Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

The Crucial Significance of Governance, Risk and Compliance in Identity and Access Management

Omer Eltayeb Omer Eltayeb[1]

Abstract

This study explores the crucial part that governance, risk and compliance play in the field of identity and access management (IAM), as well as the methods for putting IAM systems into place in an efficient manner. IAM is a crucial component of modern enterprises since it supports digitization, improves security management, and ensures compliance with regulation and information security governance. However, it is normal for businesses to face significant obstacles when attempting to use IAM solutions. The emphasis in the current discussion on IAM frequently shifts from strategic considerations to operational ones, pushing the latter to the margins. Organizations are forced to deal with growing internal and external vulnerabilities and threats while also trying to stay within budgetary and resource restrictions. Strategic decision-makers, such as chief information officers and security officers, are forced by this circumstance to make thoughtful judgments about which investment programs to prioritize. IAM investments significantly impact a wide range of strategic goals, including security, agility, assurance, productivity, compliance, and empowerment. Our preliminary findings highlight the importance of compliance-driven IAM methods in contemporary businesses. Therefore, a review is conducted using PRISMA guidelines with an emphasis on the ramifications and developments in the world. The main aim of this research is to help firms implement effective IAM strategies that not only strengthen security and regulatory conformity but also match with more general strategy goals by examining the synergy between governance, risk & compliance and IAM.

Keywords: *Identity and Access Management, Compliance, Investment Prioritization, Economic Modeling, Corporate Operations, Enterprise Security.*

Introduction

Identity and access management (IAM) is a key component of organizational cybersecurity and compliance in the ever-changing digital ecosystem of today. Businesses are becoming more and more dependent on digital technologies, cloud computing, and interconnected networks to share information, services, and resources. Thus, it is essential to protect vital assets and guarantee compliance with legal requirements (Golz & Somaini, 2017). IAM, which consists of the administration of user identities, access privileges, and security controls, is crucial in enhancing an organization's overall cybersecurity posture (Rosencrance, 2023). It serves as the foundation upon which digital ecosystem security is built, ensuring that the appropriate people or entities have access to the appropriate resources at the appropriate times for the appropriate purposes. Not only that, IAM's importance goes beyond only security considerations and encompasses a complicated web of legal obligations, industry-specific mandates, and regulatory norms (Liu et al., 2016).

Nowadays, cyber-attacks, a rise in data breaches, and a quickly changing regulatory framework illustrate today's cybersecurity scenario. Businesses must navigate a complex web of compliance rules, ranging from the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) to the Payment Card Industry Data Security Standard (PCIDSS) to different industry-specific regulations. But if we look at it in the IAM context, compliance entails coordinating identity management procedures with these laws' requirements (Yu et al., 2016). Organizational operations have undergone a fundamental change as a result of the digitization of business processes and the growth of cloud computing. Data protection is essential because it is now the backbone of contemporary businesses. As enterprises adopt digital transformation, they must also deal with a variety of difficulties, such as an ever-changing threat landscape and a changing regulatory environment.

[1] Alliance Manchester Business School, The University of Manchester, United Kingdom, University of Science & Technology, Sudan, Email: omer.eltayeb@ieee.org

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

In this scenario, IAM emerges as a crucial enabler of security and compliance in the current digital era, where the lines between on-premises and cloud environments are blurred because remote workforces access corporate resources from a variety of devices and locations (Mohammed, 2013). Understanding the intricate interactions between identity management and regulatory standards is crucial to understanding the significance of compliance within IAM. Therefore, several regulations apply to the current corporate environment, including but not limited to: GDPR, which the European Union mandates, sets high standards for data protection and imposes harsh fines for data breaches. HIPAA, which regulates healthcare data, establishes strict standards for the privacy of patient information (Tovino, 2021). The PCIDSS, which is applicable to businesses processing credit card data, specifies security criteria to guard against breaches of cardholder data. Moreover, organizations also set up reliable internal controls in accordance with Sarbanes Oxley (SOX) audit requirements, which focus on financial reporting. At the same time, several industries have set their own industry-specific rules, including banking (e.g., Dodd-Frank Act), healthcare (e.g., HITECH Act), and energy (e.g., NERC CIP) (Clark, 2021).

