Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing

Muhammad Imran Tariq[1] and Vito Santarcangelo[2,3]
[1]*Superior University, 36-L, Gulberg-III, Lahore, Pakistan*
[2]*Centro Studi S.r.l, Buccino, Italy*
[3]*Department of Mathematics and Computer Science, University of Catania, Catania, Italy*

Keywords: Information Security, Cloud Computing, ISO 27001:2013, Security Assessment, Effectiveness of ISO 27001:2013 Controls.

Abstract: Cloud Computing provides a scalable, high availability and low cost services over the Internet. The advent of newer technologies introduces new risks and threats as well. Although the cloud has a very advanced structures and expansion of services, but security and privacy concerns have been creating obstacles for the enterprise to entirely shift to the cloud. Therefore, both service providers and clients should build an information security system and trust relationship with each other. In this research paper, we analysed most widely used international and industry standard (ISO/IEC 27001:2013) for information security to know its effectiveness for Cloud Organizations, each control importance factor for on-premises, IaaS, PaaS and SaaS, and identify the most suitable controls for the development of SLA based Information Security Metrics for each Cloud Service Model. We generically evaluated ibid standards control objectives without considering Cloud organization size, nature of work, enterprise size. To know effectiveness, relevance to Cloud Computing, factor of standard control objectives for the in-house or in a public cloud, we defined a quantitative metric. We come to the conclusion that ISO / IEC 27001:2013 compliance improves service providers and customer's information security system and build a trust relationship but not fulfil all requirements and cover all relevant issues.

1 INTRODUCTION

The understanding and enforcement of security and privacy are the core steps in the successful implementation of Cloud in an organization. Although a number of researches have been conducted but information security is still big question and new security risks and threats are generating complex situation for Cloud organizations.

Cloud computing is still most favorite research able area for researchers. Cloud Computing has a number of advantages over traditional computing like pay as per use, cheap rates, web base access, virtualization, easy to deploy, licensing and less human resource required etc. However, according to (Buyya et al., 2009) security and protecting the privacy of an organization are a continuous process particularly Information Security of an organization is a critical responsibility of Cloud Service Provider. Just think to the login task to a Cloud Service to consider the amount of risks related to Information Security Management. For effective Information Security in an organization, necessary processes and measures are required to be planned and implemented especially in the scenario when organization outsource its computing services to third party (Cloud Service Provider).

The Cloud Service Providers also outsource their partial services which increase Information Security complexities, business continuity and legal obligations (Subashini and Kavitha, 2011). The effective implementation of Information Security in an organization can improve the business performance and capital component of business. The Information Security threats always effect organizational processes and operations directly (Marston et al., 2011). Therefore, Information Security is strictly related to Cloud Computing, in fact, information Security and protection of information assets are critical activities for all organizations, then it influences business performance and productivity, detect & defend threats and increases business benefits. However, the majority of companies are not sensible to the cause of IT security breaches (Ristov, 2012).

To handle these challenges, many worldwide Cloud Computing service providers and customers realized the need to establish an environment for Infor-

Tariq, M. and Santarcangelo, V.
Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing.
DOI: 10.5220/0005648702010208
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 201-208
ISBN: 978-989-758-167-0

mation Security governance and follow some type of internationally recognized reference framework, international standards and acts. (Gikas, 2010) said that several frameworks and standards already exist which can be used for governance and can be tailored to organizational requirements.

There are a number of standards, frameworks and guides that cover the information security area. Cloud organizations can improve their security by implementing ISO / IEC 27001, NIST SP 800-53 Rev.4, FISMA, PCI DSS, HIPPA, SAS 70 and COBIT 5.0. However, still these standards are not covering all the issues and complexities of Cloud Computing.

