ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/raj-vayyavur/258

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 4

Research Article

Effective Application Security Governance with Role Provisioning and Least Privileged Access Management

Raj Vayyavur*

Citation: Vayyavur R. Effective Application Security Governance with Role Provisioning and Least Privileged Access Management. *J Artif Intell Mach Learn & Data Sci 2023*, 1(4), 1089-1093. DOI: doi.org/10.51219/JAIMLD/raj-vayyavur/258

Received: 02 November, 2023; **Accepted:** 18 November, 2023; **Published:** 20 November, 2023

***Corresponding author:** Dr. Raj Vayyavur, Senior, IEEE, USA, E-mail: rvayyavur@gmail.com

ABSTRACT

In today's complex IT environments, managing access to applications and ensuring secure handling of privileged roles is crucial for preventing unauthorized access and potential security breaches. This research presents a comprehensive framework designed to lead application governance efforts, specifically focusing on role provisioning and least privileged access management. The framework addresses the growing complexity of IT environments, particularly in multi-tenant and cloud computing scenarios. It integrates best practices from information security governance, including the development of robust policies and standards, regular auditing of access controls, and continuous collaboration with application owners to implement corrective measures. Drawing on key insights from literature, the paper explores how to mitigate risks associated with privileged accounts and unauthorized access, emphasizing the principle of least privilege. By adopting a continuous improvement approach, this framework aims to enhance security posture, reduce vulnerabilities, and ensure compliance with organizational and regulatory standards. This research serves as a valuable resource for IT security practitioners, Information Security (InfoSec) professionals, application owners, and product managers, offering a structured approach to managing access controls and preventing security incidents. The framework not only addresses current challenges but also provides a foundation for future improvements in application governance. By fostering a culture of security, organizations can better protect sensitive information, maintain operational integrity, and build trust with stakeholders in an increasingly interconnected digital landscape.

Keywords: Access Control, Access Management, Auditing, Cloud Computing, Continuous Improvement, Identity Management, Information & Application Security Governance, IT Security, Lease Privilege Access, Multi-tenant and Cloud Computing, Product Management, Risk Management, Role-based Access Control (RBAC), Role Provisioning, Security Architecture, Security Policies & Standards, Sensitive Information.

1. Introduction

The rapid adoption of cloud computing, along with the increasing complexity of IT environments, has significantly elevated the importance of robust application governance. Organizations are tasked with ensuring that access to applications is managed securely, especially in scenarios where multiple users, services, and tenants interact within shared environments. Effective application governance is no longer a luxury but a necessity for preventing unauthorized access and potential security breaches that could have catastrophic consequences.

This research explores the critical aspects of application governance, with a specific focus on role provisioning and least privileged access management. Role provisioning involves the systematic assignment of access rights based on the roles within an organization, ensuring that users have the necessary permissions to perform their duties without overexposing the organization to security risks. Least privileged access management, on the other hand, is a security principle that restricts users' access rights to the minimum necessary to perform their job functions, thereby minimizing the risk of insider threats and reducing the impact of potential security breaches.

As organizations increasingly rely on cloud-based and multi-tenant architectures, the need for effective role provisioning and least privileged access management has become more pressing. The literature emphasizes the challenges posed by these environments and the importance of developing a comprehensive framework that integrates best practices from information security governance.

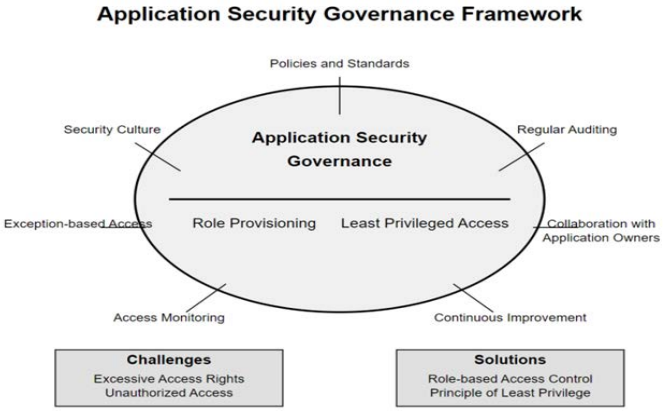

Figure 1: Comprehensive Framework for Application Security Governance.

