

**Review Form 3**

Journal Name:	<a href="#">Journal of Engineering Research and Reports</a>
Manuscript Number:	Ms_JERR_131024
Title of the Manuscript:	Innovative Approaches to Identity and Access Management for Enhancing Cybersecurity Compliance in Global Enterprises
Type of the Article	

**General guidelines for the Peer Review process:**

**Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.**

This journal’s peer review policy states that **NO** manuscript should be rejected only on the basis of ‘**lack of Novelty**’, provided the manuscript is scientifically robust and technically sound.  
To know the complete guidelines for the Peer Review process, reviewers are requested to visit this link:

<https://r1.reviewerhub.org/general-editorial-policy/>

**Important Policies Regarding Peer Review**

Peer review Comments Approval Policy: <https://r1.reviewerhub.org/peer-review-comments-approval-policy/>  
Benefits for Reviewers: <https://r1.reviewerhub.org/benefits-for-reviewers>

Review Form 3

PART 1: Comments

	<b>Reviewer's comment</b> <b>Artificial Intelligence (AI) generated or assisted review comments are strictly prohibited during peer review.</b>	<b>Author's Feedback</b> <i>(Please correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)</i>
<b>Please write a few sentences regarding the importance of this manuscript for the scientific community. A minimum of 3-4 sentences may be required for this part.</b>	This manuscript addresses a critical and timely topic in cybersecurity—enhancing compliance through innovative Identity and Access Management (IAM) approaches. It provides actionable insights for global enterprises navigating complex regulatory landscapes, making it valuable for both practitioners and researchers. The integration of case studies and emerging technologies like AI and blockchain adds practical relevance. However, deeper engagement with recent academic literature (2023–2024) would strengthen its scholarly contribution.	
<b>Is the title of the article suitable? (If not please suggest an alternative title)</b>	None required.	
<b>Is the abstract of the article comprehensive? Do you suggest the addition (or deletion) of some points in this section? Please write your suggestions here.</b>	The abstract effectively summarizes the scope, methods, and conclusions. However, it could briefly mention the specific compliance challenges addressed (e.g., cross-border data sovereignty) to better align with the body.  I suggest you rephrase this way  "...addressing challenges such as cross-border data sovereignty and regulatory fragmentation in global enterprises."	Updated the Abstract as suggested
<b>Is the manuscript scientifically, correct? Please write here.</b>	The manuscript is scientifically sound, with logical arguments supported by industry examples and compliance frameworks.	
<b>Are the references sufficient and recent? If you have suggestions of additional references, please mention them in the review form.</b>	The references are sufficient but skewed toward industry reports (e.g., SailPoint, NIST) and older academic works (pre-2020). Use more relevant and latest academic works instead.	Added new references
<b>Is the language/English quality of the article suitable for scholarly communications?</b>	The language is suitable for scholarly communication	
<b>Optional/General</b> comments	The case studies in Section 6 are a highlight, offering tangible examples of IAM implementations. Consider expanding the discussion on Zero Trust Architecture (Section 7.1) to include challenges in adoption (e.g., organizational resistance, cost).	

PART 2:

	<b>Reviewer's comment</b>	<b>Author's comment</b> <i>(if agreed with reviewer, correct the manuscript and highlight that part in the manuscript. It is mandatory that authors should write his/her feedback here)</i>
<b>Are there ethical issues in this manuscript?</b>	<i>(If yes, Kindly please write down the ethical issues here in details)</i>	