ISO / IEC 27001 information security requirements are generic in nature and applicable to all organizations without considering their type, size and nature of work. ISO 27001:2013's ANNEX A is a very important document to carry out checks and implementations related to information security, thanks to its list of 114 controls (best practices), grouped into 35 control objectives, which are grouped into 14 key points, labelled from A.5 to A.18. Some of these key points allow to focus on various aspects of IT Security, also suggesting solutions. A fundamental topic, related to these controls, is their relation with Service Level Agreement requirements. In fact, SLA defines an agreement between two or more parties (1 customers and 1 or more service providers), so it shows the Annex-A controls effectiveness for Cloud Computing.

Similarly, according to (Tariq, Haq and Iqbal, 2015) the COBIT framework has 34 information security processes out of 340 IT governance processes. Therefore, it is mandatory for standards to cover all security aspects to provide maximum level of security.

The Section 2 brief the current Information Security standards used in the renowned Cloud Service Providers. The Section 3 is about the methodology used to evaluate the ISO / IEC 27001:2013 standard and the criteria developed by the authors. Section 4 shows the results of analysis of ISO/IEC 27001:2013, effectiveness and importance factor of its controls and SLA related controls in standard that can be used for Cloud Service models.

2 EXISTING SECURITY STANDARDS AND THEIR IMPLEMENTATION

Information security assessment is very good practice to assess the performance of existing information security system and to identify potential risks and exposures (Imran Tariq, 2012). A security assessment of traditional computing is easy as compliance audit systems are already well established and supported by various existing standards. But (Takabi, Joshi and Ahn, 2010) said that in the case of Cloud Computing, additional challenges arise.

The Table 1 present the evaluation of existing security standard certifications that current renowned Cloud Service Providers have

Table 1: Existing CSPs Security Certification and Accreditation.

Organization	Security Compliance
Amazon	SOC 1, SOC 2, SSAE 16, ISAE 3402, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, FIPS 140-2, HIPPA, CSA and MPAA
Salesforce	ISO 27001, SysTrust, SAS and 70 Type II
Microsoft	FISMA, PCI DSS, HIPAA, SOX, ISO 27001, SAS 70 TYPE 1 and II and NIST SP 800-53
Google	SAS 70 Type II, FISMA, ISO 27001 and NIST SP 800-53
IBM	FISMA, SAS 70 Type II, ISO 27001-2002, SSAE 16, SOC 2, NIST SP 800-53 and HIPPA

As shown in the Table 1, Cloud Service Providers implemented more than one information security certificates and standards on their infrastructure. Moreover, many of the Cloud Service Providers also provide security assessment information to their customers to know that whether their obtained services from a service provider are secured and complaint with security standard.

3 METHODOLOGY

In recent past, process objectives and importance factor of ISO/IEC 27001:2005 has been measured by the (Ristov, 2012) but the research did not check separately each control objectives and importance. The main purpose of this research is to measure the control objectives and importance factor of ISO/IEC 27001:2013 for in-house (Private Cloud) and outsource (Public Cloud), Cloud related controls, find separate controls from the standard for each cloud service model (IaaS, PaaS, SaaS) and finally dig out Cloud related controls and process that can be included in SLA by considering the generality of the ISO 27001 standard and implementation of this standard in renowned CSPs as shown in Table 1.

Table 2: ISO 27001 Controls Evaluation Criteria.