In this paper, we propose a comprehensive framework for leading application governance efforts, focusing on role provisioning and least privileged access management. This framework is designed to help organizations mitigate risks, enhance their security posture, and comply with regulatory requirements. We will explore the development of policies and standards, the importance of regular auditing, and the need for continuous collaboration with application owners to ensure that security measures are effectively implemented and maintained. By adopting a continuous improvement approach, organizations can not only address current security challenges but also anticipate and prepare for future threats.

2. Role Provisioning in Application Governance

Role provisioning is a critical component of maintaining a secure and well-governed IT environment. Proper role provisioning ensures that users have the necessary access to perform their duties without exposing the organization to unnecessary risks. However, in many organizations, the current state of role provisioning is far from ideal. Employees are frequently granted more access than necessary, leading to significant security vulnerabilities. A prevalent issue is the indefinite or extended retention of administrative access to production environments, even after the original need for such access has expired. This practice substantially increases the risk of security breaches and unauthorized access, as it provides opportunities for the misuse or exploitation of privileged accounts.

Shin, et al.[16], in their work on role-based provisioning in Infrastructure as a Service (IaaS) environments, underscore the importance of precise and secure role assignments to mitigate such risks. Their research highlights that, in environments like IaaS, where multiple users and services interact within shared resources, a strict and well-defined role provisioning system is essential to prevent unauthorized access and ensure that each user has only the permissions required for their specific role.

To mitigate these risks, organizations should ensure that access is granted strictly based on specific roles within the organization. For instance, project managers should be provided with edit access only to the projects they are directly responsible for. While they may need view access to other projects for reference or oversight, edit permissions should be tightly controlled and limited to their specific areas of responsibility. This practice prevents project managers from inadvertently or maliciously altering projects outside their purview, thereby maintaining the integrity of the project data.

The Prima system, as discussed by Lorch, et al.[15], serves as a practical example of a privilege management and authorization system designed to enforce access control in grid environments. Such systems can be adapted to modern cloud and enterprise environments to ensure that only authorized users can access sensitive information. By implementing similar systems, organizations can enforce stringent access controls, ensuring that users have access only to the data and resources necessary for their role.

In situations where a project manager needs to support a fellow project manager who is on leave, role provisioning can allow for temporary proxy access. However, this access should be granted for a limited period and be closely monitored. The related access rights should be terminated promptly once the temporary need has passed. This approach helps to ensure that no unnecessary access remains in the system, thereby reducing the risk of unauthorized changes or access to sensitive information. By implementing these controls, organizations can manage temporary access needs effectively without compromising security.

A critical aspect of role provisioning is the ability to audit and monitor access usage continuously. Audit logs should be enabled and regularly reviewed to track how access rights are being used, ensuring proactive control over who has access to what within the organization. This continuous monitoring allows for the timely detection of any anomalies or misuse of access rights, enabling swift corrective actions to be taken. By regularly auditing access logs, organizations can identify and address potential security risks before they escalate into significant issues.

Additionally, employees may sometimes require additional access on an exception basis. Such access should be granted only when absolutely necessary and must be subject to strict monitoring and control. Exception-based access should have clearly defined expiration dates, and access logs should be reviewed to ensure that it is being used appropriately and only for the intended purpose. This controlled approach to exception-based access helps maintain the security of the IT environment while still accommodating legitimate needs for temporary elevated access.

By adopting a more disciplined and controlled approach to role provisioning, organizations can significantly reduce their risk exposure and enhance their overall security posture. This approach not only helps in preventing unauthorized access and security breaches but also aligns access management with the principle of least privilege, ensuring that employees have only the access they need to perform their job functions effectively. Through careful role provisioning, organizations can create a more secure, efficient, and compliant IT environment, protecting both their data and their operations from potential threats.

3. Least Privileged Access Management

Least Privileged Access Management is a core security principle that mandates users be granted only the minimum level of access necessary to perform their job functions. This principle is crucial in reducing an organization's attack surface, minimizing insider threats, and protecting sensitive information from unauthorized access. However, despite its importance, many organizations struggle to enforce this principle effectively, particularly in high-risk environments such as production systems, where the potential consequences of excess access are significant.

A common challenge in implementing least privileged access is the handling of administrative rights in production environments. In many organizations, employees, including project managers, are often granted administrative access that far exceeds their immediate needs. For example, a project manager might receive broad access rights, including the ability to edit projects beyond their direct responsibility. Moreover, this access is often retained indefinitely or for extended periods, even after the original need for such access has passed. This practice increases the risk of unauthorized changes, data breaches, and the exploitation of privileged accounts.

