Risk Based NIST Effectiveness Analysis for Cloud Security

Muhammad Imran Tariq, Shahzadi Tayyaba, Muhammad Waseem Ashraf, Haroon Rasheed, and Fariha Khan

***Abstract* – Cloud computing has brought new innovations in the paradigm of IT industry through virtualization and by offering low price services on pay-as-per-use basis. Since the development of cloud computing, several issues like security, privacy, cost, load balancing, power consumption, scheduling algorithms are still under research also the advent of newer technologies announces new-fangled risks and vulnerabilities. Although the cloud has a very advanced structures and expansion of services, security and privacy concerns have been creating obstacles for the enterprise to entirely shift to the cloud. A Threat Agent is an attacker, intruder, employee that takes the benefits of the vulnerabilities and risks in the system. Failure to ensure appropriate security protection when using cloud services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing. There are different Information Security standards, governance and security frameworks, and guides to protect the organizations to protect from threat agents. In this research, cloud vulnerabilities and risks have been identified that can be exploited by the threat agent and mapped into renowned information security standard by National Institute of Standards and Technology NIST SP 800-53 Rev.3 to check whether the standard provides claim security to cloud users.**

***Index Terms* – Cloud Computing, Information Security, NIST SP 800-53 Rev.3**

I. INTRODUCTION

Cloud Computing has basically 03 deployment models i.e. Private Cloud, Public Cloud and Hybrid Cloud. In Public Cloud, the organization builds its own infrastructure and manages it as well while in Public Cloud, the organization render different services of Cloud Services Provider (CSP) as per its requirements and use it as long as organization required [1]. The Hybrid Cloud is a combination of Cloud Private,

Public models. It has characteristics of all deployment models. Private and Public Clouds are connected with each other through gateways, share data, applications and resources. There is no location binding on hybrid cloud, it may located at private organization premises or Cloud Service Provider premises [2].

Cloud computing has 03 service models i.e. Software as a Service (SaaS) wherein the cloud customer render the cloud applications and its maintenance services from CSP. Salesforce, Dropbox and Google Drive are the example of SaaS. The Infrastructure as Service (IaaS) has provided hardware, storage and infrastructure relates services. Amazon EC2 is very famous example of Infrastructure as Service (IaaS). Platform as Service (PaaS) provides environment, tools, libraries to applications development framework, machines and operating system services to its customers. The Cloud computing has several advantages over the traditional computing but it has several constraints that are roadblock in the fully deployment of Cloud computing. Security, privacy, cost, energy balancing, load balancing, power consumption, scheduling algorithms are one of the major constraints that organizations are facing in the deployment of Cloud computing [3], [4].

In computer security threat always exploit the vulnerability of the system to breach security and become harmful [5]. A threat agent is an entity that have capability to carrying out attack on the Cloud. The security and privacy issues are exploited by the threat agent. Threat agent either exploit internal (malicious insider) or external vulnerabilities. It act as an anonymous attacker, malicious service agent, trusted attacker and malicious insider [6], [7].

The vulnerability is a major risk factor. There are number of chances that an asset will be unable to resist the action of a threat agent. The Cloud organizations deployed different information security standards to secure their organization. Standard making organizations have recently developed information security standards particularly for the Cloud computing but still cloud organizations are using traditional information security standards for their organization security [13], [14].

The main objective of this research is to analyze whether the renowned information security standard NIST SP 800-53 Rev. 3 provide security against the threat agent [8]. The Section 2 of this research paper describes about the NIST SP 800-53 Rev.3 and Section 3 brief about the identified cloud risks that are mapped to the NIST 800-53 Rev. 3 to know the importance of the standard regarding Cloud computing. In section 4 of this paper we in detailed and critical analyze the standard. The Section 5 presents the justification of the work we done in previous sections and in Section 6 we proposed recommendations in respect of Cloud computing controls in the standard. The last section of the research paper is conclusion and future work of the authors.

