AN ASSESSING APPROACH BASED ON FMECA METHODOLOGY TO EVALUATE SECURITY OF A THIRD PARTY CLOUD PROVIDER

[1]Bentajer Ahmed, [2]AbouElMehdi Karim, [3] Dali Loubna, [4]EL-Fezazi Said, [5] Hedabou Mustapha, [6] El Amrani FatimaEzzahra

[1,4,6] Research Team in Industrial Engineering, High School of Technology, Cadi Ayyad University, Morocco
[2]The Mohammadia Engineering School, Morocco
[3]Bowie State University, Maryland, United State of America
[5] Mathematics and Informations Processing, National School of Applied Science, Cadi Ayyad University, Morocco
E-mail: [1]a.bentajer@gmail.com , [2]karim.abouelmehdi1@gmail.com , [3]loubnadali@gmail.com , [4]selfezazi@gmail.com , [5]mhedabou@gmail.com , [6]fz.elamrani@menara.ma

ABSTRACT

Cloud Computing is recognized as a great eliminator of the hefty costs and complex processes that come with evaluating, purchasing, configuring or managing software and hardware essentials that are necessary for enterprise applications. However it presents a significant security concerns that need to be addressed when moving to the cloud that should be well studied and quantified for more visibility. In this article we will study how to quantify a risk associated with a cloud service/deployment model and use FMECA methodology to audit a third party cloud provider risks.

Keywords: *Trust Computing, Fmeca, Cloud Computing, Predictive Analysis, Confidentiality*

1. INTRODUCTION

Cloud computing is considered as a new way of delivering computing resources. It provides access to online software through a subscription, in many areas such as ERP, CRM, and other business applications. In addition, it allow access to storage services and computation through the internet. These concepts have significant trend with a potential of increasing agility, flexibility, and lowering the costs.

IT industry starts using this new wind of technology in their computation and data processing. However, during the course of using this technology, we encounter several issues: e.g. understanding its capabilities, advantages and security threats. In addition, these issues are a challenge for security professionals. The reason being is that traditional in-house IT infrastructure and/or applications where security is limited and managed inside the corporate level, which can be summarized in firewalls, network separation, security patch management, etc.

Nevertheless, in the cloud it is not only about CIA (Confidentiality, Integrity and Availability) that define the organization's security posture. The concept of security has another meaning: it can be about privacy [1] security policies, or conflict of laws [2]. Moreover, the risk of using cloud not only can be about interruption of service [3], but also user can be vulnerable to attackers, who can place their virtual machine on the same physical machine as another user [4]. In addition, data will now be under the control of a third party Cloud Service Provider (CSP). In addition, this presents a problem that should be addressed, in first case, through management initiative. The organization should clearly define security controls implemented based on asset, threat and vulnerability risk assessment matrices to audit the security issues of the CSP.

The use of this method will lead the organization choosing the best CSP, through its audit sheets that the CSP should respect especially when it's about a specific security policies of the organization.

The purpose of this paper is to show how risk assessment methods combined to FMECA (Failure mode, effects, and criticality analysis) can be useful and beneficial for an organization, which aims to move toward a cloud to use it as an auditing method. In addition, we will discuss how to evaluate the risks linked to a business process and cloud service/deployment model.

2. CLOUD OMPUTING

Referring to NIST[13] "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”. In terms of IT, cloud computing is one of the most growing and advancing technologies nowadays. However, it is not often used by companies it’s considered as a new source of complexity. Even though, millions of people around the world are using cloud-based applications (SaaS) every day, for professional or personal use, without being aware of it! As web-mail such as Gmail, AOL or Yahoo. In fact, for any application hosted by an external provider and accessible from the Internet "on demand" it is a cloud application.

The NIST[13] categorize the definition of cloud computing into four essential deployment models:

- Private cloud: The cloud infrastructure is exclusively used by a single organization, here the organization have more control and less security problems.
- Community cloud: The cloud infrastructure is only used by a specific community of consumers from organizations that have shared concerns
- Public cloud: The cloud infrastructure is open and used by the general public.
- Hybrid Cloud: The cloud infrastructure is composed of at least two different cloud infrastructures.