<table>
<tr><th>Level</th><th>Criteria</th><th>Remarks</th></tr>
<tr><td>1</td><td>How much Control is effective for cloud development and service models (SaaS, PaaS and IaaS)?</td><td>The criteria will initially check that whether the selected control is most appropriate for Public Cloud or Private Cloud deployment model of the Cloud Computing. It will facilitate the organizations to find out only appropriate controls according to their deployed cloud model. The criteria will further check how much selected control is effective for Cloud Service Models i.e. SaaS, PaaS and IaaS. The criteria has been developed to know the importance of the selected control in respect of on-premises, SaaS, PaaS and IaaS.
<table>
<tr><th>Importance Factor Value</th><th>Importance Factor Description</th><th>Remarks</th></tr>
<tr><td>-</td><td>Irrelevant</td><td>Not relevant to Cloud Computing</td></tr>
<tr><td>1</td><td>Minimal</td><td>All Responsibilities are transferred to CSP</td></tr>
<tr><td>2</td><td>Moderately important</td><td>Major responsibilities are transferred to CSP</td></tr>
<tr><td>3</td><td>Important and relevant</td><td>Partially responsibilities are transferred to CSP</td></tr>
<tr><td>4</td><td>Highly important</td><td>Minor Responsibility transferred to CSP</td></tr>
<tr><td>5</td><td>Highest importance</td><td>Cloud customer and CSPare responsible to manage their own Cloud.</td></tr>
</table></td></tr>
<tr><td>2</td><td>Suitable to be included in the SLA for Cloud?</td><td>Every ISO/IEC 27001:2013 control is not suitable to be included in the SLA, in this criteria, control suitability will be checked in this regard. The control which are relevant to SLA will be selected to facilitate the industry to formulate comprehensive SLA. Value 1 will be assigned to the Control to increase its importance in addition to values given at level 1 if it is suitable for Cloud SLA otherwise zero value will be assigned to control.</td></tr>
<tr><td>3</td><td>Relevant to Cloud Computing?</td><td>ISO / IEC 27001:2013 have 114 Information Security Controls and every defined control is not relevant to cloud computing. Therefore, to select relevant controls for cloud computing, the said criteria have been developed and it will help to select only cloud related controls for cloud computing. Value 1 will be assigned to the Control to increase its importance in addition to values given at level 1&2 otherwise zero value will be assigned to selected control.</td></tr>
<tr><td>4</td><td>Fundamental</td><td>If this control is the base of a Cloud System (e.g. Incident Management and Business Continuity) then value 1 will be assigned to the Control to increase its importance in addition to the values given at level 1, 2&3 otherwise zero value will be assigned to the selected control.</td></tr>
</table>

To evaluate the importance and control objectives of the standard, we evaluate and assign a quantitative metric for each control objectives importance factor in respect of SaaS, PaaS and IaaS Cloud service layers.

To achieve our goals, we performed both qualitative and quantitative analysis by comparing the applicability and importance of the control for the concerned service layer of the Cloud. We also assume the generic purpose of the standard for each service layer of the Cloud.

A criteria is developed given in Table 2 to achieve research goals. The criteria is divided into 04 levels, the control will be selected and pass through 04 levels to get the results.

To achieve targets, the methodology of (Ristov, 2012) used for ISO/IEC 27001:2005 has been adopted and further extended to find out exact controls for each deployment and service model, exact control related controls and controls for Cloud SLA, from ISO / IEC 27001:2013 controls. The modified / extended quantitative metric adds more filters to get more accurate results and additional information about the ibid standard. It will help organizations to focus on most significant controls during establishment of ISMS or reviewing and improving existing ISMS.

The importance factor of each control objective is defined by indicator consists of 06 possible values. Table II-Level 1 presents the detail of each importance factor value. The - value indicates that the concerned control objective of standard has no effect on in-house services (Private Cloud) or outsourced (Public Cloud) and it is irrelevant. The values 1-5 of criteria shows different importance factor values of a particular control objective based on hosted services either on in-house or public Cloud.

4 EVALUATION OF CONTROLS OBJECTIVE

To evaluate effectiveness and importance of ISO / IEC 27001 controls for cloud computing, Cloud service models (SaaS, IaaS and PaaS) are compared with traditional computing. The given below Figure 1 depicts that which resources are executed by Cloud customers and CSP. (Clayton, 2011) developed the responsibilities and services executed by the CSP, it is shown through green colour in Figure 1 and similarly, whiles the responsibilities and services executed by the Cloud customer; it is shown in red colour in the Figure 1.