In order to comply with these rules, strict control over user access, data protection, and auditability in all areas is where IAM plays a crucial role (McLaughlin et al., 2021). IAM solutions help businesses create and enforce access restrictions that comply with these laws, ensuring that only vetted users have access to sensitive information and systems. By coordinating the complex dance between user identities and the legal requirements that control data protection, privacy, and accountability, IAM essentially serves as the guardian of compliance (Phillips, 2023). By demonstrating a commitment to protecting sensitive information, this alignment ensures that businesses follow the law and cultivate trust with stakeholders and customers. A compliance framework's multidimensional approach to effective IAM includes technology, processes, and rules. It encompasses the coordination of identity lifecycle management, access provisioning, authentication, and audit trails beyond merely controlling user access (Bartol et al., 2023). However, it is reported that some goals should be kept in mind when creating IAM strategies. Businesses should implement IAM solutions that establish access rights in accordance with work duties, responsibilities, and the least privilege principle (Sandhu & Samarati, 1994), which lessen the danger of unauthorized data exposure by limiting access to only what is required for each user. In this regard, a key component of IAM strategies is multifactor authentication (MFA). It makes sure that gaining access to crucial systems and data necessitates various types of authentications, such as something the user is (biometric data), something they have (smart card), or something they know (password) (Ometov et al., 2019).

Moreover, MFA improves security and complies with legal specifications that call for strong authentication in certain situations. The whole lifespan of user identities, from onboarding to offboarding, is covered by IAM. The provisioning of users with the proper access privileges upon their entry into the organization and the fast revocation of their access upon exit are both ensured by effective identity lifecycle management (Naik & Jenkins, 2017). For controlling and observing access by privileged users, such as administrators, IAM solutions are essential. IAM tools use stringent restrictions to make sure that privileged accounts are only used for approved purposes (Tolbert, 2017). Nonetheless, organizations can also have thorough audit trails by compliance regulations through IAM solutions that record users.

In light of the knowledge mentioned above, this study examines the intricate compliance environment in relation to IAM through published literature (Tovino, 2021) by spotlighting real-world examples and best practices. Since IAM is more than just technology, it also includes procedures and regulations that strategically link to compliance and security of any organizational structure (Kipchuk et al., 2021). This study highlights the concrete and intangible advantages that firms may achieve by putting good IAM strategies in place. These advantages include improved security, reduced risk, improved operational effectiveness, and the ability to verify compliance during audits reliably (Cai et al., 2019). Moreover, this review also addresses the fundamental difficulties that companies encounter when pursuing compliance and provides workable answers and tactics to get around these obstacles by keeping up with changing legislation (Niebank & Walker, 2020).

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

Literature Review

IAM is more than simply a technological solution in today's digital landscape; it's an essential business strategy. Companies that engage in strong IAM strategies and prioritize continuing regulatory compliance will be successful in the digital age. IAM represents a commitment to securing private information, fostering stakeholder connections, and guaranteeing long-term resilience in our ever-changing digital environment. Organizations that recognize the inherent link between IAM and regulatory compliance not only meet legal duties but also unlock potential benefits such as increased operational efficiency, increased security, decreased risk, and the capacity to demonstrate compliance during audits. **Figure 1** gives a general view of how IAM systems work for any business.

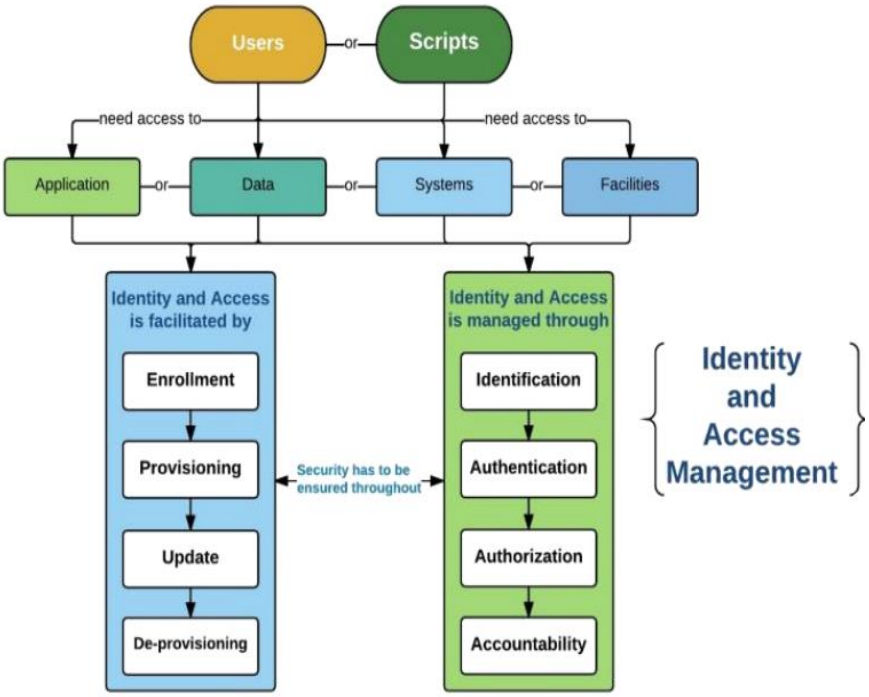


Figure 1: An overview of IAM (Mohammed, 2017)

Authentication and authorization procedures are at the heart of an IAM system. End-user validity is ensured by authentication, while authorization regulates access to cloud resources based on user permissions. (J. Werner, 2017) and (Goel, 2015) highlight recent IAM studies that investigate identity management systems, providing insights into the strengths and disadvantages of various authentication mechanisms, particularly in cloud situations. The literature also looks into IAM's data storage performance, providing several service models, including a way of proposing user ID storage for cloud computing (Anand, 2015) and addressing associated security concerns. It was reported that IAM can help mitigate security and privacy issues in Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and multi-tenancy cloud computing platforms.