And three delivery model[13]:

- SaaS : Software as a Service
- PaaS : Platform as a Service
- IaaS : Infrastructure as a Service

2.1 Risk adoption of cloud solutions

Since solutions have been shifted to the cloud, organizations should be aware of the risks and other effects to its business and operating environment. In addition, they should recognize the degree of control when depending on the type of cloud service delivery and deployment model (Figure 1 show Risk Relationship with deployments model and cloud service delivery) through its ERM (Enterprise Risk Management). In some case cloud computing can be easily integrated into an organization within a short period. This will require a very few personal, no ERM, minimal investments, and generally does not represent a risk. On the other hand, cloud which requires a big investment, has a big impact. And, the organization should carefully audit cloud risks. The reason being is that, organization, with type of investment, should define objectives and courses of actions in advance to lessen their chance of failure and/or risks.

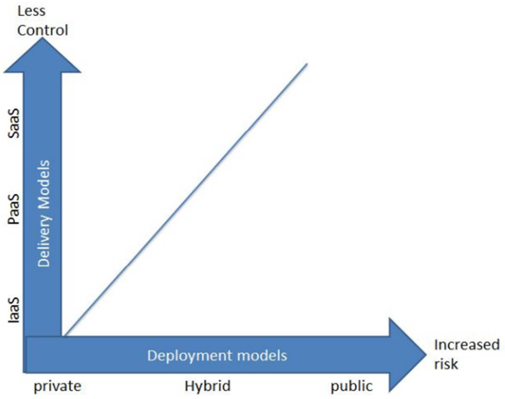

Figure 1: Risk Relationship With Deployments Model And Cloud Service Delivery [7]

CSP’s are realizing that organizations deployment choice depend on their business activities and senility of data. For example, in U.S.A. most applications are delivered as a service (SaaS), moving from on-premise to cloud, especially ones in the healthcare fields [5]. As stated earlier, SaaS is software that deliver methods and provides access to applications and its functions remotely as a web-based service. Conceptually, this architecture needs information, web flows, to go through network. As a result, they can be exposed to side channel attack [4, 5, 6] despite of using a HTTPS protection, or encryption.

3. CLOUD RISK ANALYSIS

The COSO’s [7] defined the risk, as “Risk is the possibility that an event will occur and adversely affect the achievement of objectives”. We have noticed in our survey that risk analysis is an essential process for assessing the impact of any unsafe condition or potential source of an undesirable event. The diversity in risk analysis procedures is that there are many appropriate techniques for any circumstance. To be able to assess the criticism of a risk "hazardous event", we should categorize the risk as either qualitative or quantitative [8]. The quantitative risk can be expressed as a mathematical function or relation. In cloud computing, the quality and quantity of risk associated with a system or subsystem can't have the same value of gravity, occurrence and detection. For example in the SaaS environment, the whole system is composed of humans, machines/systems and their interactions, and if data integrity is compromised it can be caused by a software error (risk in the CSP), the man in the middle attack (external risk for both stakeholder), or a malicious entry of data from users (risk in the client).

The literature of risk analysis showed that several techniques have been used and developed in different research area [8, 9] (engineering, chemistry, industry ...) with different applications. Risk analysis and assessment technique are classified into three main categories (figure 2 presents the classification of the main risk analysis and its assessments methodologies.)