II. NIST SP 800-53 REV. 3 STANDARD

The NIST SP 800-53 Rev.3 standard after a detailed analysis provides a control directory to be applied in Federal Information System (FIS), the importance and consequences of loss [8]. This standard has approximately all types of controls to meet the requirements of Information Security and risk management. The implementation of this guide will help the organization to create a secure Information Security system and effective risk management system by:

Muhammad Imran Tariq, Superior University Lahore, Shehzadi Tayyaba, Department of Computer Engineering, The University of Lahore, Pakistan, Muhammad Waseem Ashraf, Department of Physics, GC University, Lahore, Pakistan, Haroon Rasheed and Fariha Khan, Department of Electrical Engineering, Bahria University Karachi Campus, Pakistan. Email:imrantariqbutt@yahoo.com,shahzadi.tayyaba@dce.uol.edu.pk,dr.waseem@gcu.edu.pk,haroonrasheed.bukc@bahria.edu.pk,farihakhan.bukc@bahria.edu.pk. Manuscript received Feb 01, 2017; revised on April 10, 2017; accepted on July 20, 2017.

1) Facilitating organizations to select appropriate security controls from standard for security systems
2) Defining the minimum level of security controls required for information management systems
3) Foundation for creating the evaluation methods and actions to decide the effectiveness of the security controls in standard and
4) Improving communication among organizations to discuss risk management.

The standard covers a wide range of audience like Information Security professionals, project managers, Information Security system product developers, auditors, inspector general, Information Security service providers, Information Security administrators and Information Security managers.

III. CLOUD RISK IDENTIFICATION

Many cloud risks have already been identified Therefore, it is decided to use the precise approach i.e. risk assessment which has already been adopted by other experts in the field of cloud. By adopting said approach, during literature review, a number of cloud related risks have been identified that have different severity levels. It is a well-organized process to identify vis-à-vis customer concerns in the cloud.

To identify the risks of the cloud, intensive literature review was carried out to get the risks pertaining to Cloud Computing and also dig out their impact on security. The risk identified by the various government agencies, cloud security and other risks identified by individual experts were also taken into account in the process of risk identification.

Risk repository was maintained and identified risks were segregated according to their impact and effect on Cloud networks.

Table I is about name of the risks and their description is not given in the paper due to paper length constraints. Though in Table I all risks are not given but selected risks almost cover all security dimension for research [9]. The ultimate goal is to identify and mitigate risks exploited by the threat agents in the cloud. Numerous risks that can be challenged by the threat agents have been identified during the investigation process, but few ones are omitted from the list given in Table 1 because they are not related to the cloud.

TABLE I. List Of Identified Risks

S. No.	Name of Risk	S. No.	Name of Risk
1.	Loss of Governance	31.	Private information becomes public without customer notice
2.	Lock-in	32.	Subpoena and e-discovery
3.	Improper Backup	33.	The Cloud provider suspends service
4.	Network Failure	34.	The Cloud provider terminates service
5.	Improper Hardware governance and failure	35.	Unavailability of operational information
6.	Third parties communication and service change risks	36.	Data jurisdiction is not controlled by customer
7.	Unsafe working environment	37.	Restricted support access
8.	Distributed Denial of Service	38.	Business continuity
9.	Regularity Requirements	39.	Isolation failure
10.	Service provider human error	40.	Over-usage of shared resources
11.	License risks	41.	Non compliance with client instructions relating to data processing
12.	Loss of customer account and configuration data	42.	Data access and associated logs
13.	Delayed response	43.	Ambiguous security responsibilities
14.	Insecure or ineffective deletion of customer data	44.	Malicious code imbedded in software
15.	Data interception	45.	Insecure equipment disposal
16.	Theft of Data	46.	Improper security update policy
17.	Theft of Computer	47.	Lack of technical resources
18.	Loss of data ownership within network	48.	Insecure data storage
19.	Loss of control over paper based information	49.	Insufficient cryptographic management
20.	Vulnerabilities in Backup System	50.	Undependable service engine
21.	Loss of encryption keys	51.	Malicious employees
22.	Privilege escalation	52.	Economical denial of service
23.	Social engineering attacks	53.	Cloud service provider acquisition
24.	Wireless network breach	54.	Compliance to International Standards
25.	Unauthorized access	55.	Supply Chain Management Failure
26.	Malicious insider	56.	Non-compliance with legal requirements
27.	Third party personal breaches	57.	Noncompliance with data protection law requirements
28.	Improper highlight Security breaches	58.	Loss of customer privacy
29.	Poor implementation of security plan	59.	Loss of intellectual property
30.	Interfacing with third parties has vulnerabilities		