Moreover, IAM goes beyond typical security procedures to keep user profiles correct in the cloud. Database auditing (L. Deng, 2020) and claim-based identity management systems (Chatterjee, 2015) improve the security of cloud service access. As evidenced in studies by (L. Barreto, 2013) and (Y. Chi, 2018) addressing challenges of intrusion tolerance and user authentication in cloud identity management, IAM architectures incorporate policies, standards, and procedures to develop workflows and security considerations. The emphasis on scalability, independence, and consistency in IAM techniques is critical, with (Y. Yang) advocating a systematic approach. In this regard (S. Wang, 2019) offers a blockchain-based cloud user

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

identity management protocol, which aligns IAM with third-party requirements while also providing increased security for digital identities using public, private, or hybrid clouds.

Moreover, beyond the technical components, IAM is critical in cloud computing security, addressing issues like authentication, authorization, and data integrity. (S. Chong, 2014) investigates the impact of user comments on trust levels in cloud computing. (Mathur, 2019) also provides protocols for securing the availability, anonymity, and integrity of cloud resources, using a two-layer strategy that integrates authentication and cryptography to safeguard digital identities on cloud servers.

While the importance of IAM extends to mobile cloud computing, where identity management security is important, (I. Khalil, 2014) compares the efficacy of a unique IAM technique in preventing server penetration vulnerabilities. (M. Suguna, 2017) enables safe IAM for mobile cloud computing, addressing security concerns with authentication and tokens. (D. Sharma, 2016) uses an IAM security architecture built on cloud-based virtual machines to emphasize the main security qualities of secrecy, integrity, and availability.

With research like (L. Wu, 2017), (Ma, 2016), and (Y. Yu, 2016) investigating identity-based encryption approaches and protocols for cloud data integrity testing, cryptography is emerging as a critical instrument for protecting user identity privacy. (H. Deng, 2020) proposes an innovative way for tracking cloud data profiles via encrypted data exchange. As stated by (Kettani, 2019) and (W. Sim, 2020), the unique notion of blockchain technology takes centre stage in IAM, leveraging open-source blockchain technologies to check user identification profiles and defend identity management systems. Essentially, IAM becomes a pillar for organizations looking for efficient methods that not only comply with legislation but also improve operational efficiency and security. This dense network of IAM issues emphasizes its significance in the larger context of compliance and effective IAM techniques in managing the digital landscape's difficulties.

Problem Statement

IAM, the comprehensive management of identities and access in digital systems ensures secure and regulated access to organizational resources. Compliance with industry regulations, legal mandates, and internal policies is crucial to IAM system implementation and effectiveness. This review article examines the challenges, strategies, and best practices of aligning IAM systems with regulatory and internal compliance standards and how compliance shapes IAM frameworks. The article explores how compliance requirements affect IAM system design, configuration, and functionality, affecting an organization's ability to meet legal obligations, protect sensitive data, and mitigate risks from unauthorized access or data breaches. The main issue is to understand and articulate the complex relationship between compliance and IAM to help organizations create robust, regulatory-compliant access management strategies.

Methodology

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Page et al., 2021) guidelines were followed in the conduct and reporting of this review. Because this study looked at previously published research, there was no need for formal ethics approval or informed consent.

Searching Strategy

For our study, we systematically used a list of carefully selected keywords to perform a thorough literature review on different search engines. These keywords were carefully chosen to address a broad spectrum of this subject, such as "Identity and Access Management," "IAM, " "Compliance," "Cybersecurity," "Regulatory Requirements," "IAM Strategies," "Data Protection," "Access Control," "Authentication," "Authorization," "Audit Trails," "Security Standards," "Compliance Frameworks," "Legal Obligations," "Data Privacy," "IAM Technologies," "User Access," "Role-Based Access Control," "Multi-Factor Authentication," "Risk Management," "Identity Lifecycle," "Access Provisioning," "Audit and Monitoring," "Data Breaches," as well as "Cyber Threats."

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

Moreover, these keywords were carefully merged using both "OR" and "AND" operators as necessary to achieve the maximum accuracy and thoroughness in our investigation. To find additional studies that matched our inclusion criteria, we also carefully examined the reference lists of pertinent academic articles and reports, a procedure known as backward citation searching.