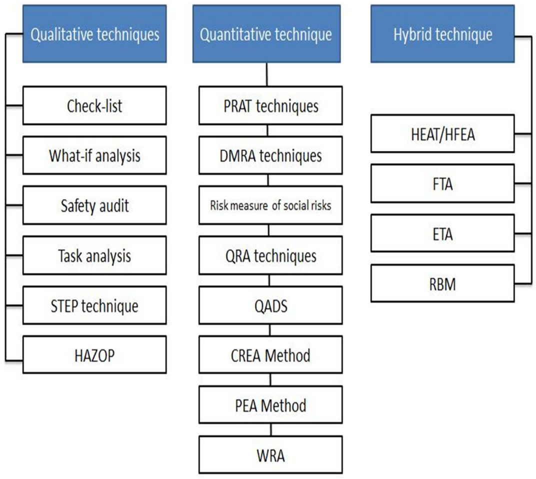

Figure 2: Main Risk Analysis And Assessment Methodologies

- Qualitative technique: Based on analytical estimation process and safety manager. This type uses simple calculations and procedures to achieve an acceptable level of risk and increase overall awareness [7].
- Quantitative technique: can be estimated by mathematical formula with the help of prior data records and/or the expertise of experts in the field.
- Hybrid technique: A combination of both methods.

Predictive analysis and models are used to forecast future probabilities into organizations. It is used to analyze current data and historical facts in order to understand and identify potential risks and opportunities.

Any change in an economic activity, such as cloud, companies are considering large amount of investment in order to migrate into system. So, they evaluate and analyze risks prior to transfer. As of today, most of organizations are seriously considering moving to cloud era. However, they should be aware of the risks that may occur when choosing a combination of cloud computing deployment and service delivery models [2,3]. (Figure 3 shows an example of combination between organization business processes and cloud service/deployment model). As we can see in this scenario, the organization has no longer full control of their business data. Thus, they should integrate risk analysis into their ERM

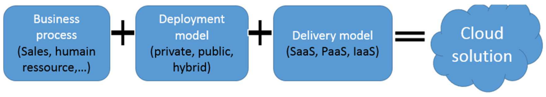
Business process (Sales, humain ressource,...)
+
Deployment model (private, public, hybrid)
+
Delivery model (SaaS, PaaS, IaaS)
=
Cloud solution

Figure 3 : Combination Between Organization Business Processes And Cloud Service/Deployment Model [13]

3.1 Method Used For Limiting Threats In Cloud Computing

Until the time of this writing, no approach to quantify the risk in the cloud based on standards safety criteria, that companies seeks to preserve, is found. However, there is common framework to assess the control systems of the organizations [7, 16, 17].

For this reason, organizations are considering framework and guidance in their ERM as a way to reduce risks associated with cloud adaptation. And, the change will undergo to improve its performance and governance. COSO [12] provide a developed framework for managing business risk and improving the control system of the organization.

When talking about CIA (Confidentiality, Integrity and Availability) triad or what was outlined by Gartner[11] about security issues, risks cannot been quantified, and ERM framework are considering what have to be done to maintain security and control system, then we proposed a method in order to try to quantify the risk and know its impact based on criteria (gravity, detection, occurrence) that will allow to determine its criticality and thus render how acceptable or in case find the best cloud deployment/delivery solution.

4. FMECA FOR RISK ANALYSIS IN CLOUD COMPUTING

Failure modes, effects, and criticality analysis (FMECA) is a methodology for preventive analysis of dependability (reliability, availability, maintainability, safety). We will use FMECA to assess and quantify security risks associated with a business process, to guide an organization in the application of good practices of security controls, and show how the contract should be negotiated with the CSP. As defined by SEMETECH [9], FMECA is a technique to resolve potential problems in a system before they occur. So, FMECA is considered as a predictive tool for risk analysis to identify and analyze all potential modes of various parts, of system that can be mitigated and/or avoided.

Initially FMECA was called Failure Modes and Effects Analysis (FMEA). The letter C indicates the criticality (severity) of different failures effects, which are considered and ranked to be able to determine what have to be done and what failure mode can be accepted or not.