Design and configuration of the network is another malaise of risks that must be managed. The cloud system is still well managed and established by the cloud service provider to confirm that all network goals are met in terms of security, confidentiality and privacy. Moreover, some legal and technical vulnerabilities were also not taken into consideration because they are not value-able. Risks of traditional networks like no DHCP server settings, Active Directory failure is also excluded [10].

Although risks that are not selected for research are not useful. These risks have their own impact and Cloud venders should take necessary measures to minimize it.

IV. ANALYSIS OF NIST SP 800-53 REV. 3 STANDARD

The analysis is focused on the implementation of the NIST SP 800-53 Rev.3 standard. The results clearly show that the implementation of the NIST SP 800-53 Rev.3 does not provide complete assurance regarding complete mitigation of Cloud risks. Moreover, the NIST SP 800-53 Rev.4 draft version has been developed for Cloud Computing. Furthermore, NIST does not provide a compliance mechanism like PCI DSS and ISO 27001.

The Table II provides a summary of the result of the analysis conducted on the controls of NIST SP 800-53 Rev.3. A detailed information and explanation about analysis is given in Table 3. The risks that are chosen for research had been mapped to NIST SP 800-53 Rev. 3 processes. Table 4 based on the possibility that a risk could have an impact on the process.

TABLE II. Summary Of The Analysis Carried Out On The Implementation Of Nist Sp 800-53 Rev.3 Standard

Completely Mitigated Risks	Partially Mitigated Risks	Risks that were Not Mitigated
Improper Backup	Loss of Governance	Delayed response
Improper Hardware governance and failure	Lock-in	Loss of data ownership within network
Unsafe working environment	Network Failure	Loss of control over paper based information
Regularity Requirements	Third parties communication and service change risks	Loss of encryption keys
Service provider human error	Distributed Denial of Service (DDOS)	Subpoena and e-discovery
License risks	Loss of customer account and configuration data	Unavailability of operational information
Insecure and ineffective deletion of customer data	Third party personal breaches	Data jurisdiction is not controlled by customer
Data interception	The Cloud provider suspends service	Restricted support access
Theft of Data	The Cloud provider terminates service	Over-usage of shared resources
Theft of Computer	Isolation failure	Compliance to International Standards
Vulnerabilities in Backup System	Noncompliance with client instructions relating to data processing and security	Noncompliance with data protection law requirements
Privilege escalation	Data access and associated logs	Loss of intellectual property
Social engineering attacks	Economical denial of service	
Wireless network breach	Cloud service provider acquisition	
Unauthorized access	Loss of customer privacy	
Malicious insider		
Improper highlight Security breaches		
Poor implementation of security plan		
Interfacing with third parties has vulnerabilities		
Private information becomes public without customer notice		
Business continuity		
Ambiguous security responsibilities		
Malicious code imbedded in the software		
Insecure equipment disposal		
Improper security update policy		
Lack of technical resources		
Insecure data storage		
Insufficient cryptographic management		
Undependable service engine		
Malicious employees		
Supply Chain Management Failure		
Noncompliance with legal requirements		

The identified Cloud risks were also mapped to possible NIST SP 800-53 Rev. 3 to get know the number of processes of ibid standard has capability to minimize the risk severity level.