To mitigate these risks, organizations must enforce the principle of least privilege by ensuring that access rights are tightly aligned with the specific roles and responsibilities of each employee. For example, project managers should have edit access solely to the projects they are actively managing. Access to other projects should be restricted to view-only permissions, unless a specific, temporary need arises. This approach helps prevent inadvertent or malicious modifications to projects outside a manager's scope, thereby reducing the risk of operational disruptions and data integrity issues.

In scenarios where a project manager needs to temporarily assume the responsibilities of a colleague-such as covering for someone on leave-proxy access can be granted for a limited duration. This temporary access should be tightly controlled, with clearly defined start and end dates, ensuring that the additional permissions are automatically revoked once the temporary need is fulfilled. This approach aligns with the recommendations of Bhaskaran et al. [3], who emphasize the importance of controlling and monitoring privileged accounts closely. By strictly enforcing the termination of temporary access, organizations can prevent the accumulation of unnecessary privileges that could be exploited if left unchecked.

Continuous monitoring and auditing are critical components of an effective least privileged access management strategy. As Carter[8] discusses, regular audits of access rights, continuous monitoring of privileged accounts, and the use of automation tools to enforce least privilege policies are essential practices. Enabling audit logs across all systems allows organizations to track how access rights are utilized, providing visibility into who accessed what and when. Regularly reviewing these logs enables the detection of anomalies, such as unauthorized access attempts or unusual patterns of behavior, which could indicate a security breach or insider threat. Proactive monitoring also allows security teams to take swift corrective action, such as revoking unnecessary access or investigating suspicious activity.

In certain cases, employees may require additional access on an exception basis to perform specific tasks outside their usual role. While such exceptions are sometimes necessary, they should be granted cautiously and under strict control. Exception-based access should have predefined expiration dates, and its use should be closely monitored to ensure it is limited to the intended purpose. This approach, as emphasized by both Bhaskaran, et al.[3] and Carter[8], helps minimize the risk of privilege escalation and ensures that temporary access does not compromise the organization's overall security posture.

Implementing least privileged access management effectively requires a disciplined approach to access control, continuous monitoring, and fostering a culture of security awareness. By adhering to the principle of least privilege, organizations can significantly reduce their exposure to security risks, ensuring that employees have only the access necessary to perform their roles without compromising the security of the broader IT environment. This approach not only enhances operational security but also aligns with regulatory requirements and best practices in information security governance.

4. Access Management Policies & Standards

Developing robust policies and standards is a fundamental step in establishing effective application governance. These policies serve as the foundation for how access is granted, managed, and monitored within an organization. In many cases, the lack of clear policies or the inconsistent application of existing policies can lead to significant security vulnerabilities, particularly in environments where employees are often granted more access than necessary.

To address this issue, organizations must establish clear, role-based access control (RBAC) policies that define the specific access rights associated with each role within the organization. For instance, a policy might state that project managers should only have edit access to the projects they are directly responsible for, with view-only permissions to other projects. These policies should also define the conditions under which temporary or proxy access may be granted, such as when a project manager needs to cover for a colleague on leave.

In line with best practices, as discussed by Brotby[4] and Blobel, et al.[5], these policies should be comprehensive, covering not just the assignment of roles and permissions, but also the processes for regularly reviewing and updating access rights. This includes defining the procedures for revoking access when it is no longer needed, such as immediately terminating temporary access granted during a colleague's absence. By implementing strict policies and standards, organizations can significantly reduce the risk of unauthorized access and ensure that access rights are aligned with the principle of least privilege.

Furthermore, policies should incorporate guidelines for continuous monitoring and auditing, as emphasized by Carter[8]. This includes ensuring that audit logs are enabled and regularly reviewed to track how access rights are used and to identify any potential security breaches or unauthorized access attempts. By embedding these practices into the organization's access management policies, security teams can maintain proactive control over who has access to what, thereby enhancing the overall security posture.

5. Auditing & Identifying Gaps in Access Management

Regular auditing is essential for maintaining effective access management and ensuring that the established policies

and standards are being followed. Without regular audits, organizations may unknowingly allow excessive or outdated access rights to persist, which can lead to security breaches and unauthorized access.