4.1 History of FMECA

FMECA was developed by the U.S department of defense (DoD) to perform a failure mode, effect, and criticality analysis. The method is usually performed during the initial design phases, where we can have the greatest impact on equipment reliability, of a system in order to ensure that all potential failure modes have been considered and the proper countermeasures have been developed to eliminate these failures. As the design matures, it becomes more difficult to alter. And, the time, cost, and resources required correcting a problem increase as well. At the end of design/development life cycle, approximately 85% of the total life cycle costs have already been locked-in [9] and 15% is consumed.

This method is used several industries, for example aerospace, railway, automotive, and medical equipment, in the process of design, development and exploitation.

HACCP (Hazard Analysis and Critical Control Points) is a method derived from the FMECA, used in the chemical and pharmaceutical food industries.

There are several types of FMECA:

- Process FMECA: focus on problems stemming from how the equipment is manufactured, maintained or operated.
- System FMECA: looks for potential problems and bottlenecks in larger processes, such as entire production lines.
- Design FMECA: carry out to eliminate failures during equipment design, taking into account all types of failures during the whole life-span of the equipment.

4.2 FMECA Methodology

The purpose of the FMECA is to assess the risks associated with manufacturing system. So, the system should be divided into manageable units (or process) by a hierarchical tree diagram, or may be beneficial to illustrate the system by a Functional Block Diagram (FBD). There may be risks to the security, quality, etc. And, it can be considered as a tool:

- To control and continue improvement;
- An inter-service tools communication;
- Reduces operating costs of maintenance work, following the hierarchy and prioritizing of interventions controls.

The first stage will consist of problem analysis to determine possible events (problems). Then, determine how the problem could occur, and the chances that client can be exposed. Finally, the criticality of the problem.

Stages of the implementation of FMECA for each device are listed below:

- Performing functional tree/FBD equipment.
- Definition of the operating phases of the equipment.
- Search for all possible failure modes (qualitative analysis).
- Search of causes and effects of these failures.
- Assessment of the criticality of these failures (quantitative analysis). And search remedies.

The second stage will consist of preparing of FMECA worksheets that fits client requirements or its risk management (figure: example of FMECA worksheet covering the most relevant columns).

For each system element (subsystem, component), analyst must consider all the functions of the elements in all its operational modes, and ask if any failure of the element may result in unacceptable system effect. If the answer is no, then no further analysis of that element is necessary. Otherwise, if the answer is yes, then the element must be examined further.

4.2.1 Risk ranking

This will allow assessing the criticality of failures based on table quotations previously defined. This is will be done by either the Index Priority Risk or risk matrix.

The Index Priority Risk, level from 1 to 10 the most critical, is calculated using levels of Severity (S), occurrence (O), and detection of failures (D).

$$IPR = S*O*D$$

5. APPLICATION OF FMECA AS AN AUDIT FRAMEWORK

Organizations should worry about the cloud provider and SLA prior to adopt cloud solution. As stated earlier, threats in cloud applications vary according to the cloud solution/deployment chosen. Our study was based on classifying threat according to CIA (Confidentiality, Integrity and Availability). This is because we believe that before processing the management and judicial part with a CSP, the company should know if it will really adopt a cloud solution with the desired CSP, and if he consider the requirements of security, and this can be done without quantifying the risks impact that may cause some threats already established by organizations as Gartner or CIA security model [1,11] (table 1, in the end of paper, show an overview of the threats according to the CIA model).

In our case study, we will focus on a company that wants to move a business process to the cloud. The goal here is **confidentiality** of data that must be retained according to the security policy of the organization and the integrity and availability must have a minimum of security (Table 2, in the end of paper, Show the application of FMECA on Confidentiality, data were collected from Laboratory in Cadi Ayyad University, The Mohammedia Engineering School and Bowie State University and other papers about security in cloud)

