Universitat Politècnica de Catalunya

FIB - Facultat d'Informàtica de Barcelona

Master in Innovation and Research in Informatics

Master in Data Mining and Business Intelligence

Cloud service data collection for cloud service selection

using crowdsourcing techniques

CANDIDATE
Maryam Pashmi

ACADEMIC ADVISOR
Prof. Abelló Alberto

INDUSTRIAL ADVISOR
Dr.Victor Muntes

Academic year 2015/2016

To my family

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Context and Problem Statement

Nowadays, cloud computing is growing everywhere and the number of cloud environments is significantly increasing. Many companies tend to use cloud computing services and select the best cloud adoption strategy for their business environment. According to Gartner, "The use of cloud computing is growing, and by 2016 this growth will have increased to become the bulk of new IT spend" [1].

Aware of business opportunities in cloud computing, a number of cloud based service vendors have rapidly joined this market and the new challenge of selecting the best cloud providers among the vendor companies has been raised.

Consequently, the task of selecting a suitable cloud service for the end user in the cloud computing environment is becoming more and more important. In fact, making a good service provider decision is one of the most important tasks for all cloud consumers.

There has been a lot of research into the development of suitable decision support systems to assist users to select their cloud services efficiently.

A Decision Support System (DSS) is a tool that allows end users to specify their requirements and suggests the most appropriate solution related to those requirements to them. In other words, DSS assists decision makers by providing a platform for the joint consideration of several requirements to make a more informed decision.

Two main categories for decision making have been defined in [8]: quality of service and quality of experience. However, there is no clear mechanism to collect data related to quality of service and experience. There are some ongoing projects that have been initiated to develop better decision support systems. One of these projects is MODAClouds project which was funded by the European Commission.

This project contains standardized sets of tools and metrics enabling monitoring and interoperability at the run time. It considers cloud application to be accommodated by different cloud providers either public or

private. The MODAClouds project is an initiative for providing a DSS tool in order to make the best decision on selecting an appropriate cloud provider in a multi cloud environment. It uses an agnostic approach which takes into account business and technical requirements, restrictions for both, from the very beginning of the application life cycle. The MODAClouds approach tries to address major customer concerns such as vendor lock-in, risk management and quality assurance [6].

The Decision Support System (DSS) provided by MODAClouds, simplifies deployment work for developers and operators by analysing and comparing different cloud options for the designed architecture along with its set of predefined requirements. We have worked on a part from the DSS MODAClouds project. The MODAClouds DSS tool can be used to determine which cloud to adopt for hosting the different components of new solutions, comparing costs, risks, and analysing non-functional characteristics for each alternative provider, and also improving the trust in cloud solutions [6].

A Multi cloud environment is the use of two or more cloud services to minimize the risk of a vendor lock-in. In [8] authors highlight the importance of creating a unified model of data gathering and curation as an inherent component of DSS. Besides they mentioned that the performance of a DSS is highly dependent on the data gathered and this requirement is often not confronted as a challenge for Cloud DSS tools in previous studies. They considered the process of data gathering as an integral part of such DSS tools [6].

An extensive survey of different theories related in general to decision support systems has been done and as a result of that we found a clear gap between several perspectives [8].

- None of the Cloud DSS tools have considered the quality of service and the quality of users' experience to make recommendations to the end user. In fact there is no integrated process to collect the user opinions.
- No efficient, innovative mechanism exists to collect these types of data.
- Current DSS tools have not considered privacy and security features in a holistic and very deep view. This means that there is no mechanism for the collection of security and privacy data to be designed to provide a better understand of the complexity of cloud's security issues.
- There are some important frameworks such as SMI and CSA which have not been considered intensively for the comparison of different cloud service providers by the Cloud DSS tools [34].

1.2 Objective of the Thesis

Our aim is to tackle these shortcomings and attempt to bridge this gap. We will propose the followings:

- The development of a crowdsourcing platform in order to enable stakeholders to collaborate in rating, commenting and replying through forms, questionnaires and forums. The rating mechanism helps to collect the data related to the quality of experience and quality of service. Also gathering data using crowdsourcing techniques is an innovative idea which can be used in the DSS tools.
- The provision of a holistic view of security and privacy based on the Cloud Security Alliance framework. We are building the visualisation tool using the CSA framework for analysing security and privacy characteristics. Visualisation will help end users to have a clear overview of the security and privacy of each service provider, thus solving the complexity of understanding the whole process. This is a completely new approach which none of the DSS tools have used before.
- The use of two frameworks, the SMI and CSA in our platforms. CSA, as a privacy and security framework, and SMI, as a generic IT framework which have considered all of the characteristics of cloud computing, have been given importance in the practice. Using CSA for our visualisation tool and SMI for the rating mechanism will help to motivate the participation of cloud providers. They will try to adapt themselves with such a framework in order to be placed in a competitive environment.

Given the above problem statement and our objectives, we identified the main requirements for our solution as follows:

- Identification of the relevant data: Identifying and procuring the exact data needed from CSP is a critical issue because of the need for drawing relevant conclusions regarding different aspects of the cloud service providers. We would like to identify what the relevant information is in terms of cloud consumer perspectives which should be taken into account. (Chapter 3, Table 3-2 toTable 3-10)
- Data source availability: The availability of data sources or data sets is another important issue that might be a problem. Data availability refers to publicly accessible data provided by the different vendors in order to comply with legal requirements, and therefore it can be used in our platform design. This data may be available partially or may be outdated. Our platform attempts to show in a transparent way partial and absent parts of information to the cloud consumer. If that data is not clear in the provider's web page then should be gathered through the crowd. (Chapter 3, Table 3-2 to Table 3-10)
- Data gathering: The data gathering process will be done through involvement of stakeholders. The purpose of data gathering is to extract the right data at the right time from cloud providers or end users. Having appropriate, accurate, up-to-date and correct data is essential in order to be able to

transfer rich data to the cloud consumers, end users and third party companies such as DSS tools' providers, etc. We divide the data gathering process into two parts, security and privacy data gathering and generic data gathering. (Chapter 4)

- Designing provider's and end user's questionnaires: Since the integrity and accuracy of the data is highly critical, we involve cloud providers in order to obtain hidden information about their services. We have designed our questions based on discarded or invisible information about security specifications. These questions will be published as an online questionnaire through our platform. Moreover, by increasing transparency and validity of the information, we involve end users in order to answer the customer survey questionnaire. (Chapter 4)
- Creating a forum for each provider: The purpose of this forum is to create a common place for potential customers to post comments, reply to comments and vote for their desired cloud provider. With this approach they are able to feed back their positive or negative opinions about the services which are offered by the providers. The voting mechanism is based on SMI security characteristics which helps to make a better collective decision about cloud provider. Customers can talk about their experiences of using different services such as SLA agreements and cost considerations etc. which can be highly influential factors in selecting cloud services. Furthermore, it helps to create trustworthy services among all the cloud service providers. (Chapter 4)
- Visualization: In order to make sense of the security and privacy data, we decided to give value to the gathered information from CSA by visualizing them in a way so that the end user will be able to extract whole ideas about security and privacy in an easier and clearer way. (chapter 4)

The following figure summarises and explains the process which needs to be done in this dissertation.

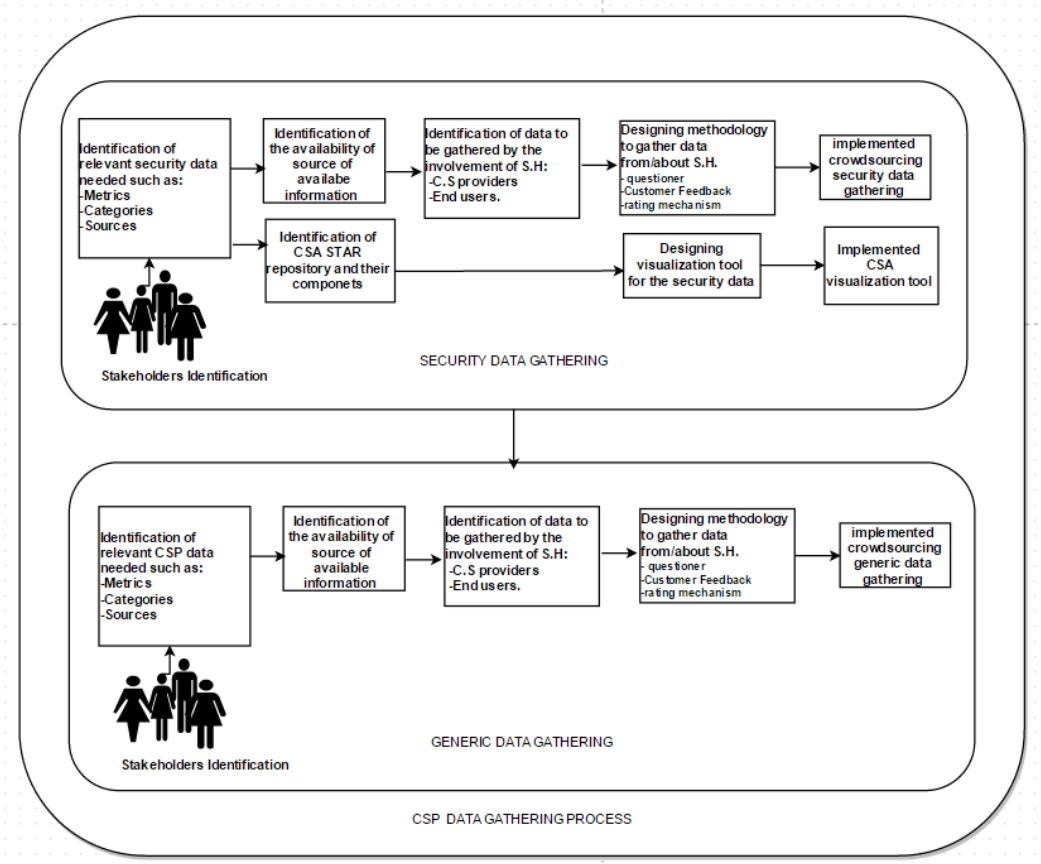

Figure 1-2 CSP data gathering process

1.3 Structure of the Thesis

This thesis is organized as follows:

- Chapter II. This chapter presents state of art in the taxonomy of cloud service features particularly in cloud security. In this chapter, we compare and contrast our work with previous research work.
- Chapter III. Here we present the cloud service data categorisation and describe four different categories such as legal, operational and technical metrics. In this chapter we list all the metrics related to each category. We also briefly explain why privacy and security requirements are becoming more and more important for customers.
- Chapter IV. Here we present how security data is gathered through crowdsourcing techniques. Each component is described in detail. Then, we extend the general case of our platform to all the cloud characteristics except of financial characteristics. The different steps are described in detail.

- Chapter V. In this chapter we describe the functional and non-functional requirements as well as architecture and data model. In this chapter, we describe an over view of technical requirements for our project.
- Chapter VI. In this chapter, we conclude the proposed data procurement platform and list down all the challenges which should be met by a holistic data procurement platform.
- Finally, in the last two chapters we describe the acknowledgement and bibliography of our work.

1.4 Planning

In this section, we visualize how long our project will take by using a Gantt chart. The Gantt chart is a simple timeline view of the project. On the left hand side there is a list of tasks for our project organized into groups. These groups have already been mentioned in the previous chapter. In fact each task is associated to each process in the whole project. Table 1-1 shows seven different tasks which began on February 9th and which will end approximately at the first of October. We also link tasks together by creating dependencies between them. Gantt chart ensures that tasks are done in the correct order [21].
Project's timeline is also provided in Figure 1-1.

	Task	Assigned To	Start	End	Dur	%	2015 Q1 Q2 Q3 Q4
	Main Topic		9/2/15	25/10/15	180	12	
1	Identification of relevant CSP categories and metrics		9/2/15	14/3/15	25	85	
2	Identification of the availability of sources of available data *		1/3/15	15/3/15	10	40	
3	Identification of data to be gathered by the involvement of S.H: -C.S providers -End users.		16/3/15	1/4/15	13	0	
4	Designing methodology to gather data from/about S.H. - questioner -Customer Feedback		2/4/15	21/4/15	12	0	
5	Implemented crowd sourcing security data gathering		22/4/15	5/5/15	9	0	
6	Designing the CSA Visualization tool		6/5/15	13/5/15	6	0	
7	Extend security characteristics to rest of the Cloud characteristics except financial		14/5/15	22/6/15	27	0	
8	Implemented Platform		23/6/15	14/8/15	39		
9	Documentation process		14/7/15	25/10/15	73		

Table 1-1 Gantt chart

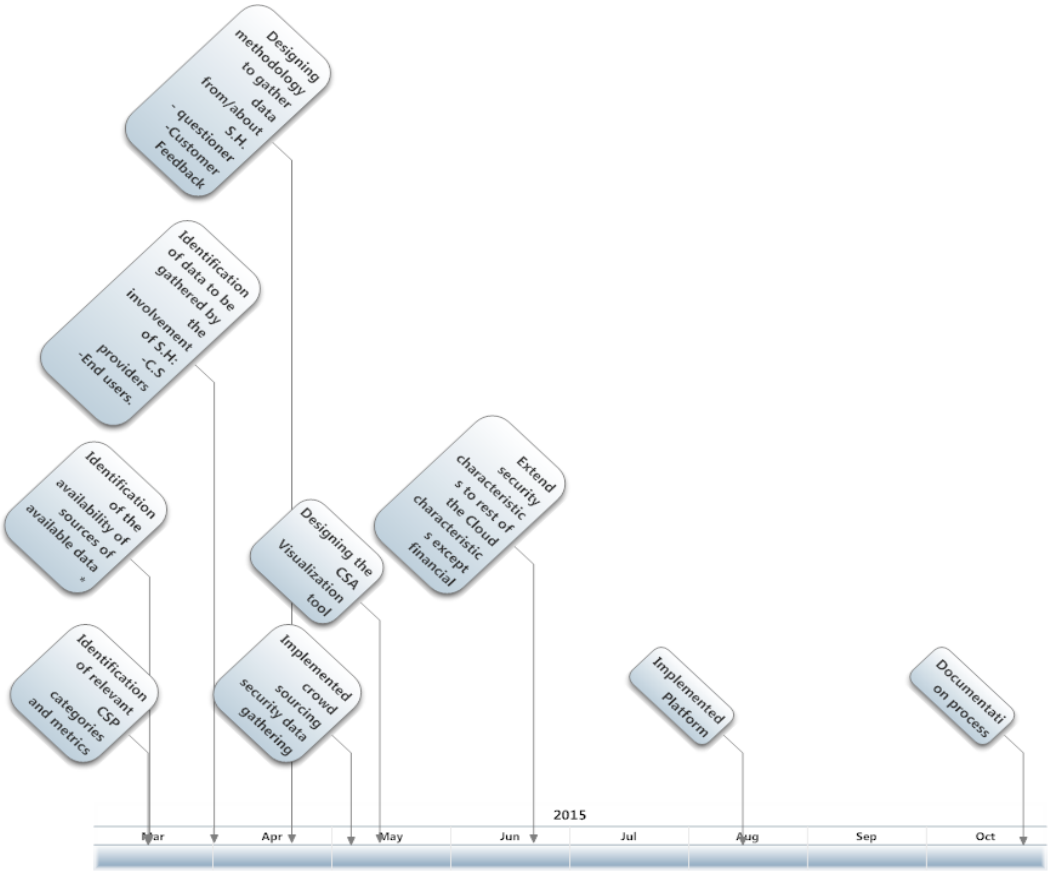

Figure 1-1Project's timeline

2. State of the Art

An initial review of popular publications, technical journals and industry white papers showed that several cloud brokers proposed a variety of monitoring tools with different functionalities. This review of their work pointed to the absence of a common conceptual framework for measuring cloud based services.

2.1 Existing Cloud Service Categorizations

Comparative characteristics of cloud computing have been discussed in terms of several perspectives in previous studies. For example, in [11], characteristics of cloud computing are considered as: negotiation, when large providers offer negotiation and customization for SLA, the location of the servers when resources are located in third-party datacentres, the use of multi-tenant architecture and resource management to realize economies of scale, a pricing model linked to usage, a high degree of automation when automatic scaling of required resources is demanded, the standardization of IT services.

Cloud computing challenges also considered in [12] were: (1) Service Level Agreement (SLA) when the user needs to be sure of service delivery in terms of quality, availability, reliability and performance, (2) a charging model for elastic resource pools when the cloud provider calculates his costs based on the consumptions of static computing, (3) migration, when an organization decides to move into the cloud and consequently security and privacy become prominent concerns, (4) cloud interoperability which refers to links between different clouds or connections between a cloud and an organization's local systems, (5) cost, when cloud consumers must consider the trade-offs between computation, communication and integration.

Also, in August 2008, the authors referred to in [12] presented a graph based on IDC Enterprise Panel, Figure 2-1, which shows security, performance and availability respectively as being the most important factors in hindering cloud computing. The same authors also referred to well-known security issues such as data loss, phishing and botnets, all of which pose serious threats to an organization's data and software.

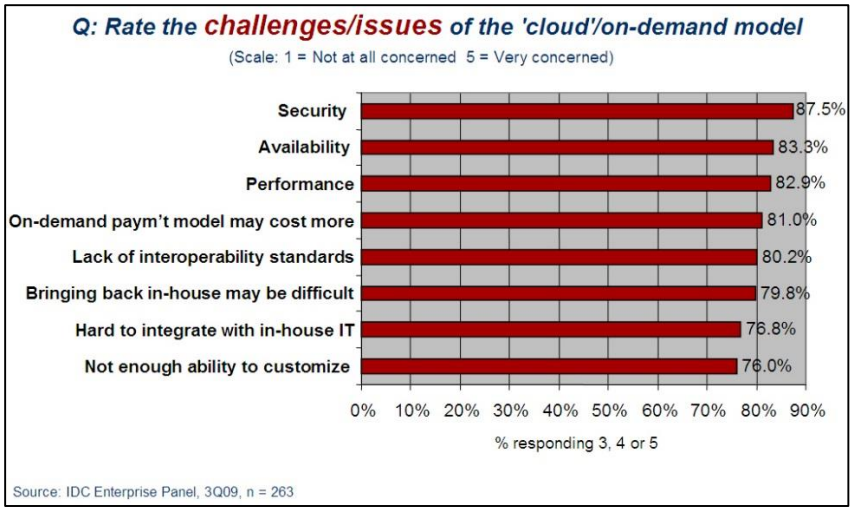

Figure 2-1 IDC Enterprise Panel[1]

In [13], the authors classified cloud architecture issues as follows: (1) Fault tolerance i.e. the disruption of applications and back-ups and the outage of services, (2) Security i.e. confidentiality of data, availability in terms of infrastructure and visualization, policy and privacy, (3) Load balancing i.e. monitoring of continuity of services, (4) Interoperability i.e. allowing applications to be ported between clouds and user accessibility, (5) Scalable data storage i.e. horizontal and vertical scaling, (6) Service models i.e. SaaS, PaaS and IaaS. Moreover the authors suggest a number of major challenges defined in 2013 by Zhen such as (1) Data management and governance, (2) Service management and governance, (3) Product and process control and monitoring, (4) Infrastructure and system reliability and availability and, (5) Information and visualization security. Zhen also described technological challenges in a cloud environment such as (1) Scale and elastic scalability where scale in, scale out and replication came into account, (2) Trust, security and privacy when multi-tenancy arise and control over data location, (3) Handling data where consistency, efficiency and legalistic issues came into account, (4) Programming models in cloud which should have highly scalable applications, (5) Systems development and management where all cloud consumers should be able to control and restrict distribution and scaling behaviours.

The above reviews pointed to more or less similar technical cloud computing concerns. The most important concerns are security, data privacy, data loss, as well as cost and flexibility when companies intend to deploy their product into cloud rather than subjective attributes.

[1] http://www.comp.leeds.ac.uk/mscproj/reports/1112/bavage.pdf

However, the lack of emphasis on quality attributes has led to the development of new work by a consortium of academic and industrial members of the Cloud Services Measurement Index Consortium (CSMIC), called Service Measurement Matrix. It is a customized framework for measuring the quality of service specifications in the cloud environment which is designed to allow for the quick and reliable comparison of IT business services.

2.1.1 Service Measurement Index (SMI)

SMI is a comprehensive framework of cloud related attributes for clients which is being developed by a consortium of academic and industrial members of the CSMIC. SMI is intended for use by industry and decision-makers. This extended hierarchical framework includes seven major characteristics with four or more attributes associated with each group of characteristics. It addresses a total of 51 attributes where each category has a series of measures [52].

Major categories are defined as: accountability, agility, assurance, financial, performance, security and privacy and usability. In fact, authors combine both the subjective and objective requirements of the cloud service providers and try to employ good service provisioning in terms of customers' perspectives, as well as providers' perspectives. They guarantee most of the required and essential user metrics such as availability, agility, security, trust, price, etc. In [54] authors have done a survey of important cloud service provider attributes using the SMI Framework. The result which were obtained from this survey have shown that security, privacy and performance have major attributes, with 16% and 15% respectively on importance when choosing a provider. It is really important to assure organizations that their data is kept safe and private.

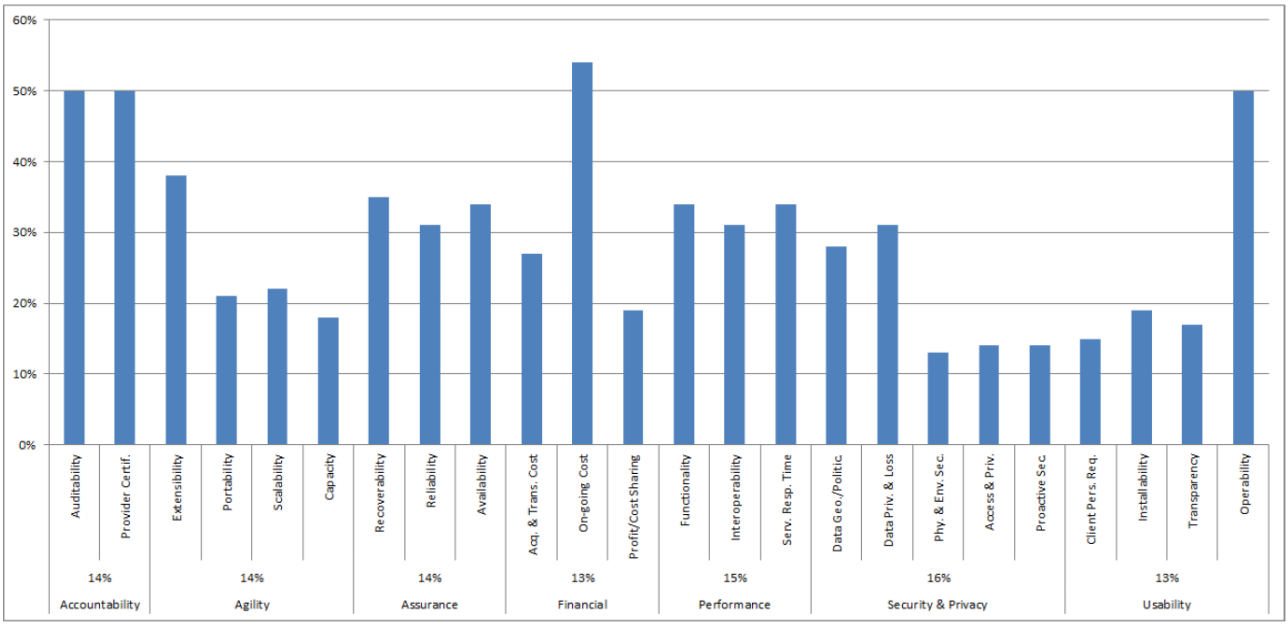

Figure 2-2 Survey results on SMI attributes-2013 [54]

Some examples of major categories in SMI are: [52]

- Accountability: Can we count on the provider's organization? To what extent can we expect it to be responsive to its clients? Are they providing any standards and / or compliances? How will the SLA conditions be met by the provider? Are these conditions completely manageable by the clients in order to mitigate risk? How stable will the provider's business be during the contract term? What are the levels of rights that a client has over client data? How sustainable is it in terms of economy, society and the environment? There are many more attributes of accountability which are shown in Table 2-1.
- Agility: Can it be changed and, if so, then how quickly? Agility refers to those attributes that indicate the impact of service upon a client's ability to change direction, strategy or tactics quickly and with minimum disruption. In many cases, clients would like to increase or decrease the number of their services, add new features of the same service, or change the amount of resource consumption, moving services internally or externally. Any of these kinds of requests by clients should be done in an agile way. This is really important from the client's perspective and has to be taken into account. All the attributes of agility appear in Table 2-1.
- Assurance: Attributes that indicate how likely it is that the service will be available as specified. Clients have to be sure about provided services in the cloud in terms of different attributes such

as availability. For example, they have to know whether the service provider has stated whether the service will be available for 99.99% of the year. Clients have to be sure about receiving appropriate reparation should the service fail or prove to be unsatisfactory. Clients have to be sure that the service will normally operate without failure under all conditions, but should there be an unplanned disruption that the service will quickly resume a normal state of operation. Further explanations appear in Table 2-1.

- Financial: What are the costs? What will be the amount of money spent on the service by the client? One of the important issues about financial concerns is the elasticity and flexibility of the financial aspects of the cloud service provider. Is the bill predictable for the clients? How responsive to the client's needs are the cloud service providers' pricing and billing components?
- Performance: Does it meet the client's needs in terms of accuracy, functionality, interoperability, service response time and suitability? Does the service provide all the specific features that clients need? To what extent does the service meet the client's requirement? How easily can one service interact with the next service (internally or externally)? How much of a delay is there between service requests and service responses?
- Security & Privacy: Is the service safe and is privacy protected? Are there mechanisms that indicate the effectiveness of a service provider's controls on access to services, service data and the physical facilities from which services are provided, such as where data is being stored locally? Does the cloud provider store data with respect to data integrity? Is data being stored with accuracy and validity? Are there any mechanism for detecting data loss? To what extent are services secure against recurring threads and vulnerabilities? To what extent are provider security policies close to client security requirement?
- Usability: Is it easy to learn and use? How easily can the service be used by clients? Can the service generally work well in terms of client perspective of accessibility, operability, learnability, transparency, understandability, installability and client personnel requirements? What kind of efforts have providers made in order to improve the learnability of the whole system? What impact will any changes or modifications to the service features have on usability? Are these changes transparent to the end user? How much time and effort will be required to get a service ready for delivery?

Accountability	Agility	Assurance	Financial	Performance	Security & Privacy	Usability
Auditability	Adaptability	Availability	Billing process	Accuracy	Access control & privilege management	Accessibility
Compliance	Elasticity	Maintainability	Cost	Functionality	Data geographic/political	Client personnel requirements
Contracting experience	Extensibility	Recoverability	Financial agility	Interoperability	Data integrity	Installability
Ease of doing business	Flexibility	Reliability	Financial structure	Service response time	Data privacy & data loss	Learnability
Governance	Portability	Resiliency/fault tolerance		Suitability	Physical & environmental security	Operability
Ownership	Scalability	Service stability			Proactive threat &vulnerability management	Transparency
Provider business stability		Serviceability			Retention/disposition	Understandability
Provider certifications					Security management	
Provider contract/SLA verification						
Provider ethicality						
Provider personnel requirements						
Provider supply chain						
Provider support						
Sustainability						

Table 2-1 SMI v2.0 categories and attributes

2.2 Existing Cloud Service Selection Tools

As mentioned in the previous sections, there is a need to assist the cloud consumers in selecting the best service provider to meet their requirements. In fact, there are several tools that are using different mechanisms in order to clarify the relationship between a cloud provider and its customers.

In previous studies, several cloud brokers, that represent such comparative information through their web portal, have been found. They proposed comparison tools among different cloud service providers [37, 2, 39, 40, 41, 43 and 3] by providing online resources in order to help cloud consumers to identify and locate cloud providers which meet their requirements.

