

**Review Form 1.7**

Journal Name:	<b>Journal of Engineering Research and Reports</b>
Manuscript Number:	<b>Ms_JERR_115511</b>
Title of the Manuscript:	<b>From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts</b>
Type of the Article	

**Review Form 1.7**

**PART 1: Review Comments**

	<b>Reviewer's comment</b>	<b>Author's comment</b> (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)
<p><b>Compulsory</b> REVISION comments</p> <ol style="list-style-type: none"> <li>1. <b>Is the manuscript important for scientific community?</b> (Please write few sentences on this manuscript)</li> <li>2. <b>Is the title of the article suitable?</b> (If not please suggest an alternative title)</li> <li>3. <b>Is the abstract of the article comprehensive?</b></li> <li>4. <b>Are subsections and structure of the manuscript appropriate?</b></li> <li>5. <b>Do you think the manuscript is scientifically correct?</b></li> <li>6. <b>Are the references sufficient and recent? If you have suggestion of additional references, please mention in the review form.</b></li> </ol> <p><b><u>(Apart from above mentioned 6 points, reviewers are free to provide additional suggestions/comments)</u></b></p>	<ol style="list-style-type: none"> <li>1. Yes, the manuscript is important for the scientific community as it investigates the effectiveness of RBAC systems in mitigating insider threats across diverse organizational contexts, offering valuable insights for enhancing data security practices.</li> <li>2. Yes, the title "From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts" effectively summarizes the study's focus on implementing RBAC strategies to mitigate insider threats across various organizational settings.</li> <li>3. Yes, the abstract of the article is comprehensive as it provides an overview of the research objectives, methodology, key findings, and recommendations, effectively summarizing the study's scope and significance.</li> <li>4. Yes, the subsections and structure of the manuscript are appropriate as they logically organize the content into sections such as Introduction, Challenges and Limitations of RBAC, Recent Advances and Future Directions, and Methods, facilitating clarity and readability for the reader.</li> <li>5. Yes, the manuscript appears scientifically correct as it employs quantitative research methodologies, discusses relevant literature, and draws conclusions based on empirical evidence and analysis.</li> <li>6. Yes, the references provided appear to be sufficient and recent, covering relevant literature in the field of cybersecurity and RBAC. However, depending on the specific focus of the study, additional references from recent publications in reputable journals or conference proceedings could further enrich the discussion and support the findings.</li> </ol> <p><b>Additional suggestions/comments:</b></p> <ol style="list-style-type: none"> <li>1. Discuss limitations of the study methodology, like survey sample biases or data collection constraints, for a balanced perspective.</li> <li>2. Incorporate case studies showcasing RBAC implementation across diverse organizations for practical relevance.</li> <li>3. Explore implications of regulatory frameworks (e.g., GDPR, HIPAA) on RBAC and insider threat mitigation.</li> <li>4. Discuss scalability and feasibility of proposed RBAC enhancements considering resource constraints.</li> <li>5. Include a section on future research directions, such as integrating RBAC with emerging technologies.</li> <li>6. Provide brief section summaries to reinforce key points and engage readers.</li> </ol>	
<p><b>Minor</b> REVISION comments</p> <ol style="list-style-type: none"> <li>1. <b>Is language/English quality of the article suitable for scholarly communications?</b></li> </ol>	<p>Yes, the language and English quality of the article appear suitable for scholarly communications, with clear and coherent expression that effectively conveys complex concepts in the field of cybersecurity and RBAC.</p>	

## Review Form 1.7

<b>Optional/General</b> comments	<ol style="list-style-type: none"><li>1. The manuscript demonstrates a proficient command of language and English quality suitable for scholarly communications, ensuring clarity and coherence in conveying complex concepts.</li><li>2. Integration of case studies or real-world examples could enhance the practical relevance and applicability of the study's findings, providing tangible illustrations of RBAC implementation in diverse organizational settings.</li><li>3. Consideration of potential limitations in the study methodology would contribute to a more balanced perspective on the research findings, fostering transparency and credibility.</li><li>4. Exploring the implications of regulatory frameworks such as GDPR and HIPAA on RBAC implementation would add depth to the discussion, addressing legal and compliance considerations relevant to organizations.</li><li>5. Discussion on the scalability and feasibility of proposed RBAC enhancements, considering resource constraints and organizational complexities, would provide valuable insights for practitioners seeking to optimize their security measures.</li><li>6. Including a section on future research directions would stimulate scholarly discourse and guide future investigations, particularly in exploring the integration of RBAC with emerging technologies for enhanced security solutions.</li></ol>	
----------------------------------	---	--

### **PART 2:**

	<b>Reviewer's comment</b>	<b>Author's comment</b> (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)
<b>Are there ethical issues in this manuscript?</b>	<i>(If yes, Kindly please write down the ethical issues here in details)</i>	

### **Reviewer Details:**

Name:	V Sheeja Kumari
Department, University & Country	Saveetha School of Engineering, SIMATS University, India