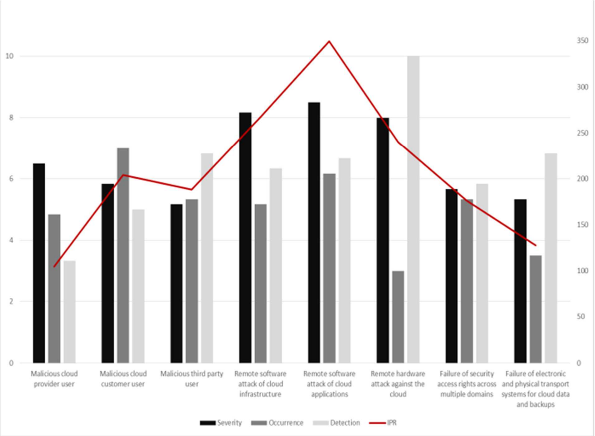

Figure 4: Generated diagram of possible hazards and IPR

By analyzing the graph, here instead of relying on an IPR threshold to process failure modes we will try to build on the intersections between the IPR curve with those of S, O and D (table 4), which will allow at first to treat the index or indices that allow for a high IPR therefore a high risk

Table 4: Interpretation And Audit Of Possible Hazards

Threat	Interpretation
Confidentiality	
Malicious cloud provider user	Here the customer must ensure that the CSP stock data and makes them available on-demand.
Malicious cloud customer user	Malicious users outside the cloud often perform DoS or DDoS attack, so the client should be sur that the CSP have an optimal security issues and understand about hiring practices used by the CSP to enhance the risks.
Malicious third party user	Security researchers have discovered many new security threats targeting cloud services and it's important that the CSP work with the customer to gain it's trust and this by diminishing the occurrence and if it's possible to reduce it to 0 echo
Remote software attack of cloud infrastructure	Recent revelation[14] said that a group gained access to the source code of pcAnywhere the client need now to be sure that the CSP is able to protect its software by reducing the echo of the Severity attacks
Remote hardware attack against the cloud	This is the critic point, and the client here need to be safe from industrial cyber-attacks while using side channel attacks, the CSP must present how he can protect the customer from the Severity of attacks, and how he could detect the attacks
Failure of security access rights across multiple domains	The CSP should respect policies and protocols that will prevent data leakage amongst many potentially competitor organizations, using the same cloud provider my get access through human error or faulty hardware
Failure of electronic and physical transport systems for cloud data and backups	The CSP should present an adequate recovery and incident management procedures when cloud users consider recovery of their own in house systems in parallel with those managed by third party cloud service providers by reducing the eco of Severity when performing the recovery and increasing the detection of problem

To assess compliance with the organization's security policy, and in order to avoid exposure to a multitude of risks that can reach the assets of the organization and make it vulnerable its business, the CSP must be able to respond to the first sheet audit requested by the organization of such kind that the intersection of the IPR diagram is above histograms of possible cases (figure 5).

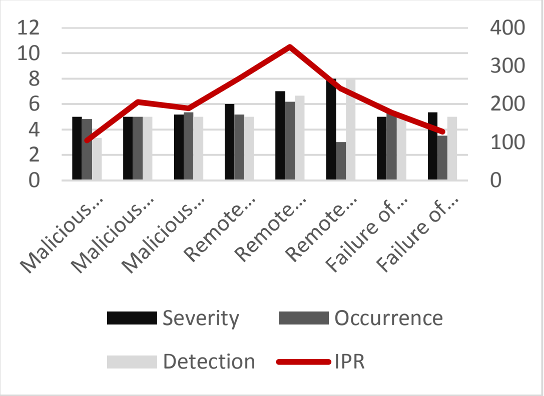

Figure 5: Example of CSP diagram response

Once completed with a CSP, the organization must ensure the continuity of the document, as required by the FMECA method, and integrate it into its frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

When applying this method and in order to have a tangible value for IPR, study should focus on one and only one failure mode and also on a single case study as the security problem in the CSP or for internal audit or to assess the safety of web flows. The primary goal of this paper is to enable organization to have a clear idea about its own CSP and know how it can negotiate the implementation of security policies in the CSP. In addition, this work will be considered as a first step towards a quality approach and compliance with the international standards ISO and/or COSO. This, will facilitate the procedures of audits and interventions, in case of incidents, to ensure the reliability, availability and robustness of subcontracted services