Inclusion Criteria

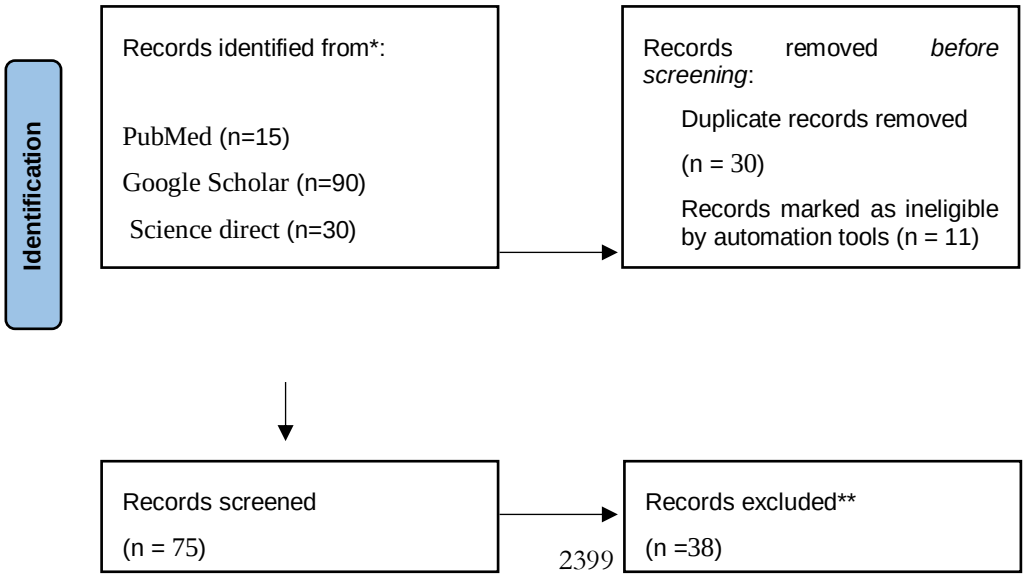
- The inclusion of research looks at different facets of compliance in IAM and its function within the IAM system.
- Consideration of articles published in peer-reviewed journals during the period from 2017- 2023.
- A focus on articles written in English to ensure consistency with our research goals.
-

Exclusion Criteria

- Exclude sources lacking technical depth or substantial information on compliance in IAM technologies or strategies.
- Exclude duplicate or multiple versions of the same study to avoid redundancy in the research.
- Exclude articles not written in English to ensure linguistic consistency in the collected literature.
- Exclude sources lacking essential data, methodology, or results irrelevant to the IAM and compliance research.

Data Collection

To evaluate the factors, a small group of scholars independently chose the paper titles and abstracts and read the entire transcripts. Disagreements were settled through conversation or, if necessary, by involving a different team member. **Table 1** aggregates and displays the data gathered from the included investigations. A thorough web search across numerous databases revealed 135 studies related to the topic of interest that were accessible online. **Figure 1** shows the final articles chosen for the review after duplicate entries were removed and studies were excluded that did not match the inclusion criteria based on their titles, full texts, and abstracts.



Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

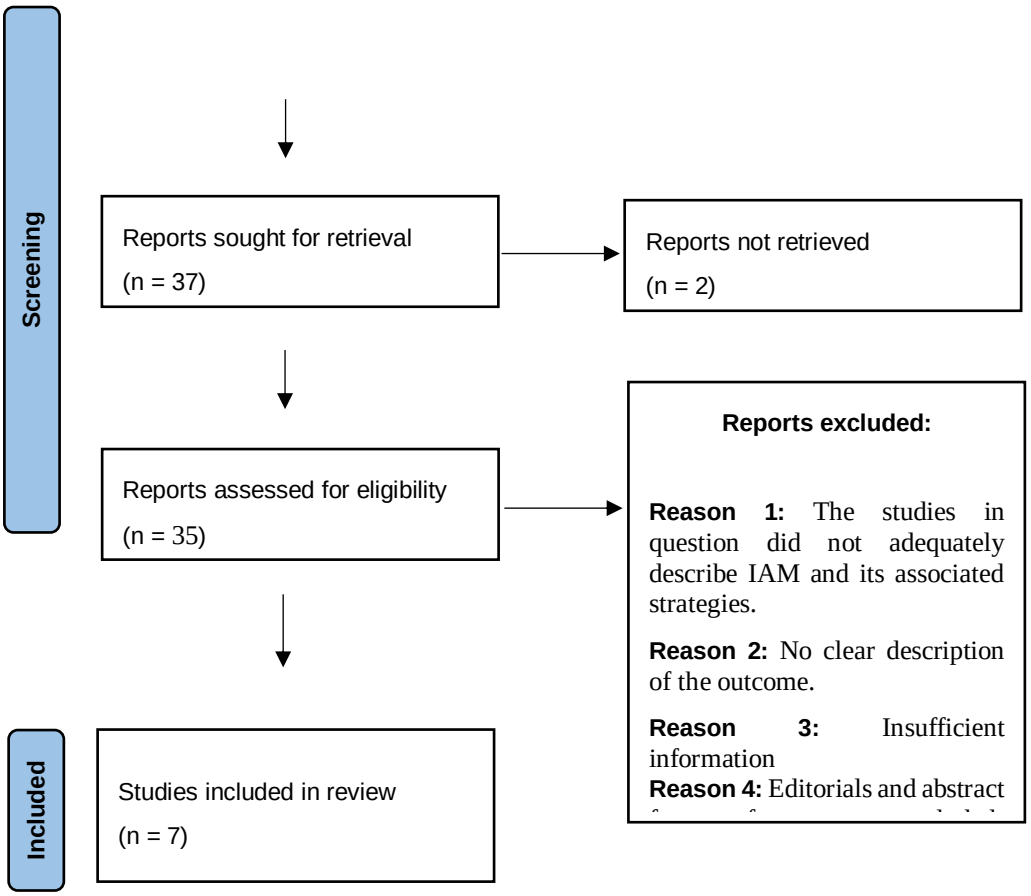


Figure 1: The PRISMA flow diagram for the selected studies

Table 1: Summaries Of IAM Studies

References	Objectives	Key Findings
(Singh et al., 2023)	IAM's role in data securing, user access managing, and challenges by evolving technologies	The study places a strong emphasis on IAM's function in monitoring user behavior, controlling access privileges, and incorporating authentication into organizational infrastructure. The difficulties in safeguarding identity-based activities brought about by developing technologies, like cloud services, are noted by the researcher. One important security mechanism that is emphasized is data-centric authentication, which uses techniques like public key management to safeguard communication.
(Indu et al., 2018)	To identify the adoption of cloud computing, highlight associated security risks, and stress the need for a robust IAM mechanism.	This research addresses how organizations are rapidly adopting cloud computing because of its cost-effectiveness and flexibility. Still, they also emphasize the inherent security concerns and vulnerabilities associated with multi-tenancy and third-party management. The emphasis is on the importance of strong IAM techniques for dealing with authentication, access, security, and service challenges in the cloud environment.
(Karlsson & Jönrup, 2023)	To address cloud computing access rights management issues, particularly in Amazon Web Services.	This research examines the difficulties of maintaining access rights in cloud computing, specifically in Amazon Web Services (AWS). IAM and access control concepts such as Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC) are introduced. According to the study, RBAC lacks scalability, and ABAC lacks administrative capabilities. To address these concerns, a new paradigm known as Entity-centric

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

		Attribute- and Role-based Access Control (EARBAC) is developed, which demonstrates efficiency, security, flexibility, and scalability. In AWS IAM, EARBAC with Tags and roles is shown to be 27% faster than RBAC. The study seeks to strike a compromise between security and developer efficiency, and it investigates a hybrid paradigm that combines the benefits of RBAC and ABAC in AWS IAM. The proposed EARBAC architecture is provided as a viable approach for fine-grained and scalable access control in AWS, leveraging Tags and roles to improve security and efficiency over traditional RBAC. The study issues center on developing an effective security policy strategy, balancing security and developer efficiency, and leveraging AWS IAM for an integrated access control model.
(Nahar & Gill, 2022)	to introduce a research initiative to model an integrated IAM system in a secure enterprise architecture. The main objective is to create an ontology-based IAM metamodel that is business domain and technology agnostic and adaptable to various information systems.	This research goal is to model an integrated IAM system for a secure enterprise architecture to protect information system digital assets. The way forward is to create an ontology-based IAM metamodel. The metamodel can create IAM models for different information systems due to its versatility. The study uses the well-known Design Science Research method. The IAM metamodel is evaluated using demonstration. The evaluation process also creates an eight-IAM pattern system. These patterns solve IAM issues. The research helps enterprise architects, IAM professionals, and researchers design and implement IAM models for specific situations within a secure enterprise architecture for information systems.
(Mohammed, 2021)	To to examine the role of IAM systems in various businesses, particularly in the integration of AI and intelligent authentication.	This article reviews IAM-related intelligent authentication studies and acknowledges the difficulty of creating a universal authentication system. This research highlights the challenges of traditional authentication methods in modern IT environments and proposes integrating IAM with AI. This integration simplifies identity management, condenses multiple user identities, and improves efficiency, safety, and compliance. The research also discusses financial institutions' use of these concepts and the challenges of transitioning from analog to virtual environments, emphasizing the need for secure and privacy-conscious digital solutions.
(Mohammed, 2017)	To provide a systematic review of IAM in information security. This research discusses IAM implementation challenges, including data security, compliance, and BYOD vulnerabilities.	The study evaluates how IAM contributes to information security and emphasizes the need for a reliable IAM program to balance security, risk reduction, education, and efficient service usage. IAM provides tools, procedures, and policies for managing user identities and access in organizations to create and control a unique digital identity for each user. IAM implementation is complicated, highlighting the difficulty of managing multiple accounts and access restrictions with a single digital identity. IAM's broader organizational interests include data security, compliance, and vulnerabilities related to personal mobile technology like BYOD. The study's main goal is to assess IAM's information security benefits.
(Alamri et al., 2022)	Blockchain (BC) is important in IAM systems during Health Internet of Things (HIoT) applications.	BIAM is crucial in information systems, especially in healthcare, where high-volume and sensitive health data make HIoT applications prime targets for cyberattacks. This systematic literature suggests that BC is a promising technology, but security