Five different approaches have been used in the existing cloud comparison monitoring tools. One is Cloud Testing Benchmark tools where the performance of one system versus another is measured and compared. There are already big companies, such as Google and Yahoo that are working on such cloud benchmarking

tools[23]. These kind of benchmarking tools are intended to deal initially with various performance, scalability, availability, replication and quality requirements.

Likewise, some Small Medium Enterprises (SME) such as CloudHarmony [3] are also providing a broad range of performance characteristics of all the service types. Their goal is to create an impartial and reliable source for objective cloud performance analysis. This company covers most of the performance factors such as service availability, network throughput, latency, as well as SLA and price. Moreover, all the information is available through APIs.

In the second approach a web service for cloud metadata application is provided. One of the ongoing attempts is being made by York University where they introduce Cloudymetrics [4] as a RESTful web service for micro benchmarking. This API is provided in three different category levels: Provider-level metadata which considers information applicable for all resources of a provider and the properties of the provider itself, Resource-level properties which includes constant reportable properties about the resources, and Resource level metrics which includes measurable values about the resources.

In the third approach a cost forecasting, beside the representation of the cloud providers characteristic, is offered. One of these platforms is PlanForcloud [5] which is a part of RightScale [50]. This platform is a cloud cost calculator dashboard for multi-cloud resources which reports cost with regard to characteristics such as servers, storage units, databases and data transfer between different resources, as well as usage scenarios that incorporate growth, seasonality and other variability in the consumption of cloud resources in the long term. Moreover, an overview of the different categories of services such as compute instance, relational database, NoSQL databases, block storage, object storage, archival storage, support, live status, security and certifications has been given.

Another approach has added a monitoring capability of objective characteristics to the subjective characteristic such as price. They offer a comprehensive perspective of all the quantitative metrics in the cloud environment. One of these companies is Cloudorado [2] which is slightly similar to the previously mentioned examples but which is a more comprehensive platform. This tool estimates the cost of 26 IaaS, providers and offers different types of comparisons such as cloud server comparison, cloud hosting comparison, cloud computing providers' comparison and cloud storage comparison. It details most of the different properties of the cloud providers such as networking, security, locations, reliability and failover,

[2] https://labs.yahoo.com/news/yahoo-cloud-serving-benchmark/

[3] https://github.com/GoogleCloudPlatform/PerfKitBenchmarker

services, support, billing, trial and specials, third-party tools support, provider Information and many others.

Another example of an approach, is Cloud Screener [40] which proposes a unique cloud comparison software. It compares, in terms of infrastructure, 120 criteria such as price, performance, security, stability and flexibility. These criteria are similar to those mentioned previously, expect that they allow the selection of medium, important and critical priorities of price, performance and security.

The next example of this approach is Software Insider [14], which is a search engine organization that allows users to compare 188 cloud service providers including PaaS and IaaS. Search criteria are classified into service model, deployment model (e.g. hybrid cloud, private cloud and public cloud), frameworks available, subscription options (e.g. reserved instances, spot instances, annual fees, etc.), features (e.g. auto scaling, block storage, bring your own OS, cloud storage, etc.), service locations and average user ratings.

Another tool is Intel Cloud Finder which uses different approaches to compare cloud providers [39]. They have considered 82 cloud providers with three different variants. The criteria for each of the variants have been classified to sub criteria. The quick search criteria of Cloud Finder is presented in Table 2-2.

Table 2-2 Service Provider Quick Search

As shown above, the quick search is subdivided into five categories. Another search, the detailed search, allows specialized searches by using criteria such as security, usability, quality, availability, technology and business. Several questions related to each of the search criteria have been provided in detail. The final search is the ODCA usage model search tool which is divided into infrastructure as a service (e.g. IO Control, security provider assurance, security monitoring, VM interoperability, etc.), platform as a service (e.g. carbon footprint, security provider assurance, long distance workload migration), location and information as a service which is categorised in a similar way to PaaS.

The two latest cloud monitoring tools added extra qualitative and quantitative characteristics. One of them is Cloud Surfing [41] which is a collaborative community effort based on user experience reviews. It allows

the user to write a review, make a suggestion, add a rating (e.g. usability, popularity, value, support, security, integration and access), etc. It is not a free solution for all its options. IaaS search is based on automation, backup, cloud management, communication, data centre, database, hosting, optimization, security, servers, storage and virtualization while PaaS search contains advertising, app development, app hosting, app integration, communication platform, computing framework, database platform, governance and support. The last one is Cloud Offerings Advisory Tool (COAT) [46] which is a part of A4cloud project, a web based independent cloud brokerage tool based on predefined questions regarding the user's requirements which filters the variety of offers to the user in terms of security and privacy attributes such as subcontracting, location of datacentres, use restriction, applicable law, data backup, encryption, data portability, law enforcement access etc. The main difference between existing cloud brokers and COAT is priority of elucidation and comparison for privacy and security-related non-functional requirements in cloud service offerings. It can be concluded that every platform takes some aspects into account, either from technical perspectives or non-technical perspectives of cloud service providers. Some other products allow specification of multiple aspects from both technical and non-technical perspectives, and offer a more comprehensive solution than others. It means that they have tried to include missing characteristics of the other product. For example, they bring some more additional characteristics to performance such as security and privacy. However, they do not cover all the security and privacy characteristics. Some other products add subjective characteristics such as customer feedback to their tool. In our work we propose security and privacy characteristics, as well as user feedback for a purpose of such cloud comparison tools.

2.3 Security Assessment in Cloud Service Selection

It can be concluded that two main critical concerns in the cloud computing environment are security and privacy issues which are preventing customers from deploying into the cloud environment easily. Hence, cloud service providers are assuring security issues by complying with some third party or compliance authorities. Some best security practices and compliances have been defined by different non-profit organizations, industry-accepted security standards, regulations and controls frameworks, such as the National Institute of Standard and Technology (NIST), the European Network and Information Security Agency (ENISA), the International Organizations for Standardization (ISO) and the Cloud Security Alliance (CSA). To secure their cloud environment, cloud service providers need to adapt to embrace the best security practices and standards. Therefore, we have done a further research of potentially useful standards related to security and privacy on cloud based services. As a matter of fact, security should be implemented

in every layer of cloud architecture. In this part we describe important security and privacy metrics which have been mentioned in previous studies.

In [22], authors survey threads and security risks that have emanated due to the nature of the service model delivery in the cloud environment. They categorised relevant risks for security in IaaS, SaaS and PaaS service models. They illustrated critical aspects that must be covered across SaaS architecture layers in order to ensure security of the enterprise data. One of the SaaS security issues is data security. In the SaaS model, data is not stored in the vendor's domain, which reinforces the need to prevent any kind of security breaches in the client's domain. Some kinds of assessment tests are proposed by authors in this article.

The other issue is network security where encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) have been suggested. Another issue is the location of the data because it is important to know where data is going to be stored locally. Authors relate this issue to the compliance and data privacy laws. The next issue is data access which is highly related to policies applied by users while accessing the data. Usually cloud providers give flexibility to the user in order to configure their own settings. Author proposed many more security issues such as data integrity, data segregation, authentication and authorization, data confidentiality, web application security, data breaches, vulnerability in virtualization, availability, backup, identity management and sign-on processes. Similarly, they have explored security risks and issues for IaaS and PaaS service models.

In [13], authors explore potential issues with which both end users and providers might be faced within the cloud environment. They have done a survey of some standards and best practices, which have been investigated for several years, on the consequences of moving into cloud environment.

2.3.1 European Network and Information Security Agency (ENSIA)

One of these standards is ENSIA which has been divided into three categories. ENSIA involves sharing the best practices and advice related to the information security industry, specifically network and information security. These categories are the top-level classification of security, like policy and organisational issues and technical and legal issues. Policy and organization issues are described as data and service portability and its impact on organisation assets, risk and vulnerabilities. Technical issues include all the relevant threads of cloud environment such as VM monitoring vulnerability, insider threads and so on. Finally, legal issues are described as risk for data manipulation, data location, data protection and so on.

2.3.2 International Organizations for Standardization (NIST)

The other standard is NIST. This defines security as a cross-cutting function that spans all layers of the reference architecture (see Figure 2-3 – The Combined Conceptual Reference Diagram). It involves end-to-end security that ranges from physical security to application security where, in general, the responsibility is shared between cloud providers and federal cloud consumers. They identified various security characteristics based on conceptual reference diagram and mapped into known cloud security standards like ISO. These security characteristics are subdivided into authentication & authorization, confidentiality, integrity, identity management, security monitoring & incident response, security controls, security policy management, availability, service interoperability, data portability, system portability, service agreements and accessibility [53].

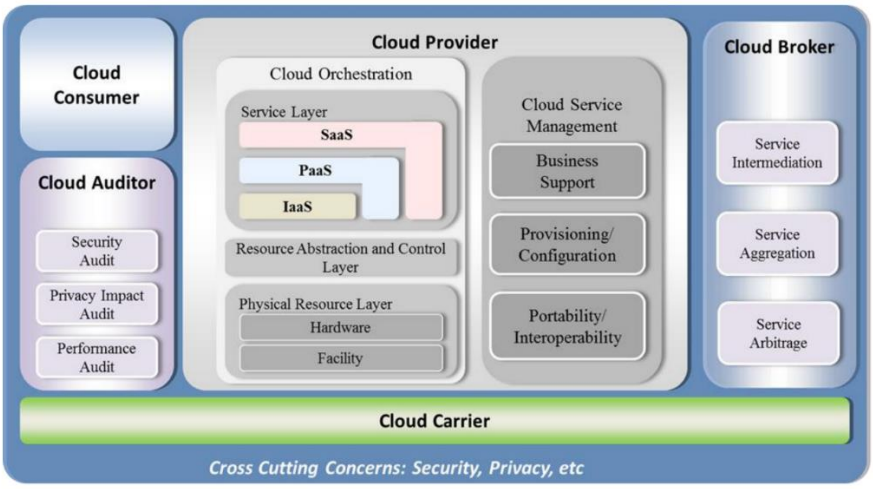

Figure 2-3 The Combined Conceptual Reference Diagram

2.3.3 ISO/IEC 27001:2005

ISO/IEC 27001:2005 has published by International Organization for Standardization, which contains best practice framework in the areas of information security management system. It considers common principles for initiating, implementing, maintaining and improving information security management in an organization. The figure below illustrates a set of characteristics defined in ISO/IEC 27001 [23].

It helps end users to identify the risks of important information and put in place the appropriate controls to help reduce the risk. It also helps to build confidence in inter-organizational activities. Right now ISO 27001: 2005 is no longer valid and a new revision of that is ISO 27001: 2013.

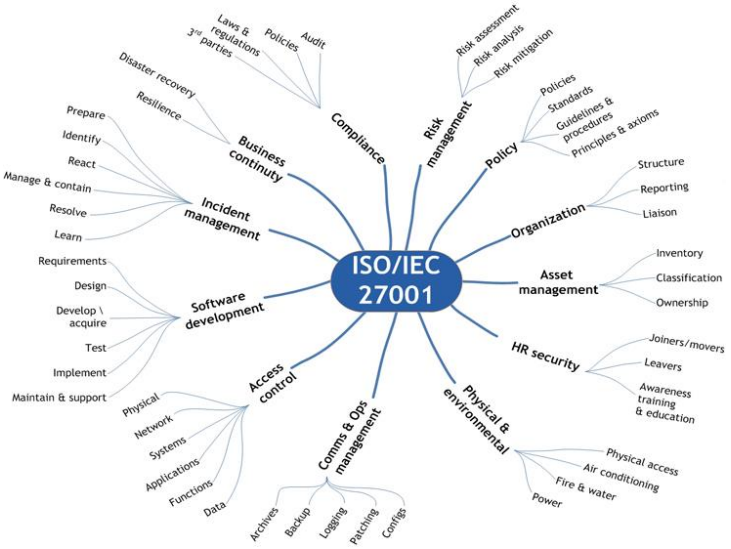

Figure 2-4 Auditagency.com

2.3.4 Control Objectives for Information and Related Technology (COBIT)

COBIT is a comprehensive and acceptable framework, developed by ISACA, which provides metrics and maturity models to measure its achievement and identify the associated responsibilities of business and IT process owners. It optimises IT-related investment by addressing the governance and management of the information.

COBIT 5 has defined five principals which assist enterprises to build an effective governance framework. In other words, COBIT is a business framework for enterprise IT management and governance aimed at linking business goals with IT goals.

It organises IT activities into a generally accepted process model which identifies the major IT resources as leverage and the consideration of the definition of management control objectives They attempt to mitigate organizational risk for IT and business as a whole, strengthen security, ease auditing and compliance burden and reduce cost while improving the consistency of IT delivery [26].

Figure 2-5 2012 ISACA. All Rights Reserved [25].

2.3.5 Health Insurance Portability and Accountability (HIPAA)

"The HITECH Act is transformational legislation that anticipates a massive expansion in the exchange of electronically protected health information (ePHI). The HITECH Act widens the scope of privacy and security protections available under HIPAA, increases potential legal liability for non-compliance; and provides more enforcement of HIPAA rules." [60]

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goals of the law are to make it easier for people to maintain health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs. HIPAA provides tools for organizations to begin their compliance initiative. They help organisations to assess, educate and implement different rules that address unique aspects of health insurance reform. Two main rules are privacy and security [24].

The Security Rule (SR) operationalizes the protections contained in the Privacy Rule (PR) by addressing the technical and non-technical safeguards that organizations, called "covered entities", must put in place to secure individuals' "electronic Protected Health Information" (e-PHI). Whereas the HIPAA Privacy Rule deals with Protected Health Information (PHI) in general, the HIPAA Security Rule deals with electronic Protected Health Information (ePHI), which is essentially a subset of what the HIPAA Privacy Rule encompasses [27].

The Security Rule specifies a series of administrative, physical and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity and availability of electronic Protected Health Information. HIPAA Security Rule is highly technical in nature. For all intents and purposes this rule is the codification of certain information technology standards and best practices. To summarize,

HIPAA Security Rule requires the implementation of three types of safeguards: 1) administrative, 2) physical, and 3) technical.

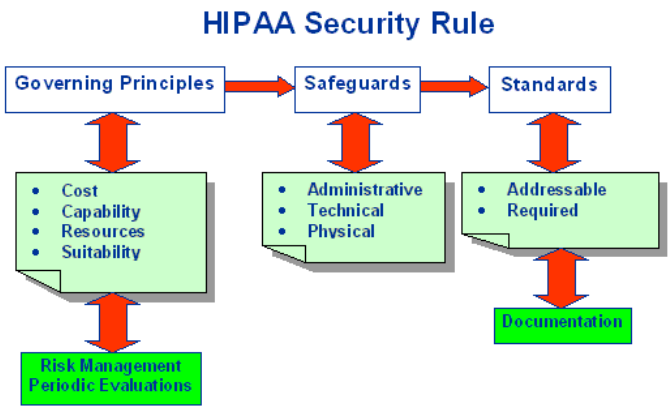

Figure 2-6 SPHER. Web. 5 Oct. 2015 [49].

The Privacy Rule standards address the use and disclosure of individuals' health information called Protected Health Information by organizations subject to the Privacy Rule called covered entities, as well as standards for individuals' privacy rights to understand and control how their health information is used. The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes [47].

2.3.6 ISGcloud

In [15], authors have made an empirical evaluation of their framework called ISGcloud which is a security governance framework that tackles the security risks and awarenesses of using cloud environment especially storage services. They used real case study in their work and investigated the impact and usefulness of their framework on organisations. They considered security requirements as tabled below.

Security requirements.

Security requirements	
1. Authentication	2. Confidentiality
1.1. User identification	2.1. Data isolation
1.2. Management of user's certificates	2.2. Anonymisation
3. Integrity	4. Availability
3.1. Encryption	4.1. Data recovery
3.2. Remote device management	4.2. Fault tolerance
3.3. Data backup	4.3. Data location
5. Transparency	6. Auditability
5.1. Incident reporting	6.1. Coverage
5.2. Data monitoring	6.2. Independence of verification
5.3. Service interoperability	6.3. SLA enforcement

Figure 2-7 ISGcloud security requirements

Two hierarchical levels of security requirements are illustrated in Figure 2-7. They assess cloud deployment security and the extent to which the organisation's security requirements are addressed and satisfied.

2.3.7 Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) maintains a list of top vulnerabilities to cloud based or SaaS models which is updated as the threat landscape changes (''OWASP'', 2010). These vulnerability issues respectively are (1) injection, (2) broken authentication and session management, (3) Cross-Site Scripting (XSS), (4) insecure direct object references, (5) security misconfiguration, (6) sensitive data exposure, (7) missing function level access control, (8) Cross-Site Request Forgery (CSRF), (9) using known vulnerable components and, (10) invalidated redirects and forwards. The table below shows all the 10 top vulnerabilities from top to bottom and left to right respectively.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability EASY**	**Prevalence COMMON**	**Detectability AVERAGE**	**Impact SEVERE**	**Application / Business Specific**
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends simple text-based attacks that exploit the syntax of the targeted interpreter. Almost any source of data can be an injection vector, including internal sources.	Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code. They are often found in SQL, LDAP, Xpath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, program arguments, etc. Injection flaws are easy to discover when examining code, but frequently hard to discover via testing. Scanners and fuzzers can help attackers find injection flaws.		Injection can result in data loss or corruption, lack of accountability, or denial of access. Injection can sometimes lead to complete host takeover.	Consider the business value of the affected data and the platform running the interpreter. All data could be stolen, modified, or deleted. Could your reputation be harmed?

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability AVERAGE**	**Prevalence WIDESPREAD**	**Detectability AVERAGE**	**Impact SEVERE**	**Application / Business Specific**
Consider anonymous external attackers, as well as users with their own accounts, who may attempt to steal accounts from others. Also consider insiders wanting to disguise their actions.	Attacker uses leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to impersonate users.	Developers frequently build custom authentication and session management schemes, but building these correctly is hard. As a result, these custom schemes frequently have flaws in areas such as logout, password management, timeouts, remember me, secret question, account update, etc. Finding such flaws can sometimes be difficult, as each implementation is unique.		Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.	Consider the business value of the affected data or application functions. Also consider the business impact of public exposure of the vulnerability.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability AVERAGE**	**Prevalence VERY WIDESPREAD**	**Detectability EASY**	**Impact MODERATE**	**Application / Business Specific**
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends text-based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.	XSS is the most prevalent web application security flaw. XSS flaws occur when an application includes user supplied data in a page sent to the browser without properly validating or escaping that content. There are three known types of XSS flaws: 1) Stored, 2) Reflected, and 3) DOM based XSS. Detection of most XSS flaws is fairly easy via testing or code analysis.		Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.	Consider the business value of the affected system and all the data it processes. Also consider the business impact of public exposure of the vulnerability.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability EASY**	**Prevalence COMMON**	**Detectability EASY**	**Impact MODERATE**	**Application / Business Specific**
Consider the types of users of your system. Do any users have only partial access to certain types of system data?	Attacker, who is an authorized system user, simply changes a parameter value that directly refers to a system object to another object the user isn't authorized for. Is access granted?	Applications frequently use the actual name or key of an object when generating web pages. Applications don't always verify the user is authorized for the target object. This results in an insecure direct object reference flaw. Testers can easily manipulate parameter values to detect such flaws. Code analysis quickly shows whether authorization is properly verified.		Such flaws can compromise all the data that can be referenced by the parameter. Unless object references are unpredictable, it's easy for an attacker to access all available data of that type.	Consider the business value of the exposed data. Also consider the business impact of public exposure of the vulnerability.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability EASY**	**Prevalence COMMON**	**Detectability EASY**	**Impact MODERATE**	**Application / Business Specific**
Consider anonymous external attackers as well as users with their own accounts that may attempt to compromise the system. Also consider insiders wanting to disguise their actions.	Attacker accesses default accounts, unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.	Security misconfiguration can happen at any level of an application stack, including the platform, web server, application server, database, framework, and custom code. Developers and system administrators need to work together to ensure that the entire stack is configured properly. Automated scanners are useful for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc.		Such flaws frequently give attackers unauthorized access to some system data or functionality. Occasionally, such flaws result in a complete system compromise.	The system could be completely compromised without you knowing it. All of your data could be stolen or modified slowly over time. Recovery costs could be expensive.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability DIFFICULT**	**Prevalence UNCOMMON**	**Detectability AVERAGE**	**Impact SEVERE**	**Application / Business Specific**
Consider who can gain access to your sensitive data and any backups of that data. This includes the data at rest, in transit, and even in your customers' browsers. Include both external and internal threats.	Attackers typically don't break crypto directly. They break something else, such as steal keys, do man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's browser.	The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm usage is common, particularly weak password hashing techniques. Browser weaknesses are very common and easy to detect, but hard to exploit on a large scale. External attackers have difficulty detecting server side flaws due to limited access and they are also usually hard to exploit.		Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive data such as health records, credentials, personal data, credit cards, etc.	Consider the business value of the lost data and impact to your reputation. What is your legal liability if this data is exposed? Also consider the damage to your reputation.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability EASY**	**Prevalence COMMON**	**Detectability AVERAGE**	**Impact MODERATE**	**Application / Business Specific**
Anyone with network access can send your application a request. Could anonymous users access private functionality or regular users a privileged function?	Attacker, who is an authorized system user, simply changes the URL or a parameter to a privileged function. Is access granted? Anonymous users could access private functions that aren't protected.	Applications do not always protect application functions properly. Sometimes, function level protection is managed via configuration, and the system is misconfigured. Sometimes, developers must include the proper code checks, and they forget. Detecting such flaws is easy. The hardest part is identifying which pages (URLs) or functions exist to attack.		Such flaws allow attackers to access unauthorized functionality. Administrative functions are key targets for this type of attack.	Consider the business value of the exposed functions and the data they process. Also consider the impact to your reputation if this vulnerability became public.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability AVERAGE**	**Prevalence COMMON**	**Detectability EASY**	**Impact MODERATE**	**Application / Business Specific**
Consider anyone who can load content into your users' browsers, and thus force them to submit a request to your website. Any website or other HTML feed that your users access could do this.	Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. If the user is authenticated, the attack succeeds.	CSRF takes advantage of the fact that most web apps allow attackers to predict all the details of a particular action. Because browsers send credentials like session cookies automatically, attackers can create malicious web pages which generate forged requests that are indistinguishable from legitimate ones. Detection of CSRF flaws is fairly easy via penetration testing or code analysis.		Attackers can trick victims into performing any state changing operation the victim is authorized to perform, e.g., updating account details, making purchases, logout and even login.	Consider the business value of the affected data or application functions. Imagine not being sure if users intended to take these actions. Consider the impact to your reputation.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability AVERAGE**	**Prevalence WIDESPREAD**	**Detectability DIFFICULT**	**Impact MODERATE**	**Application / Business Specific**
Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools, expanding the threat agent pool beyond targeted attackers to include chaotic actors.	Attacker identifies a weak component through scanning or manual analysis. He customizes the exploit as needed and executes the attack. It gets more difficult if the used component is deep in the application.	Virtually every application has these issues because most development teams don't focus on ensuring their components/libraries are up to date. In many cases, the developers don't even know all the components they are using, never mind their versions. Component dependencies make things even worse.		The full range of weaknesses is possible, including injection, broken access control, XSS, etc. The impact could range from minimal to complete host takeover and data compromise.	Consider what each vulnerability might mean for the business controlled by the affected application. It could be trivial or it could mean complete compromise.

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	**Exploitability AVERAGE**	**Prevalence UNCOMMON**	**Detectability EASY**	**Impact MODERATE**	**Application / Business Specific**
Consider anyone who can trick your users into submitting a request to your website. Any website or other HTML feed that your users use could do this.	Attacker links to unvalidated redirect and tricks victims into clicking it. Victims are more likely to click on it, since the link is to a valid site. Attacker targets unsafe forward to bypass security checks.	Applications frequently redirect users to other pages, or use internal forwards in a similar manner. Sometimes the target page is specified in an unvalidated parameter, allowing attackers to choose the destination page. Detecting unchecked redirects is easy. Look for redirects where you can set the full URL. Unchecked forwards are harder, because they target internal pages.		Such redirects may attempt to install malware or trick victims into disclosing passwords or other sensitive information. Unsafe forwards may allow access control bypass.	Consider the business value of retaining your users' trust. What if they get owned by malware? What if attackers can access internal only functions?

Table 2-3 OWASP Top 10 2013

2.3.8 Cloud Security Alliance (CSA)

The other enterprise which is working on security control frameworks is CSA, a non-profit organization initiated by industry representatives in November 2008. It is supported by a large number of IT companies. Its motivation is to provide security assurance and education in the field of cloud computing. CSA v3.x provides a controls framework which contains 16 domains supporting 136 controllers that are cross-walked to other industry-accepted frameworks. CSA offers best practices and security assurance in cloud environments. Also, it promotes transparency and visibility to the cloud consumer such as customers, providers, industries and governments.

CSA provides a repository of comprehensive sets of offerings for cloud providers, called Security, Trust & Assurance Registry (STAR) which is free and publicly accessible, and it is designed to recognize the varying assurance requirements and maturity levels of the providers [13, 18].

2.3.8.1 Cloud Controls Matrix (CCM)

One of the important projects in CSA is the Cloud Controls Matrix (CCM). CCM is a control framework that gives detailed descriptions of security concepts and principles in 13 domains which are aligned with Cloud Security Alliance guidance and information security. The foundations of the CCM rest on its customized relationship with other industry-accepted security standards, regulations and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, HIPAA and NIST, and will augment internal control direction for service organization control reports. CCM is a framework which provides needed structure, detail and clarity relating to information security tailored to the cloud industry. CCM empowers existing information security control environments by highlighting business information, security control requirements, reducing security threats and vulnerabilities, providing operational risk management and normalizing security expectations [18].

2.3.8.1.1 CCM Versions

CCM has several versions. Each version introduces several new control domains as well as new regulations, standards and best practices. They have considered most of the today's security issues for all the different service models such as SaaS, PaaS and IaaS. It relates each controller to one relevant category such as compliance, human resource, data governance etc. The table below presents two main versions of the CCM. Top level of abstraction can be shown in both versions. However, in v3.x, child levels are broken into more detailed and precise components compared with the old version. In fact they increase a number of controllers from 98 controllers in v1.x to 136 controllers in v3.x. Priority of version 3.x is that they have

incorporated mobile security for the critical areas of mobile computing as well as associated risks with governing data within the cloud providers' supply chain. The next priority is interoperability and portability which can be considered to minimize service disruptions while deploying into cloud.

CO			LG		FS	HR	OP
Compliance			Legal		Facility Security	Human Resources	Operation Management
AAC	SEF	STA	HRS	STA	DSC	HRS	BCR
Audit Assurance & Compliance	Sec. Incident Mgmt, E-Disc & cloud Forensics	Supply Chain Mgmt, Transparency & Accountability	Human Resources Security	Supply Chain Mgmt, Transparency & Accountability	Datacentre Security	Human Resources Security	Business Continuity Mgmt & Op Resilience

DG			IS				
Data Governance			Information Security				
BCR	DSI	GRM	EKM	GRM	IAM	SEF	TVM
Business Continuity Mgmt & Op Resilience	Change Control & Configuration Management	Governance & Risk Management	Encryption & Key Management	Governance & Risk Management	Identity & Access Management	Sec. Incident Mgmt, E-Disc & cloud Forensics	Threat & Vulnerability Management

RI	RM	RS	SA				
Risk Management	Release Management	Resiliency	Security Architecture				
AAC	CCC	BCR	AIS	IVS	TVM	IPY	MOS
Audit Assurance & Compliance	Change Control & Configuration Management	Business Continuity Mgmt & Op Resilience	Application & Interface Security	Infrastructure & Virtualization	Threat & Vulnerability Management	Interoperability & Portability	Mobile Security

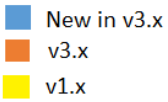

Table 2-4 Mapping v1.x to v3.x

The last priority is the number of existing practices or standards. V1.1 began with a smaller number of them such as COBIT4.119, HIPAA11, ISO/IEC 27002-200516, NIST SP800-5320, FedRAMP15, PCI DSS v2.021, BITS Shared Assessments and GAPP5 whilst in version 3.0.1 this number increases up to 32. Mapped regulations, standards and best practices have been used in both versions, and are presented in the following table.