6. CONCLUSION

This method analysis is a tool that contribute to improve designs and the choice for CSP based on criteria as confidentiality, integrity and/or availability or according to specifics needs of the organization business, resulting in higher reliability, better quality, and increased safety, enhanced satisfaction and reduced costs. The tool can also be used to establish and optimize areas of intervention during security problem and/or contribute to control plans and other quality of security policies procedures. It provides knowledge base of most security threats so the organization can anticipate corrective action information that can be used as a resource in future troubleshooting efforts and as a training tool for new engineers. In addition, FMECA is often required to comply with safety and quality requirements that may be integrated into organization ERM[15]. Based on historical events and the expertise of experts, this approach can be used to analyze risks in an unstable environment where risk and hazard do not have a tangible value by performing some basic mathematical calculations yielding results, which may give firm guidance towards improving the security of a chosen cloud solution.

In our next work, based on this study, we are about to study the possibility of establishing a bridge of trust with the CSP and enables transparency to the physical location of data in the cloud.

REFRENCES:

[1]. Ronald L. Krutz And Russell Dean Vines, Cloud Security. A Comprehensive Guide To Secure Cloud Computing.

[2].Chian Ku Fan, Tien-Chun Chen, The Risk Management Strategy Of Applying Cloud Computing Vol. 3, No. 9, 2012.

[3].Anthony Gray. Conflict Of Laws And The Cloud.Computer Law & Security Review Volume 29, Issue 1, February 2013, P. 58–65 .

[4].Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage “Hey You, Get Off My Cloud: Exploring Information Leakage In Third-Party Compute Clouds”. Proceeding CCS ’09 Proceedings Of The 16th ACM Conference On Computer And Communication Security.

[5].Shuo Chen, Rui Wang, Xiaofeng Wang ; Kehuan Zhang Chen, Side-Channel Leaks In Web Application : A Reality Today A Challenge Tomorrow. Security And Privacy, IEEE Symposium On 2010. P. 191-208

[6].Sebastian Schinzel. Time Is Not On Your Side : Mitigating Timing Side Channels On The Web. 29th Chaos Communication Congress .

[7].Enterprise Risk Management-Integrated Framework Executif Summary September 2004.Pdf.

[8].H.J. Pasman, S. Jung, K. Prem, W.J. Rogers, X. Yang. Is Risk Analysis A Useful Tool For Improving Process Safety?. Journal Of Loss Prevention In The Process Industries 22 (2009) P. 769–777

[9].P.K. Marhavilasa, D. Koulouriotisb , V. Gemenib. Risk Analysis And Assessment Methodologies In The Work Sites: On A Review, Classification And Comparative Study Of The Scientific Literature Of The Period 2000–2009. Journal Of Loss Prevention In The Process Industries Volume 24, Issue 5, September 2011, Pages 477–523.

[10].Cloud Security Alliance, Security Guidance For Critical Areas Of Focus In Cloud Computing V2.1 5.

[11].J.Heiser And Mark Nicolett: "Assessing The Security Risks Of Cloud Computing." Gartner, 3 June 2008 <Www.Gartner.Com/Displaydocument?Id=685308>Ages. SPIE.

[12].Coso 2: Improving Organizational Performance And Governance.

[13] Peter Mell, Timothy Grance "The NIST Definition Of Cloud Computing Special Publiction 800-142"

[14] Http://Www.Darkreading.Com/Cloud/Cloud-Means-More-Secure-Remote-Access/D/D-Id/1137019? Visited 13-12-2014 At 10:36 Pm

[15] John Fraser, Betty Simkins, Kristina Narvaez, Implementing Enterprise Risk Management: Case Studies And Best PRACTICES

[16]Hemanth Khambhammettu, Sofiene Boulares, Kamel Adi, Luigi Logrippo, "A Framework For Threat Assessment In Access Control Systems" Information Security And Privacy Research IFIP Advances In Information And Communication Technology Volume 376, 2012, Pp 187-198