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

		frameworks, risk assessments, and evaluation metrics for BC-based IAM in HIoT need further study.

Finding In Selected Studies

The selected studies merge to offer useful insights across multiple dimensions in the quest of completely understanding the role of compliance in IAM and investigating viable IAM techniques. In conclusion, the convergence of findings from many studies emphasizes the critical significance of compliance in IAM. The investigation of IAM services, spanning from monitoring user behaviour to addressing privacy concerns in electronic transactions, reveals the importance of IAM in organizational infrastructure and security. The problems provided by emerging technologies such as cloud services, as well as the adoption of innovative paradigms such as EARBAC, highlight the dynamic character of IAM methods. The focus on data-centric authentication, AI integration, and ontological IAM metamodels represents a comprehensive approach to improving information security. The complexity of IAM deployment, as emphasized in the evaluation of IAM's contribution to information security, underscores the need for dependable IAM programmes that strike a balance between security, risk reduction, and efficient service consumption. The inquiry into IAM in health applications reveals interesting technology trends, but it also highlights the need for additional research in security frameworks and risk assessments. These findings collectively fuel the conversation around effective IAM techniques, placing compliance as a keystone in navigating the complex world of IAM.

Recommendations

Several recommendations come to light while analyzing the function of compliance in IAM and considering efficient IAM tactics. They are given below.

- *Continuous Alignment with Evolving Regulations*: because regulations are dynamic, businesses should keep their IAM strategies current with changing compliance standards. Keep up with any changes to the laws governing user access and data protection.

- *Investment in Advanced IAM Systems:* think about investing in cutting-edge IAM systems that include multifactor authentication, granular access control, and effective identity lifecycle management. These innovations simplify compliance procedures while simultaneously enhancing security. Employers should implement thorough training programs to inform staff of the critical role IAM plays in compliance. Make certain that everyone on staff is aware of their duties regarding adherence to IAM policies and procedures.

- *Continual Auditing and Monitoring*: IAM solutions must include robust auditing and monitoring functionalities. Frequently check user access, access to privileged accounts, and compliance. Monitoring proactively makes it easier to spot and quickly correct abnormalities. Encourage cross-functional cooperation between compliance specialists, legal professionals, and IT teams. This multidisciplinary approach ensures the alignment of IAM strategies with technical specifications and legal compliance. Scalability and flexibility IAM methods ought to be created with scalability and flexibility in mind. IAM solutions should smoothly adapt as enterprises expand and change to meet shifting compliance needs.

Boundaries of IAM in Business Structures

Due to staffing shortages and budget restrictions, complex IAM solutions may be difficult for small or resource-constrained enterprises to adopt. IAM systems frequently use human administrators to configure and administer them. Security flaws and compliance problems during IAM installation might result from human error. Organizations may find it difficult to stay compliant, given how quickly regulations can change; therefore, IAM techniques must be continuously modified to reflect these developments. Employee and stakeholder resistance to changes in IAM technologies and practices could obstruct their effective

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

deployment. It can be difficult and time-consuming to integrate IAM solutions with current IT infrastructure, which could have an adverse effect on business operations.

Conclusion

In conclusion, the intricate interaction between IAM and compliance highlights the crucial role that IAM plays in modern company operations. The key part IAM plays in enhancing cybersecurity, easing regulatory compliance, and strengthening enterprises' overall security posture has been made clear by this inquiry. The symbiotic relationship between IAM and compliance emerges as a strategic need as firms continue to manage the shifting digital landscape.

