framework

Chisom Elizabeth Alozie

Department of Information Technology, University of the Cumberlands, Kentucky, United States
aloziechisom23@gmail.com

A B S T R A C T

Modern businesses need cloud computing because it provides flexibility and scalability. Adoption of technology, however, brings up privacy and security issues, necessitating strong frameworks to safeguard vital resources. The integration of baseline security measures into cloud systems within an Enterprise Risk Management (ERM) framework is examined in this study. Role-based access control (RBAC) and the principle of least privilege to restrict access are important security tactics. Using secure software development techniques, including following the OWASP Top 10 standards, can help stop vulnerabilities like cross-site scripting (XSS) and SQL injections. For data protection, encryption methods are essential. These include TLS for data in transit and AES-256 for data at rest. Authentication mechanisms, safe communication, and ongoing monitoring all contribute to database security. To stop unwanted access, authentication, authorization, and encryption are the main components of API security. The availability, confidentiality, and integrity of cloud-based resources are among the risks that can be managed by matching security to business goals. By providing real-time threat intelligence, AI-driven threat detection and automated response systems improve security. By implementing standards like NIST, ISO 27001, and CIS guidelines, cloud security is improved, cyber threats are reduced, and a robust, trust-based digital ecosystem is fostered.

Keywords Application Security, System Security, Database Security, Network Security. Risk Assessment.

1. Introduction

Cloud computing has developed into a platform for on-demand data processing and storage that is very scalable. Governments, charitable organizations, and businesses have used it widely, which has enhanced productivity but has raised security and privacy concerns. Organizations continue to have holes in their risk management frameworks for cloud security even as they integrate cybercrime and data protection measures. Uncertainty in data access, storage, and transmission results from the lack of strong evaluation procedures**.** Ensuring data integrity, secure operations, and proper planning for damage risks remains a highly significant challenge in modern cloud environments (Saeed et al., 2023). However, as more and more companies shift their operations to the cloud, strong security frameworks are needed to protect vital data, networks, and applications from cyber threats. When designing and implementing cloud computing systems, it is essential to incorporate baseline security requirements, particularly when using an enterprise risk management (ERM) architecture. This approach helps organizations manage risks related to the availability, confidentiality, and integrity of cloud-based resources by making sure that business objectives and the overall security posture are alignment.

This study investigates the fundamental security requirements that must be met by various cloud computing components, such as databases, apps, systems, network infrastructure, and information processing. To provide a comprehensive, risk-aware approach to cloud adoption, it also examines how these security measures might be included in the broader ERM framework.

2. Baseline Security Requirement for Cloud Computing

Application Security: When developing and implementing cloud-based services, security should be incorporated into every stage of the software development lifecycle (Daniel Ajiga et al., 2024). This includes: First, developers should adhere to industry standards like the OWASP Top 10 and secure coding guidelines to avoid vulnerabilities like buffer overflows, SQL injection, and cross-site scripting (XSS) (Kunduru, 2023) (Lim et al., 2024). Second, utilize role-based access control (RBAC) to specify user privileges based on their job responsibilities. The principle of least privilege should be used to limit users' access to only the systems and data that they need. Third, sensitive data must be encrypted both in transit and at rest using strong cryptographic algorithms, such as TLS for data in transit and AES-256 for data at rest (Pattnaik et al., 2022). Finally, to prevent unauthorized access and data exposure, application programming interfaces (APIs) should be secured with encryption, permission, and authentication (Pattnaik et al., 2022).

Database Security: Databases contain the most important information about a business, making them prime targets for hackers. Among the fundamental security measures for databases are: All sensitive information in the database should be encrypted when not in use. Database communications also require the use of secure transmission techniques, such as TLS (Zeidler et al., 2024). Then, to control database access, put strong authentication procedures in place, such as multi-factor authentication (MFA). Per authorization methods, only authorized users should be allowed to query or change the data. Additionally, logging, activity monitoring, and continuous database access should be used to spot anomalous behavior. Automated alerts could identify possible intrusions or unauthorized access (Barika et al., 2020). Moreover, During the observation required by all parties, the actual data values, data masking techniques can be used to obscure sensitive information.