The process of NIST could be helpful for organization to mitigate more than one risks and this thing is shown in Fig.1.

After applying Risk evaluation methods, it has discovered that Access Control (AC Family), System, System and Communications Protection (SC Family) and Service Acquisition (SA Family) and Physical and Environmental Security (PE Family) are looking most effected processes of an organization because of the Cloud Computing implementation. However, for Cloud Computing, Media Protection (MP Family), Security Assessment and Authorization (CA Family) and Incident Response (IR Family) are very important in respect of Cloud Computing.

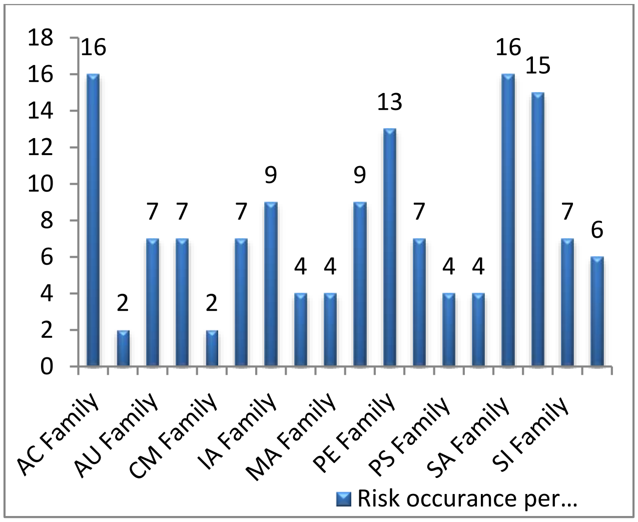

Fig. 1 Processes most likely to be effected by risks in relation to implementation of NIST SP 800-53 Rev.3

Furthermore, based on quantities analysis of Fig. 1, the NIST SP 800-53 Rev.3, AC Family and SA Family are 27% effective for the mitigation of Cloud risks and subsequently SC Family is 25% and CM Family is 22% beneficial for Security experts to resolve the issued relates to Cloud security. The quantitative figures emphases on AC Family, SA Family, SC Family and CM Family while implementing NIST SP 800-53 Rev.3 for Information Security. Fig. 2 and Fig. 3 clearly indicates that selected risks has been removed and minimized after the implementation of ibid NIST guide.

The Fig. 3 further reflects that 54.24% risks are completely mitigated and 25.42% are partially mitigated; it means that the NIST controls have potential to secure cloud organizations as well as traditional IT. The 20.34% risks that are not mitigated can be dressed by adding more controls in the NIST to make it more secure. NIST may select these controls from Cloud Control Matrix (CCM) developed by the Cloud Security Alliance (CSA).

The 32 among selected risks can be removed / minimized, 15 out of 59 somewhat reduced and 12 selected risks are still unresolved. From above narrated statistics, security experts can estimate that NIST SP 800-53 Rev.3 is able to mitigate majority of the Cloud risks and wherein it partially mitigates Cloud risks. In order to make system more effective, more controls and processes are required to be inserted in the guide relates to Cloud Computing.