The literature suggests that organizational operations have undergone a fundamental change as a result of the digital transformation sweeping through industries. IAM has gained notoriety as the defender of data integrity, privacy, and accountability in this era of cloud computing, remote workers, and networked systems. In order to ensure that the right people have access to the right resources at the right times, it serves as the cornerstone around safe interactions with clients, partners, and staff. HIPAA, GDPR, and industry-specific standards like the PCIDSS are just a few of the legal frameworks that place a strong emphasis on data security, privacy, and audibility-and-find IAM to be the key to success.

However, the environment for complying with regulations was found to be more difficult and complex. The necessity for enterprises to proactively integrate IAM plans with changing compliance standards is one of the main lessons learned from this inquiry. Organizations must make sure that their IAM systems are not only compliant but also flexible enough to handle changes without disrupting the way new mandates are announced. Moreover, IAM compliance has many facets, so a comprehensive strategy is required. It is a strategic framework that includes processes, policies, and controls rather than just a technology solution. Granular access control, strong identity lifecycle management, and multi-factor authentication are requirements for IAM solutions. These technologies help compliance adherence while also enhancing security.

Additionally, employee education and awareness are crucial in this situation. Organizations should engage in extensive training programs to inform employees about the value of IAM in compliance. The organization as a whole becomes more resistant to attacks when employees are aware of their responsibilities in upholding data security and regulatory conformity.

But then again, effective IAM techniques have many advantages; some restrictions need to be understood. The adoption of sophisticated IAM systems may be difficult for smaller enterprises with limited resources. Human mistake is still a possible weakness when implementing IAM, too. Furthermore, it might be challenging because of how often regulations change. In order to maintain the effectiveness and compliance of their IAM initiatives, organizations must invest in the procedures and technologies necessary to keep ahead of regulatory revisions. Another restriction is internal organizational resistance to change. Effective change management strategies are essential since stakeholders and employees may be reluctant to adopt new IAM processes and technology.

Declaration and Statement

Author Biography

Omer Eltayeb, a dedicated researcher, and former Cloud Solution Architect at Microsoft, focuses on cutting-edge cybersecurity issues. His research interest showcases his commitment to addressing pressing challenges in digital security. Omer's is currently affiliation with the University of Science & Technology underscores his dedication to higher education and scholarly pursuits. Through his work, he aspires to contribute valuable insights that enhance cybersecurity strategies and foster a safer digital landscape. Omer Eltayeb is also an active IEEE member (Membership: #100379961) under the affiliation of Europe, Middle East, and Africa Region (Region R8) acting as section Co-Lead and focuses on Technology Research and Devolopement.

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763

References

Alamri, B., Crowley, K., & Richardson, I. (2022). Blockchain-based identity management systems in health IoT: A systematic review. IEEE Access, 10, 59612-59629.

Anand, I. I. a. P. (2015). Identity and access management for cloud web services. IEEE Recent Advances in Intelligent Computational Systems (RAICS), India,

Bartol, J., Vehovar, V., & Petrovčič, A. (2023). Systematic review of survey scales measuring information privacy concerns on social network sites. Telematics and Informatics, 102063.

Cai, F., Zhu, N., He, J., Mu, P., Li, W., & Yu, Y. (2019). Survey of access control models and technologies for cloud computing. Cluster Computing, 22, 6111-6122.

Chatterjee, A. S. a. K. (2015). Identity management in cloud computing through claim-based solution. IEEE Int. Conf. on Advanced Computing & Communication Technologies,

Clark, C. (2021). Could SOX be better?: exploring the advantages and shortfalls of Sarbanes-Oxley.

D. Sharma, C. D., M. Potey. (2016). Identity and access management as security-as-a-service from clouds. Procedia Computer Science, Elsevier, 79, 170–174.

Goel, A., Gupta, G., Bhushan, M., & Nirwal. (2015). Identity management in hybrid cloud. IEEE International Conference on Green Computing and Internet of Things (ICGCIoT), India,

Golz, M., & Somaini, J. (2017). Cybersecurity in the age of digital transformation. MIT Technol. Rev.

H. Deng, Z. Q., Q. Wu, Z. Guan, R. Deng, et al. (2020). Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Transactions on Information Forensics and Security, 3168–3180.

I. Khalil, A. K., M. Azeem. (2014). Consolidated identity management system for secure mobile cloud computing. Computer Networks, Elsevier, 65, 99–110.

Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.

J. Werner, C. M., C. Westphall. (2017). Cloud identity management: A survey on privacy strategies. Computer Networks, 29-42.

Karlsson, R., & Jönrup, P. (2023). Increasing Efficiency and Scalability in AWS IAM by Leveraging an Entity-centric Attribute-& Role-based Access Control (EARBAC) Model. In.

Kettani, S. E. H. a. M. E. (2019). Analysis of identity management systems using blockchain technology. IEEE Int. Conf. on Advanced Communication Technologies and Networking (CommNet), Morocco.