CCM v3.0.1 Compliance Mapping	AICPA TSC 2009[4]	BSI Germany[5]	COPPA[6]	ENISA IAF[7]	GAPP (Aug 2009)[8]	Jericho Forum[9]	NZISM[10]
	AICPA Trust Service Criteria (SOC 2SM Report)	Canada PIPEDA[11]	CSA Enterprise Architecture (formerly the Trusted cloud Initiative)[12]	95/46/EC - European Union Data Protection Directive[13]	HIPAA/HITECH (Omnibus Rule)[14]	Mexico - Federal Law on Protection of Personal Data Held by Private Parties[15]	ODCA UM: PA R02.0[16]
	AICPA TSC 2014	CCM V1.X[17]		FedRAMP Security Controls (Final Release, Jan 2012) --LOW IMPACT LEVEL--[18]	ISO/IEC 27001:2005[19]	NERC CIP[20]	
	BITS Shared Assessments AUP v5.0[21]	COBIT 4.1[22]		FedRAMP Security Controls (Final Release, Jan 2012) --MODERATE IMPACT LEVEL--[15]	ISO/IEC 27001:2013[23]	NIST SP800-53 R03[24]	PCI DSS v2.0[25]
	BITS Shared Assessments SIG v6.0[18]	COBIT 5.0[26]	CSA Guidance V3.0[27]	FERPA[28]	ITAR[29]	NIST SP800-53 R03 Appendix J	PCI DSS v3.0

Table 2-5 Number of standards in v3.x

4 http://www.aicpa.org/

5 https://www.bsi.bund.de

6 http://www.coppa.org/

7 https://www.enisa.europa.eu/

8 http://www.aicpa.org/

9 https://collaboration.opengroup.org/jericho/index.htm

10 http://www.gcsb.govt.nz/news/the-nz-information-security-manual

11 https://www.priv.gc.ca/leg_c/leg_c_p_e.asp

12 https://cloudsecurityalliance.org/research/eawg/#_get-involved

13 http://ec.europa.eu/justice/data-protection/index_en.htm

14 http://www.hipaasurvivalguide.com/

15 http://www.itlawgroup.com/resources/articles/98-mexicos-new-federal-law-on-the-protection-of-personal-data

16 http://www.opendatacenteralliance.org/accelerating-adoption/usage-models

17 https://cloudsecurityalliance.org/research/ccm/

18 https://www.fedramp.gov/

19 http://www.iso.org/iso/catalogue_detail?csnumber=42103

20 http://www.subnet.com/solutions/nerc-cip.aspx

21 https://sharedassessments.org/about/

22 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-4-1.aspx

23 http://www.iso.org/iso/catalogue_detail?csnumber=54534

24 http://www.nist.gov/

25 https://www.pcisecuritystandards.org

26 http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx

We decided to select version 1.1 for our work for two reasons. First of all, the majority of provider's responses are based on CAIQ v1.1. Therefore, we can gain access to the bigger dataset. Secondly, the initial version is a base version which considers a smaller number of controllers and has been chosen as it matches the scope of this project.

2.3.8.2 The Comparison of Several Standards Applied to CSA

Each standard contains a set of clauses in the hierarchical structure. The level of hierarchy is different for each of the standards. For instance COBIT, FedRAMP, NIST, PCI and BITS have two levels of hierarchy while HIPAA and ISO have three and GAPP only has one. CSA mapped 136 security controllers mentioned in Table 2-6 with the child level in the hierarchy of each standard. To give an overall view of relevant domain area for each standard, we summarized a list of higher hierarchical levels for each standard which are mapped with the CSA security controllers.

COBIT	PCI	HIPAA	BITS AUP	FEDRAMP	ISO	NIST	GAPP	
Acquire and Maintain Application Software	Build and Maintain a Secure Network	Breach notification requirement	Communications and Operations Management	Security Assessment and Authorization	Security policy	Access Control	Privacy Policies	Disposal, Destruction and Redaction of Personal Information
Manage Changes	Regularly Monitor and Test Networks	Methods of notice	Information Security Policy	Risk Assessment	Organization of information security	Awareness and Training	Responsibility and Accountability for Policies	Access by Individuals to Their Personal Information
Install and Accredit Solutions and Changes	Maintain an Information Security Policy	Affirmative defences	Organization of Information Security	System and Services Acquisition	Asset management	Audit and Accountability	Review and Approval	Confirmation of an Individual's Identity
Monitor and Evaluate Internal Control	Protect Cardholder Data	Security standards(General rules)	Asset Management	System and Communications Protection	Human resources security	Security Assessment and Authorization	Consistency of Privacy Policies and Procedures With Laws and Regulations	Communication to Third Parties
Ensure Compliance With External Requirements	Maintain a Vulnerability Management Program	Administrative safeguards	Human Resources Security	Incident Response	Physical and environmental security	Configuration Management	Personal Information Identification and Classification	Disclosure of Personal Information
Manage Third-party Services	Implement Strong Access Control Measures	Physical safeguards	Physical and Environmental Security	Contingency Planning	Communications and operations management	Contingency Planning	Risk Assessment	Protection of Personal Information
Ensure Systems Security		Technical safeguards	Communications and Operations Management	Media Protection	Access control	Identification and Authentication	Consistency of Commitments With Privacy Policies and Procedures	New Purposes and Uses

[27] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[28] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[29] https://www.pmddtc.state.gov/regulations_laws/itar.html

COBIT	PCI	HIPAA	BITS AUP	FEDRAMP	ISO	NIST	GAPP	
Manage the Physical Environment		Organizational requirements	Access Control	Access Control	Information systems acquisition, development and maintenance	Incident Response	Infrastructure and Systems Management	Misuse of Personal Information by a Third Party
Ensure Continuous Service		Policies and procedures and documentation requirements	Information Systems Acquisition, Development and Maintenance	System and Information Integrity	Information security incident management	Maintenance	Privacy Incident and Breach Management	Information Security Program
Manage the Configuration			Information Security Incident Management	Physical and Environmental Protection	Business continuity management	Physical and Environmental Protection	Qualifications of Internal Personnel	Logical Access Controls
Manage Data			Compliance	Maintenance	Compliance	Planning	Privacy Awareness and Training	Physical Access Controls
Manage Operations				Configuration Management	Compliance with security policies and standards, and technical compliance	Program Management	Changes in Regulatory and Business Requirements	Environmental Safeguards
Define the Information Architecture				Identification and Authentication	Establishing and managing the ISMS	Personnel Transfer	Consent for Online Data Transfers To or From an Individual's Computer or Other Similar Electronic Devices	Transmitted Personal Information
Define the IT Processes, Organization and Relationships				Planning	Documentation requirements	Personnel Security	Types of Personal Information Collected and Methods of Collection	Personal Information on Portable Media
Manage IT Human Resources					Management responsibility	Risk Assessment	Collection Limited to Identified Purpose	Testing Security Safeguards
Manage Quality					Resource management	System and Services Acquisition	Collection From Third Parties	Accuracy and Completeness of Personal Information
Assess and Manage IT Risks					Management review of the ISMS	System and Communications Protection	Use of Personal Information	Relevance of Personal Information
						System and Information Integrity	Retention of Personal Inform	Communication to Individuals
							Instances of Noncompliance	Inquiry, Complaint, and Dispute Process
							Ongoing Monitoring	Compliance Review

Table 2-6 Standards' characteristics

2.3.8.3 CSA Security, Trust & Assurance Registry (STAR)

According to CSA, STAR is the industry's most powerful program for assurance in the cloud. STAR encompasses key principles of transparency, rigorous auditing and harmonization of standards and eventually continuous monitoring. The best practices and initial levels can be achieved at no cost, and we encourage providers and consumers to adopt STAR to enable trust in the cloud environment.

All cloud stakeholders have free access to the CSA STAR self-assessment. Consensus Assessments Initiative Questionnaire (CAIQ) and Cloud Control Matrix (CCM) are two key research components in CSA STAR [35].

Cloud service providers as well as cloud consumers can receive many benefits by participating in this program.

CSA CAIQ provides a series of security assertion control questions which are tailored to match the cloud customer's requirements. These questions are designed based on CCM which is a comprehensive list of the cloud-centric control objectives.

The CSA STAR offers self-assessment, attestation, certification and continuous monitoring. Self-assessment contains security controls which cloud providers can assess themselves through CAIQ, and it is provided in three different main versions: V1.0, V1.1 and V3.0. Each version is differentiated with some improvements over time. CSA STAR attestation is a collaboration between CSA and the AICPA, and is based on type 2 SOC attestation. The CSA STAR certification is a third party independent assessment for the security of a cloud service provider. CSA STAR's continuous monitoring enables the automation of the current security practices of cloud providers which is still under development.

2.3.8.4 Consensus Assessments Initiative Questionnaire (CAIQ)

CAIQ is a questionnaire which is available in spreadsheet format, and provides a set of 'yes or no' control assertion questions that cloud consumers and cloud auditors may wish to know about cloud providers. It is based on CCM security controls within IaaS, PaaS and SaaS models. For example, compliance-independent audits is a controller which involves the following questions. If the answer to each of these questions is 'yes', then it means that a particular provider satisfies current security requirements.

Some questions in CAIQ questionnaire are: 'Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?' ,'Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?', 'Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?' ,'Do you conduct internal audits regularly as prescribed by industry best practices and guidance?', 'Do you conduct external audits regularly as prescribed by industry best practices and guidance?', 'Are the results of the network penetration tests available to tenants at their request?', 'Are the results of internal and external audits available to tenants at their request?' [36].

2.3.9 Existing Data Gathering Mechanisms

The data collection process is the major part for each platform. Wikipedia defines data collection as: "Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses and evaluate

outcomes. The data collection component of research is common to all fields of study including physical and social sciences, humanities, business etc. While methods vary by discipline, the emphasis on ensuring accurate and honest collection remains the same. The goal for all data collection is to capture quality evidence that then translates to rich data analysis and allows the building of a convincing and credible answer to questions that have been posed [38]."

Having reliable and accurate data is an integral part of the data collection process which leads to correct decisions along with company strategies and at the end will have a huge impact on business goals. Two approaches for extracting and assimilating relevant cloud related information have been used so far:

- One is through published data. This means that a lot of web scrapping techniques exist for extracting such data through original providers' web pages. This kind of information is offered voluntarily by providers. This approach is not within the scope of our project.
- The second approach is through web queries and APIs. These APIs provide metadata information about cloud providers examples of which can be found through a few broker companies such as CloudHarmony, Cloudy Metrics etc. or original providers' webpages. However, relevant information gathered by those companies is not sufficient. Moreover it doesn't cover all the existing dimensions of either quality of information. Some of them such as Cloudorado [2] and PlanforCloud [5] compare cloud service providers in terms of characteristics particularly of performance and cost. On the other hand, there are some other tools that attempt to provide information about the technical aspects of cloud providers which go beyond price and performance such as CloudyMetrics [4], Cloudharmony [3] etc. While finance and technical comparisons are available in these platforms, the lack of focus on other important dimensions such as legal and organizational dimensions is a huge challenge. These additional dimensions, apart from price and performance, are highly subjective in nature and come into play while making a decision. Such aspects need to be accounted for while improving cloud comparison tools. This approach is not within the scope of this project.
- The third approach is through the crowdsourcing mechanism. Below, we discuss this approach in detail as this approach is within the scope of this project.

2.3.10 Data Gathering through the Crowdsourcing Mechanism

The popularity of the social web has caused many connectivities between huge numbers of people from all around the world, and allows them to take advantage of the online social web in many different ways. One of these approaches is crowdsourcing which appropriates certain advantages of the social web such as

connectivity and distributed population, and established itself as a collaborative platform for facilitating collective content creation. Bruns in 2007 said, “It extends or modifies social web features into an outsourcing platform through which potential online workers who are involved in the process of production”.

Crowdsourcing term is popularized by Howe and it originated when companies such as Amazon started to provide outsourcing services relying on anonymous communities or crowds (generally large network of people who were interested in and capable of collaborating) throughout the web.

There are several definitions of crowdsourcing. Brabham defined crowdsourcing as follows: “It is a model capable of aggregating talent, leveraging ingenuity while reducing costs and time formerly needed to solve problems”. Also, he delineated crowdsourcing according to for-profit or non-profit (not-for-profit and governmental) applications, for the latter, he focused exclusively on the innovation and problem-solving role of crowdsourcing [28].

Zwass (2010) relates crowdsourcing to the notion of co-creation which refers to participation of the consumers along with value creation procedure [29].

Many examples of crowdsourcing applications appear in existing works. Dawson and Alexandrov (2010) published a diagram of the landscape of crowdsourcing. They distinguish thirteen categories for crowdsourcing [55]. Some of the examples of crowdsourcing platforms include: Amazon Mechanical Turk[30], Threadless[31], InnoCentive[32], iStockPhoto[33], Tripadvisor[34] and Delicious[35]. Amazon uses crowdsourcing to provide general reviews by asking for comments or votes for its product whilst Threadless uses that to create a soft competition environment within the user community in order to design marketable t-shirts by promoting online competitions. Threadless uses participatory voting and commenting systems as a proxy for general ideas about consumer preferences. Votes and comments are used as the basis for rewarding community designers and product-selection decisions. InnoCentive crowdsources the research and development of scientific problems as challenges whereas iStockPhoto sells photographs, animation and video clips produced by its crowd of artists. Interestingly, surveys of the iStockPhoto crowd showed the main motivation behind their time and effort was not only monetary but also enjoyment and the

[30] https://www.mturk.com/mturk/welcome

[31] https://www.threadless.com/

[32] http://www.innocentive.com/

[33] http://www.istockphoto.com/

[34] http://www.tripadvisor.com/

[35] https://delicious.com/

development of individual skills [51]. TripAdvisor provides descriptions and evaluations of hotels, etc. through user reviews and ratings. Delicious relies on user reviews and/or ratings.

In fact outsourcing and crowdsourcing share the same objectives in that they source in their business needs from outside entities to achieve their business goals. However, crowdsourcing involves the management of a community via web based collaborative technologies to elicit the community's knowledge and/or skill sets, thus fulfilling a pre-identified business goal and reliable result. Crowdsourcing has led to our having more control over the process.

There are several challenges discussed in the studies such as recruiting and retaining users, defining which contributions can be made by users, combining these contributions and evaluating user performance. There is great potential for quickly generating and spreading disaster-related information through a crowdsourcing system. Doan, Ramakrishnan and Halevy discussed crowdsourcing systems on the web from a variety of perspectives. In addition to classifying the characteristics of tasks and stakeholders in such systems, they also discussed several process-related aspects such as the explicit or implicit nature of collaboration and the combination and evaluation of inputs, for instance crowd contributions [29].

As well as the definition of crowdsourcing, there are several other challenges regarding the characteristics of crowdsourcing that are discussed in previous studies, such as the extent of collaboration, types of human intelligence tasks, the use of systems of managerial control, reward systems, voting and commenting, trust building systems, worker identification, quality control and evaluation systems, aggregation and the visualization of results.

2.3.10.1 Existing Validation Techniques in Crowdsourcing Platforms

Quality control in crowdsourcing platforms is really important and can be checked either before or after the participation of workers. Kittur et al. stated that evaluation can be done through surveys, usability tests, rapid prototyping, cognitive walkthroughs, quantitative ratings and performance measures [29]. For instance, in order to analyse the performance of the previous tasks, task owner can ask questions for which the answers are already known (called expertise tests in certain domains), or the quality of the previously submitted explanations can be assessed by voting mechanisms according to their relevance, clarity and plausibility of statement.

Voting, commenting and rating mechanism are used in both social media and e-businesses to express community members' opinions in addition to evaluating the quality of others' ideas, products and services. In fact, crowdsourcing employs these strategies to exchange and evaluate ideas about products and services as well as to check buyers' and sellers' past history. They directly integrate the results of

community-driven voting, rating and commenting systems into their decision making processes. They employ these type of strategic virtual management control tools to draw and refine product ideas, to predict consumer product preferences, to control product and community member qualities, and to make compensation decisions. To qualify the answers of the participants of the questionnaire, those surveyed can be restricted to only allow contributions from company employees (e.g., InnoCentive@Work) or their customers (e.g., e-Rewards). In the first case, this may be due to available implicit knowledge or privacy concerns. In the second case, organizations are only interested in their customers' opinions.

Several strategies and algorithms have been defined in previous studies which discussed different mean rating techniques, and rating mechanisms for the recommender systems. For example, in [42], authors described state of the art approaches on modelling, formulation and social choice theory of the recommender systems in the context of the social web. Some approaches such as Collaborative Filtering (CF), meta-search, multi-agent systems, rank aggregation, majority-based and consensus-based strategies, additive utilitarian strategy, multiplicative utilitarian strategy, average strategy, average without misery strategy, least misery strategy, fairness strategy etc. have been discussed.

Another example which can be used for the ranking system is the Likert scale [30] which is proposed by Rensis Likert, and is used for assessing quality in questionnaire and survey data when participants answer on a scale from strongly disagree, disagree, neither agree nor disagree, agree and strongly agree.

Another example is Harmonic mean which is also used for the average rating. The Harmonic Mean is the number which when placed between two numbers forms a harmonic progression with the two numbers [43].

3. Cloud Service Data Categorizations

As mentioned earlier, there are many challenges in identifying cloud service characteristics. One of these challenges is Service Measurement Index (SMI), which is a selection model that can be used to classify services. We have considered the characteristics proposed by the SMI as guidelines to identify the nature of the data to be procured for two reasons:

Firstly, SMI tends to develop a comprehensive framework in order to provide performance and quality provisions. This is in alignment with our objectives. As previously mentioned we want to consider subjective and objective cloud characteristics for our work.

Secondly, as our project is a part of MODAClouds, it also considered SMI as a basis for its cloud selection model. We did a comprehensive investigation of the cloud computing characteristics of major cloud organizations such as Amazon Web Service, Google Cloud Platform, Microsoft Azure, Rackspace Cloud and cloud brokers such as CloudHarmony, PlanForCloud, as well as standardization organisation such as SMI, NIST, ISO, etc. The results shows the range and variety of cloud service metrics. We divided all these metrics into four abstract categories and then, mapped them to the SMI characteristics.

SMI	New categorization
Accountability / Security & Privacy	Legal/security /privacy
Usability	operational
Agility, Assurance, Performance	Technical
Financial	Financial

Table 3-1 Mapping between SMI with our cloud classification

3.1 Legal/security /privacy Category

The first category considers privacy, legal and security issues which are at the forefront of everybody's mind. As matter of fact, when data arrives in the cloud we know that it can be accessed by third party companies and we are not the only ones who can access it. Each company needs to ensure the privacy of its employees' and clients' data with regard to its legal obligations. So information about data protection awareness should be considered as a prerequisite for each cloud consumer before making any definite decision about deploying into the cloud. Knowing about the location of the data is another privacy concern. Data can be stored in different locations or regions. We should be aware of both primary and backup data locations. Vic (J.R.) Winkler stated in TechNet Magazine (2011) regarding data protection, "The transfer of

personal data outside any regions needs to be handled in very specific ways. For instance, the EU requires that the collector of the data, the data controller, must inform individuals that the data will be sent and processed in a region outside of the EU. The data controller and end processor must also have contracts approved by the Data Protection Authority in advance. This will have different levels of difficulty depending on the region that is processing the data. The United States and EU have a reciprocal agreement, and the U.S. recipient only has to self-certify its data procedures by registering with the U.S. "[31]

Below are the legal categories with related metrics and their descriptions. 'A' represents 'Availability' and 'C' represents 'Crowd'. This shows where data is gathered through the crowd and where it is available through published provider's information.

LEGAL/COMPLIANCE				
Category	**#**	**Metrics**	**A/C**	**Description**
Certifications	1	names_of_certifications	A	This metric represents the names of cloud provider's certifications.
	2	types_of_certificates	A	This metric represents the type of certificates that a cloud provider has.
Data privacy	3	distributed_service_region	A	This metric represents where data is located or their geographical region. This metric is used for the CDN and DNS services where content caches at physical nodes across the world.
	4	non_distributed_service_region	A	This metric represents where data is located or their geographical region. This metric is used for all the services except CDN/DNS, called non-distributed services. In this case data is going to be located in data centres.
	5	data_access	A/C	This metric displays who can access the provider's data and at what level. Whether or not customers' data can be mined by the supplier or others. Customers should be aware in their contracts, depending on the sensitivity of data, the limitation of access to their data.
	6	data_ protection	A/C	This metric represents the data protection laws. Data protection laws are different and extremely complex in different regions such as U.S and E.U. Customers should be aware of the transfer of personal data outside the regions. For instance, if data will be sent and processed in a region outside the EU. The data controller and end processor must also have contracts approved by the Data Protection Authority in advance. This will have different levels of difficulty depending on the region that is processing the data. The United States and EU have a reciprocal agreement, and the U.S. recipient only has to self-certify its data procedures by registering with the U.S. Department of Commerce.[36]
	7	data_transfer_regulation	A/C	This metric indicates whether or not the data is covered by some kinds of regulations. One of the regulation can be the Safe Harbour commitments of U.S.-EU. should it be transferred to another country.

Table 3-2 Legal and compliance metrics

3.2 Operational Category

This term refers to the usability and operability aspects of the web application. It can include essential characteristics for ensuring that the website is user friendly and aligns with customer satisfaction. We have

[36] http://technet.microsoft.com/en-us/magazine/jj554305.aspx

also considered several metrics which have highly impacted on user expectations of a provider's web page. Operational characteristics include a number of considerations such as direct 24/7 support, the availability of comprehensive and high-quality documentation, a high quality user interface etc. The operational metrics with their descriptions are listed below. For further details refer to Appendix A.

OPERATIONAL				
Category	**#**	**Metrics**	**A/C**	**Description**
Direct 24/7 support	8	technical_support_availability	A/C	This metric represents the technical support availability by provider.
	9	non_technical_support_availability	A/C	This metric represents the availability of non-technical support. Non-technical support refers to the sale of support, financial support, etc.
	10	ticket_system _availability	A/C	This metric represents the availability of support through the ticket system.
	11	phone _ availability	A/C	This metric represents the availability of support through phone contact by this provider.
	12	email_availaability	A/C	This metric represents the availability of support by email by this provider.
	13	livechat_availability	A/C	This metric represents the availability of support through live chat by this provider.
	14	livechat_support_languages	A/C	This metric represents supported languages by live chat.
	15	support_languages	A/C	This metric represents supported languages for technical or non- technical support.
	16	community_based_availability	A/C	This metric represents the existence of community behind a support system in order to get answers.
	17	remotely_support_availability	A/C	This metric represents the existence of the on-site, or remotely support by support technician.
	18	prenium_support_availability	A/C	This metric represents the existence of premium support by the service provider.
	19	pilot_solution_ availability	A/C	This metric represents the ability to pilot the solution by this provider. It is really important to look for proof points and results before you make a large investment especially in cloud computing areas.
	20	support_response_time	A/C	This metric represents the required response time to an issue.

Table 3-3 Operational metrics

3.3 Technical Category

The technical characteristics of cloud computing vary based on the available service models such as Infrastructure as a Service (IaaS), Platform as a service (PaaS), Software as a Service (SaaS), Storage as a Service (STaaS), Database as a service (DBaaS), DNS and Content Delivery Network (CDN).

In IaaS, providers lease infrastructure, physical resources such as hardware and network component or datacentre space. One example of IaaS is visualisation, where the amount that users should pay is based on the quantity of allocated resources. It is usually offered by data centres, and providers are responsible for running and maintaining the service. Examples of technical characteristics for IaaS are performance, availability, memory size, storage size and ram and many more [Appendix B].

SaaS is one of the common delivery models which has been used so far. One example of SaaS is Customer Relationship Management (CRM) which continues to be the largest market for SaaS [32]. SaaS has many advantages, such as lower initial cost, easier administration, business agility, compatibility, elasticity and ubiquitous accessibility. Some examples of technical metrics with their descriptions are listed below. For further details refer to Appendix B.

TECHNICAL				
Category	**#**	**Metrics**	**A/C**	**Description**
Auto scaling features[37]	58	processBased _autoscaling _supported	A/C	This metric represents whether the service provider supports process based auto scaling. This requires an automatic increase in the number of processes when demand increases. Each process generally runs in an isolated container that provides memory, (ephemeral) storage and CPU capacity. In general there are two different types of processes on-demand or dedicated processes (may also be referred to as workers, threads or another name)
	59	VMBased_autoscaling_ _supported	A/C	This metric represents if provider supports VM based auto scaling. This metric is used by VM based platforms. Automatic scaling in case of VM based platforms refers to automatic increase in VM resource allocation.
	60	CPU_bursting_availaility	A/C	This metric represents if CPU bursting is available by the service provider. When there is a need to have more CPU cycles than is allocated to a virtual machine, this metric provides a temporary performance boost.
	61	resvrd_ procese_suport	A/C	This metric represents if provider supports reserved processes. This metric can be applicable when the provider offers auto scaling.

Table 3-4 Technical metrics

The technical services are classified in different categories such as compute instance, platform as service, storage, data base, CDN and DNS. Below, in Table 3-5, 3-6, 3-7, 3-8, 3-9 and 3-10 are listed some examples of compute instance categories and related metrics with their descriptions. For further details refer to Appendix C to Appendix H.

COMPUTE INSTANCE				
Category	**#**	**Metrics**	**A/C**	**Description**
Technical features	125	CPU_model	A	This metric represents the CPU model allocated for each compute instance. For example Intel Xeon E5-2620.
	126	number_CPU_sockets	A	This metric represents the number of cores per CPU allocated for each compute instance.
	127	CPU_clock	A	This metric represents the amount of CPU clock allocated for each instance type.
	128	CPU_sockets	A	This metric represents the number of CPU sockets allocated for this compute instance.
	129	CPU_cores	A	This metric represents the number of CPU cores allocated for this compute instance.
	130	CPU_quantity	A	This metric represents the quantity of CPU allocated to each compute instance.
	131	RAM_quantity	A	This metric represents the quantity of RAM allocated to each compute instance.
Finance	148	purchase_ options	A	This metric represents the predefined purchase options by the service provider.

Table 3-5 Compute instance metrics

[37] http://www.ijarcce.com/upload/2013/july/67-o-kriushanth%20krish%20-An%20Overview%20of%20Cloud%20Auto%20Scaling.pdf

In PaaS, providers lease computing platforms include operating systems, hardware, programming language execution environments, servers and databases. This service provides the end user with many advantages. For example, end users can rent complex hardware and change operating systems dynamically while developing their applications. However, it is not always sufficiently flexible and agile to accommodate the evolving requirements of its customers. Examples of technical characteristics for PaaS are operating systems, data bases, user management and security [58]. Below, in Table 3-6 are listed some examples of PaaS categories and related metrics with their descriptions. For further details refer to Appendix D.

PLATFORM AS A SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
Platform properties	153	supported_programming_Languages	A	This metric represents the list of the programming languages supported by the PaaS provider.
	154	dataBase_supported	A	This metric represents the list of the data bases supported by the PaaS provider.
	155	additional _services_supported	A	This metric represents the list of the additional services supported by the PaaS provider. Some examples are logging services, monitoring services, emailing services, queuing services, DNS services, payment services etc.
	157	security_regulation_types	A/C	This metric represents the types of the security and regulatory compliance taken by the PaaS provider.
	163	disasterRecovery_readiness	C	This metric represents the readiness of policies and procedures to operate DR (disaster recovery) by the PaaS provider.