As highlighted by Johnston and Hale[13], improved security governance can be achieved through regular audits and assessments of access controls. These audits should focus on identifying any gaps between the current access rights and the defined role-based access control policies. For example, an audit might reveal that a project manager still has edit access to a project they are no longer responsible for, or that temporary proxy access was not revoked after the agreed period. By identifying these discrepancies, organizations can take corrective action to align access rights with the principle of least privilege.

In addition to identifying gaps, audits should also assess the effectiveness of the existing access management processes. This includes evaluating whether the processes for granting, modifying, and revoking access are efficient and aligned with the organization's security goals. The findings from these audits can inform updates to policies and standards, ensuring that the organization's access management practices remain robust and effective in the face of evolving security threats.

Bhaskaran, et al.[3] emphasize the need for close monitoring of privileged accounts, which should be a key focus during audits. This involves reviewing the use of administrative and privileged accounts to ensure that they are being used appropriately and that access is being granted and revoked in a timely manner. By continuously auditing and monitoring access controls, organizations can maintain a strong security posture and minimize the risk of unauthorized access.

6. Collaboration with Security Team & Application Owners

Collaboration between security teams and application owners is crucial for the effective implementation of access management policies. Application owners are often the individuals most familiar with the specific access needs of their applications, and their input is essential for ensuring that access controls are appropriately configured and maintained.

Becker and Drew[6] discuss the challenges of deploying user provisioning and identity access management systems, highlighting the need for close collaboration between security teams and application owners. This collaboration is particularly important when it comes to identifying and addressing gaps in access management. For example, if an audit reveals that a project manager has excessive access to multiple projects, the security team should work with the relevant application owners to revoke unnecessary permissions and ensure that access is aligned with the principle of least privilege.

Application owners should also be involved in the continuous improvement of access management practices. This includes regularly reviewing the access needs of their applications and working with security teams to update access controls as necessary. By fostering a collaborative approach, organizations can ensure that access controls remain effective and responsive to changing security requirements.

Furthermore, application owners should play an active role in monitoring access to their applications. This includes regularly reviewing audit logs to detect any unauthorized access attempts or unusual patterns of behavior. By working closely with security teams, application owners can help to identify potential security risks early and take corrective action to mitigate those risks.

Gashgari, et al.[12] propose a best-practice framework for information security governance that includes guidelines for working with application owners to maintain secure access controls. This framework emphasizes the importance of communication and collaboration in achieving effective application governance. By involving application owners in the access management process, organizations can ensure that access controls are not only aligned with security policies but also tailored to the specific needs of each application.

7. Continuous Improvement in Application Security Governance

Application security governance is an ongoing process that requires continuous improvement to remain effective in the face of evolving security threats and changing IT environments. As new vulnerabilities are discovered and as organizational needs change, access management practices must be regularly reviewed and updated to ensure they remain effective.

Tan, et al.[17] discuss the importance of continuous improvement in information security governance, particularly in ensuring that security measures remain effective over time. This approach involves regularly reviewing and updating access management policies and standards to address emerging security challenges. For example, as organizations increasingly adopt cloud-based services and multi-tenant architectures, access management practices must be adapted to address the unique risks associated with these environments.

Continuous improvement also involves the regular auditing of access controls, as discussed earlier, and the proactive identification of gaps and weaknesses in the organization's access management practices. By continuously monitoring and reviewing access controls, organizations can ensure that any issues are identified and addressed promptly, reducing the risk of security breaches and unauthorized access.

Furthermore, continuous improvement requires a commitment to ongoing education and training for all stakeholders involved in application governance. This includes ensuring that security teams, application owners, and end-users are aware of the importance of least privileged access management and are equipped with the knowledge and tools to implement and maintain effective access controls.

Daase and Friesendorf[9] argue that security governance must be flexible and adaptable, allowing organizations to respond to new security challenges as they arise. By adopting a continuous improvement approach, organizations can ensure that their application governance efforts remain effective and that any gaps in security controls are promptly addressed.

7. Conclusion

In conclusion, the increasing complexity of modern IT environments necessitates a comprehensive approach to application governance, particularly in the areas of role provisioning and least privileged access management. As organizations continue to embrace cloud computing and multi-tenant architectures, the need for robust access management frameworks has become more critical than ever.

This paper has outlined a comprehensive framework that integrates best practices from information security governance, focusing on the development of policies and standards, regular auditing, and continuous collaboration with application owners. By adhering to the principle of least privilege, organizations can significantly reduce their exposure to security risks, ensuring that employees have only the access necessary to perform their roles without compromising the security of the broader IT environment.