Kipchuk, F., Sokolov, V., Skladannyi, P., & Ageyev, D. (2021). Assessing Approaches of IT Infrastructure Audit. 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T),

L. Barreto, F. S., J. Fraga, E. Feitosa. (2013). An intrusion-tolerant identity management infrastructure for cloud computing services. IEEE Int. Conf. on Web Services, United States.

L. Deng, B. Y., and X. Wang. (2020). A lightweight identity-based remote data auditing scheme for cloud storage. IEEE Access, 8, 206396-206405.

L. Wu, Y. Z., K. Choo, D. He. (2017). Efficient and secure identity-based encryption scheme with equality test in cloud computing. Future Generation Computer Systems, Elsevier, vol. 73, 22–31.

Liu, Z., Luo, J., & Xu, L. (2016). A fine-grained attribute-based authentication for sensitive data stored in cloud computing. International Journal of Grid and Utility Computing, 7(4), 237-244.

M. Suguna, R. A., S. Shalinie, S. Deepti. (2017). Secure identity management in mobile cloud computing. IEEE International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), India,

Ma, S. (2016). Identity-based encryption with outsourced equality test in cloud computing. Information Sciences, Elsevier, 328, 389–402.

Mathur, A. S. a. S. (2019). Concealing the user identity in cloud services. IEEE Int. Conf. on Electronics, Communication and Aerospace Technology (ICECA), India,

McLaughlin, P. A., Sherouse, O., Febrizio, M., & King, M. S. (2021). Is dodd-frank the biggest law ever? Journal of Financial Regulation, 7(1), 149-174.

Mohammed, I. A. (2013). Intelligent authentication for identity and access management: a review paper. International Journal of Managment, IT and Engineering (IJMIE), 3(1), 696-705.

Mohammed, I. A. (2017). Systematic review of Identity Access Management in information security. International Journal of Innovations in Engineering Research and Technology, 4(7), 1-7.

Mohammed, I. A. (2021). The interaction between artificial intelligence and identity and access management: an empirical study. International Journal of Creative Research Thoughts (IJCRT), ISSN, 2320(2882), 668-671.

Nahar, K., & Gill, A. Q. (2022). Integrated identity and access management metamodel and pattern system for secure enterprise architecture. Data & Knowledge Engineering, 140, 102038.

Naik, N., & Jenkins, P. (2017). Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect. 2017 11th International Conference on Research Challenges in Information Science (RCIS),

Niebank, K., & Walker, J. (2020). Evolving regulation and the role of compliance since the 2008 financial crisis. Journal of Financial Compliance, 4(1), 83-94.

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., & Gerla, M. (2019). Challenges of multi-factor authentication for securing advanced IoT applications. IEEE Network, 33(2), 82-88.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. International journal of surgery, 88, 105906.

Journal of Ecohumanism
2024
Volume: 3, No: 4, pp. 2395 – 2405
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i4.3763
Phillips, H. (2023). Cybersecur [ing] the Electric Grid: A Comparative Analysis of Policy Generation Transmission, and Distribution in the US and EU. Tul. J. Tech. & Intell. Prop., 25, 257.
Rosencrance, S. G. a. L. (2023). What is identity and access management? Guide to IAM. TechTarget Retrieved 7 November from https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system
S. Chong, M. A., I. Hamid, J. Abawajy. (2014). Enhancing trust management in cloud environment. Procedia Social and Behavioral Sciences, Elsevier, 314–321.
S. Wang, R. P., Y. Zhang. (2019). EIDM: Ethereum-based cloud user identity management protocol. IEEE Access, 7, 115281–115291.
Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. IEEE communications magazine, 32(9), 40-48.
Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. European Journal of Engineering and Technology Research, 8(4), 30-38.
Tolbert, J. (2017). Adaptive Authentication. Leadership Compass, 1-38.
Tovino, S. A. (2021). HIPAA compliance. The Cambridge Handbook of Compliance, 895-908.
W. Sim, H. C., and M. Tahir. (2020). Blockchain for identity management: The implications to personal data protection. IEEE Conf. on Application, Information and Network Security (AINS), Malaysia.
Y. Chi, G. L., Y. Chen, X. Fan. (2018). Design and implementation of open stack cloud platform identity management scheme. IEEE Int. Conf. on Computer, Information and Telecommunication Systems (CITS), France.
Y. Yang, X. C., G. Wang, L. Cao. An identity and access management architecture in cloud. IEEE Int. Symp. on Computational Intelligence and Design, China.
Y. Yu, L. X., M. Au, W. Susilo, J. Ni, et al. (2016). Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, Elsevier, 62, 85–91.
Yu, Y., Xue, L., Au, M. H., Susilo, W., Ni, J., Zhang, Y., Vasilakos, A. V., & Shen, J. (2016). Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, 62, 85-91.