Table 3-6 PaaS metrics

In StaaS, the service provider leases the amount of space in the storage infrastructure to the end user by subscription. This is defined by WhatIs.Com of StaaS as: “Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement and maintain their own storage infrastructure. “ [38]

Below, in Table 3-7 are listed some examples of storage service categories and related metrics with their descriptions. For further details refer to Appendix E.

[38] http://searchstorage.techtarget.com/definition/Storage-as-a-Service-SaaS

STROAGE SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
Storage properties	179	storage_type_supported	A	This metric represents the types of storage service such as block storage, object storage and archive storage.[39]
	180	type_of_volume_supported	A	This metric represents the standard volume types have been supported by this provider such as SSD volumes.[40]
	181	data_ durability[41]	A/C	This metric represents the percentage of data durability which the service provide indicated for storage service.
	182	data_ availability[39]	A/C	This metric indicates whether the data availability of the service has been mentioned by the cloud service provider.

Table 3-7 Storage metrics

In DBaaS, providers deliver database functionality to the end user. According to Wikipedia [44], "there are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model". Below, in Table 3-8 are listed some examples of data base as a service categories and related metrics with their descriptions. For further details refer to Appendix F.

DATA BASE AS A SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
Database features[42]	206	relational_ database_services_supported	A/C	This metric indicates whether the relational data base has been supported by the service provider.
	207	NoSQL_ database_ services	A/C	This metric indicates whether the NOSQL data base is supported by the service provider.
Finance	218	purchase_ option	A	This metric represents the predefined purchase options by the service provider.

Table 3-8 Database metrics

CDN is a large distributed system of servers located throughout the world with the same content, and users are redirected automatically to the closet server to their visitors. The goal of a CDN is to serve content to end-users with high availability, high performance and fastest download speeds. According to Wikipedia[43], CDNs serves a large proportion of the Internet content today, including web objects (text, graphics and scripts), downloadable objects (media files, software and documents), applications (e-commerce, portals), live streaming media, on-demand streaming media and social networks. Akamai is one example of CDN

[39] http://cloudacademy.com/blog/object-storage-block-storage/

[40] http://www.rackspace.com/knowledge_center/article/cloud-block-storage-overview

[41] http://www.seagate.com/es/es/tech-insights/data-durability-in-highly-fault-tolerant-cloud-systems-master-ti/

[42] https://en.wikipedia.org/wiki/Cloud_database

[43] https://en.wikipedia.org/wiki/Content_delivery_network

which everybody knows. They have a huge network of over 100,000 servers all over the world.[44] Amazon Cloudfront is another example of a global CDN which works seamlessly with any origin server.[45] Below, in Table 3-9 are listed some examples of CDN categories and related metrics with their descriptions. For further details refer to Appendix G.

CDN SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
CDN technical properties[46] [47]	219	limiting_access_ content_supported	A/C	This metric represents the limiting of access to content supported by provider.
	221	content_push_suppo rted	A/C	This metric represents the availability of the CDN content Push method in order to serve customer content. This is similar to Poll method, the difference is that in content push, the CDN provides a means of FTP, SCP, rsync, etc. for customers to upload content to a storage repository. In this case, clients are responsible for providing content to the CDN, pushing it to the network, specifying the content that is uploaded, when it expires and when is updated.
	222	access_federatedServ erLogs_supported	A/C	This metric represents the availability of access to federated server access logs by CDN provider. These logs include the history of CDN edge servers where customer content was accessed and stored on a user accessible storage platform.

Table 3-9 CDN metrics

DNS is a service that uses a distributed database to provide a mapping of IP addresses to domain names and hosts to access resources on the internet and internal networks [45]. Cloud DNS service is a way of making the applications and services available to end users. Their aim is to provide a high-performance, resilient, scalability and global DNS service in a cost-effective way. It should be programmable to allow DNS records to be easily published and managed. Below, in Table 3-10 are listed some examples of DNS categories and related metrics with their descriptions. For further details refer to Appendix H.

[44] http://www.cdnplanet.com/cdns/

[45] https://aws.amazon.com/cloudfront/

[46] http://www.cachefly.com/company/faq/

[47] http://patentimages.storage.googleapis.com/pdfs/US20130046664.pdf

DNS SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
DNS technical properties[48]	232	routing_locationBased_Edns	**A/C**	This metric represents if the location based routing support EDNS (IP forwarding from the name server) is available by this provider. IP forwarding helps to determine over which path a packet or datagram can be sent in multiple networks.
	233	DNS_ sync_method	**A/C**	This metric represents which methods for DNS synchronisation are operated by this provider. These methods are standard master/slave DNS synchronization including support for NOTIFY (ability to send or receive), AXFR (full zone transfer), IXFR (incremental zone transfer) and TSIG (Transaction Signature).
	234	DNSSEC_mngmnt _supored	**A/C**	This metric represents the availability of the domain Name System Security Extensions by the service provider. DNSSEC is used to protect clients from forged DNS responses by digitally signing DNS responses. By checking the digital signature, DNS clients can verify the authenticity of those responses.

Table 3-10 DNS metrics

3.4 Financial Category

The financial aspect of cloud provider services is one of the important issues in the cloud computing area which effects final customers' decisions. It is classified by SMI into billing process, cost, financial agility and financial structure. There are also several pricing models described in the studies such as fixed priced regardless of volume, fixed price plus per unit rate, assured purchase volume plus per unit price rate, per unit rate with a ceiling, and per unit price [33]. This is a complex research area which is not within the scope of this thesis.

3.5 Availability of Data

Availability of data usually refers to the accessibility of relevant data from which we are able to derive value. We specify the availability of relevant information for each of the metrics, indicating whether or not this data were displayed clearly on the provider's web page.

We perform the following step for each cloud service provider. We look at all the candidate metrics noted in Table 3-2, Table 3-3 and Table 3-4 to Table 3-10 and we mapped a source of data availability to each of them. This source is a link which can be used to retrieve relevant information for a particular metric.

The following example shows the way the availability of a metric can be checked. 'Direct 24/7 support' is an example of operational categorisation. This category consists of several metrics such as email_availability, ticket_system, premium_support etc. These metrics can be used for measuring customer support systems. The availability of these metrics can be checked by looking at the provider's web page to

[48] ftp://ftp.isc.org/isc/bind/9.8.0-P4/doc/arm/Bv9ARM.ch04.html

discover, for example, whether or not corresponding information to the metric ‘premium support’ on the provider's web page can be easily found.

In the tables indicated in this chapter, there is a column which represents two letters ‘A’ and ‘C’. ‘A’ indicates the available and published metrics in a provider’s web page while ‘C’ shows those metrics which should be gathered through the crowd. If the desired information already exists as published data in the provider’s web page, we can design the questions for gathering the validation and feedback related to the particular metric through the crowd. We have checked the data availability of more than 200 different metrics between a variety of different services such as IaaS, Storage, PaaS, CDN, DNS, etc. The results for this part of the research are already shown in Table 3-2 to Table 3-10.

4. Security Metrics in Crowdsourcing Applied to the Cloud Computing

As described previously, security metrics play an important role in selecting cloud service providers. The security attribute was selected from among the other cloud computing attributes in order to initialise the practical part of this dissertation. Below is the block diagram of security data gathering process.

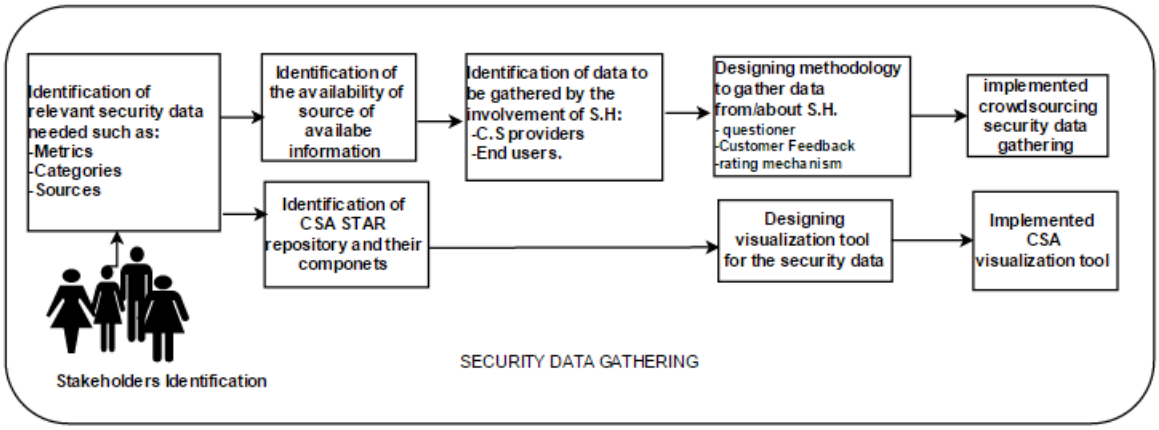

Figure 4-1 Block diagram – Security Data Gathering process

4.1 Stakeholders Identification and their Contributions

This section initially clearly indicates stakeholders who participate in the platform. The contribution of each stakeholder in the whole system is also indicated and the crowd is restricted to several stakeholders such as system administrator, cloud provider and cloud consumer.

1. System Administrator: The system administrator is the administrator of a system who must have adequate control in order to manage the end-to-end processes of the platform. Related tasks carried out by system administrators are:

    a. End-to-End coordination

    They must coordinate everything from the starting point to the end point of the process. For example, they can be responsible for adding identified providers to the system, and then assigning sufficient permission for them to perform predefined tasks.

    b. Modification

    The highest level of accessibility is modification. The role of the system administrator is to

allow the modification and deletion of information.

2. Cloud provider: Cloud providers are a group of experts who have sufficient knowledge about the security and privacy characteristics of the company for which they are working. They should cooperate in the system by helping with the collection of necessary data for customers, and should share up-to-date, factual, detailed, exact and comprehensive information with the end users. Related tasks carried out by a cloud provider are:
    a. The identification of a specialized security group in the provider's company.

       Every cloud provider is responsible for the identification and the creation of a security/privacy specialist group, and then the assignment of specific tasks to it. These tasks include: the forum management, the revision of any outdated information and the completion of the CSA form and security questionnaire.
    b. The completion of the privacy/security questionnaire.

       The privacy/security questionnaire includes a list of security and privacy questions that are not visible on the cloud provider's webpage. Usually, answers associated with each of these questions can be gathered indirectly through email, chat and phone.
    c. Information consolidation

       Information consolidation can be achieved by the combination of human interactivity and computer computation, thus ensuring reliability, accuracy and up-to-date data.
    d. Forum management

       A forum was dedicated to all providers, so that they can easily share their information with their customers. Also, customers can evaluate providers according to the security SMI characteristics. Thus the collaboration of providers can help to improve customer satisfaction.
3. Cloud consumer: This type of stakeholder can be assigned to either cloud brokers or end users. They are able to rate and comment on a specific service provider.

4.2 Identification of Relevant Data

In this section, a list of all the available and unavailable data is identified. If relevant data is not available or partially available on the provider’s web page, it will be gathered through the crowdsourcing platform. This is a prerequisite step in building a security questionnaire. Results have been listed in Chapter 3, Tables 1 to 10, Column A/C.

4.3 Mechanisms for Gathering Data from Stakeholders

The first part of the data gathering refers to the crowdsourcing part of the application, and the second part of data gathering refers to the security data visualization. Two different frameworks, SMI and CSA, form those two parts respectively. Also, it should be noted that SMI leverages security standards created by the Cloud Security Alliance (CSA) to assess security offerings for the attributes listed in the SMI.

4.3.1 Data Gathering Mechanisms through the Crowd

As mentioned earlier, by taking advantages of crowdsourcing, we are able to reach a large number of people with a variety of backgrounds. Online users play a critical role in our application. We can ask the crowd to contribute either by writing comprehensive reviews of the specific cloud service provider, by commenting and rating the existing ones and by completing the questionnaire.

Three techniques are considered for the gathering of security data through the crowd: Security questionnaires, Security polls forums and CSP form. They are constructed in accordance with the SMI security characteristics and CSA. A comprehensive explanation of SMI and CSA is provided in section 2.1.1 and 2.3.8, respectively. Mainly, these techniques are helpful for validating and consolidating cloud provider information which is publicly available on the internet. In fact, we want to evaluate the level of validity of the information. For example, a provider may have written in SLA that the level of availability of data is 99.99% whereas the client does not agree with this. This type of conflict should be recognized by gathering customer opinion or feedback on the particular service. On the other hand, we know that some parts of data is partially accessible on the provider's web site, so we have to contact the provider to obtain further details, usually by phone or email. In the following sections, several techniques have been applied in our application in order to resolve such problems in an easier way.

4.3.1.1 Security Questionnaire

According to the identified security metrics in Appendix B, a list of comprehensive questions was compiled for different types of services such as IaaS, PaaS etc. These questions should be outsourced to the stakeholders of the platform. As mentioned earlier, stakeholders are a predefined group of restricted and identified experts inside each cloud provider's company. The stakeholder identification process can help to add reliable and accurate data because these stakeholders are experts, and are selected by their company in order to answer the questionnaire. The two groups of questions considered in our platform are: cloud

provider questions and cloud consumer questions.

4.3.1.1.1 Cloud Provider Questions

For several reasons, such as page structure, site design, lack of transparency, marketing strategies etc. some parts of the information are partially embedded on the provider's web site, and are not clearly visible. In other words, some parts of the information are missing. However, an awareness of such information is critical for the end users, and an exploration of this kind of information will help a better decision to be made when selecting an appropriate cloud service provider which is matched to their specific requirements. According to the identified security metrics in Appendix B, we have created a set of 16 security questions, the answers to which can be collected through the crowd. The list of questions appear in the following table.

Map Q[49] with Metrics	#	Cloud Provider Questions Security Questioner
79	1	**Does your organization provide VPN connectivity to VPC networks for the customers?** Yes/No
82	2	**Does your organization provide dedicated network links for the compute instance?** Yes/No
80	3	**Does your organization provide shared network links for the compute instance?** Yes/No
83	4	**Does your organization support any SSL certificates?** Yes/No
85	5	**Does your organization support any SSL content delivery?** Yes/No
85	6	**Does your organization support dedicated IP Custom SSL for the customers?** Yes/No
84	7	**Does your organization support SNI Custom SSL for the customers?** Yes/No
84	8	**Does your organization allow customers to custom configure the domain?** Yes/No
86	9	**Does your organization support SSH connection for the customers?** Yes/No
93	10	**Does your organization provide data encryption for the customers?** Yes/No
87	11	**Does your organization allow customers to use their own encryption mechanisms to use services?** Yes/No
95	12	**Does your organization provide incident response in order to organize approaches to addressing and managing the aftermath of a security breach or attack?** Yes/No
96	13	**Does your organization allow customers to secure their virtual servers?** Yes/No
96	14	**Does your organization allow customers to implement their own security architecture?** Yes/No
97	15	**Does your organization allow customers to secure and manage access from clients, such as PC and mobile devices?** Yes/No
98	16	**Would customers' data be encrypted while in storage and when being transmitted over the Internet?** Yes/No

Table 4-1 Questionnaire for the Cloud Provides

[49] Q refers to question. The questions are mapped to the relevant metrics, for example question 1 is mapped to metric 79.

4.3.1.1.2 Cloud Consumer Questions

Cloud consumer questions are designed in order to evaluate provider information. The quality of the information is vital for the customers because important decisions are always made based on its quality, such as evidence of its authenticity, reliability, credibility, reasonableness, fairness, objectivity, moderateness and consistency. However, there is no single perfect indicator of reliability, truthfulness, credibility or value [8]. If we need evidence to support (or rebut) a provider's claims, such evidence will be more compulsive if it is derived from a respected and trusted source. Therefore, we generate opinion/feedback questions about a provider's services to the customers to ensure that the data is indeed reliable.

We designed the questionnaire to contain 30 items which aggregate cloud consumers' responses in order to reach the desired outcome. For instance, some of the questions which began with 'How satisfied are you with'. These questions can be used to measure the level of satisfaction for the services. Other questions which began with 'Does this cloud company provide'. These questions check the validity of providers' information.

Map Q with metrics	#	Cloud Consumer Questions Security Survey Questioner
79	1	**How satisfied are you with the VPN connectivity to the VPC networks provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
82	2	**How satisfied are you with the network link dedicated for the compute instance?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
80	3	**How satisfied are you with the network link shared with other VMs on the same host?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
83	4	**How satisfied are you with the SSL certificates provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
85	5	**How satisfied are you with the SSL content delivery provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
85	6	**How satisfied are you with the dedicated IP Custom SSL provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
84	7	**How satisfied are you with the SNI Custom SSL provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
84	8	**How satisfied are you with the custom domain configuration provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
86	9	**How satisfied are you with the SSH connection provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
93	10	**How satisfied are you with the data encryption mechanism provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
90	11	**How satisfied are you with the ease of obtaining information about physical security from the provider's web page?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
91	12	**How satisfied are you with the ease of getting information about internal control from the provider's web page?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
94	13	**How satisfied are you with the cloud provider IAM program?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

Table 4-2 Questionnaire for the measurement of satisfaction level

Map Q with metrics	#	Cloud Consumer Questions Security Survey Questioner
79	1	**Does this cloud company provide the VPN connectivity to the VPC networks for the customers?** Yes/No/Don't know
81	2	**Does this cloud company disclose confidentiality and integrity checking algorithms as means of securing?** Yes/No/Don't know
82	3	**Does this cloud company provide dedicated network link for the compute instance?** Yes/No/Don't know
80	4	**Does this cloud company provide shared network link for the compute instance?** Yes/No/Don't know
83	5	**Does this cloud company support any SSL certificates?** Yes/No/Don't know
85	6	**Does this cloud company support any SSL content delivery?** Yes/No/Don't know
85	7	**Does this cloud company support dedicated IP Custom SSL for the customers?** Yes/No/Don't know
84	8	**Does this cloud company support SNI Custom SSL for the customers?** Yes/No/Don't know
84	9	**Does this cloud company allow customers to custom configure the domain?** Yes/No/Don't know
86	10	**Does this cloud company support SSH connection for the customers?** Yes/No/Don't know
93	11	**Does this cloud company provide data encryption for the customers?** Yes/No/Don't know
87	12	**Does this cloud company allow customers to use their own encryption mechanisms to use services?** Yes/No/Don't know
95	13	**Has the provider ever experienced a security breach?** Yes/No/Don't know
96	14	**Has the provider ever allowed you to secure your virtual servers?** Yes/No/Don't know
96	15	**Has the provider ever allowed you to implement your own security architecture?** Yes/No/Don't know
97	16	**Does this provider allow you to secure and manage access from clients, such as your PC and your mobile devices?** Yes/No/Don't know
98	17	**Have you ever had a bad experience with encrypted data while transmitted over internet?** Yes/No/Don't know

Table 4-3 Questionnaire for validating security information

4.3.1.2 Polls Forum

Another approach to gathering data from the crowd can use polls forums which are collaborations between all the stakeholders such as providers, consumers and system administrators. In fact, one of the main requirements of the polls forum is stakeholder identification. We should keep a record of the stakeholders' contributions. This can easily become a challenge when the stakeholder is required to participate in the different parts of the application. We characterized the accessibility of peer stakeholders in section 4.1. According to the level of permission, stakeholders can alter or even delete each other's stakeholders' comments in order to correct, update and improve. In general, this is the case when stakeholders come together to build something in a highly collaborative way.

Polls forums are classified using SMI security attributes such as access control and privilege management, data integrity, privacy and loss, physical and environmental security, proactive threat and vulnerability management, retention and disposition. According to each of the categories, the crowd can contribute either by writing new reviews, or by commenting and voting on existing ones. They can express explicitly their opinion of the service attributes. These contributions are aggregated in what in the studies is referred to as an integrative approach [29], thus providing in most cases a comprehensive review of the service.

The aim of using the SMI security characteristics are: (1) As SMI is a known framework so we mapped our categorisation to something which has been used so far in the cloud environment, (2) Making it much easier for the end user to distinguish between security characteristics, (3) Our idea is to extend our work to all the other cloud computing characteristics. We found the SMI to be a comprehensive framework which details all the different cloud characteristics as well, (4) MODAClouds categorisation are also defined based on the SMI characteristics, and as this thesis is a collaborative work we have to follow some common mandatories. For these reasons we have a better chance of measuring and validating each provider based on the SMI characteristics.

4.3.1.3 Questionnaire Validation

In order to assure the quality of the crowd's answers, we restricted the distribution of the different categories of questions to the skilful and trusted professional members of the company. These groups can be identified by senior employees. Moreover, they should have enough knowledge of the security and privacy strategies that apply to their company.

Questionnaire validation should be considered as a collaborative enterprise, for which the responsibility should be divided equally between all the stakeholders and in which the identified employees are expected to share correct information about their company. However, expectation alone is not enough and the information provided needs to be validated. In this case, we designed a set of questions about the provider's service, based on the respondent’s level of agreement with the statements of satisfaction,

Below is an example of users' rates of agreement for each of the questions. As can be seen, ‘Strongly Agree’ has only been selected by one user for Q1 whereas ‘Strongly Agree’ has been selected by twelve users for Q2. However, this interpretation alone is too simplistic as there are different numbers associated with each group. Even, if we use a percentage instead, it will still be difficult for the reader to quickly reach an accurate interpretation. To improve readability we used Likert scale.

	Strongly Agree	Agree	Disagree	Strongly Disagree
Q 1	**1**	**2**	**10**	**2**
Q 2	**12**	**3**	**11**	**3**
Q 3	**3**	**14**	**12**	**0**

Table 4-4 Example of Likert scale

The Likert scale measures the level of agreement relevant to each service. The following table shows how satisfaction levels are evaluated relative to each provider statement. Point have been assigned to each of the levels as follows: Strongly Agree (4), Agree (3), Disagree (2) and Strongly Disagree (1)

Then, we use the equation

$$\frac{1}{n}\sum_{l=1}^{levels} N_l P_l$$

to calculate the average for each major.

- $levels$ represents the number of levels we have. The number of levels can be four, as shown in this example, or there could be five levels were we to include 'Neither agree nor disagree'.
- P_l represents the point which has been assigned to each of the levels.
- N_l represents the number of the users who selected option x.
- n represents the total number of respondents for each question in the questionnaire.

According to Table 4-4, the equation to use for the first group is:

1*4 + 2 *3 + 10*2 + 2* 1 = 32

So following the formula 32/15 =2.13 provided the average for this major.

Factors		Satisfaction
Q1	(n=15)	2.13
Q 2	(n=25)	3.28
Q 3	(n=10)	7.8

Table 4-5 Example of measuring satisfaction level

This method clearly indicates the level of customer satisfaction for each of the provider statements and can be used to demonstrate satisfaction levels for each service.

Other types of questions require the answers 'yes', 'no', 'don't know'. We have opted to use the mean harmonic for them because this average penalises rates that are very different from one another. Moreover as we have no knowledge of what the answers should be, or what is the importance of each of them, we cannot assign any weight to them, and so they all carry the same importance. On the other hand, as our data set so far is small, we will probably have to do an outlier removal. In the case of opinion

questions, we would argue that some people tend to answer randomly or inconsistently or using the extreme values of the scale (e.g. everything is bad). These specific entries should be detected and eliminated and consider as outliers. The following formula shows how the Harmonic Mean works.

$$HM = \frac{n}{\sum_{j=1}^{n} \frac{1}{x_j}}$$

Where n represents the total number of samples, and x_j represents the value of each sample.

4.3.1.4 Polls Forum Validation

We used a five-star rating mechanism (1-worst, 5-best) to assess the SMI security characteristics for each provider. In this case, the user can be asked to compare and rank his level of satisfaction. The overall provider rating can be determined based on the number of rates he receives. Table 4-6 shows an example of how a rating mechanism is used for measuring corresponding SMI characteristics and overall provider rating. We use the Harmonic Mean in order to rate the SMI characteristics.

- $\boldsymbol{c_x}$ rates an SMI characteristic by calculating the mean harmonic among all users which have rated this feature. $\boldsymbol{c_x} = n/\sum_{i=1}^{n} \frac{1}{u_i}$
- $\boldsymbol{u_y}$ rates a provider by calculating the mean harmonic among all the SMI characteristics which are rated by an user $\boldsymbol{u_y} = m/\sum_{j=1}^{m} \frac{1}{c_j}$
- $\boldsymbol{\bar{P}_r}$ is the final rate for a provider by calculating the mean harmonic among all SMI characteristics and also among all users which have rated a provider so far $\bar{P}_r = \frac{n*m}{\sum_{j=1}^{n}\sum_{i=1}^{m} 1/u_i c_j}$

Characteristics / user	C1	C2	Per user
U1	★★	★★★	2.5
U2	★★★★	★	2.5
U3	★★★★★	★★★★	4.5
Per characteristics	3.67	2.67	3.17

Table 4-6 Provider Assessment

Prior research has suggested that a mean rating of 4 on a five point scale indicates a good level of service satisfaction. We argue that a mean value of between 4 and 5 indicates that the provider satisfies a particular SMI characteristic. Table 4-7 shows customer satisfaction levels with scores. We use this in order to interpret the results.

★	★★	★★★	★★★★	★★★★★
Very dissatisfied	Somewhat dissatisfied	Neither satisfied nor dissatisfied	somewhat satisfied	Very satisfied

Table 4-7 Customer satisfaction- Wikipedia

4.3.2 Data Gathering Mechanisms through the CSA CCM

As previously mentioned, CSA CCM is a security control matrix which includes essential security principles for assessing and clarifying overall security risk in the cloud. CSA CCM provides a detailed understanding of the security concept in order to assist prospective cloud consumers to simplify and accelerate the vetting of providers, while ensuring a more consistent level of security practices by cloud providers on a global basis.

CSA is considered as a main security data source for the following reasons:

- The variety of the security controllers in CCA CCM. It has supported 16 different domains (e.g. compliance, data Governance, facility security, human resources, etc.) with 136 controllers (e.g. audit planning, employment termination, management program, utility programs access, non-disclosure agreements and policy) which have considered all the security issues in detail [18].
- The availability of security cloud information. CSA provides self-assessment and certification for the cloud providers. In that way, every company can participate in the STAR program and complete the assessment form which is a set of consensus assessment questions, and then submit it to the CSA STAR repository for public accessibility. According to the number of STAR repositories, almost 120 providers have done the self-assessment of whom 18 have obtained the certification and of whom 2 have completed the attestation.
- The acceptability of the CSA CCM security control framework by the big providers. CSA CCM is an acceptable security control framework for most of the big companies such as Amazon, Azure, Rackspace, and HP etc. all of whom have participated in and completed the self-assessment.
- Most of the best security practices have been encapsulated in the CSA CCM. There is a mapping to most of the leading existing standards and certifications such as SMI, AICPA, COBIT 5.0, COPPA, ISO/IEC 27001, NIST, etc. with CSA security controllers. In fact, CSA identified most of the security controllers and then, mapped them to the security clauses and sub clauses of the known standards. The controllers and sub-controllers were assessed for multilayers architecture in SaaS, PaaS and IaaS.

For the above reasons, we selected CSA as a data source to assess the level of security in cloud service providers.

4.3.2.1 Overall View of CSA CAIQ

The following conceptual model abstracts the different components and their relationships. As illustrated in Figure 4-2, each provider can fulfil one or all of the security requirements of the CSA sub-controllers. Moreover, each controller contains a set of sub-controllers. Sub-controllers are the same as the security assertion questions which were discussed earlier. The main idea behind CSA is to map its security controllers to the several known certifications and the best practices. Therefore, users can gain a comprehensive knowledge of security concerns in a particular cloud service provider without needing to have a general knowledge of each certification. In fact the end user does not need to worry about what the certifications' scopes are, instead he only needs to follow up the sub-controller so that he can compare different security criteria among several cloud providers in a much easier way. As shown below, the clauses are used as a bridge between the certification and the CSA controller.