The Figure 1 shows that the SaaS can be used as and when required as well as anywhere in the world. In a private Cloud Computing scenario, the Cloud organization is responsible to manage all the resources and take all necessary measures to mitigate the vulnerabilities, risks and threats. In Public Cloud context, the Cloud customer has handover its partial responsibilities to the CSP.

Hence, security responsibilities are also transferred to CSP that is loss of governance risk. The ISO / IEC 27001: 2013 is actually made to manage in-house Information Security and its performance decreased in the scenario of public Cloud (Almorsy, Grundy and Ibrahim, 2011).

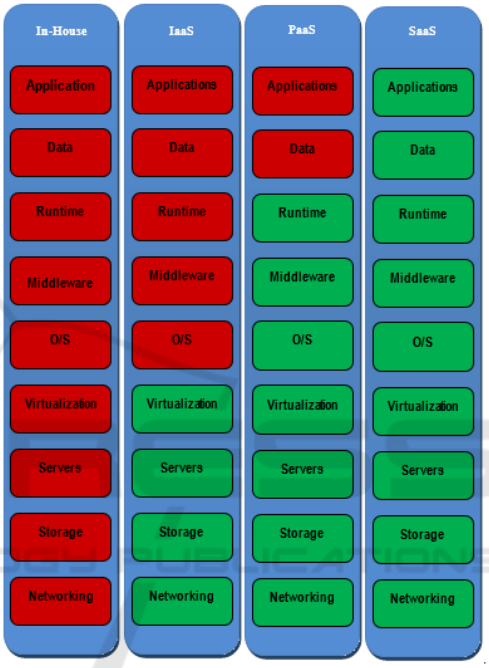

Figure 1: Comparison between Private and Public Cloud Service Models (Clayton, 2011).

By using the comparison given in Figure 1 and defined metrics in Table 2, the importance factor of each control is evaluated for in-house, SaaS, IaaS and PaaS Cloud service layers. It is pertinent to mention here that the management related controls importance factor does not depend if the organizational cloud services are hosted in-house (private Cloud). For example, the Cloud organization must develop, document, implement and review security policies, no matter the size of the organization and Information Security system. The importance factor of operational and technical related controls are depreciated due to services are outsourced and their management responsibilities are also shifted to CSP to enjoy the benefits of public Cloud (SaaS, IaaS and PaaS). The values of the importance factor assigned to the ISO / IEC 27001:2013 controls for private and public Clouds are based on our evaluation. Due to article length consid-

erations, the details of the evaluation is given in DOI No. 10.13140/RG.2.1.4683.7603. It may be observed that many controls importance factor is decreased and many controls importance factor sustained. Depreciation in importance factor does not mean that control is not worthwhile, irrelevant and may exclude from SLA. The depreciated controls may become the part of SLA signed between Cloud customer and CSP. The evaluation of ISO / IEC 27001:2013 is very beneficial for organizations during establishing and reviewing the ISMS for ISO certification and the Cloud organizations may select or exclude ISO 27001 controls to meet their exact requirements and use their resources on highly important controls. It is concluded from the given below Figure. 2 that the importance factor of standard control objectives for each cloud computing services layer is decreased five to eight times as compared to on premises Cloud. The ISO/IEC 27001:2013 has 114 controls. If we calculate the controls which have 5 values then the Fig.2 shows that 94 (82%) controls may be used for on-premises, 12 (11%) out of 114 controls are irrelevant for on-premises. The SaaS have 71 (62%), IaaS have 69 (61%), PaaS have 71 (62%) and in average have 96 (84%) controls that may be used for the Cloud Service models respectively. The SaaS, IaaS and PaaS have 26 irrelevant Controls. The Fig. 3 demonstrates the number of ISO/IEC 27001:2013 controls can be used in respect of Cloud computing in percentage.