[17]National Security Agency, Systems And Network Analysis Center " A Framework For Assessing And Improving The Security Posture Of Industrial Constrol Systems (ICS)"

Table 1 : Overview Of The Threats According To The CIA Security Model [1, 10,11,13]

Threat	Description
Confidentiality	
Insider user threat : • Malicious cloud provider user • Malicious cloud customer user • Malicious third party user (Supporting either the cloud provider or customer organizations)	The threat of insiders accessing customer data held within the cloud is greater as each of the delivery models can introduce the need for multiple internal users: SaaS cloud customer and provider administrators PaaS application developers and test environment managers IaaS- third party platform consultants
External attacker threats: • Remote software attack of cloud infrastructure • Remote software attack of cloud applications • Remote hardware attack against the cloud • Remote software and hardware attack • Social engineering of cloud provider users, and cloud customer users	The threat from external attackers may be perceived to apply more to public Internet facing clouds, however all types of cloud delivery models are affected by external attackers, particularly in private clouds where user endpoints can be targeted. Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.
Data leakage: • Failure of security access rights across multiple domains • Failure of electronic and physical transport systems for cloud data and backups	A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise
Integrity	
Data segregation: • Incorrectly defined security perimeters • Incorrect configuration of virtual machines and hypervisors	The integrity of data within complex cloud hosting environments such as SaaS configured to share computing resource amongst customers could provide a threat against data integrity if system resources are effectively segregated
User access: • Poor identity and access management procedures	Poor access control procedures creates many threat opportunities, for example an ex-employees of cloud provider maintain remote access to administer customer cloud services.
Data quality: • Introduction of faulty application or infrastructure components	The threat of data quality is increased as cloud providers host many customers' data. The introduction of a faulty or misconfigured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure
Availability	
Change management: • Customer penetration testing impacting other cloud customers • Infrastructure changes upon cloud provider, customer and third party systems impacting cloud customers	As the cloud provider has increasing responsibility for change management within all cloud delivery models, there is a threat that changes could introduce negative effects. These could be caused by software or hardware changes to existing cloud services
Denial of service threat: • Network bandwidth distributed denial of service • Network DNS denial of service • Application and data denial of service	The threat of denial of service against available cloud computing resource is generally an external threat against public cloud services. However, the threat can impact all cloud service models as external and internal threat agents could introduce application or hardware components that cause a denial of service
Physical disruption • Disruption of cloud provider IT services through physical access • Disruption of cloud customer IT services through physical access • Disruption of third party WAN providers services	The threat of disruption to cloud services caused by physical access is different between large cloud service providers and their customers. These providers should be experienced in securing large data center facilities and have considered resilience among other availability strategies. There is a threat that cloud user infrastructure can be physically disrupted more easily whether by insiders or externally where less secure office environments or remote working is standard practice.
Exploiting weak recovery procedures: • Invocation of inadequate disaster recovery or business continuity processes	The threat of inadequate recovery and incident management procedures being initiated is heightened when cloud users consider recovery of their own in house systems in parallel with those managed by third party cloud service providers. If these procedures are not tested then the impact upon recovery time may be significant.

Table 2 : Application Of FMECA On Confidentiality Of The Desired Process

Features	Failure mode	Cause	Effects on system	Possible hazards	S	O	D	IPR
The desired Business process	Confidentiality	Insider user threats	Loss of confidentiality	Malicious cloud provider user	7	5	3	105
				Malicious cloud customer user	6	7	5	204
				Malicious third party user	5	5	7	188
		External attacker threats		Remote software attack of cloud infrastructure	8	5	6	267
				Remote software attack of cloud applications	9	6	7	349
				Remote hardware attack against the cloud	8	3	10	240
		Data leakage		Failure of security access rights across multiple domains	6	5	6	176
				Failure of electronic and physical transport systems for cloud data and backups	5	4	7	128