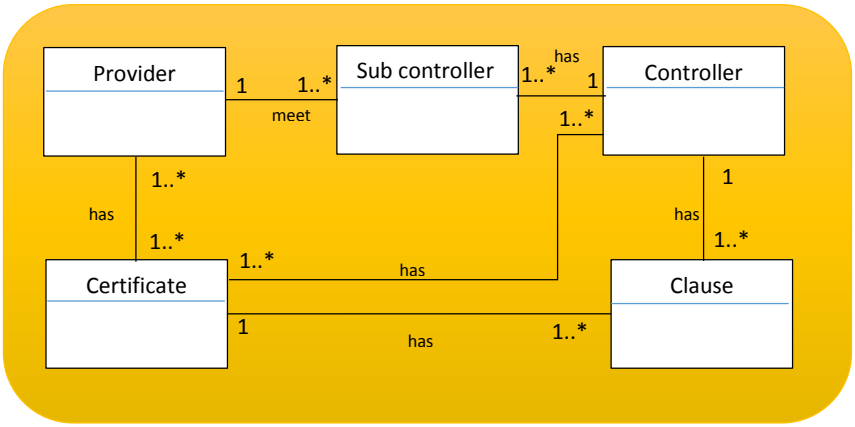

Figure 4-2 Conceptual Model of CAIQ

4.3.2.2 The Advantage to Present Data from CSA repository in an User Friendly Way

CSA STAR repository contains a list of 120 different cloud providers' consensus assessments. As discussed earlier, CAIQ is provided in the pre-created Excel template which can cause several problems.

Cloud consumers should go through a slow consolidation process in order to extract security information. This process includes checking manually, and comparing 136 different security controllers among 120 different cloud providers. Thus, the end users would have to collect the data from different files and spreadsheet, consolidating it, summarizing the information, and submitting the final result to their departmental heads in order to reach a decision, all of which is a time consuming process.

Also spreadsheets are clearly susceptible to errors and everyone involved in information processing, especially cloud providers, has to be careful to maintain data integrity. Hence, it would be prudent to double-check as much as possible. However, in some cases, the provider does not store data uniformly. This means that some providers do not follow the exact same protocol as others. Some, like Amazon and Azure, use Word or Pdf for CSA assessment instead of Excel templates. So, end users are forced to go through the entire document in order to find the particular piece of information they need.

With the growing number of cloud provider assessments in CSA STAR, we are likely to encounter more problems which can be extremely challenging to spot and rectify especially with larger volumes of data. The increased likelihood of data errors is almost inevitable with larger quantities of information. Furthermore all formats, such as Excel, Word and Pdf documents, can easily become too complex, and can inhibit quick data analysis, and prevent a clear perception of what is relevant. All these factors cause difficulties in decision making when selecting an appropriate cloud service provider.

Providing information in Excel, Word and Pdf format is not the best option as it can waste customer time validating and tracking data. Instead, there is a clear need to present these data in a concise and economical way. Currently, however, there is an obvious lack of proper presentation of CSA security assessment information in the STAR repository.

To rectify the situation, we introduce into our platform a visualization tool. This tool provides the customer with information about the security issues of the variety of cloud providers in a more efficient way by means of a graphical user interface. The use of this approach saves customers a great deal of time and provides a better assessment solution.

4.3.2.3 Needs for CSA Visualization

Employing visualization technique helps us to see the pattern and connection between all of the data in the CSA STAR repository. It allows us to focus solely on the information that is considered to be important. In this way, end users can explore all the information with their own eyes. They can also gain a better insight into the selection of a suitable provider who can match their requirements.

Visualization is a form of information compression, and is a method of compacting an enormous amount of information into a very small space thus enabling the instant visualisation of any answer to any question. It takes the form of an information map which gives a complete and comprehensive picture of all the existing data. It also provides user friendly features that facilitate the process of extracting the data from Excel documents, and it makes interaction with the CSA much more comprehensive. In general, the display of information in a visual format enables us to make more sense of the data and gain an overall perspective.

The conceptual model presented as our prototype appears in Figure 4-2. The visualization prototype is comprised of four basic building blocks: certificate, controller, sub-controller and provider. The first block lists the number of certifications, regulations or standards. Each of these provides benefit and supports every industry and domain.

Sometimes, understanding relevant benefits across the other certifications is not an easy task for end users, and it requires an extensive knowledge of particular certifications' scopes (what it is, how it works, which certificates are preferable). The main task in CSA is to map CSA security controllers with the relevant security clauses of each certification. Making a connection between certifications and CSA controllers gives an extensive understanding to both sides. On the one side are relevant security issues which are discussed in each certification, and on the other side are common attributes which are offered by CSA.

In fact, the end user doesn't need to have a general knowledge of the variety of certifications' scopes in order to select an appropriate provider that matches his requirements. He only needs to explore the CSA controller or sub-controller in order to achieve two objectives which are to discover which certification fulfils his needs, and which provider matches his specifications.

The second block lists all the security controllers mentioned in CSA CCM and adds the functionality of selecting desired controllers based on them. The third block lists all the relevant sub-controllers for each controller, and adds the functionality of selecting desired controllers based on them. Therefore, the selection of an appropriate cloud service provider can be done through controllers and sub-controllers. Finally, the fourth block of the visualization process involves a list of the cloud providers which fulfils the CSA sub-controller requirements. Table 4-8 is an example of how CAIQ CSA looks. Appendix M demonstrates a complete example of CAIQ V 1.1 for a provider called, the Terremark.

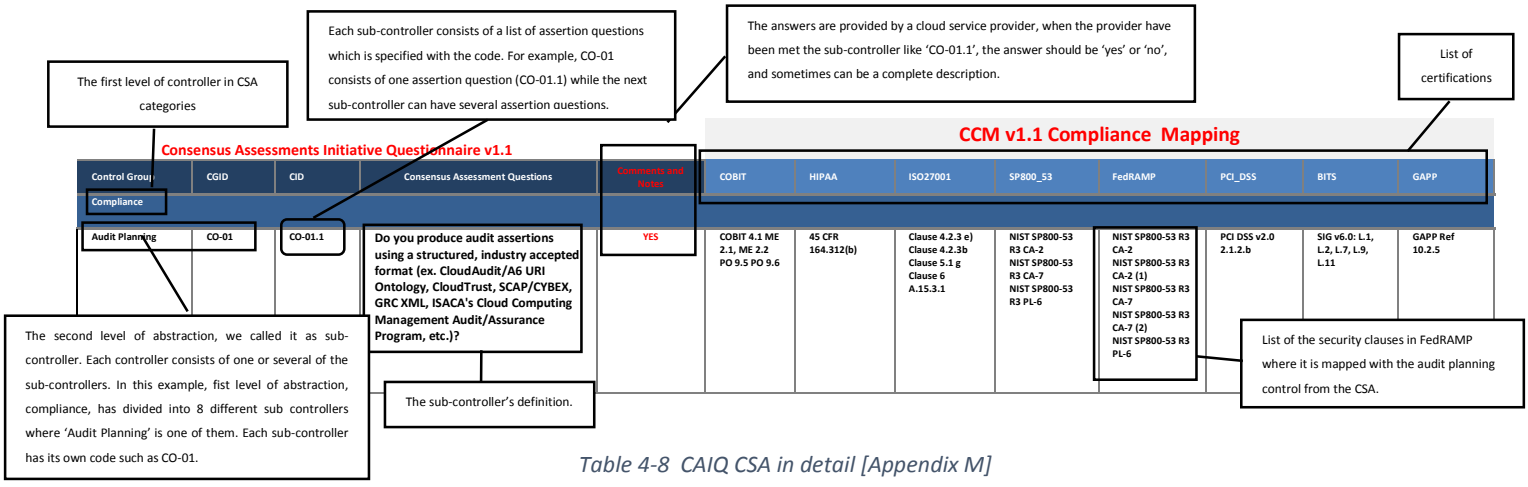

Table 4-8 CAIQ CSA in detail [Appendix M]

CSA Visualization gives two pieces of security information to help us choose a provider:

We can either select an appropriate cloud provider based on the particular controller and sub-controller in the simple way outlined above or we can investigate in more depth to discover whether or not a particular certificate satisfies all the CSA controllers. In other words having some controllers can be the equivalent of having some of the best practices. We have tried to select a visualization technique that makes it easier to determine whether a particular cloud provider can fulfil customer's requirements.

Figure 4-3 illustrates our concept of the visualization structure. Clearly a hierarchical structure exists between all the blocks which at first sight may appear to be tree hierarchical. This however is not the case as there is a cycle between the nodes. In fact, there are parent/child relationships between the different hierarchical levels, for example the provider level can have several parent nodes, so the relationships can be complicated because of the growing number of providers, and therefore a lot of edges can be revealed. To summarize, visualization shows a representation of the fulfilment of CSA sub-controllers by each provider using an extensive parent/child structure.

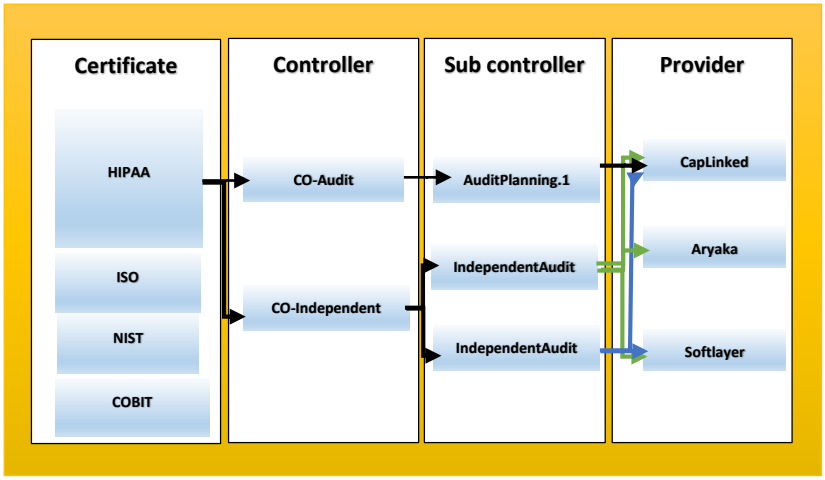

Figure 4-3 Conceptual view of the CSA visualisation

The results which have obtained from the CSA visualisation tool are shown in the Figures 4-4 and 4-5.

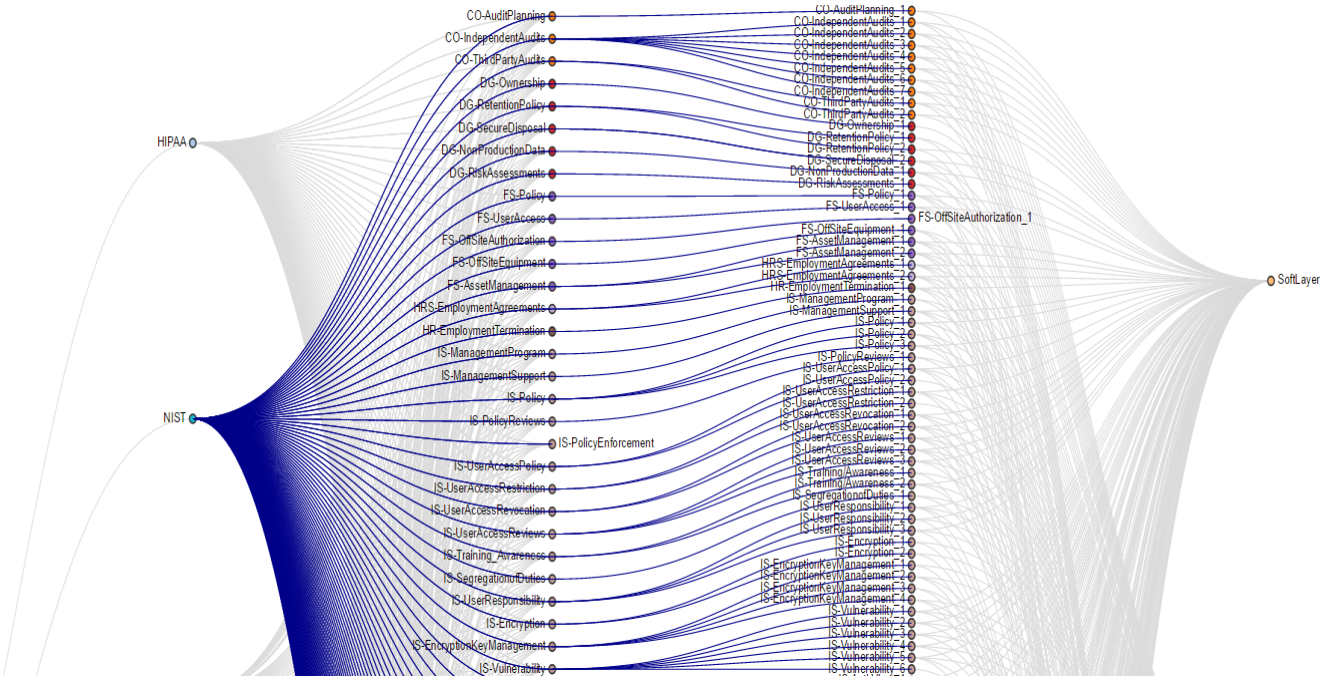

Figure 4-4 Visualisation (NIST consists of several controllers and sub-controllers).

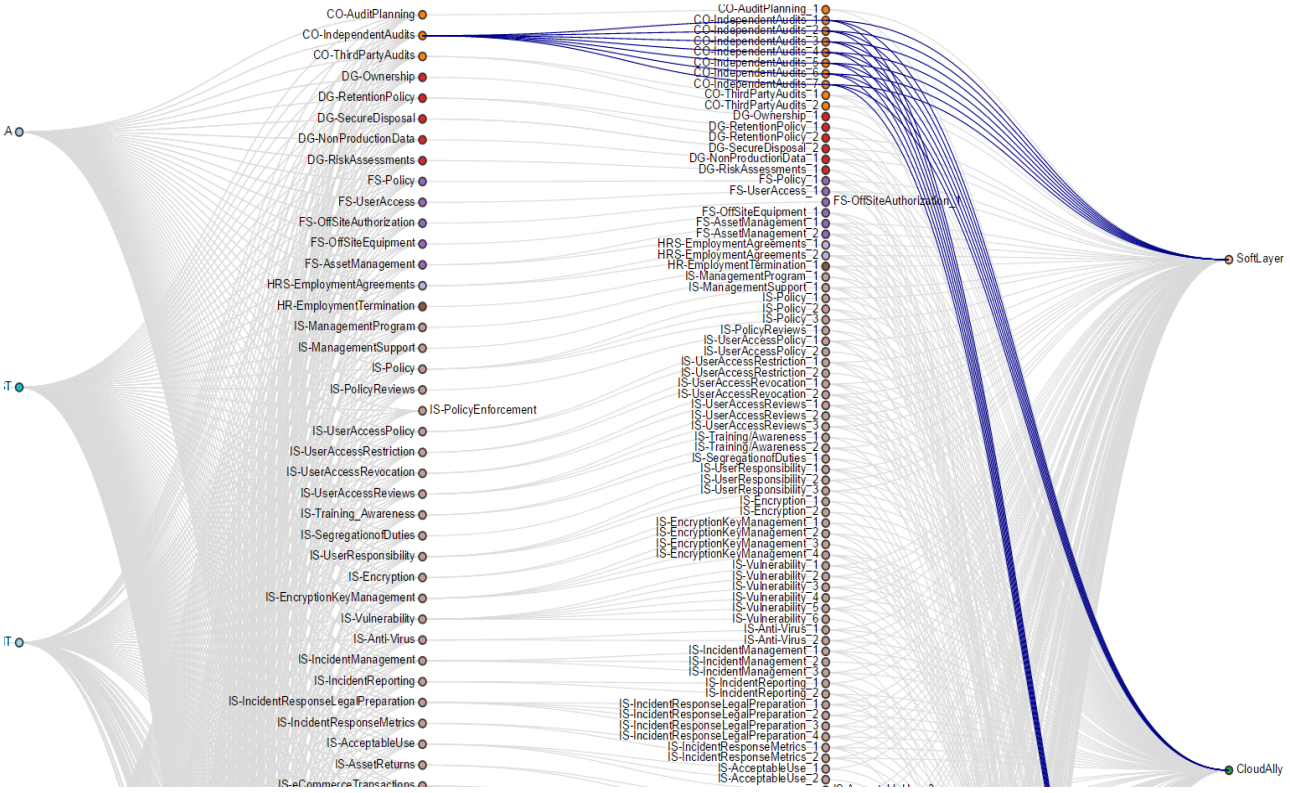

Figure 4-5 Visualisation view (The controllers/sub-controllers can be fulfilled by one or more providers).

4.4 Generalized Data Gathering in Crowdsourcing

As mentioned in Table 3-1, four different categories are proposed in cloud computing where the SMI characteristics are mapped. However, we have selected to base our work on security characteristics.

In this section, we generalize our idea to cover other categories such as operational and technical characteristics as well as security characteristics because they are all essential, each playing an important and critical role in the cloud environment. We also considered these two characteristics in designing a methodology to gather relevant cloud data from the crowd.

Generally speaking, collecting data through the crowd (e.g. end users) can be used to validate cloud provider information. Usually, we use this information in order to measure the validity of the providers' statements. On the other hand, providers can help to complete the incomplete part of information and present it in a comprehensive way to the end users. The following figure shows the flow of the process, most of the steps track the similar flow as described in Figure 4-1.

A list of critical questions was designed for both providers and consumers which they were then asked through the crowd sourcing platform. The mechanism for gathering data is similar as previously explained. In order to gather relevant data for each of the cloud metrics, end users still use different approaches such as forums and questionnaires.

The following figure shows the block diagram for the data collection process for generic cloud characteristics such as technical and operational characteristics.

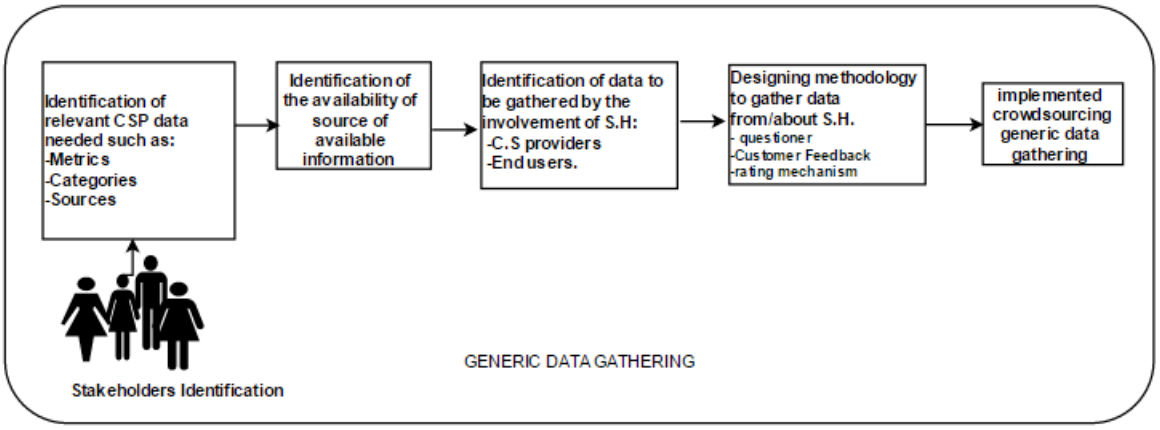

Figure 4-6 Block diagram for the generic data gathering through the crowd

Below we differentiate between generalised data gathering and security data gathering.

- **Stakeholders and their contribution**

  Although the role of stakeholders, as previously defined in 4.1, remains unaltered their contributions have been changed. As discussed earlier, in some cases, gathered information is not corrected because of some technical and logical reasons. So if cloud service providers can revise their company's information we can be sure that the information will be correct. As mentioned earlier, cloud data is usually gathered from external data sources such as APIs and web scrapping techniques. For this reason, we have decided to ask providers to complete questionnaires or forms to guarantee the authenticity of the information. Such information needs to be verified, and this should be done by involving stakeholders such as providers and cloud consumers. We ask providers for their collaboration in modifying any incorrect and incomplete parts of their own information. For this reason, we have designed a form which includes suspect information from providers' web pages, and which we ask providers to confirm and modify as necessary. Therefore, should there be a need for any modification of outdated and incorrect information, cloud providers are able to fulfil this role and so enable us to deliver enriched data to the end users. From the previous sections, we already know that cloud consumers are able to rate and comment on any of the providers' statements. For example, in the case of questionnaires they can rate providers against levels of service satisfaction. Polls forum can rate providers from one to five (where one is worst and five is best) regarding the SMI characteristics and in customer validation questionnaires, customers can comment on whether or not they agree with the current information.

- **Identification of the Relevant Data**

  We have already provided a list of the relevant metrics for other cloud computing characteristics such as operational and technical as well as security characteristics in Chapter 3. Those metrics are related to information that is not available on the provider's webpage and we must gather them through the crowd. We have identified this data, as we have done previously for the security data, and then we have provided a list of the operational and technical questions which we need to ask the stakeholders. For instance, we classified operational characteristics according to metrics such as support, availability of comprehensive and high-quality documentation etc. In addition to that, we classified technical characteristics according to metrics such as availability of fault tolerance features, service availability etc. It should be noted that we designed the questions for all types of services such as PaaS, CDN, SaaS, IaaS, etc. (Table 4-9, 4-10 and 4-11)

- **Mechanisms for Gathering Data from Stakeholders**

  The mechanisms for gathering data is the same as before using forms, forums and polls. The only difference is that providers are able to manipulate data gathered using other web techniques such as API and web scrapping. Extracted data can be error-prone and we want to correct and enrich those data by collaborating with the provider on our platforms. For example such information can be gathered by CSA forms. On the other hand, information manipulation by providers can help to reduce the number of errors in existing information. While programing errors can cause machines to produce unintended results, revision of these outcomes by users can rectify the situation, and enable us to provide accurate and enriched data.

  Polls forum can be extended to other SMI characteristics where they can be matched with the operational and technical characteristics of the cloud. We have tried to retain, with some modifications, the same approach as we used earlier for the security characteristics. The mapped characteristics of SMI with our categorisation are shown in Table 3-1.

  The scope of questionnaires can be widened to include a list of operational and technical questions. Lists of the identified matrices for each category along with lists of the designed questions are proposed in Table 4-9, 4-10 and 4-11.

- **Validation Techniques**

  As discussed earlier, validation is an important issue in crowdsourcing platforms. We have discussed validation techniques in 4.3.13 and 4.3.1.4. We used the same techniques in the generalized data gathered through the crowd, and we also added some questions regarding each cloud provider, for instance 'Does this information need to improve?' Should there be a need for improvement, end users can modify or suggest new provider statements, so if cloud consumers have any suggestions to improve existing information they can pass these on to the cloud providers. These contributions will be used to improve information quality, and may be used by providers or system administrators to update existing information.

4.4.1 Generic Cloud Consumer Questions

Below is a list of the customer satisfaction questions which involves most of the service's models such as PaaS, CDN, etc. Moreover the answers are measured by the Linkers scale. These questions are repeated for each cloud service provider in order to be able to rate them. There are two types of questions. The first

table shows the customer satisfaction questions in which the questions began with 'How satisfied are you' [Table 4-9]. The second table shows the validation of the cloud services' information, questions which began with 'Does, Is, Have etc.' [Table 4-10]. The questions are designed separately for the end users and later for cloud service providers. For further details refer to Appendix I and J.

Map Q with metrics	#	End Users Questions Generic Survey Questioner – part one
107	1	**How satisfied are you with the way which the data in the cloud is integrated with your company data?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
8-9	2	**How satisfied are you with the quality of non-technical support in this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
1-2	3	**How satisfied are you with this cloud provider´s certifications?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
1-2	4	**How satisfied are you with the way the cloud provider´s certification meets your needs?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
8	6	**How satisfied are you with the technical support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

Table 4-9 Generic Survey Questioner (1) -Measuring satisfaction level

Map Q with metrics	#	End users Questions Generic Survey Questioner – part two
107	1	**Is your current business environment compatible with this cloud service?** Yes/No/Don't know
113-114	2	**Does the provider allow customers to move data on and off storage as needed?** Yes/No/Don't know
115	3	**Can the data stored by this service provider be exported at your request?** Yes/No/Don't know
5	4	**Have you had any bad experiences regarding authorization access to your data?** Yes/No/Don't know **If Yes give a brief summary**

Table 4-10 Generic Survey Questioner (2) - Validating provider information

4.4.2 Generic Cloud Provider Questions

The following table shows the list of questions designed to be answered by cloud service providers. These questions help customers to find the answer to the more frequently repeated queries that appear in cloud consumer forums or web blogs, where they cannot find such information easily through the cloud service providers' web page. For further details refer to Appendix K.

Map Q with metrics	#	Generic Cloud Provider Questions Generic Provider Questioner
5	**1**	**Apart from your company, can anyone else access the customer data?** Yes/No **If Yes, Who? Under what conditions? At what level are they allowed access?**
52	**2**	**Are there Service Level Agreements (SLAs) that back everything up?** Yes/No
56	**3**	**Does your organization work with third-party suppliers?** Yes/No
7	**4**	**Does your company provide a data processing agreement with customers?** Yes/No
9	**5**	**Does your organization provide sales/ financial supports for free?** Yes/No
10	**6**	**Does your organization support ticket systems?** Yes/No

Table 4-11 Generic Provider Questioner

5. Technical implementation

Figure 5-1 illustrates an actor diagram of the application and their tasks. By employing collaborative techniques between different stakeholders, this application gathers relevant data from cloud service providers which it then uses to enrich existing DSS dataset by storing accurate data. We already know that DSS tools need to store accurate and correct data from cloud service providers, and that they aim to deliver high quality results to the end user. The interaction between the stakeholders and the rest of the components can be clearly seen in the figure below.

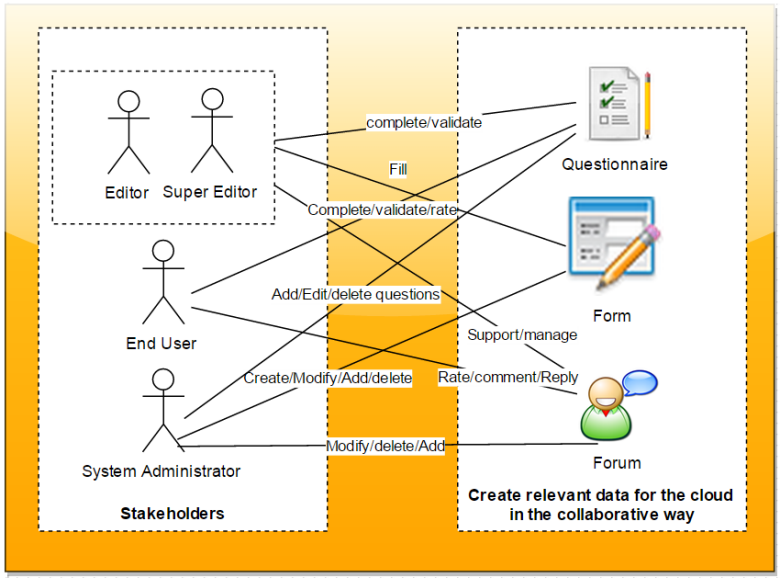

Figure 5-1 Actor diagram - Data gathering by using crowdsourcing techniques

This figure displays data entry approaches and is used to enrich the data set. The types of data entry which are used in the application are: forms, forums, polls and questionnaires. The web site provides the four different stakeholders – System Administrator, Super Editor, Editor and End User. The privilege level is defined from left to right where the system administrator has the highest level of permission and the End User has the lowest level of permission. For instance, the system administrator is able to add new administrators to the system with the same permission as he has. In general the role of a system administrator includes complete control over the whole system. It can easily modify, delete, create or add users, roles, groups of questions, comments and replies.

The system administrator and Super Editor have access to the user management screen. They can delete or modify the users and their associated roles. The difference between these two roles are that System

Administrator has control over whole the system while Super Editor has control only over its internal groups defined by the company and can only add internal users in his system.