In another qualitative analysis, the values of the importance factor of each cloud service layer (IaaS, PaaS, SaaS and Average) are summed and compared with the total value of the in-house importance factor. The results are shown in Figure.4. The result shown in Figure 4 depicts that importance factor of processes, sub-processes and control objectives for each cloud service layer is depreciated as compared to in-house Cloud Computing. There are total 13 processes and if every process assigned 5 value then it would be total 65. After applying the criteria given at Table II, 13 processes got total 56 value out of 65 in Private Cloud. The Figure 4 show clearly shows that SaaS has only attain total 26 numbers because in SaaS case, majority of the responsibilities are transferred to the Cloud Service Providers. The IaaS, PaaS and Average attained 38, 32 and 38 total numbers respectively due to the nature of Cloud service model. Similarly, there are 32 sub-processes in ISO/IEC 27001:2013 and if 5 value is assigned to each sub-process then it would be 160. The Figure 4 shows that on-premises attained total 136 out of 160 in sub-processes and SaaS got 59 out of 160 due to its nature of service. The importance factor of other service models are also depreciated because less responsibilities were transferred to

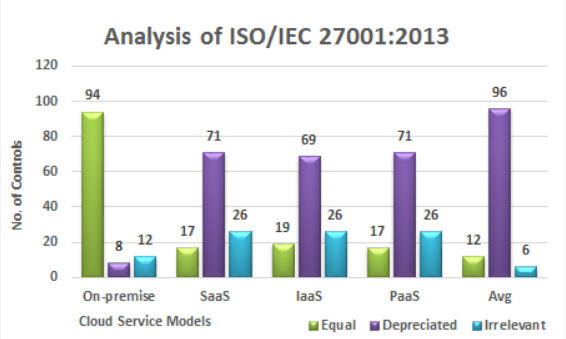

Figure 2: Comparison of the Private Cloud (in-house) with Cloud Service Layers (SaaS, IaaS and PaaS).

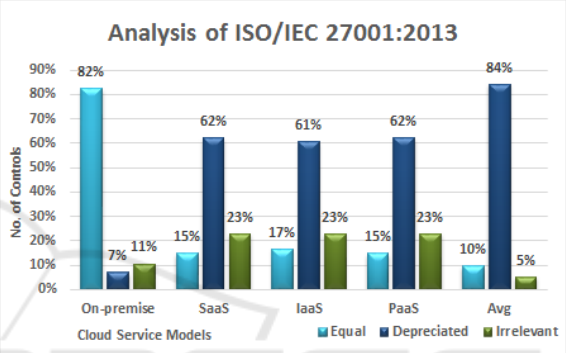

Figure 3: Comparison of the Private Cloud (in-house) with Cloud Service Layers (SaaS, IaaS and PaaS) in percentage.

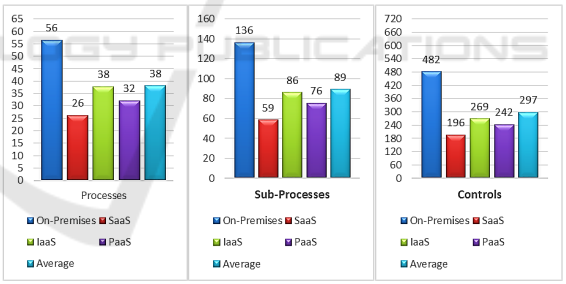

Figure 4: Effectiveness of ISO / IEC 27001: 2005 Controls when Switched to Cloud Service Layers (SaaS, IaaS and PaaS).

them. In last, as we stated above, there are 114 controls and if every control is assigned 5 value then total would be 720. The Figure 4 shows the depreciation of controls. Furthermore, we supposed on-premises got 100% values, it would facilitates us to know the depreciation of ISO/IEC 27001:2013, according to it, the importance factor of controls are depreciated 59%, 44%, 50% and 38% for SaaS, IaaS, PaaS and average respectively as shown in Figure 5. The depreciation of importance factor of processes and sub-processes are also shown in the Figure 5. Now, if we take 3 instead of 5 value of the criteria to check the importance factor of each control and how much controls are de-