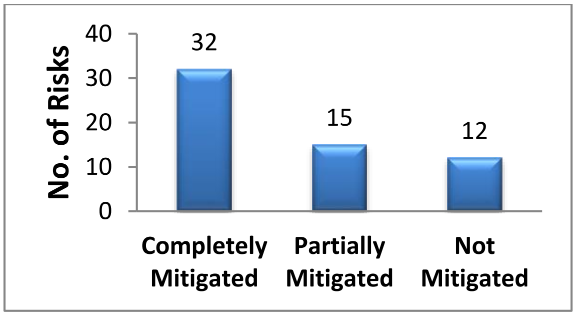

Fig. 2 Number of risks mitigated through NIST SP 800-53 Rev.3

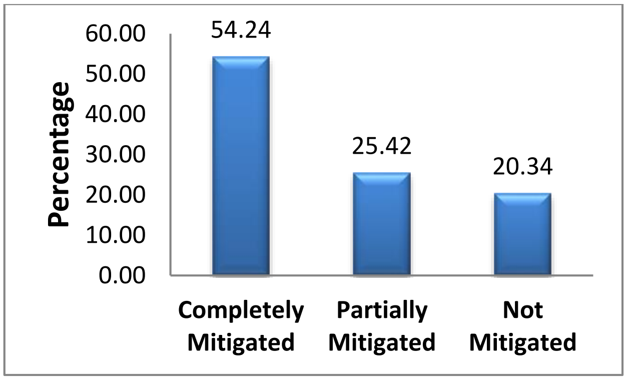

Fig. 3 Number of risks mitigated through NIST SP 800-53 Rev.3 in percentage

V. RESULTS & ANALYSIS

The NIST SP 800-53 Rev.3 publication was developed with the support of Federal Information Security Management Act of 2002 (FISMA) [11]. The publication has a number of controls which address the issues related to security, privacy, hostile cyber-attacks, natural disasters, structural failure and human errors of the organization.

Although the results of the analysis is a negative one but it is worthwhile to mention here that if the CSP implement NIST SP 800-53 Rev.3 program then many of the identified Cloud risks are mitigated or partially mitigated. If NIST SP 800-53 Rev.3 compares with ISO / IEC 27001 standards then NIST does not completely mitigate risks as ISO does. During analysis, it is revealed that there are two main positive things. First, the NIST has a number of processes to manage organization security, asset security and protection, physical and environmental protection, risk management and especially program management. Second, the description of each control is very detailed especially when compared to ISO 27002. As per opinion, if the standard has detailed controls for Cloud Computing, then it is very convenient for the Cloud customer to know how the risks are being mitigated and thus does not need to further find out additional the CSP's security details. The detailed controls have one more advantage that it provides more transparency on which controls the CSP is implemented since there is no room for interpretation. However, a risk base approach is required to ensure that no other risk is overseen. Furthermore, during implementation of the standard, a cost analysis is mandatory to make certain that controls are cost effective.

The NIST SP 800-53 Rev.4 has recently been published and it has a number of controls relates to Cloud Computing, the inclusion of Cloud related controls will directly address Cloud related issues [12].

VI. RECOMMENDATIONS

The authors after intensive literature review, in-depth analysis of different security standards and framework already proposed or implemented has recommended the following improvements in the Ibid NIST revision to make it more useful for Cloud organizations and reduce the level of risks relates to Cloud Computing.

1) Key Performance Indicators (KPIs) are required to measure the claimed level of security of vender.
2) Cloud is based alias of outsourcing. Hence, external parties related controls will more help to Security experts to outsource their Cloud services to another Cloud.
3) Transparent and fair audit of vender is required to be published publically so that customers may estimate their level of offered security and privacy.
4) Cloud vender must to obey the terms and conditions with its customer and it must submit to its customer upon its demand.
5) Cloud vender must provide assurance regarding vender lock-in and portability of data among different venders.
6) Risk based approached should be part of standard under research.

VII. CONCLUSION & FUTURE WORK

The detailed analysis of each process and control of the standard was carried out and revealed that NIST SP 800-53. Rev. 3 does not have cloud specific controls to mitigate all risks that are identified and given in this paper, but despite this, it is widely used for the implementation of information security within an organization. NIST SP 800-53 Rev. 4 has a number of cloud relevant controls that may be useful to implement the information security. ISO / IEC WD 27017 and ISO / IEC 27018 standards are relevant to the management of information security, security controls for the use of cloud computing and data protection controls for the public cloud computer respectively.

There are many organizations that are presently working in the security of the Cloud computing like Cloud Security Alliance (CSA), ISO / IEC 27001, ISACA, NIST, KPMG and ENISA. The SANS organization also published various guides for the cloud security. In addition to this, there are many other organizations that are working on the cloud security issues.