In fact, the Supper Editor is a senior person inside a provider's company who is interested in collaborating and sharing company information with our application. He is an identified person who has the highest responsibility after System Administrator for assigning tasks to his group. One of these task is the identification of specialist groups inside the company called Editors. These Editors can be specialists in different subjects such as security, legal, privacy, etc. Their task is to respond to the questionnaires, to follow up the polls forums and to complete forms.

Finally, the End Users are groups of people who derive many benefits from the whole system. As defined previously, they can either be cloud brokers or cloud customers.

To enhance the quality of the cloud data, we applied existing validation methods to evaluate the user rating mechanism in the questionnaire and polls forum by employing the Likert scale and the mean harmonic respectively. In fact our assessment of the validity of the information informs us about the extent of the end user's satisfaction with the provider's statements.

Figure 5-2 displays the architecture diagram of our application. The backend and server part of the system which will be described in detail.

The data entry process also uses the Cloud Security Alliance for the visualization of security. Finally, the results of our work are data gathering through the crowd using rating mechanism, and CSA visualisation tool.

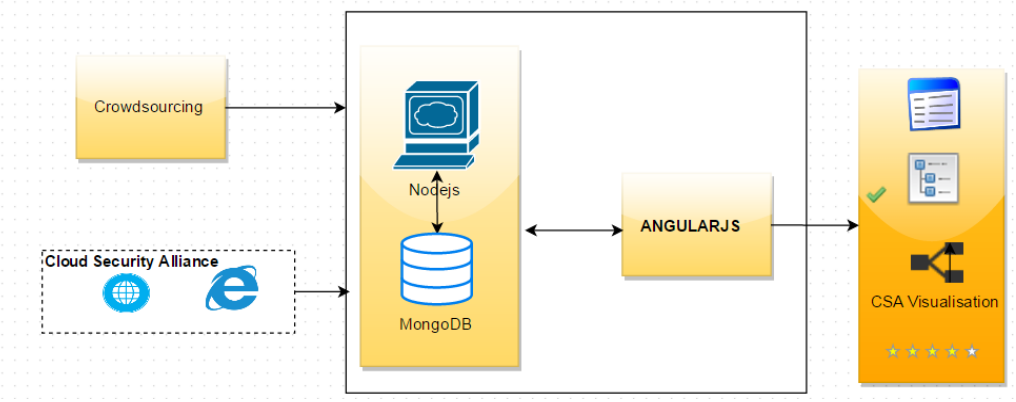

Figure 5-2 Architecture Diagram

5.1 Functional Requirements

The functional requirements describe a set of system's behaviours and technical details that define what a system is supposed to do. The website contains various different pages. All the functional requirements associated with each page are listed in the following tables.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
Screen			
FR001	All	The website shall have the following screens: Home page, CSA (Cloud Security Alliance) page, Polls, Settings, Login page	The key features of the system shall determine this structure.
Homepage			
FR002	All	The home page shall list different cloud providers and their associated information like location, type of services, support options and security certifications	Associated cloud data shall exist in the system.
FR003	All	On the homepage, visitors shall be able to review all the provider information.	Associated cloud data shall exist in the system.
FR004	All	The homepage shall have a search and sort option based on the name, number of services, location etc.	Associated cloud data shall exist in the system.
FR005	Super Editor/ Editor	Registered providers shall modify incorrect and outdated information for their own record.	Eligible users shall exist in the system. Eligible users shall login into the system.
FR006	End User	Logged in users shall be able to give their feedback related to a provider.	Eligible users shall exist in the system. Eligible users shall login into the system.
FR007	All	Each provider shall have a polls forum. In the polls forum all the stakeholders shall interact and exchange opinions.	Associated cloud data shall exist in the system. All the eligible participants to the system shall contribute to it.
Login/Log out/Sign Up			
FR008	All	The website shall have a login page. Registered users shall input their email and password and click on the Login button to login into the system	The user shall exist in the system. The user and its associated data shall be valid.
FR009	All	The system shall provide Single Sign On(SSO) integration with Google, Facebook and LinkedIn	The user shall be valid. The associated information shall be valid.
FR010	All	The website shall provide a sign up page.	The user shall not exist in the system. The user and its associated data shall be valid.
FR011	All	The user shall be able to register by giving name, email address and desired password	The user shall not exist in the system. The user and its associated data shall be valid.
FR012	All	Email address shall be unique for registering	Users shall exist in the system. The user shall login into the system. The email shall be reparative and shall be valid.
FR013	All	The website shall provide logout functionality.	Users exist in the system. The user shall login into system.
FR014	All	The logged in user shall be redirected to the homepage after logout from the system.	Users shall exist in the system. The user data shall be valid. The user shall login into system.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
			The system shall redirect to the homepage.
FR015	All	The sign in page shall redirect to home page once login is success	The user doesn't exist in the system. The user data shall be valid. The user shall sign into the system. The system redirects to the homepage.
FR016	All	The system shall show an error message and redirect to the login page if a visitor tries to access any non-privileged areas.	A visitor performs a prohibited tasks.
FR017	All	Logged in users, shall see their name in the toolbar as for example: 'Welcome Maryam'	The user shall exist in the system. The user data shall be valid. The user shall login into system. The system shall redirect to the homepage. The system shall display the user's name.
Polls Forum			
FR018	All	The polls forum shall be the page listing all the security SMI characteristics for a provider.	The provider data shall exist in the system SMI characteristics shall exist in the system. A system shall exist to rate each characteristic. The user shall login into the system to make a contribution. All the eligible participants to the system shall contribute in the polls forum.
FR019	All	The polls forum page shall present a short summary about the provider.	The provider's data shall exists in the system.
FR020	All	The poll form page shall display the current ratings and comments of the provider to any visitors.	SMI characteristics shall exist in the system. A system shall exist to rate providers. A system shall exist to make comments. The user shall have already defined the comments. The user shall have already rated the SMI characteristics. All the eligible participants to the system shall contribute to it. The system shall display existing ratings and comments.
FR021	End User	Logged in users shall give ratings and comments for each SMI characteristic.	The user shall exist in the system. The user shall login into the system. SMI characteristics shall exist in the system. There shall be a system to create a rating campaign. A system shall exist for the creation a comments. The comments shall already have been defined. The user shall have already rated the SMI characteristics. All the eligible participants to the system shall contribute to it.
FR022	End User	The system shall evaluate user ratings in the polls forum based on the harmonic mean.	The user shall exist in the system. The user shall login into the system. SMI characteristics shall exist in the system. There shall be a system to create a rating campaign. A system shall exist for the creation of comments. The user shall have already evaluated the SMI characteristics. All the eligible participants to the system shall contribute to it. A provider evaluation shall have been given by the system to the end user. All the eligible participants to the system shall contribute to it.
FR023	End User	The system shall provide rating modifications for each user.	The user shall exist in the system. The user shall login into the system. The user shall have defined the ratings. System shall store all the modification in the system.
FR024	End User	The user shall rate one or more SMI characteristics.	The user shall exist in the system. The user shall login into the system. SMI characteristics shall exist in the system. There shall be a system to create a rating campaign. There shall be a system for the creation of a rate of the SMI characteristics. The end user shall have already evaluated the provider. There shall exist an SMI rating to be evaluated.
FR025	All	In the polls forum ratings shall be displayed in a numeric and a visual (stars) way.	The user shall have rated the cloud SMI characteristics. There shall be a system to create a numeric view of harmonic mean as well as visualize view of the harmonic mean.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
FR026	End User	Visitors shall click on the comments link next to SMI characteristics to open the comments page.	The system shall redirect to the comments page. A list of the comments for each SMI shall exist in the system. The system shall keep track of the authors. All the eligible participants to the system shall contribute to it. Visitors shall not able to comment on any post unless they login.
Comment Page			
FR027	All	The comments page shall display all the previous comments and the names of the authors.	Comment shall already have been defined in the system. Previous comments shall exist in the system. The system shall keep track of the authors. Authors shall exist in the system. The system shall display the names of the authors.
FR028	End User	The comments page shall provide a 'like' option to show how many people agree with the other comments.	Comments shall have already been defined already in the system. The system shall keep a count of 'likes' comment in the system. All the visitors to the software system shall see the number of 'likes'.
FR029	End User	Logged in users shall create a new comment and, like other comments. (the author shall not be able to 'like' his own comment)	The user shall exist in the system. The user shall login into the system. A placeholder shall exist in the system to display comments. A placeholder to display 'like' shall exist the system. All the eligible participants to the software system shall contribute to comment except authors. All the eligible participants to the software system shall contribute to like a comment except authors.
FR030	System Administrator End User	Only System Administrators and Authors shall edit and delete a comment	The user shall login into the system. The user shall exist in the system. The role of the user shall have to be 'System Administrator'. Comment shall have already been defined in the system. The role of the system administrator shall include edit, delete and modify.
FR031	All	The comments page shall show 'no comment' when no comment has been made by anyone.	The SMI characteristics for each provider shall have already been defined in the system. The system shall count the number of comments on each SMI characteristic. The system shall display 'No comments', if the number of comments is zero.
FR032	All	The comment page shall display the number of comments associated with each SMI characteristic.	The SMI characteristics for each provider shall already have been defined in the system. The system shall count the number of comment on each SMI characteristic. The system shall display the exact number of comments.
FR033	All	Visitors shall click on the replies link next to each comment to open the reply page.	Comment shall have already been defined in the system. The system shall provide a reply option in comment page. All the visitors to the system shall be able to see this option.
Reply Page			
FR034	All	The reply page shall provide a place to write a reply associated with each comment.	The user shall exist in the system. The user shall login into the system. The system shall redirect to the reply page. The system shall provide a placeholder for posting a reply associated with each comment. All the eligible participants to the system shall contribute to it.
FR035	All	The reply page shall keep track of all the registered users while they exchange their opinions.	The user shall login into the system. The user shall exist in the system. Replies shall have already been defined in the system. The system shall record all the authors associated with each reply. All the eligible participants to the system shall contribute to it.
FR036	All	Logged in users shall create a new reply.	The user shall login into the system. The user shall exist in the system. Replies shall have already been defined in the system. All the eligible participants to the system shall contribute to it.
FR037	All	The reply page shall provide a 'like' option to show how many people agree with other replies.	Replies shall have already been defined in the system. The system shall count the number of liked replies. All the visitors to the software system shall see the number of 'likes'.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
FR038	All	Only System Administrator and Author shall edit/delete a reply	The user shall login into the system. The user shall exist in the system. The role of user shall be that of 'System Administrator'. Replies shall have already been defined in the system. The role of System Administrator' shall include edit, delete and modify.
FR039	All	The reply page shall show a title and summary of relevant comments.	The user shall exist in the system. The user shall login into the system. Comment data shall already exist in the system. Replies shall have already been defined in the system which shall have been associated with each comment. All the eligible participants to the system shall contribute to it.
FR040	All	The reply page shall show 'no reply' when no replies have been made by anyone.	Comments for each provider shall have already been defined in the system. The system shall redirect to the comments page. The system shall count the number of replies for each comment. The system shall display 'No reply', if the number of replies is zero.
FR041	All	The reply page shall display the number of replies associated with each comment.	Comment for each SMI characteristic shall have already been defined in the system. The system shall count the number of replies for each comment. The system shall display the exact number of replies.
Poll			
FR042	All	The website shall have a poll page for logged in users in order to complete surveys and polls.	The user shall exist in the system. The user shall login into the system. The system have shall have different views for different roles. Questions shall have already been defined in the system by the system administrator. All the eligible participants to the system shall contribute to it.
FR043	All	The poll page view shall have different views for the different roles in the system.	The user shall exist in the system. The user shall login into the system. Different roles shall define in the system. All the eligible participants to the software system shall have different view on system.
FR044	All	The poll page shall distinguish between different groups of questions based on the cloud categorization. (e.g. operational, technical, security)	The user shall exist in the system. The user shall login into the system. The key features of the system shall have been agreed upon. Questions shall have already been defined in the system in different categories. All the eligible participants to the system shall contribute to it.
FR045	All	The poll page shall provide a list of questions in a form format.	The user shall login into the system. The user shall exist in the system. The key features of the system shall have been agreed upon. Questions shall have already been defined in the system.
FR046	All	In the poll page, each group of questions shall assess different group of expertise such as security, privacy etc.	The super editor shall login into the system. The super editor shall exist in the system. The super editor shall assign each question to the group of internal expertise. Different type of questions shall have already been defined in the system.
FR047	All	The system administrator shall be able to add new groups of questions to the system.	The system administrator shall login into the system. The system administrator shall exist in the system. The system shall offer to add new groups to the system via the 'System Administrator'. The system shall keep track of all the defined groups in the system. Questions shall have already been defined in the system.
FR048	All	The poll page shall provide a 'customer survey' where all the end users are able to poll on the provider information.	The user shall login into the system. The user shall exist in the system. Customer survey questions shall have already been defined in the system. All the eligible participants to the system shall contribute to it.
FR049	All	The customer survey on the poll page shall provide a list of the questions based on the Likert Scale.	The user shall login into the system. The user shall exist in the system. Replies shall have already been defined in the system. All the eligible participants to the system shall contribute to it.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
			The key features of the system shall have been agreed upon.
FR050	All	The website shall have a user management page which shall offer to create, define, add and remove users depending on the predefined permissions in the system.	The user shall login into the system. The user shall exist in the system. Replies shall have already been defined in the system, All the eligible participants to the system shall contribute to it.
Settings Page			
FR051	All	The website shall offer to change passwords for all the different user roles.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR052	All	The webpage shall offer different roles with different levels of permissions. (Predefined roles shall be System Administrator, Super Editor, Editor, End User)	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR053	All	The web site shall provide different views for the different roles.	The user shall login into the system. The user shall exist in the system. Roles shall have already been defined in the system. All the eligible participants to the system shall contribute to it.
System Administrator			
FR054	System Administrator	The webpage shall provide a role for 'System Administrator' with complete control of the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR055	System Administrator	The System System Administrator shall be the user with the role of System Administrator created initially. The System System Administrator shall create any number of 'System Administrator' users.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR056	System Administrator	The role of the system administrator shall include the right to delete any comments/replies created by any user on the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR057	System Administrator	The system administrator shall have the highest privileges for modification and control of whole the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR058	System Administrator	The system administrator shall have access to the user management screen.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR059	System Administrator	The user management screen shall display a list of all the users on the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR060	System Administrator	The system administrator shall be able to define new users with any given role from the user management screen.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR061	System Administrator	The system administrator shall define several users from the provider's company in the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR062	System Administrator	The system administrator shall be able to assign/modify roles to any user in the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
			All the eligible participants to the system shall contribute to it.
FR063	System Administrator	The system administrator shall be able to delete any users of the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR064	System Administrator	The system administrator shall have access to a complete view of everything on the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR065	System Administrator	The System System Administrator shall be able to add multiple users with System Administrator privilege.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR066	System Administrator	The System System Administrator shall be able to define different type of questionnaires such as security, operational, technical.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system by himself/herself All the eligible participants to the system shall contribute to it.
FR067	System Administrator	The System System Administrator shall have access to the poll page, and in this case the system administrator shall be able to modify/delete any questionnaire.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it. The key features of the system shall have been agreed upon.
Super Editor			
FR068	Super Editor	The webpage shall provide roles for the super editor with the highest level of modification. (He / she shall have fewer privileges than the system administrator).	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system, The user shall be valid. All the eligible participants to the system shall contribute to it.
FR069	Super Editor	The super editor shall be able to see a list of internal users inside his own company on the 'user management' screen.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR070	Super Editor	The super editor shall have the ability to completely modify and control over the selected editor group.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR071	Super Editor	The super editor shall be able to define new users in his company from the user management screen.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR072	Super Editor	Only the super editor shall be able to assign the editor roles to each user created by him/her.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR073	Super Editor	The super editor shall be able to delete a user from his internal groups.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR074	Super Editor	The super editor shall be able to assign new roles to each limited selected specialist in his company.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
FR075	Super Editor	The super editor shall be able to respond to all questions.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR076	Super Editor	The Super editor shall be able to have a view of customer surveys.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR077	Super Editor	The super editor shall have access to the polls page and all the questionnaires listed there.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR078	Super Editor	The super editor shall not have access to customer surveys.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system by himself/herself The user shall be valid. All the eligible participants to the system shall contribute to it.
FR079	Super Editor	In the polls page, the super editor shall be able to assign a group of questions to The editors.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR080	Super Editor	The super editor shall be able to respond to different groups of questions.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR081	Super Editor	The super editor shall be able to modify incorrect responses in his group.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR082	Super Editor	Super Editors shall be able to add, delete and modify Editors	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR083	Super Editor	Supper editors shall be able to reward his Editors in order to motivate them to insert correct information.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
Editor			
FR084	Editor	The webpage shall provide an 'Editor' role with a medium level for modification.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR085	Editor	Editors shall be able to respond to any questions.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR086	Editor	Editors shall be able to change and modify their answers to all questions.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
			The user shall be valid. All the eligible participants to the system shall contribute to it.
FR087	Editor	The editor's role shall not include access to the customer survey screen.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR088	Editor	The editor role shall include a poll page from which he shall be able to access questionnaires.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
FR089	Editor	The role of the editor shall include an ability to modify his answers to questionnaires.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. The user shall be valid. All the eligible participants to the system shall contribute to it.
End User			
FR090	End User	The end user shall able to respond to all the questions.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR091	End User	The webpage shall provide an 'End User' role with a low level of modification.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR092	End User	The end user shall be able to modify his answers before submitting them to the system.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR093	End User	Customer surveys shall be used to evaluate providers and shall include feedback from users.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR094	End User	Customer surveys shall be evaluated using the Likert scale.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. A system shall exist to evaluate customer survey responses. All the eligible participants to the system shall contribute to it.
FR095	End User	Responses to customer surveys shall be linked to each provider.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR096	End User	End users shall select providers for the completion of the customer surveys.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR097	End User	Customer surveys shall be available for viewing by all users.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR098	End User	End users shall have access to customer survey screens.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR099	End User	End users shall be able to modify their answers to customer surveys before submission.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.

Functional requirements			
RID	**Involved Stakeholders**	**Requirements Statement**	**Preconditions**
FR100	End User	Any logged in users shall have access to the settings page and shall be able to change their own passwords.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
FR101	End User	The system shall have a security visualization page called 'Cloud Security Alliance' which shall be visible to all visitors.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system. All the eligible participants to the system shall contribute to it.
Visualization			
FR102	All	The visualization page shall include a list of the cloud providers from CSA STAR.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR103	All	The visualization page shall indicate the different security levels in a simple user-friendly format.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR104	All	The design of the visualization page shall follow the conceptual model in Chapter 4 Figure 4-3.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system by himself/herself
FR105	All	The visualization page shall provide a description related to each controller.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR106	All	The visualization page shall show all the controllers, sub-controllers, providers and best practices accommodated in CSA STAR.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR107	All	The visualization page shall provide connections between the certifications level and the sub-controllers' level.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR108	All	The visualization page shall provide connections between the controllers' level and The providers' level.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR109	All	The visualization page shall indicate the connection between sub-controller levels to provide level.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.
FR110	All	The visualization page shall follow the hierarchy of multi parent structure.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system,
FR111	All	The visualization page shall group the controllers and their associated sub-controllers with the same colours.	The user shall login into the system. The user shall exist in the system. A password shall have already been created in the system.

Table 5-1 Functional requirements

5.2 Non-Functional Requirements

Non-functional requirements are those requirements necessary to achieve the project's objectives. Non-functional requirements are known as a quality of service by the International Institute of Business Analysis. Non-functional requirements are overviewed as follows.

5.2.1 Software Requirements

The following table specifies the software requirements of our system.

Software Requirements	
Requirement ID	**Requirement Statement**
SR01	The application shall be maintainable.
SR02	The software shall be scale and flexible.
SR03	The application shall have high performance.
SR04	The application shall be agile and fast and have a short development cycle.
SR05	The application shall be a Single-Page Application (SPA).
SR06	The application shall respect the reusability features.
SR07	The software shall be easy to develop.
SR08	The software shall be a MVC pattern.
SR09	The application shall use a REST full services.
SR10	The application shall also work on modern browsers such as Chrome (40+), Firefox (30+) Safari and IE (9+).

Table 5-2 Software requirements

In order to meet our requirements we have selected MEAN stack technology [Table 5-3]. MEAN stack has a full stack java script solution. This uses the power of AngularJs the frontend part, Node.js runtime, Express.js backend framework and MongoDB database, combines them in order to build the dynamic website. It is robust, maintainable and fast for writing web applications. These technologies work well together.

Software Selection (MEAN Stack)			
RID	**Name**	**Version**	**Comment**
SS1	Monngodb	V2.6.7	database
SS2	Express	V4.0.0	back-end web framework
SS3	Angularjs	V1.3.15	front-end framework
SS4	Nodejs	V0.12.2	back-end platform / web framework

Table 5-3 Software selection

MongoDB, which is classified as a NoSQL database, allows developer to quickly change the structure of the data. It helps scalability and can also improve performance. It can interact well with the JavaScript. Java Script on the server side can power web APIs, and the developer can switch easily between server and client code easily. This is a major advantage when developers use the same language on the client and server side.

Nodejs is a cross platform which is written in Java Script. It is a runtime environment for server-side and network applications. Node.js is available for many different platforms, such as Linux, Microsoft Windows and Apple OS X. Node.js applications are built using many library modules and a very rich ecosystem of libraries is available, some of which we will use to build our application [Table 5-4]. It also deals with locking and concurrency issues and is scalable and also has a huge performance, so the main reasons for the adoption of Node.js in enterprise environments include scalability, short development cycles and performance.

Express is a flexible web framework for Node.js that is responsible for providing the web API and routing, and basically enables the easy creation of web applications by providing a slightly simpler interface for creating request endpoints, handling cookies, etc. The modularity of Express allows developers to plug in external middleware for additional functionality easily. Node itself can do everything Express can do, but Express just wraps it in a nicer package.

Angularjs is a web application framework and a comprehensive language, developed by Google which uses Java Script framework. It is pretty small considering its functionality. Angular works quickly independent of internet speed. We have used Angularjs in the client part of the application. Angularjs has a lot of advantages compared with other web technologies such as two way data-binding, MVC pattern, static template, Angular template, custom directive, REST full services, form validations, client and server communication, dependency injection, applying animations and event handlers. Also, it helps to create software faster and with less effort than other programming languages. Moreover, we decided to use single-page application (SPA) for our implementation that is supported by Angularjs. Also, Angularjs helps to improve performance and reusability of the system because it is a responsive web app on different devices such as Mac, Windows and Linux, and it is a Java program that works easily on different kinds of computers. Following tables summarize the main dependencies and requirements for the backend and frontend as follows:

RID	Frontend	
Dependency Requirements		
	Name	Version
DR05	angular-animate	^1.3.15
DR06	angular-aria	^1.3.15
DR07	angular-material	^0.10.0
DR08	angular-resource	^1.3.15
DR09	api-check	~7.2.3
DR10	Angular	~1.3.15
DR11	json3	~3.3.1
DR12	es5-shim	~3.0.1
DR13	Jquery	~1.11.0
DR14	Bootstrap	~3.1.1
DR15	angular-resource	>=1.2.*
DR16	angular-cookies	>=1.2.*
DR17	angular-sanitize	>=1.2.*
DR18	angular-bootstrap	~0.13.0
DR19	font-awesome	>=4.1.0
DR20	angular-ui-router	~0.2.10
DR21	angular-material	~0.8.3
DR22	angular-animate	~1.3.15
DR23	d3	~3.5.5
DR24	angular-formly	~6.10.0
DR25	angular-formly-templates-bootstrap	~4.3.1

RID	Backend	
Dependency Requirements		
	Name	Version
DR26	body-parser	~1.5.0
DR27	composable-middleware	^0.3.0
DR28	compression	~1.0.1
DR29	connect-mongo	^0.4.1
DR30	cookie-parser	~1.0.1
DR31	ejs	~0.8.4
DR32	errorhandler	~1.0.0
DR33	express	~4.0.0
DR34	express-jwt	^0.1.3
DR35	express-session	~1.0.2
DR36	json3	^3.3.2
DR37	jsonwebtoken	^0.3.0
DR38	lodash	~2.4.1
DR39	method-override	~1.0.0
DR40	mongoose	^3.8.31
DR41	morgan	~1.0.0
DR42	passport	~0.2.0
DR43	passport-facebook	latest
DR44	passport-google-oauth	latest
DR45	passport-local	~0.1.6
DR46	passport-twitter	latest
DR47	q	^1.3.0
DR48	serve-favicon	~2.0.1
DR49	sleep	^2.0.0

Table 5-4 Dependency requirements

5.2.2 Hardware Requirements

The hardware requirements are similar to those required by Nodejs and MongoDB. For our application we suggest a minimum hardware requirement of:

Hardware Requirement		
Requirement ID	Requirement Statement	Comment
HR01	CPU	Core 2 Duo or Athlon X2 at 2.4 GHz
HR02	Memory	512 MB RAM minimum, 2 GB RAM recommended
HR03	Hard drive	8 GB of free space
HR04	Graphic hardware	DirectX 9.0c compatible video card. Hardware Accelerator- 256 of memory minimum

Table 5-5 Hardware requirements

5.2.3 Security Requirements

The security requirements is an emergent property of the system which is required to ensure fulfilment of requirements in the face of abuse or misuse. We have summarized the main security requirement as follows.

Security Requirements	
Requirement ID	**Requirement Statement**
SR01	All account modification events shall be logged. The event log shall contain date, time, user, action, object, prior value and new value.
SR02	The application shall keep track of changes and modifications. (security audits)
SR03	The application shall respect security features such as data encryption.
SR04	Passwords shall be encrypted before storing in DB. (user data)
SR05	Access to various features shall be based on user roles. Role hierarchy shall be followed.
SR06	System identification and authentication shall be considered in the system.
SR07	All accounts shall have passwords.

Table 5-6 Security requirements

We have established Passport[50] for the authenticating part of our applications. Passport uses robust authentication strategies. Following figure shows the state diagram of sign-on using OAuth providers.

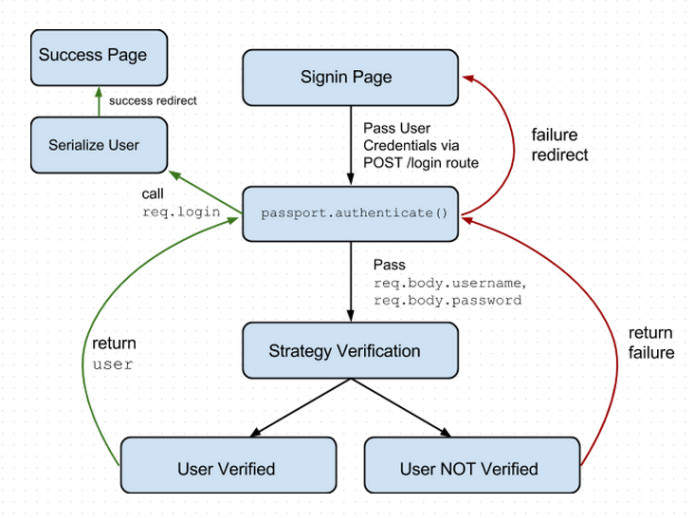

Figure 5-3 QAuth State diagram [48]

[50] http://passportjs.org/

5.2.4 Interface Requirements

The following table describes the general interface's requirements for our system. Moreover, the requirements of each page with their design are described along with the way that users interact with the system in order to store required information and retrieve desired information.

Interface Requirements	
Requirement ID	**Requirement Statement**
IR01	The user interface shall provide basic structure which follows the Windows style conventions.
IR02	The application shall have multi-platform compatibility. It shall be compatible with platforms such as Windows, Linux and Mac.
IR03	The application shall be a responsive user Interface
IR04	The application shall be a user friendly interface.
IR05	The system shall display accurate and precise data.
IR06	There shall be interface notifications should a user face a problem with the system.
IR07	The interface shall contain main tabs at the top of the screen where the users can easily switch between the different tabs of the program.