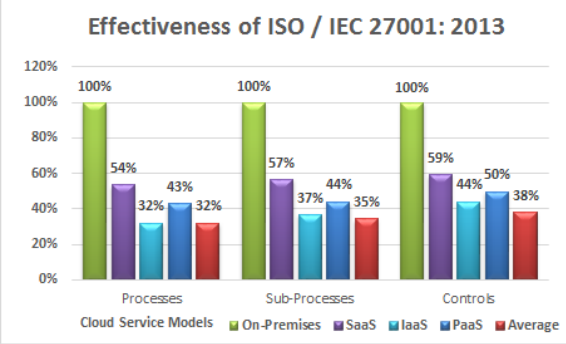

Figure 5: Depreciation of Importance Factor when Switched to Cloud Service Layers.

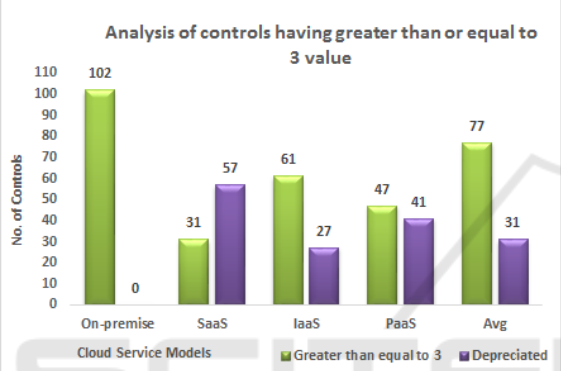

Figure 6: Analysis of Controls having greater than or equal to 3 value.

preciated then we come to know that 102 out of 114 controls can be used on-premises and there is no depreciation. It is pertinent to add here that we do not consider the irrelevant controls and base on rest of the controls calculated the depreciation of controls. The Figure 6 show the results. The results of the Figure 6 shows that ISO/IEC 27001:2013 controls are now less depreciated as compared to the results shown in Figure 2 and the importance factors of the controls are increased like in SaaS case, Figure 2 shows that 71 controls have less than 5 values and Figure 5 shows that 57 controls have less than 3 value. Similarly, the importance factor of other Cloud service models controls are also increased vice versa as compared to Figure 2.

For reader convenient and better understanding, the statistics of the Figure 6 are converted into percentage. The statistics of Figure 7 are compared with the statistics of Fig. 3 and revealed that if we consider 5 value (responsibility completely transferred) then importance factor of the controls are decreased 7% for on-premises, 62% for SaaS, 61% for IaaS, 62% for PaaS and 84% for average while if we consider value 3 of criteria (responsibility partially transferred to CSP) then the importance factor of the con-

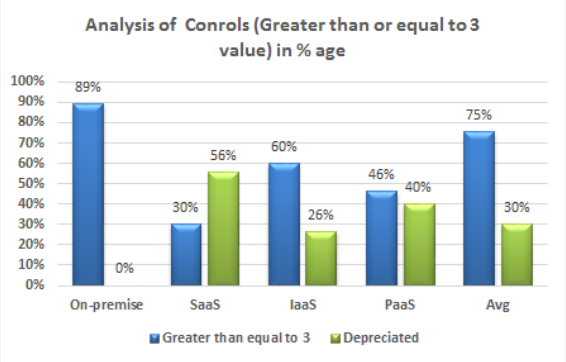

Figure 7: Analysis of Controls having greater than or equal to 3 value in percentage.