System Security: To protect against cyberattacks, cloud systems need to be hardened, as this webinar illustrates. This comprises the assets and data of the organization. The bare minimum of security requirements for cloud systems are as follows: Initially, confirm that operating systems have the latest security patches and upgrades installed (Daniel Ajiga et al., 2024). Disable unnecessary services and features that increase the attack surface. Second, it is necessary to implement a vulnerability management process that includes regular system scans, vulnerability fixes, and timely software and system component upgrades (Castillo, 2024). Third, ensure that system backups are created on a regular basis, stored securely, and that recovery point objectives (RPO) and recovery time objectives (RTO) are set for business continuity. Systems should then use intrusion detection and prevention systems (IDPS) to promptly identify and thwart any attempts at attacks or unauthorized access.

Network Infrastructure Security: In cloud architecture, communication and data sharing depend on the underlying network. Network infrastructure security must be given top importance to maintain the integrity of the cloud environment (Lu et al., 2022). Some fundamental network infrastructure security measures are as follows: Use software-defined networking (SDN), VLANs, or firewalls to isolate vital networks from less important networks to limit the spread of attacks. Additionally, firewalls and security groups ought to be configured to limit all incoming and outgoing traffic to and from cloud services and to only allow necessary network interactions (Hieu et al., 2024). Make sure that all network traffic, including communications within and across clouds, is encrypted using TLS or IPsec. In a similar vein, implementing Distributed Denial of Service (DDoS) prevention techniques can shield cloud services from traffic overload attacks.

Information processing Security Cloud data processing handles sensitive data; hence privacy and compliance depend on its protection (Raja, 2024). Typical security precautions include the following: Establishing a framework for data classification is the first step in determining the sensitivity of different types of data. The right security methods must be chosen based on the classification level (for instance, highly secret content may require more effective encryption or restricted access) (C. Alozie, 2025). Next, make sure that data processing adheres to the data minimization principle, which stipulates that only necessary data should be collected and processed, to lower the possible danger of overexposure (Grigaliūnas et al., 2023). Continuous surveillance and monitoring of data processing procedures is necessary to spot any security lapses or data misuse. Lastly, cloud processing must comply with relevant legislation such as GDPR, HIPAA, or PCI-DSS, depending on the type of data and the location.

3. Integrating ERM Framework with Baseline Security Requirements

This section demonstrates that to ensure that cloud computing security satisfies business objectives, enterprise risk management (ERM) frameworks must include certain baseline security criteria. By balancing security measures with business needs, this approach helps manage risks associated with the cloud (Alozie et al., 2024).

Risk Assessment and Identification: Evaluating the risks associated with the cloud, including insider threats, data breaches, and service interruptions, should be the first step in any ERM approach (Oladoyinbo et al., 2023). Security teams can successfully mitigate these threats by prioritizing and customizing baseline security measures and being thoroughly aware of the risks (Richard Arogundade, 2023).

Risk Mitigation Strategy: The initial stage in any ERM methodology should be to evaluate the risks related to the cloud, such as insider threats, data breaches, and service outages (Oladoyinbo et al., 2023). According to Richard Arogundade (2023), security teams can effectively reduce these dangers by prioritizing and tailoring basic security measures and having a solid understanding of the hazards.

Continuous Monitoring and Improvement: Cloud infrastructures are dynamic, and security requirements evolve with time (Alozie et al. 2024). The ERM framework must include ongoing security control and cloud service monitoring to recognize and handle emerging threats. Regular evaluation and update of the security framework will ensure that baseline security measures remain effective.

Compliance Management: The ERM framework must incorporate regulatory compliance and industry requirements (Nalluri et al., 2023). To make sure that cloud services and security measures comply with regulations like GDPR, HIPAA, or PCI-DSS, regular audits and assessments must be conducted.

4. Conclusion

It is essential to integrate fundamental security principles with cloud computing in order to safeguard sensitive data, systems, and network infrastructure. Adopting security frameworks like NIST, ISO 27001, and CIS guidelines is crucial for protecting vital assets as more and more businesses move to cloud environments. The confidentiality, integrity, and availability of data are guaranteed by putting strong access controls, encryption techniques, and ongoing monitoring systems into place. Furthermore, by integrating these security measures into an Enterprise Risk Management (ERM) framework, businesses may effectively manage the risks associated with cloud adoption while ensuring business continuity and regulatory compliance. Finding weaknesses, reducing threats, and coordinating security plans with corporate goals are all made easier with this proactive approach. Businesses may improve their

security posture and enable real-time threat intelligence and adaptive defensive methods by utilizing AI-driven threat detection and automated reaction systems. By lowering potential cyber risks, guaranteeing resilience against new threats, and promoting a trust-based digital ecosystem, this comprehensive approach provides a safe basis for using cloud services.