Table 5-7 Interface requirements

5.2.4.1 Home Page

The first tab, named 'Home', shall list cloud service providers in different panels containing general information such as the description, the URL, the list of their services and their locations.

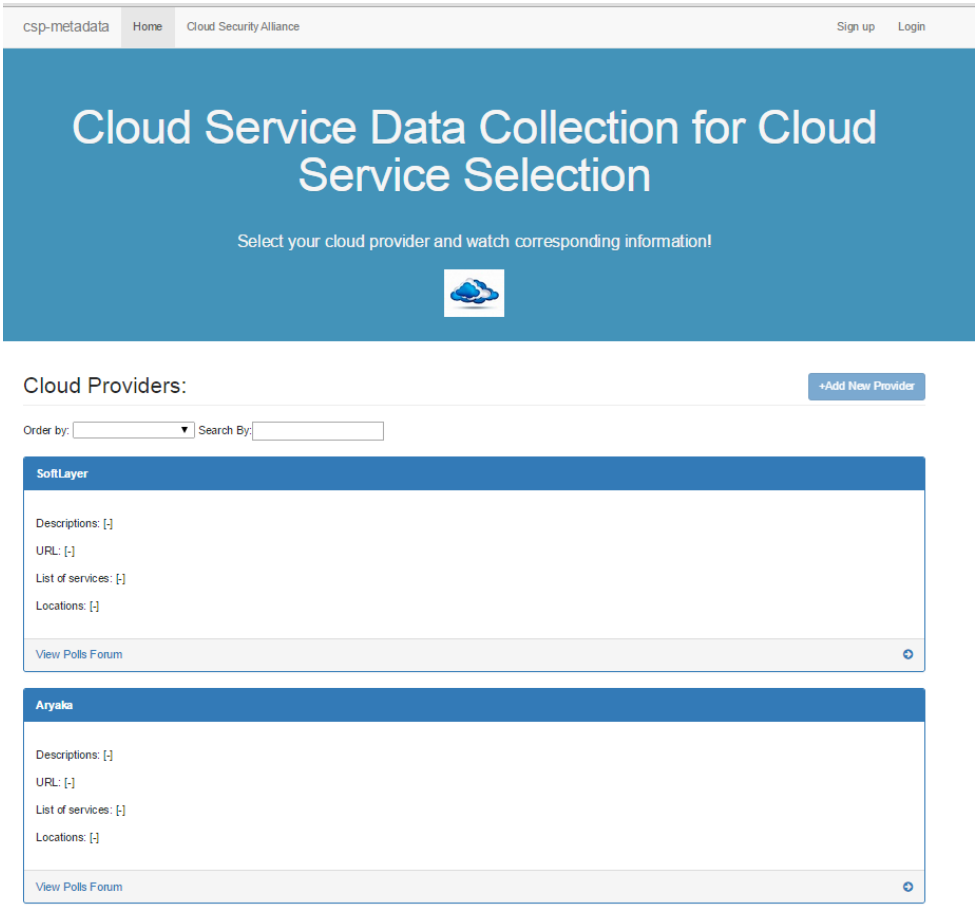

Figure 5-4 Home page

Providers shall fall into two categories and shall be inserted into the system in two ways.

- Listed providers – these shall be automatically dumped from various sources.
- Registered providers – these shall arrive via the internet in collaboration with our platform where they shall be defined by the system administrator

A dropdown box shall also be displayed which end users can use to define their searches, and one text field in which end users may enter any key search which can help to search for a specific cloud service provider. On the right hand site of the search section, there shall be a button which allows registered providers to insert their information into the system.

Associated with each panel in the home page, there shall be a link to the polls forum page. Once 'view polls forum' link is selected, the end user shall be taken to another screen containing the list of the SMI characteristics and related average rate. Once logged in, the end user shall be able to rate the corresponding SMI characteristics.

5.2.4.2 Polls Forum

This screen shall display the SMI characteristics rate visually and numerically. The system shall keep track of end users who rate the SMI characteristics. If end users need to comment on the specific SMI characteristics, the corresponding comment page shall be available. Once 'comment is selected, the end user shall be taken to another screen which has the list of comments related to each SMI characteristic, and the number of likes accomplished by other end users. The system shall display 'No comments', if the number of comments is zero.

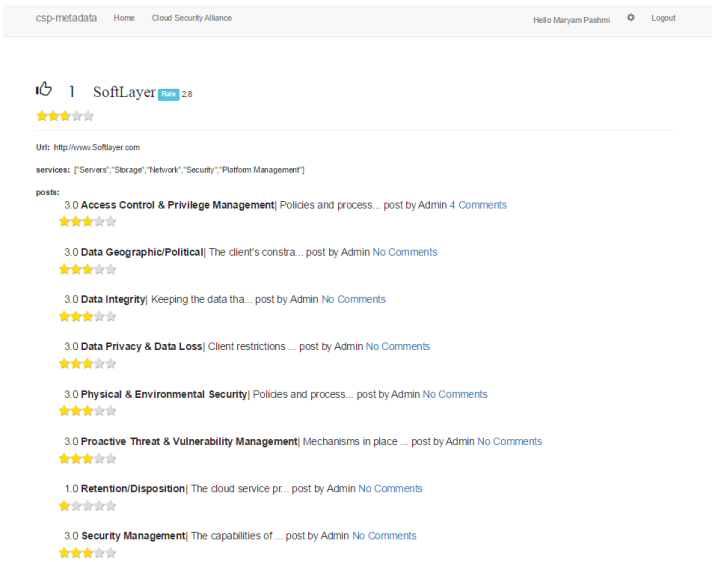

Figure 5-5 SMI rating mechanism

5.2.4.3 Cloud Provider Register Form

Once 'Add provider' button in home page is selected, the end user shall be taken to another screen in order to enter and submit some information about their company such as company name, home page, product name, locations etc. Once the information is completed and the submit button is pressed, the screen shall be changed to the home page view. This screen shall display several text fields and dropdown boxes to input the information.

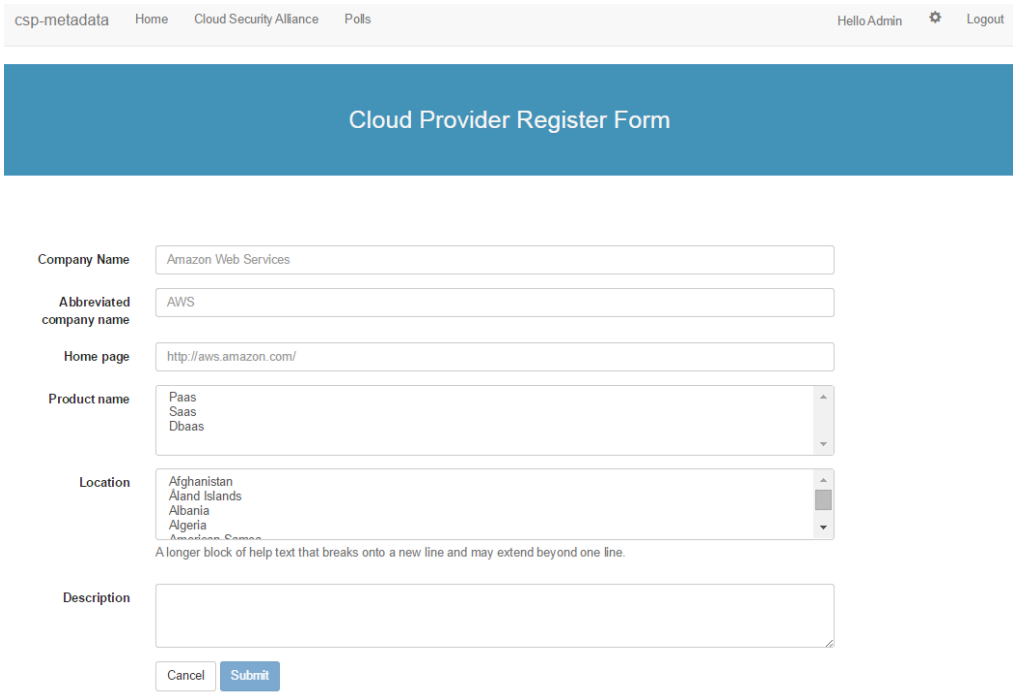

Figure 5-6 Cloud Provider Register Form

5.2.4.4 Reply Page

In the comment page, there shall be a reply link corresponding to each comment which end users can select to switch to the reply page. This page shall display a list of the replies corresponding to each comment. This screen shall also provide a 'like' for each of the replies. Thus end users shall be able to see how many people agree with their replies. The system shall display 'No replies', if the number of replies is zero. In order to like or rate any reply, end users shall be logged on to the system.

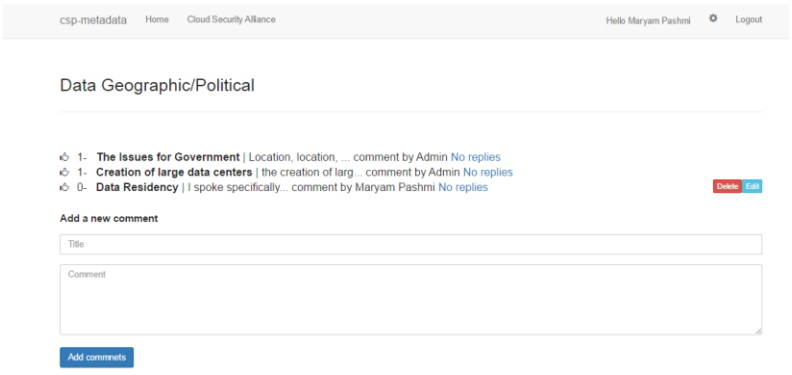

Figure 5-7 Reply page screen

5.2.4.5 Cloud Security Alliance Visualisation

The second tab, 'Cloud Security Alliance', shall allow end users to view the visualisation of the Cloud Security Alliance within the cloud provider companies. This screen shall use multi parent tree structures to allow the user to search for a specific security controller which can be fulfilled by a specific provider. This screen shall display links between the standards and best practices' clauses with the CSA's controllers and sub-controllers as well as cloud service providers.

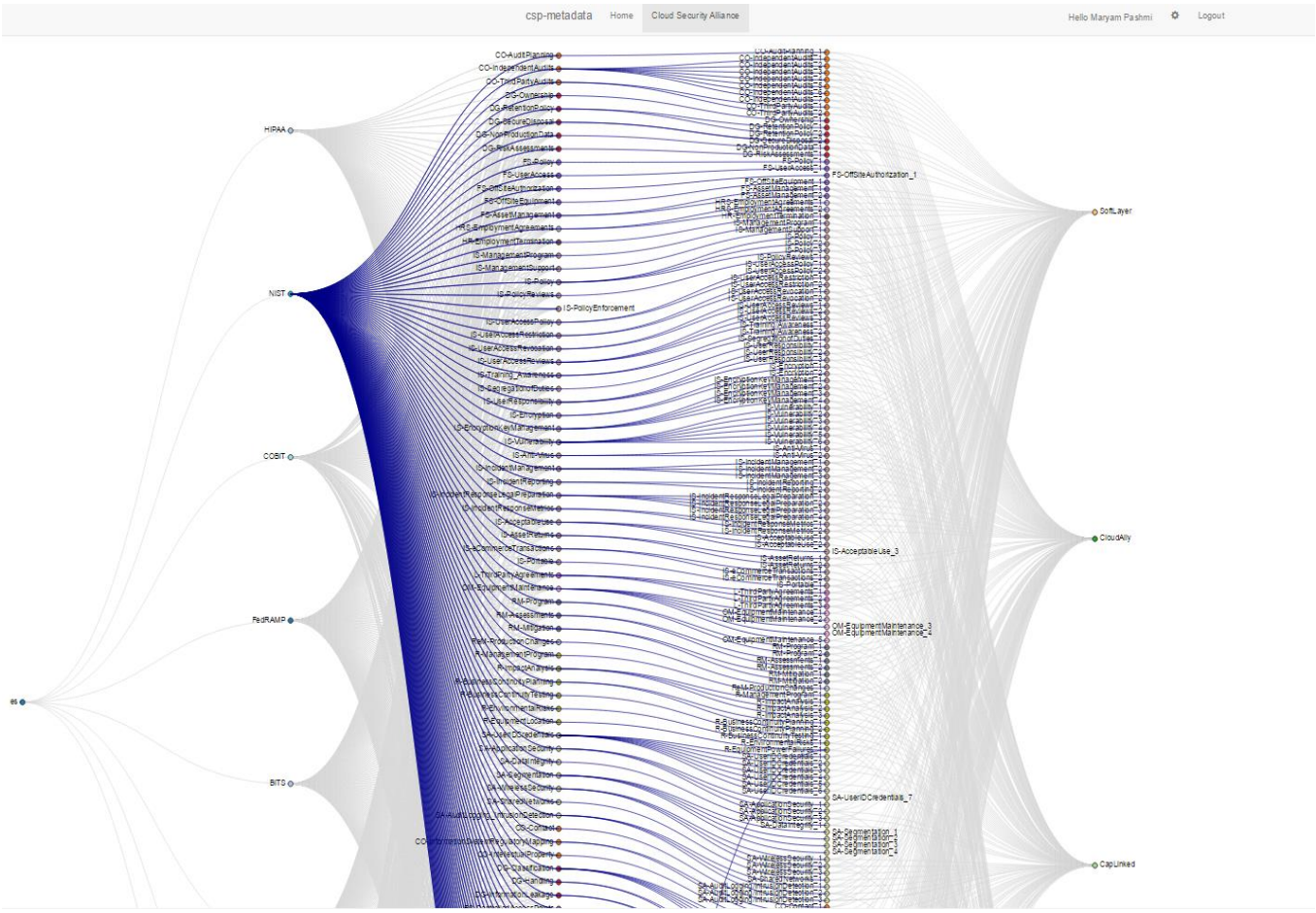

Figure 5-8 Visualisation view

5.2.4.6 Polls Page

The third tab, 'polls', shall allow end users to select groups of questions to survey. This screen is hidden until the user enters the system. The system administrators shall be able to publish the group of questions. Two types of questions shall be defined in this screen, provider questions and consumer questions. The provider questions shall be able to be legal questions, privacy questions, security questions, etc. It shall be

possible to select a group and submit the answers. The customer questions shall be defined based on the level of user satisfaction. This screen shall also display statistical information associated with each answer derived from an average of respondents. There shall exist different types of input fields such as the text box, the dropdown menu, etc.

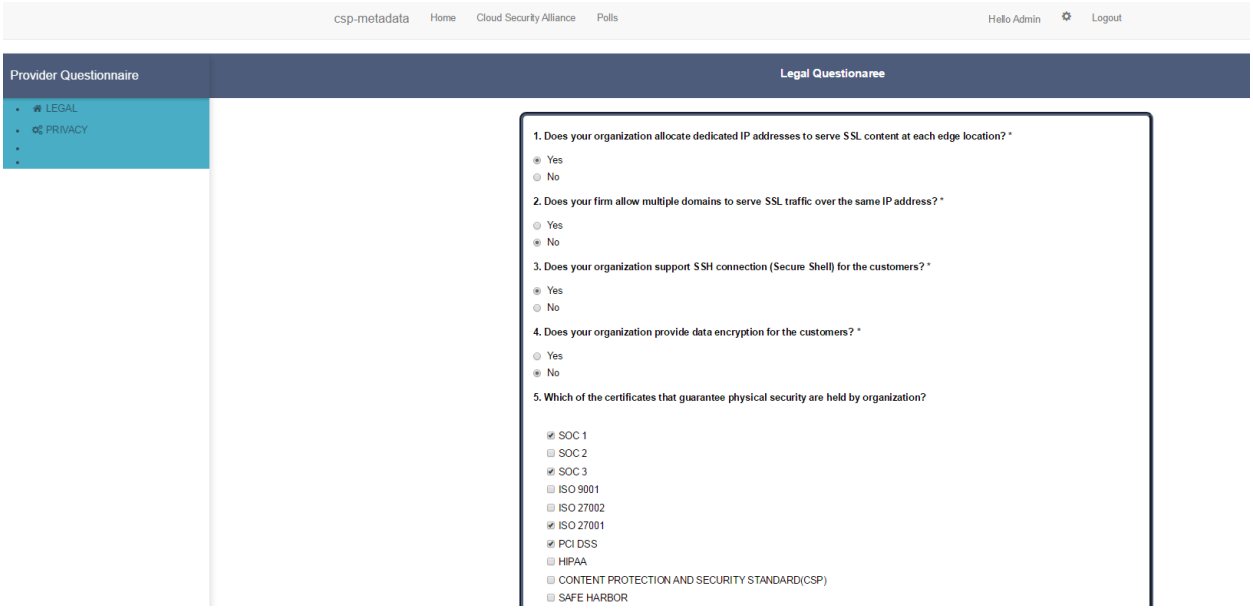

Figure 5-9 Poll questionnaire

5.2.4.7 Settings Page

The fourth tab, 'settings', shall allow end users to change their passwords. This interface shall be different for the different stakeholders, for example the end user view shall be different from the administrator view and so on. Once the administrator is logged into the system, the left panel shall appear which contains two parts. The first part shall be for user management and the second part shall be for the settings. The first part shall display the user information in the whole of the system and shall permit the removal of a user from the system. The administrator shall be able to manage all users in this screen. The second part displays the placement in order to change the administrator's password. The super editor view shall be the same as the administrator view. However only the super editor shall be able to manage his own editors.

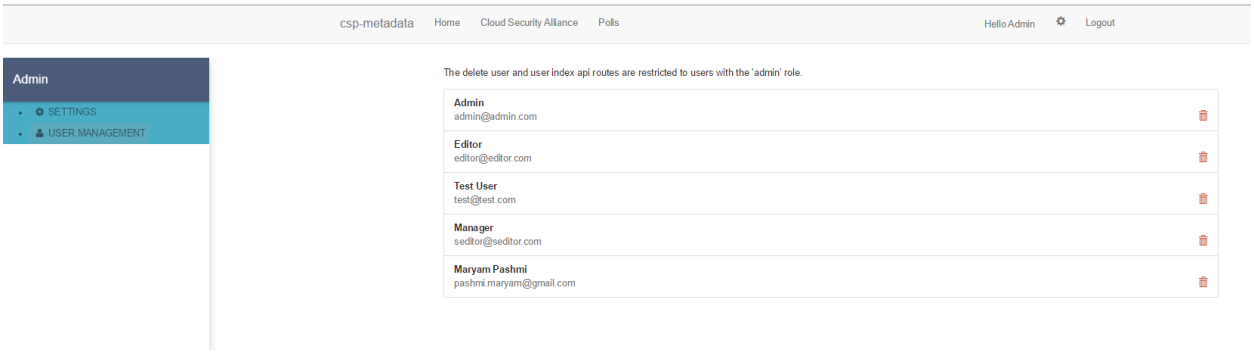

Figure 5-10 Setting page screen

The final tab shall be the logout or login tab. Once an end user has logged on to the system, the logout tab shall be activated and vice versa. The end user shall be able to click over the login or logout button and switch easily between the two pages.

5.2.4.8 Login Page

The login screen shall display two text fields for email and password. If the end user enters the correct information, he shall be able to enter the system.

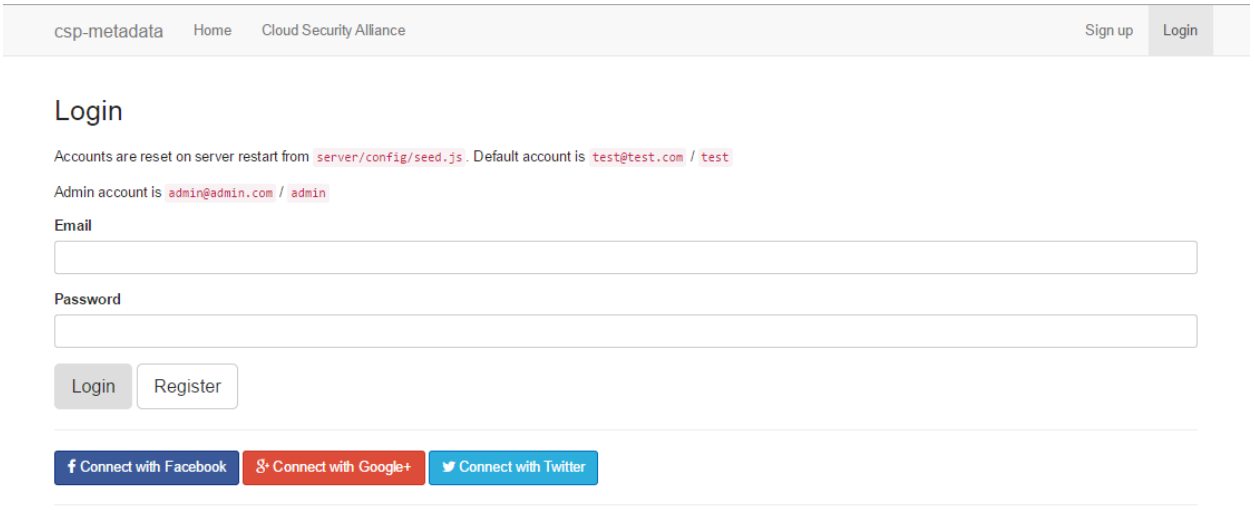

Figure 5-11 Login page screen

The end user shall be able to register his personal information through Facebook, Google and Twitter. Otherwise, he shall be able to click on the register button on the login screen. Once the register button is clicked, the end user shall open the sign up page. This screen shall display four text fields contains the name,

the email, the password and repeat password. The end user shall click on the sign up button in order to register his information. Once the end user has signed up to the system, the system shall switch to the home page and display the welcoming message.

5.2.5 Software Constraints

This section describes any technical assumptions and constraints related to our project's requirements.

Software Constraints	
Requirement ID	Requirement Statement
SC01	The application shall be compatible with MODAClouds DSS tools.
SC02	The same data base as MODAClouds shall be used for the project.
SC03	The application shall have an MIT license.
SC04	The application shall be an open source project.

Table 5-8 Software constraints

5.3 Implementation of the System

The following describes the technological and physical environment in which the system is implemented. Our architecture is divided into client and server architecture which is described below.

- **The server**

The server part is the core of the application which is deployed on Nodejs server. The server is responsible for creating a consistent view of the data obtained from the data entry approaches. It provides access to this data by means of a JSON API. Node.js exposes APIs that send JSON responses directly to the client rather than through the server. If Node.js renders server-side then this sends back an HTML page for every request. Using client side rendering in Node.js environments can dramatically save bandwidth and reduce latency.

The server has following responsibilities:

- Delivering the client's source code
- Building a consistent view of the data and delivering it through the APIs for modifying the cloud meta data

The data is stored in a MongoDB instance. In fact the application uses mongoose as an object-database library. Access is provided using a Representational State Transfer (REST) API. In this case the server is an HTTP server and the client sends HTTP requests such as POST when a client wants to insert or create an

object, GET when a client wants to read an object, PUT when a client wants to update an object, and DELETE when a client wants to delete an object. These HTTP requests are sent along with a URL and variable parameters that are URL-encoded.

- **The middleware**

The application needs a mid-layer between the client request and the application logic. This connectivity in the node application can be called middleware. Middleware is a list of functions through which a request must flow before hitting the actual application logic.

- **The client**

The client is an SPA which provides a GUI for the JSON API of server. The client makes calls to this API in order to retrieve the data and display it to the end user in a more intuitive way. The client is served by the server statically. For instance, the server will not embed any type of information into the delivered Html/Js files. The JS code of the client is responsible for querying the relevant information using the server's JSON API. The following architecture appears in the diagram below:

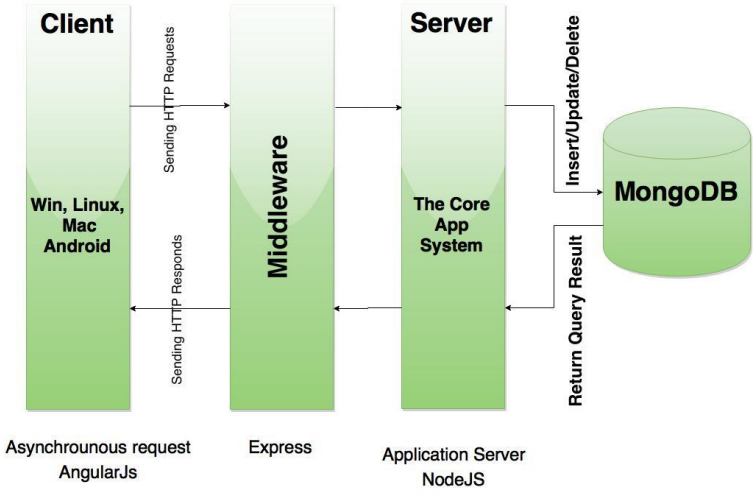

Figure 5-12 Client and service architecture model

5.3.1 Data Model

In the following figure, the data model of our system is presented as a diagram. This flowchart illustrates the relationships between data and the way it has been stored in the data base.