trols is not decreased in the context of on-premises, 56% decreased for SaaS, 26% decreased for IaaS, 40% decreased for PaaS and only 30% decreased in average. In the same analogy, the process and sub-processes are examined according to criteria value 3. The given below Figure 8 and Figure 9 depicts the decrease of importance factor of processes and sub-processes of ISO/IEC 27001:2013. There are 13 processes in ISO/IEC 27001-2013. The Figure 8 shows that importance factor of 10 out of 13 processes are decreased in SaaS and PaaS Cloud service model because majority of the responsibilities transferred to Cloud Service Provider while in average only 6 processes importance factor is affected. The ISO/IEC 27001:2013 have 32 sub-processes and the analysis of the Figure 9 shows the same type of results as Figure 8. The importance factor of sub-process in respect of SaaS and PaaS are mainly decreased and in average 10 out of 32 sub-processes are decreased. The analysis shows that sub-processes of ISO/IEC 27001:2013 are more beneficial for IaaS as compared to other service models. The research also find out the number of the controls which can be used during the development of SLA between both customer and CSP. The

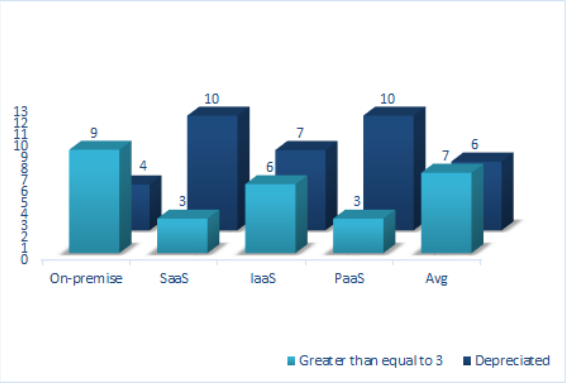

Figure 8: Analysis of Controls having greater than or equal to 3 value in percentage.

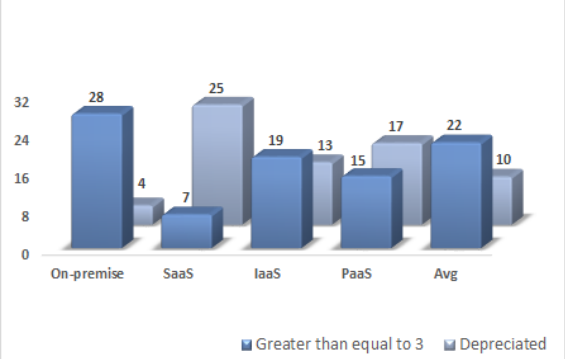

Figure 9: Analysis of Controls having greater than or equal to 3 value in percentage.

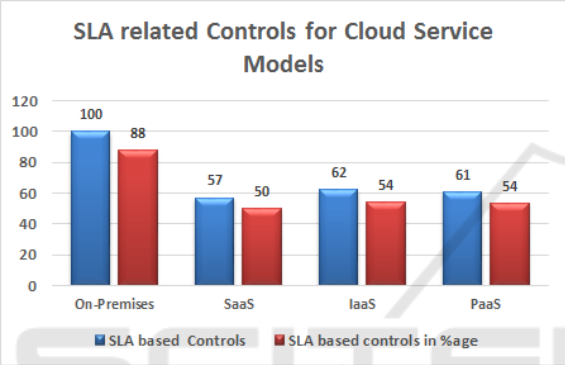

Figure 10: Analysis of Controls having greater than or equal to 3 value in percentage.

research find out Cloud service model related controls to facilitate both customer and CSP to select only specific Cloud service model related controls. The authors find out a number of cloud service model specific controls which shown in Figure 10. The Figure 10 shows that 57 out of 114 controls can be used in Service Level Agreement which is based on Software as Service (SaaS). The Platform as Service as 61 controls and Infrastructure as Service has 62 controls that can be used in a Service Level Agreement. The detail of these controls is given at Appendix-II that is given in DOI No. 10.13140/RG.2.1.4683.7603. It is revealed from quantitative and qualitative study that controls implementation for each cloud service layer is varied and depreciating according to it. In Cloud Computing SaaS service layer, ISO 27001 control objectives are expected near to zero as all responsibilities are transferred to CSP but its value is around 50%. It means the Cloud customer is required implement standard controls to maintain its information security, in-house assets, personal and deal with legal obligations, etc.

