



SDI Review Form 1.6

Journal Name:	Asian Journal of Research in Computer Science
Manuscript Number:	Ms_AJRCOS_47898
Title of the Manuscript:	Assessing and Managing Risks in Virtual Environments
Type of the Article	Original Research Article

General guideline for Peer Review process:

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 guideline for Peer Review process, reviewers are requested to visit this link:

(<http://www.sciencedomain.org/page.php?id=sdi-general-editorial-policy#Peer-Review-Guideline>)



SDI Review Form 1.6

PART 1: Review Comments

	Reviewer's comment	Author's comment (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)
Compulsory REVISION comments	<ol style="list-style-type: none"> 1) The Section Introduction should include how the paper is organized (sections and sub-sections). It would help to understand the structure of the paper from the beginning. 2) One of the critical aspect of this paper are the objectives. It is not clear the main objectives of this study or analysis. The paper should include as well a summary of them on the abstract and detail it into the introduction section. Is the main objective of the paper to present a framework? A risks management model for virtual environments? It is not clear at all. 3) It is related to the previous comment. What is the difference between the virtual environments and others? In the paper it is not clear. It seems that the model presented can be applicable to any environment. If not, why? Could you detail more it? 4) The title of the paper is about risks management. However, at the end, the paper does not mention or analyse the risks and the threats and countermeasures associated to the problems. What is the link with the risk management? 5) The main risks management methodologies and standards are not even mentioned into the paper? Why? Is it not one of the goals of this paper analyse it? 6) The multilayer model doesn't consider continuity. Why? 7) The multilayer model doesn't consider privacy. It is one of the most critical requirements nowadays related to these environments. Could you clarify it? 8) Please, re-consider the title of the paper. This paper doesn't describe a new process to manage risks on virtual environments, with clear steps and methods. 9) Another critical aspect of the paper is that the threats and malicious activities are not mentioned, there is not a detailed analysis about it. How is it possible to 	<ol style="list-style-type: none"> 1. Done 2. Mentioned clearly in the last four lines of the abstract. 3. It means non traditional environments where you deal with someone whom you can't see face-to-face. Like buying online or applying to something online. Are they real? Are they what they are claiming to be? 4. It is addressing the risk in terms of: preventing non authorized physical access, identity theft, hacking, human errors and misuse, etc. 5. This paper only addresses risk management in online transactions (identify, manage, and contain). 6. It is just a tool to evaluate how secure the system is. 7. Please refer to figure 2. All privacy information is within "Confidentiality". It also addressed at the front-end security. 8. We tried few but found this one to be more appropriate. Please suggest some if you have something in mind. 9. This is addressed at the back-end security through the use of firewalls and identity checks. 10. Only applies to online transactions B2B, B2C, G2C.



SDI Review Form 1.6

	<p>analyse the risks without taking into account these items?</p> <p>10) The paper doesn't include any information about the type of organizations involved on the studies, the type of them, the sectors, as transport, defence and so on. It would help to understand the dimension of the problem and to understand if the scope is enough to obtain general conclusions. Is this framework valid for all the organizations?</p> <p>11) It seems that, according to the paper and the model described, the physical security is only used to protect the access to the information (section named as Business Environment and Physical Security). However, physical security is related to continuity and/or availability of the systems as well in a lot of cases. Could you clarify it?</p> <p>12) According to the paper, into the risks management section, <i>An effective and efficient security framework depends mainly on the organization's security policies and procedures</i>. It is clear that with only policies and procedures without the proper resources (human resources, tools and technology involved), the security won't work. Could you, please, clarify it?</p> <p>13) It seems that the paper recommends to perform a ROI calculation in order to measure and decide about the risks. However, not in all the environments it can be applicable (governments, public, non-profit organizations and so on). Are we talking here about profit organizations only? Please, clarify it.</p> <p>14) Could you, please, include some references about the calculation of ROI on risks management related to cyber security? It is related to the previous comment.</p> <p>15) The paper doesn't mention threats or the impact of these threats. It is crucial within the risks management area.</p> <p>16) The paper mentions losses and one table related to it, but due to WHAT? It is not clear if these losses are really related to the virtual environments or other issues. It is not clear at all the dependency with this study.</p> <p>17) The paper mentions incidents and one table related to it, but due to WHAT? It is not clear if these incidents are really related to the virtual environments or other</p>	<p>11. It means restricting the none authorized physical access to the systems and the facility in general.</p> <p>12. Policies and procedure include everything. Like having a policy that none one will do the job before going into a proper training. Using fingerprints instead of password for critical jobs to avoid sharing or cracking passwords.</p> <p>13. We are talking about all but ROI in this case is not necessarily monetary. It is comparing savings vs. expenses. How much to install and maintain the systems vs. reaching to more customers and beneficiaries (compared to opening offices and branches).</p> <p>14. Done</p> <p>15. This is not within the scope of this paper. A whole field of study.</p> <p>16. Losses could be direct (identity theft) or indirect (downtime) and losing potential customers.</p> <p>17. Same as 16.</p> <p>18. Totally different and will not be addressed in this study.</p> <p>19. In the first place: if there are no threats, reported incidents, reported losses, we will not be doing this work. Threats and losses are there, our role is to minimize them or eliminate them if possible.</p>
--	--	---



SDI Review Form 1.6

	<p>issues. It is not clear at all the dependency with this study.</p> <p>18) The paper doesn't analyse the viability of the virtual environments. Is only the ROI the only variable to take into account? What about vulnerabilities, threats, impacts...?</p> <p>19) One comment related to the previous one is that there is not a clear map between the threats, incidents, losses and risks on these environments. The model should take into account it. Correct?</p>	
Minor REVISION comments	<p>20) Please, put the numbers in the sections and sub-sections properly.</p> <p>21) The number of references about the subject could be updated with more recent studies. Mainly about other studies performed by CSA or other organizations that reflect other figures about cloud computing and security incidents.</p> <p>22) Is this researching finished? Are there not future steps to complete the study?</p>	<p>20. Done</p> <p>21. Done</p> <p>22. We will look further in how this research can be enhanced in the future. We didn't put it in the paper so we can commit ourselves.</p>
Optional/General comments	<p>23) In general, the contents of the paper are interesting, but the objectives are not explained in detail, there is not a list of recommendations to avoid the risks analysed on the paper and the model needs to be explained in more detail in order to cover some inconsistencies. Some basic concepts as vulnerabilities, impacts or threats should be taken into account into the model.</p>	<p>23. Thank yoi.</p>

PART 2:

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