References

Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise Software Applications to protect Data Integrity. *Computer Science & IT Research Journal*, *5*(8), 1920–1941. https://doi.org/10.51594/csitrj.v5i8.1451

Alozie, C. (2025). Literature review on the application of blockchain technology initiative. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5085115

Alozie, C. E., Akerele, J. I., Kamau, E., & Myllynen, T. (2024a). Capacity planning in cloud computing: A site Reliability Engineering approach to optimizing resource allocation. *International Journal of Management and Organizational Research*, *3*(1), 49–61. https://doi.org/10.54660/ijmor.2024.3.1.49-61

Alozie, C. E., Akerele, J. I., Kamau, E., & Myllynen, T. (2024b). Disaster recovery in cloud computing: Site Reliability Engineering strategies for resilience and business continuity. *International Journal of Management and Organizational Research*, *3*(1), 36–48. https://doi.org/10.54660/ijmor.2024.3.1.36-48

Alozie, C. E., & Chinwe, E. E. (2025). *Developing a cybersecurity framework for protecting critical infrastructure in organizations*. ICONIC RESEARCH AND ENGINEERING JOURNALS. https://doi.org/10.5281/ZENODO.14740463

Barika, M., Garg, S., Zomaya, A. Y., Wang, L., Van Moorsel, A., & Ranjan, R. (2020). Orchestrating big data analysis workflows in the cloud: Research challenges, survey, and future directions. *ACM Computing Surveys*, *52*(5), 1–41. https://doi.org/10.1145/3332301

Castillo, F. (2024). IT security. In *Managing Information Technology* (pp. 251–284). Springer International Publishing.

Chinwe, E. E., & Alozie, C. E. (2025). *Adversarial tactics, techniques, and procedures (TTPs): A deep dive into modern cyber attacks*. ICONIC RESEARCH AND ENGINEERING JOURNALS. https://doi.org/10.5281/ZENODO.14740424

Grigaliūnas, Š., Schmidt, M., Brūzgienė, R., Smyrli, P., & Bidikov, V. (2023). Leveraging taxonomical engineering for Security Baseline compliance in international regulatory frameworks. *Future Internet*, *15*(10), 330. https://doi.org/10.3390/fi15100330

Hieu, N. D., Mutaher, H., & Bijalwan, A. (2024). Design and implementation of a secured enterprise network infrastructure. In *Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society* (pp. 509–527). Wiley. https://doi.org/10.1002/9781394272303.ch32

Kunduru, A. R. (2023). Security concerns and solutions for enterprise cloud computing applications. *Asian Journal of Research in Computer Science*, *15*(4), 24–33. https://doi.org/10.9734/ajrcos/2023/v15i4327

Lim, P.-C., Chieng, G.-W. A., Ling, H.-C., & Jali, N. (2024). OWASP A03 Injection vulnerability in web application development. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, 107–116. https://doi.org/10.37934/araset.57.1.107116

Lu, J., Wang, J., Wei, X., Wu, K., & Liu, G. (2022). Deep anomaly detection based on variational deviation network. *Future Internet*, *14*(3), 80. https://doi.org/10.3390/fi14030080

Nalluri, S., Malyala, M. M., Konatam, S., & Kandagiri, K. K. (2023). Cybersecurity risk management in cloud computing environment. *International Journal of Science and Research Archive*, *10*(1), 1062–1068. https://doi.org/10.30574/ijsra.2023.10.1.1127

Oladoyinbo, T. O., Adebiyi, O. O., Ugonnia, J. C., Olaniyi, O., & Okunleye, O. J. (2023). Evaluating and establishing baseline security requirements in cloud computing: An enterprise risk management approach. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4612909

Pattnaik, P. K., Le, D.-N., & Pal, S. (2022). Security paradigms in cloud computing. In *Cloud Computing Solutions* (pp. 181–196). Wiley. https://doi.org/10.1002/9781119682318.ch11

Raja, V. (2024). Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *4*(1), 121–144. https://doi.org/10.60087/jaigs.v4i1.86

Richard Arogundade, O. (2023). Strategic security risk management in cloud computing: A comprehensive examination and application of the risk management framework. *International Advanced Research Journal in Science, Engineering and Technology*, *11*(1). https://doi.org/10.17148/iarjset.2024.11105

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors (Basel, Switzerland)*, *23*(15). https://doi.org/10.3390/s23156666

Zeidler, O., Sturm, J., Fraunholz, D., & Kellerer, W. (2024). Performance evaluation of transport layer security in the 5G core control plane. *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*.