5 CONCLUSIONS

Whenever a technology is newly launched, risks always exist in spite of all its advantages. At present, there are many security, regulatory, privacy and legal issues in Cloud Computing, therefore, every organization should evaluate Cloud risks and compare to traditional computing solutions before moving its services to the Cloud.

The paper presents an overview of renowned industrial and international standard for information security and we analyze its worth for Cloud Computing. There are various kinds of security risks, vulnerabilities, threats and their mitigation techniques in order to make sure Cloud security as well.

ISO 27001 Annex A is a very important flexible approach that allows CSP to decide what level of risk is acceptable (in line with business objectives) and the needed controls to reach the target.

The ISO 27001 standard is generic standard that covers all management, operational, technical areas to deal with threats and vulnerabilities. Due to its generic nature, it does not cover all Cloud information security system challenges. Hence, many further controls are required like virtulization management to mitigate Cloud security risks. It is important to consider that the document about ISMS of an organization certified as ISO 27001 is public for scrutiny and it contains a high level description of ISMS implemented controls without underlining if the controls mitigate the Cloud risks.

The paper by using its methodology quantifies ISO 27001 control objectives for in-house and public Cloud. After evaluation, we revealed that by moving into the Cloud, 03of 39 control objectives are not affected in case of private Cloud and Public Cloud and importance factor of these 03 control objectives on average does not change. The 33 out of 39 control objectives are depreciated. Therefore, while moving into Cloud, the organization has to re-evaluate their security system as in public Cloud; the organizations transferred their security control to their CSPs, and expect from them that they will secure their application and data.

To sum up, the analysis shows that ISO 27001:2013 provides a good reference to create a secure Cloud Computing, however it's necessary that the CSP is committed to Information Security. Cloud Service Provider needs to include these aspects in risk assessment that are directly related to Cloud Computing.

Following this approach is also possible also to include controls that are not specified in ISO 27001. The analysis of the ISMS implemented would guide

Cloud customers to understand up to what level of Cloud risks have been included and mitigated within risk assessment by CSP. However, unfortunately the CSP usually does not provide all information to public, then it would be appreciated to obtain this information by CSP as a needed contract requirement to evaluate Cloud Security Level of their service.

In conclusion, this research adopts ISO/IEC 27001:2013 as Information Security Standard while the other Information Security Standards like COBIT, GAISP, SSE-CMM, FISMA, ISNI/ISA 99 and NIST can also be used to map the security risks and to increase the volume of this study. Moreover, real time and practical issues will be improved through interview, questioners and other techniques with Cloud stakeholders. As future work, the other security standards will be evaluated and quantified in addition to the existing Cloud risk database to provide their importance and effectiveness more accurately to the Cloud customer.

REFERENCES

Almorsy, M., Grundy, J. and Ibrahim, A. (2011). Collaboration-Based Cloud Computing Security Management Framework. 2011 IEEE 4th International Conference on Cloud Computing.

Buyya, R., Yeo, C., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), pp.599-616.

Clayton, C. (2011). Standard Cloud Taxonomies and Windows Azure - Practical Development - Site Home - MSDN Blogs. [online] Blogs.msdn.com. [Accessed 2 Aug. 2015].

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards.Information Security Journal: A Global Perspective, 19(3), pp.132-141.

Imran Tariq, M. (2012). Towards Information Security Metrics Framework for Cloud Computing. IJ-CLOSER, 1(4).

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011). Cloud computing The business perspective. Decision Support Systems, 51(1), pp.176-189.

Ristov, S. (2012). Cloud Computing Security in Business Information Systems. International Journal of Network Security & Its Applications, 4(2), pp.75-93.

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), pp.1-11.

Takabi, H., Joshi, J. and Ahn, G. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy Magazine, 8(6), pp.24-31.

Tariq, M., Haq, I. and Iqbal, J. (2015). SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework. International Journal of Computer Networks and Communications Security, 1(3), pp.95-101.