The proposed framework emphasizes the importance of continuous improvement in application governance, ensuring that access management practices remain effective in the face of evolving security threats. For IT security practitioners, InfoSec professionals, application owners, and product managers, this framework provides a structured approach to managing access controls and preventing security incidents.

Ultimately, the success of any application governance effort depends on the commitment of all stakeholders to foster a culture of security within the organization. By prioritizing security governance and continuously improving access management practices, organizations can better protect themselves against the ever-evolving landscape of digital threats and ensure a secure and resilient IT environment for the future.

8. References

1. S. A. Almulla and C. Y. Yeun, “Cloud computing security management,” in *Proc. 2010 Second Int. Conf. Eng. Syst. Manage. Appl.*, Sharjah, UAE, Mar. 2010, pp. 1-7.
2. P. Abos, *Multi-Tenant Access Control: Developing Access Control Mechanisms*, 2010. [Online]. Available: http://example.com
3. K. Bhaskaran et al., “Privileged identity management in enterprise service-hosting environments,” in *Proc. 2012 IEEE Netw. Oper. Manage. Symp.*, Maui, HI, USA, Apr. 2012, pp. 736-749.
4. K. Brotby, *Information Security Governance: A Practical Development and Implementation Approach*, vol. 53, John Wiley & Sons, 2009.
5. B. Blobel, R. Nordberg, J. M. Davis, and P. Pharow, “Modelling privilege management and access control,” *Int. J. Med. Inform.*, vol. 75, no. 8, pp. 597-623, Aug. 2006.
6. M. Becker and M. Drew, “Overcoming the challenges in deploying user provisioning/identity access management backbone,” *BT Technol. J.*, vol. 23, no. 4, pp. 71-79, Oct. 2005.
7. M. Carcary, K. Renaud, S. McLaughlin, and C. O’Brien, “A framework for information security governance and management,” *IT Prof.*, vol. 18, no. 2, pp. 22-30, Mar./Apr. 2016.
8. M. K. Carter, “Techniques to approach least privilege,” *IDPro Body Knowl.*, vol. 1, no. 9, pp. 1-10, 2022.
9. C. Daase and C. Friesendorf, *Rethinking Security Governance: The Problem of Unintended Consequences*, London, U.K.: Routledge, 2010.
10. G. A. de Oliveira Alves, L. F. R. da Costa Carmo, and A. C. R. D. de Almeida, “Enterprise security governance: A practical guide to implement and control Information Security Governance (ISG),” in *Proc. 2006 IEEE/IFIP Bus. Driven IT Manage.*, Munich, Germany, Apr. 2006, pp. 71-80.
11. H. G. Ehrhart, H. Hegemann, and M. Kahl, “Towards security governance as a critical tool: A conceptual outline,” in *Putting Security Governance to the Test*, London, U.K.: Routledge, 2017, pp. 37-54.
12. G. Gashgari, R. J. Walters, and G. B. Wills, “A proposed best-practice framework for information security governance,” in *Proc. IoTBDS 2017*, Porto, Portugal, Apr. 2017, pp. 295-301.
13. A. C. Johnston and R. Hale, “Improved security through information security governance,” *Commun. ACM*, vol. 52, no. 1, pp. 126-129, Jan. 2009.
14. K. Koh, A. B. Ruighaver, S. B. Maynard, and A. Ahmad, “Security governance: Its impact on security culture,” in *Proc. 2005 Australas. Conf. Inf. Secur. Privacy (ACISP)*, Brisbane, Australia, Jul. 2005, pp. 123-134.
15. M. Lorch et al., “The PRIMA system for privilege management, authorization and enforcement in grid environments,” in *Proc. 2003 First Latin Amer. Web Congr.*, Santiago, Chile, Nov. 2003, pp. 109-116.
16. D. Shin, H. Akkan, W. Claycomb, and K. Kim, “Toward role-based provisioning and access control for infrastructure as a service (IaaS),” *J. Internet Serv. Appl.*, vol. 2, pp. 243-255, Sep. 2011.
17. T. C. Tan, A. B. Ruighaver, and A. Ahmad, “Information security governance: When compliance becomes more important than security,” in *Proc. 25th IFIP TC-11 Int. Inf. Secur. Conf. (SEC 2010)*, Brisbane, Australia, Sep. 2010, pp. 55-67.