Future work of the research is the continuation of this intensive analysis of the existing security agents in order to dig out the cloud security areas that can be compromised and its improvement is required in order to implement better security in cloud organization. The cloud risks that were excluded due to their impact and worth will also be taken into consideration in the security agent risk dataset to make dataset more comprehensive about cloud security risks. The identified risks shall be used to check the importance factor of the CCM V.3.01, ISO / IEC WD 27017 and latest version of the NIST 800-53. Rev. 4. The result of future research shall be very helpful for the cloud organization before its adoption of security standards and the risks mitigation through these standards.

Table III given in Appendix section of this paper is in depth analysis of the mapping of risks. During this mapping process, we considered due care while selecting appropriate controls and process against each risk. Description of each risk was first studied and considered and then we mapped it to appropriate controls. Furthermore, we also studied that up to what level of risk is mitigated through implementing selected controls. The left side of the Table is the risks that we have selected for research in question and columns of the Table III are NIST SP 800-53 Rev.3 processes. The tick mark indicates that process have controls to mitigate risk mentioned against processes. Each process have several controls and due to length constraints of the paper, we could not map risks against each control of the NIST SP 800-53 Rev. 3. The analysis is in Table III given in Appendix, revealed that standard NIST SP 800-53 Rev.3 has a number of controls and recommendations which can be used to mitigate Cloud specific risks. However, due to shortcomings, the standard is not providing the desired level of security that a Cloud customer is looking for in a standard to manage its cloud.

ACKNOWLEDGMENT

The authors thanks to Mark Edward Stirling Bernard, ISO / IEC 27001- ISMS and NIST expert for his assistance and guidance in this paper.

REFERENCES

[1] D. Feng, M. Zhang, Y. Zhang and Z. XU, 'Study on Cloud Computing Security', Journal of Software, vol. 22, no. 1, pp. 71-83, 2011.

[2] Y. Yu, A. Miyaji, M. H. Au, and W. Susilo, “Cloud computing security and privacy: Standards and regulations,” Computer Standards & Interfaces, vol. 54, pp. 1–2, 2017.

[3] B. Kandukuri, R. V. and A. Rakshit, 'Cloud Security Issues', 2009 IEEE International Conference on Services Computing, 2009.

[4] F. Sabahi, 'Cloud computing security threats and responses', 2011 IEEE 3rd International Conference on Communication Software and Networks, 2011.

[5] B. Grobauer, T. Walloschek and E. Stocker, 'Understanding Cloud Computing Vulnerabilities', IEEE Security & Privacy Magazine, vol. 9, no. 2, pp. 50-57, 2011.

[6] A. Honarvar, 'Developing an Elastic Cloud Computing Application through Multi-Agent Systems', International Journal of Cloud Applications and Computing, vol. 3, no. 1, pp. 58-64, 2013.

[7] K. Dahbur, B. Mohammad and A. Tarakji, 'A survey of risks, threats and vulnerabilities in cloud computing', Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA '11, 2011.

[8] NIST, 'Content / Special Publications - SP 800 series / NIST SP 800-53 rev 3 - Recommended Security Controls for Federal Information Systems - NIST IT Security', 2011. [Online]. Available: http://www.nist.org/nist_plugins/content/content.php?content.18. [Accessed: 01- Oct- 2015].

[9] M. Tariq, Providing Assurance to Cloud Computing through ISO 27001 Certification: How Much Cloud is Secured After Implementing Information Security Standards. CreateSpace, 2015, p. 134.

[10] A. Aich, A. Sen and S. Dash, 'A Survey on Cloud Environment Security Risk and Remedy', 2015 International Conference on Computational Intelligence and Networks, 2015.

[11] FISMA, 'NIST Computer Security Division - FISMA Implementation Project', 2014. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/index.html. [Accessed: 01- Oct- 2015].

[12] NIST, 'NIST Special Publication 800-53 (Rev. 4)', 2013. [Online]. Available: https://web.nvd.nist.gov/view/800-53/Rev4/home. [Accessed: 01- Oct- 2015].

[13] A. Alshammari, S. Alhaidari, A. Alharbi, and M. Zohdy, “Security Threats and Challenges in Cloud Computing,” 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017.

[14] M. I. Tariq and V. Santarcangelo, “Analysis of ISO 27001:2013 Controls Effectiveness for Cloud Computing,” Proceedings of the 2nd International Conference on Information Systems Security and Privacy, pp. 201-208, 2016.

APPENDIX

TABLE III. Cloud Risks Mapped to NIST 800-53 Rev. 3 Processes

Name of Risk	ACF	ATF	AUF	CAF	CMF	CPF	IAF	IRF	MAF	MPF	PEF	PLF	PSF	RAF	SAF	SCF	SIF	PMF
Loss of Governance															✓			
Lock-in															✓			
Improper Backup						✓												
Network Failure				✓												✓		
Improper Hardware governance and failure									✓	✓	✓							
Third parties communication and service change risks				✓											✓			
Unsafe working environment											✓							
Distributed Denial of Service																✓		
Regularity Requirements															✓			
Service provider human error	✓	✓						✓				✓	✓					
License risks					✓										✓			
Loss of customer account and configuration data	✓							✓									✓	
Delayed response																		
Insecure or ineffective deletion of customer data										✓							✓	
Data interception	✓		✓							✓	✓				✓	✓	✓	
Theft of Data	✓		✓							✓	✓	✓		✓				✓
Theft of Computer										✓	✓					✓		
Loss of data ownership within network																		
Loss of control over paper based information																		
Vulnerabilities in Backup System						✓				✓								
Loss of encryption keys																		
Privilege escalation	✓																	
Social engineering attacks	✓		✓								✓					✓		
Wireless network breach	✓																	

Name of Risk	ACF	ATF	AUF	CAF	CMF	CPF	IAF	IRF	MAF	MPF	PEF	PLF	PSF	RAF	SAF	SCF	SIF	PMF
Unauthorized access	✓			✓			✓				✓					✓		
Malicious insider	✓			✓			✓					✓	✓					
Third party personal breaches	✓			✓														
Improper highlight Security breaches								✓										
Poor implementation of security plan												✓						✓
Interfacing with third parties has vulnerabilities	✓						✓								✓	✓	✓	
Private information becomes public without customer notice	✓		✓								✓					✓		
Subpoena and e-discovery																		
The Cloud provider suspends service						✓									✓			✓
The Cloud provider terminates service						✓									✓			✓
Unavailability of operational information and																		
Data jurisdiction is not controlled by customer																		
Restricted support access								✓										
Business continuity						✓												
Isolation failure															✓	✓		✓
Over-usage of shared resources																		
Non compliance with client instructions relating to data processing	✓														✓			
Data access and associated logs			✓															
Ambiguous security responsibilities	✓											✓						
Malicious code imbedded in software																	✓	
Insecure equipment disposal										✓								
Improper security update policy											✓							
technical resources															✓	✓		
Insecure data storage							✓		✓	✓	✓					✓		

Name of Risk	**ACF**	**ATF**	**AUF**	**CAF**	**CMF**	**CPF**	**IAF**	**IRF**	**MAF**	**MPF**	**PEF**	**PLF**	**PSF**	**RAF**	**SAF**	**SCF**	**SIF**	**PMF**
Insufficient cryptographic management							✓									✓		
Undependable service engine	✓		✓	✓		✓	✓				✓			✓		✓	✓	
Malicious employees							✓				✓		✓					
Economical denial of service																✓		
Cloud service provider acquisition															✓			
Compliance to International Standards																		
Supply Chain Management Failure															✓			
Non-compliance with legal requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Noncompliance with data protection law requirements																		
Loss of customer privacy												✓		✓	✓			
Loss of intellectual property																		