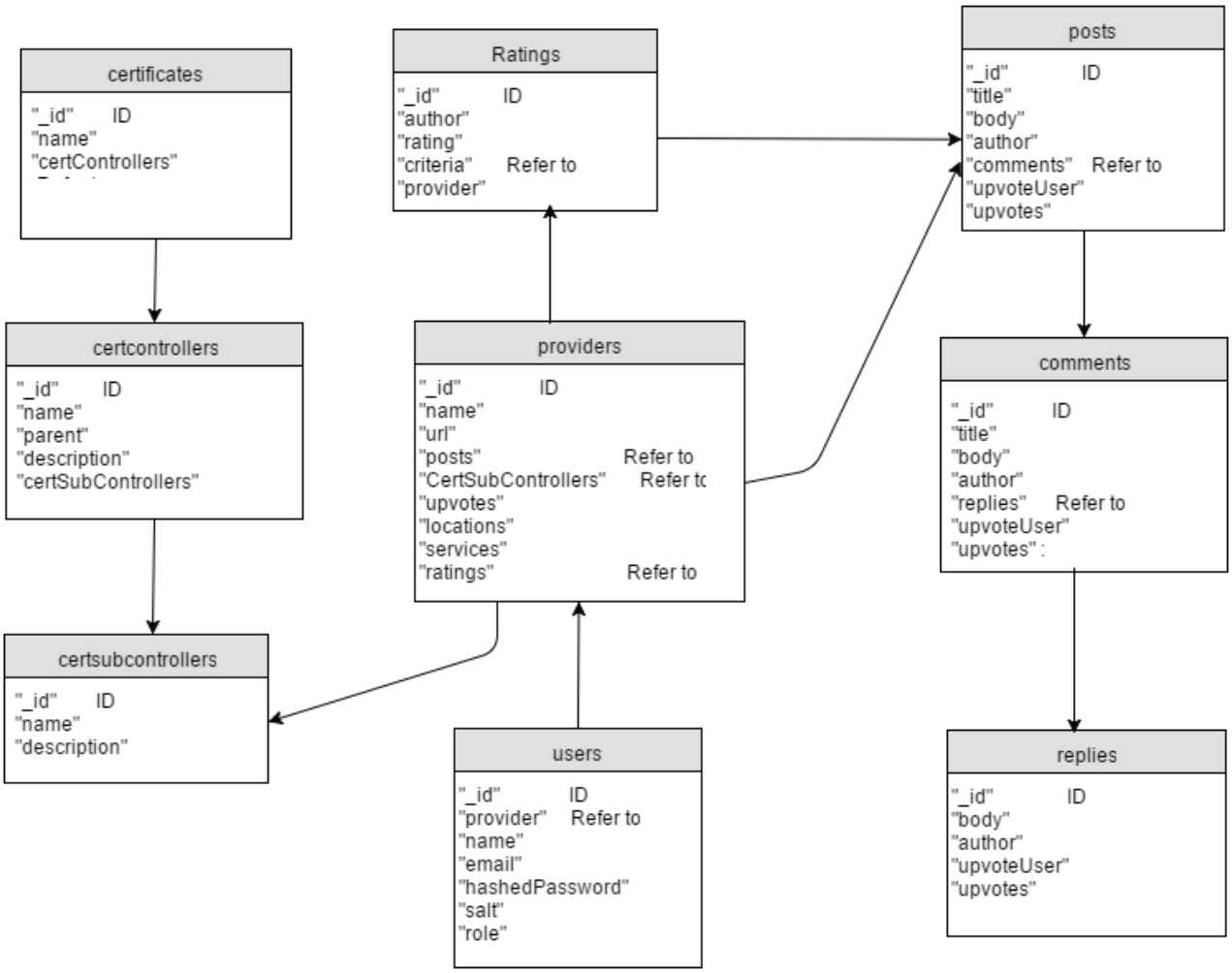

Figure 5-13 Class diagram (Data Model)

Two examples of our data collections (e.g. Certcontroller, provider) are presented below.

```
{
    "_id" : ObjectId("55647cd1ab74fc30966ff5b7"),
    "name" : "CO-AuditPlanning",
    "parent" : [
        "COBIT",
        "HIPAA",
        "ISO27001",
        "NIST",
        "FedRAMP",
        "PCI_DSS",
        "BITS",
        "GAPP"
    ],
    "description" : "",
    "certSubControllers" : [
        ObjectId("5576d8b994da4bbe2d34c9d2")
    ]
}
```

Figure 5-14 Certcontrollers' collection

```
{
    "_id" : ObjectId("5577019294da4bbe2d34ca96"),
    "name" : "SoftLayer",
    "url" : "http://www.Softlayer.com",
    "description" : "Founded in 2005, SoftLayer Technologies, Inc. is a dedicated server, managed hosting and cloud computing provider.",
    "posts" : [
        ObjectId("55857fd29891d398229ae5f5"),
        ObjectId("5585808a9891d398229ae5fc")
    ],
    "CertSubControllers" : [
        ObjectId("5576d8b994da4bbe2d34ca92"),
        ObjectId("5576d8b994da4bbe2d34ca93"),
        ObjectId("5576d8b994da4bbe2d34ca94")
    ],
    "upvoteUser" : [
        "Maryam Pashmi"
    ],
    "upvotes" : 1,
    "locations" : [
        "Dallas"
    ],
    "services" : [
        "Servers",
        "Storage",
        "Network",
        "Security",
        "Platform Management"
    ],
    "createdOn" : "",
    "__v" : 25,
    "ratings" : [
        ObjectId("5586d3962b8e22241a9ecfb9"),
        ObjectId("5586e1fe1f7f116c1a0beda5")
    ]
}
```


Figure 5-15 Provider's Collection

CRUD operations against the data model can help to create, read, update and delete an object to/from the database. These database operations map very nicely to the HTTP verbs such as POST, GET, DELETE, etc. Also we have used some of the common HTTP status codes e.g. 200 (OK), 201 (Created), 400 (Bad Request), 401 (Unauthorized), etc. in order to help the operations become clearer. We have also taken advantage of parallel features through a call named async. This is a Node.js module that helps the better management of asynchronous JavaScript. The best way around this is to always use asynchronous APIs in the code, especially in performance critical sections. An example of asynchronous call is presented in Figure 5.14.

```
// Get list of comments
exports.index = function(req, res) {
  Post.findById(req.originalUrl.split('/')[5]).select('comments').populate('comments').exec( function(err, post) {
    if(err) { return handleError(res, err); }
    if(!post) { return res.status(404).send('Post not found'); }

    var promises = [];

    _.forEach(post.comments, function(commentId) {
      promises.push(Comment.findById(commentId).exec());
    });

    q.allSettled(promises)
      .catch(_.partial(handleError, res))
      .then(function(results) {
        console.log(_.map(results, _.property('value')));
        return res.status(200).json(_.map(results, _.property('value')));

      })
  })
};
```

Figure 5-16 Example of async call

6. Conclusion and works

The dissertation is mainly aimed at analysing the internship project developed for four-six months at CA Technology. During these months we have been part of the European project, called MODAClouds which provided several tools such as Decision Support System for the cloud service providers. We have mentioned before that MODAClouds tackles two important subjects: the first is the involvement of both business and technical perspectives in decision making simultaneously and the second is the multiple-clouds service which is based on the selection of using a single DSS. In depth studies of previous Cloud Services DSS tools showed the lack of quality of experience as well as a holistic view of security and privacy which are considered to make decision support systems.

In fact no integrated process exits to collect user opinions on which, to recommend cloud services. Moreover, security and privacy metrics have not been considered very deeply in previous works.

Our dissertation aims to implement a Cloud Service Data Collection for Cloud Service Selection aimed at enriching DSS data by integrating the user experience in the DSS tools and also providing a deep security and privacy view of the cloud service providers by designing a visualisation tool.

The entire work has been divided into two principal sub-projects, the security and privacy visualisation and the generic part for the data collection which uses crowdsourcing techniques to gather the relevant data.

The process is a very time consuming part of analysing cloud computing's standards and metrics.

We realised that first, security and privacy are major concerns in the cloud computing area, and second, none of the DSS tools analysed security and privacy issues in a comprehensive way. That is why we have chosen Cloud Security Alliance (CSA) from the best practices and frameworks as our data source on which to build our visualisation. CSA gives a holistic and very deep security and privacy view over the hundreds of security characteristics. This organisation provided a lot of data regarding the security and privacy of cloud service providers however there is not an easy mechanism to use this data for comparing different cloud service providers. The problem with the current data in CSA is that understanding all the provided information is a complex and very time consuming process. It requires a holistic analysis from the STAR registry in CSA, which contains hundreds of different Excel, Word and PDF's documents, to understand and discover the relation between all the different parts of the CSA template. We need to analyse and classify the different metrics, and provide the CSA visualisation tool.

Our tool can assist customers who are interested in analysing the security and privacy characteristics of cloud service providers, and selecting the appropriate ones. In fact, not all the cloud service providers have certified themselves with the CSA so providing our tool will motivate those who want to strengthen

themselves by obtaining CSA self-assessment, assertion or certification, in order to enter a highly competitive cloud environment.

Even worse, most of the biggest and important cloud service providers such as Amazon, Google, Azure, have obtained the CSA self-assessment or certification. The outcome of our visualisation tool is a multi-parent structure tree from more than 110 different cloud service providers, and also more than 200 security and privacy characteristics.

The generic part of the application is where the relevant security and privacy data of cloud providers can be collected through the crowdsourcing platform. This mechanism is used to collect data, and to evaluate the cloud service provider by involving the stakeholders, and allowing them to select an appropriate cloud service provider based on their satisfaction level with a service.

The collection of user opinions, which is highly important in selecting the best cloud service provider, has not previously been considered in existing works for making a recommendation to the end user. This issue shows the maturity of data gathering mechanism in the current Cloud DSS tools. The solution we have proposed to this problem involves designing two different types of questionnaires and providing a provider's forum for evaluating the cloud services. The first type of questionnaire is the customer survey questionnaire where we can evaluate the level of satisfaction of each cloud service provider by cloud consumers. The second type of questionnaire is for completion by cloud service providers, thus involving cloud services providers in the data collection process.

We have identified a list of metrics which are difficult to find through the provider's web page. However they are very important for the customer who sometimes needs to spend a lot of time obtaining such information. These questions are identified based on security and privacy characteristics.

This process required a complete research of, and a thorough understanding of all the cloud characteristics, classifying characteristics of the cloud computing, checking the availability and unavailability of data in the cloud provider's web page, and finally designing the questionnaire which is based on those metrics. These metrics were obtained from the different customer complaints blogs, several interviews with technical supports specialists, articles, surveys, etc.

Every provider has its own forum. In this forum they can be rated regarding to the SMI characteristics. SMI is a framework provided by Cloud Services Measurement Initiative Consortium (CSMIC) which measures the relative strengths of an IT Service. We have elicited the security characteristics from the SMI framework and proposed the provider's rating based on the security SMI characteristics. Each customer on the home page is able to see the different rating value such as customer survey rating and SMI rating. The evaluation part of our application follows the Harmonic Mean where it penalises rates that are very different from one

another. To complete our dissertation, we have decided to generalise the generic part of the data gathering to all the characteristics of cloud computing such as operational and technical characteristics.

All the processes were exactly the same as when we collected data solely for security and privacy characteristics. It should be noted that the questionnaires have been already used by CA technologies, who created the community to distribute them, for collecting the missing part of cloud data.

This dissertation has helped us to improve our technical and theoretical knowledge in the area of cloud computing. This work motivated me to learn how to program web application using new technologies such as mean stack.

As the scope of the project has only focused on data collection in general and the visualisation tool of security and privacy, many opportunities remains for future work. Academics, students and cloud consumers can apply many data mining and data analysis techniques to this data for further investigation.

The project's codes are located in the github repository.[51]

[51] https://github.com/maryampashmi/CSPPlatform

7. Acknowledgment

I would like to thank my advisors, Dr.Abelló Alberto and Dr.Victor Muntes for guiding and supporting me over this year. You have set an example of excellence as researchers, mentors, instructors and role models. I would like to thank my thesis committee members for all of their guidance throughout the process; your discussion, ideas and feedbacks have been absolutely invaluable. I would like to thank my fellow graduate students, research technicians, collaborators and the many undergraduates who contributed to this research. I am very grateful to all of you. I would like to thank to senior programmer and research advisors, Jacek Dominiak and also Dr. Gupta. Smrati for their constant enthusiasm and encouragement.

I would especially like to thank my amazing family and great husband Juan Antonio Frances Lopez for the love, support and constant encouragement he has given me over the years. You are the salt of the earth, and I undoubtedly could not have done this without you. In particular, I would like to thank Duncan Gill for his advice regarding English grammar and vocabulary. Finally, I would like to thank and dedicate this thesis to my wonderful father, Fariborz Pashmi. You were the one who originally generated my love for science with visits to your laboratory and lessons in life. Although it has been a year since your passing, I still carry your example with me every day.

8. Bibliography

[1]. Cloud computing will become the bulk of new it spend by 2016: Gartner. Retrieved September 27, 2015, from http://www.telecomtiger.com/technology_fullstory.aspx?storyid=18881&section=s210

[2]. Cloud Computing Comparison Engine. Retrieved September 27, 2015, from http://www.cloudorado.com/

[3]. CloudHarmony transparency for the cloud. Retrieved September 27, 2015, from https://cloudharmony.com/

[4]. Cloudy Metrics. Retrieved September 27, 2015, from http://api.cloudymetrics.com/

[5]. Free Cloud Cost Calculator. Retrieved September 27, 2015, from http://planforcloud.com/

[6]. Ardagna, D., Nitto, E. D., Mohagheghi, P., Mosser, S., Ballagny, C., D'andria, F., … Sheridan, C. (2012). MODAClouds: A model-driven approach for the design and execution of applications on multiple Clouds. *2012 4th International Workshop On Modeling in Software Engineering (MISE)*. http://doi.org/10.1109/mise.2012.6226014

[7]. Poster - Model-driven approach for design and execution of applications on multiple Clouds. Retrieved September 27, 2015, from http://www.cloudscapeseries.eu/content/demosandposters.aspx?id=404

[8]. Gupta, S., Muntes-Mulero, V., Matthews, P., Dominiak, J., Omerovic, A., Aranda, J., & Seycek, S. (2015). Risk-Driven Framework for Decision Support in Cloud Service Selection. *2015 15th IEEE/ACM International Symposium On Cluster, Cloud and Grid Computing*. http://doi.org/10.1109/ccgrid.2015.111

[9]. Cloud Armor Project Website - Dataset. Retrieved September 27, 2015, from http://cs.adelaide.edu.au/~cloudarmor/ds.html

[10]. Hompel, M. T., Rehof, J., & Wolf, O. *Cloud computing for logistics*.

[11]. Martens, B., & Teuteberg, F. (2011). Decision-making in cloud computing environments: A cost and risk based approach. *Information Systems Frontiers Inf Syst Front*, *14*(4), 871–893. http://doi.org/10.1007/s10796-011-9317-x

[12]. Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *2010 24th IEEE International Conference On Advanced Information Networking and Applications*. http://doi.org/10.1109/aina.2010.187

[13]. Ghobadi, A., Karimi, R., Heidari, F., & Samadi, M. (2014). Cloud computing, reliability and security issue. *16th International Conference On Advanced Communication Technology*.

http://doi.org/10.1109/icact.2014.6779012

[14]. FindTheBest Software. Retrieved September 28, 2015, from http://www.softwareinsider.com/

[15]. Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information And Software Technology*, *58*, 44–57. http://doi.org/10.1016/j.infsof.2014.10.003

[16]. Prpić, J., Shukla, P. P., Kietzmann, J. H., & Mccarthy, I. P. (2015). How to work a crowd: Developing crowd capital through crowdsourcing. *Business Horizons*, *58*(1), 77–85. http://doi.org/10.1016/j.bushor.2014.09.005

[17]. Glinz, M. (2007). On Non-Functional Requirements. *15th IEEE International Requirements Engineering Conference (RE 2007)*. http://doi.org/10.1109/re.2007.45

[18]. Cloud Controls Matrix Working Group. Retrieved September 27, 2015, from https://cloudsecurityalliance.org/research/ccm/

[19]. STAR Attestation. Retrieved September 27, 2015, from http://www.cloudsecurityalliance.org/star/attestation/

[20]. STAR Certification. Retrieved September 27, 2015, from http://www.cloudsecurityalliance.org/star/certification/

[21]. Wikipedia. Retrieved September 27, 2015, from http://en.wikipedia.org/wiki/gantt_chart

[22]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal Of Network and Computer Applications*, *34*(1), 1–11. http://doi.org/10.1016/j.jnca.2010.07.006

[23]. Home. Retrieved September 28, 2015, from http://www.iso.org/iso/catalogue_detail?csnumber=42103

[24]. Department of HealthJohn J. Dreyzehner, MD, MPH, Commissioner. Retrieved September 28, 2015, from http://health.state.tn.us/hipaa/

[25]. Implementing an ISO-integrated Management System Using COBIT 5. Retrieved September 28, 2015, from http://www.isaca.org/cobit/focus/pages/implementing-an-iso-integrated-management-system-using-cobit-5.aspx

[26]. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Retrieved September 28, 2015, from http://www.isaca.org/cobit/pages/default.aspx

[27]. HIPAA Security Rule. Retrieved September 28, 2015, from http://www.hipaasurvivalguide.com/hipaa-security-rule.php

[28]. Luz, N., Silva, N., & Novais, P. (2014). A survey of task-oriented crowdsourcing. *Artificial*

Intelligence Review Artif Intell Rev, *44*(2), 187–213. http://doi.org/10.1007/s10462-014-9423-5

[29]. AIS Electronic Library (AISeL). Retrieved September 28, 2015, from http://aisel.aisnet.org/amcis2011_submissions/430/

[30]. Wikipedia. Retrieved September 28, 2015, from https://en.wikipedia.org/wiki/likert_scale

[31]. Cloud Computing: Data Privacy in the Cloud. Retrieved September 28, 2015, from https://technet.microsoft.com/en-us/magazine/jj554305.aspx

[32]. Wikipedia. Retrieved September 28, 2015, from https://en.wikipedia.org/wiki/software_as_a_service

[33]. Laatikainen, G., Ojala, A., & Mazhelis, O. (2013). Cloud Services Pricing Models. *Lecture Notes In Business Information Processing Software Business. From Physical Products to Software Services and Solutions*, 117–129. http://doi.org/10.1007/978-3-642-39336-5_12

[34]. Felici, M., & Pearson, S. (2014). Accountability, Risk, and Trust in Cloud Services: Towards an Accountability-Based Approach to Risk and Trust Governance. *2014 IEEE World Congress On Services*. http://doi.org/10.1109/services.2014.29

[35]. “CSA Security, Trust &Amp; Assurance Registry (STAR).” *: Cloud Security Alliance*. Web. 29 Sep. 2015. <https://cloudsecurityalliance.org/star/>

[36]. “Consensus Assessments Working Group.” *Consensus Assessments : Cloud Security Alliance*. Web. 29 Sep. 2015. <https://cloudsecurityalliance.org/group/consensus-assessments/>

[37]. Compare Cloud Computing Providers. Retrieved September 27, 2015, from http://cloud-computing.findthebest.com/#main

[38]. “Wikipedia.” *Wikipedia*. Wikimedia Foundation, n.d. Web. 29 Sep. 2015. <https://en.wikipedia.org/wiki/data_collection>

[39]. Intel® Cloud Finder - Cloud Service Providers Search Tool. Retrieved September 27, 2015, from http://www.intelcloudfinder.com/.

[40]. CloudScreener.com - Make the best decision for your Cloud. Retrieved September 27, 2015, from http://www.cloudscreener.com/en

[41]. Browsing category: Infrastructure - CloudSurfing. Retrieved September 27, 2015, from http://www.cloudsurfing.com/browse/categories/576-infrastructure

[42]. Cantador, Iván, and Pablo Castells. “Group Recommender Systems: New Perspectives In the Social Web.” *Recommender Systems for the Social Web Intelligent Systems Reference Library* (2012): 139–157. Web.

[43]. Heisler, Sanford I. *The Wiley Engineer's Desk Reference: a Concise Guide for the Professional*

Engineer. New York: J. Wiley, 1984. Print.

[44]. "Wikipedia." *Wikipedia*. Wikimedia Foundation, n.d. Web. 30 Sep. 2015. <https://en.wikipedia.org/wiki/cloud_database>

[45]. "DNS In the Cloud: The Designate DNS as a Service Project » OpenStack Open Source Cloud Computing Software." *DNS in the Cloud: The Designate DNS as a Service Project » OpenStack Open Source Cloud Computing Software*. Web. 30 Sep. 2015. <https://www.openstack.org/summit/openstack-summit-hong-kong-2013/session-videos/presentation/dns-in-the-cloud-the-designate-dns-as-a-service-project>

[46]. Alnemr, R., Pearson, S., Leenes, R., & Mhungu, R. (2014). COAT: Cloud Offerings Advisory Tool. *2014 IEEE 6th International Conference On Cloud Computing Technology and Science*. http://doi.org/10.1109/cloudcom.2014.100

[47]. HHS.gov. Retrieved September 27, 2015, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

[48]. "Build User Authentication With Node.Js, Express, Passport, and Orchestrate." - *The Orchestrate Blog*. Web. 5 Oct. 2015. <https://orchestrate.io/blog/2014/06/26/build-user-authentication-with-node-js-express-passport-and-orchestrate/>

[49]. "HIPAA Security Rule Compliance Needs: Administrative Safeguards." *SPHER*. Web. 5 Oct. 2015. <https://www.amsspher.com/hipaa-security-rule-compliance-needs-administrative-safeguards/>

[50]. RightScale Cloud Portfolio Management accelerates application delivery, gives you control over cloud usage and spend, and ensures application SLAs. Retrieved September 27, 2015, from http://www.rightscale.com/

[51]. Brabham, Daren C. "Moving The Crowd at IStockphoto: The Composition of the Crowd and Motivations for Participation in a Crowdsourcing Application." *First Monday* 13.6 (2008): n. pag. Web.

[52]. Siegel, J., & Perdue, J. (2012). Cloud Services Measures for Global Use: The Service Measurement Index (SMI). *2012 Annual SRII Global Conference*. http://doi.org/10.1109/srii.2012.51

[53]. NIST Cloud Computing Standards Roadmap. (2013). http://doi.org/10.6028/nist.sp.500-291r2

[54]. Monteiro, L., & Vasconcelos, A. (2013). Survey on Important Cloud Service Provider Attributes Using the SMI Framework. *Procedia Technology*, *9*, 253–259. http://doi.org/10.1016/j.protcy.2013.12.028

[55]. Getting Results from Crowdsourcing. Retrieved September 27, 2015, from

http://crowdsourcingresults.com/competition-platforms/crowdsourcing-landscape-discussion./

[56]. Cloud Computing: Data Privacy in the Cloud. Retrieved September 27, 2015, from https://technet.microsoft.com/en-us/magazine/jj554305.aspx

[57]. Financial services firms still cagey about cloud computing » Banking Technology. Retrieved September 27, 2015, from http://www.bankingtech.com/282821/financial-services-firms-still-cagey-about-cloud-computing/

[58]. Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., & Ahmad, I. (2013). Cloud Computing Pricing Models: A Survey. *International Journal Of Grid and Distributed Computing IJGDC*, *6*(5), 93–106. http://doi.org/10.14257/ijgdc.2013.6.5.09

[59]. Wikipedia. Retrieved September 27, 2015, from https://en.wikipedia.org/wiki/software_as_a_service

[60]. Welcome to HIPAA Survival Guide. Retrieved September 27, 2015, from http://www.hipaasurvivalguide.com/

[61]. HIPAA Security Rule compliance needs: Administrative safeguards. Retrieved September 27, 2015, from https://www.amsspher.com/hipaa-security-rule-compliance-needs-administrative-safeguards/

[63]. Evaluating Internet Research Sources. Retrieved September 27, 2015, from [61]. HIPAA Security Rule compliance needs: Administrative safeguards. Retrieved September 27, 2015, from https://www.amsspher.com/hipaa-security-rule-compliance-needs-administrative-safeguards/

[64]. In the olden days, spreadsheets were the holy grail for managing assets, but are they still efficient? Retrieved September 27, 2015, from http://www.cheqroom.com/blog/5-reasons-trade-in-excel-for-more-effective-software-tool/

[65]. Gong, Chunye et al. “The Characteristics Of Cloud Computing.” *2010 39th International Conference on Parallel Processing Workshops* (2010): n. pag. Web.

[66]. Abdelmaboud, Abdelzahir et al. “Quality Of Service Approaches in Cloud Computing: A Systematic Mapping Study.” *Journal of Systems and Software* 101 (2015): 159–179. Web.

[67]. Heilig, Leonard, and Stefan Voß. “Decision Analytics For Cloud Computing: A Classification and Literature Review.” Bridging Data and Decisions (2014): 1–26. Web.

[68]. Kavis, Michael. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). Print.

[69]. Mehak, Faria et al. “Security Aspects Of Database-as-a-Service (DBaaS) in Cloud Computing.” Computer Communications and Networks Cloud Computing (2014): 297–324. Web.

[70]. Pal, Shantanu. “Storage Security And Technical Challenges of Cloud Computing.” Data Intensive Storage Services for Cloud Environments (2013): 225–240. Web.

9. Appendix

APPENDIX A (OPERATIONAL METRICS)[52]

OPERATIONAL				
Category	**#**	**Metrics**	**A/C**	**Description**
Direct 24/7 support	8	technical_support_availability	A/C	This metric represents the technical support availability by provider.
	9	non_technical_support_availability	A/C	This metric represents the availability of non-technical support. Non-technical support refers to the sale of support, financial support, etc.
	10	ticket_system _availability	A/C	This metric represents the availability of support through the ticket system.
	11	phone _ availability	A/C	This metric represents the availability of support through phone contact by this provider.
	12	email_availaability	A/C	This metric represents the availability of support by email by this provider.
	13	livechat_availability	A/C	This metric represents the availability of support through live chat by this provider.
	14	livechat_support_languages	A/C	This metric represents supported languages by live chat.
	15	support_languages	A/C	This metric represents supported languages for technical or non- technical support.
	16	community_based_availability	A/C	This metric represents the existence of community behind a support system in order to get answers.
	17	remotely_support_availability	A/C	This metric represents the existence of the on-site, or remotely support by support technician.
	18	prenium_support_availability	A/C	This metric represents the existence of premium support by the service provider.
	19	pilot_solution_ availability	A/C	This metric represents the ability to pilot the solution by this provider. It is really important to look for proof points and results before you make a large investment especially in cloud computing areas.
	20	support_response_time	A/C	This metric represents the required response time to an issue.
Comprehensive and high-quality documentation	21	video_availability	A/C	This metric represents the availability of tutorial videos on the provider web site.
	22	quality_documentation_translation	A/C	This metric represents the quality of document's translations on the provider's web page indicated by end user.
	23	list_languages_supported	A/C	This metric represents names of translations that have been indicated in the provider's web page.
	24	UI_languages_supported	A/C	This metric represents names of the factual translation languages that have been indicated for user interface in the provider's web page.
	25	documentation_languages_supported	A/C	This metric represents the names of the documentation translation languages that have been indicated in providers' documentation.
High quality user interface controlling services	26	costCalculator_availability	A/C	This metric represents the availability of the cost calculator in the provider's web site.
	27	discountCalculator_availability	A/C	This metric represents the availability of the discount calculator in the provider's web site.
	28	console_ access_availability	A/C	This metric represents the availability of consoles in order to access to the system's performance and monitor potential issues. In this way the customer will know how well the system is working.
	29	control_ panel_availability	A/C	This metric represents the availability of access to the control panel if needed.

[52] [66]

OPERATIONAL				
Category	**#**	**Metrics**	**A/C**	**Description**
	30	GUI_ linux_ supported	A/C	This metric represents the availability of GUI for Linux.
	31	manageable_firewall_supported	A/C	This metric represents the availability of manageable firewalls for compute services by this provider.
	32	command_line_supported	A/C	This metric indicates whether the service provider supports the command line in order to manage the service.
High financial stability of the provider	33	sustain_ business_available	C	This metric represents the financial stability of the cloud provider and whether their business is stable in the long run.It is really important for customers to choose a cloud provider that is financially stable and not likely to go out of business. Cloud providers should inform their customers about their financial health, if they are secure and whether or not their services will be interrupted or fail entirely.
	34	audited_financial_provided	C	This metric represents the availability of audited financial statements by this provider.[53]
	35	price_frequency	C	This metric represents a history of the frequency of the reduction or increase in the cost to provide the services over time. This might be unexpected in terms of customer perspective and customer should be aware of that.
Low delay between service order and service delivery to the client	36	service_delivery_time	A/C	This metric represents the time taken from requesting a service to it being accessible via SSH. This metric is important in terms of quality standard for service delivery and would also be beneficial in ensuring that good service delivery standards are in place. (in seconds/minutes/hours/days)
	37	average_ issue_response_ time	A/C	This metric represents the average issue response time indicated by this provider. It should be written in the SLA.
	38	average_resolution_time	A/C	This metric represents the resolution time indicated by this provider. It should be written in the SLA.
Availability of discount feature	39	discount_supported	A	This metric represents the discount features supported by this provider.
		type_of_discount	A	This metric represents the types of discounts supported by this provider.
		discount_percentage	A	This metric represents the percentage of each discount type offered by this provider.

[53] http://en.wikipedia.org/wiki/Financial_audit

APPENDIX B (TECHNICAL MTRICS)[54]

TECHNICAL[55]				
Category	**#**	**Metrics**	**A/C**	**Description**
General information about cloud providers	40	name	A	This metric represents the name of the service provider.
	41	description	A	This metric represents the description and summary about cloud provider.
	42	URL	A	This metric represents cloud provider web site.
	43	abbreviated_name	A	This metric represents the abbreviated name for cloud provider.
	44	service_types	A	This metric represents the variety of services provided by the cloud service provider such as IaaS, PaaS and SaaS
	45	abbreved_serviceName	A	This metric indicates if an abbreviated name defines for the service.
	46	service_URL	A	This metric represents the associated link for each service type such as storage service, DNS service, etc.
	47	service_version	A	This metric represents the version of each service provided by the provider.
	48	service _is_singleTen	C	This metric indicates whether the service provider offers the single tenancy for the service. This feature shows how their data is isolated from other customers' data. This selection refers to how sensitive the elements of customers' system are.[56]
	49	service_is_ muTenancy	C	This metric represents whether the service provider offers multi tenancy for the service. This feature shows how their data is isolated from other customers' data.
	50	service_hosted_ pubCld	C	This metric represents whether the service is hosted in the public cloud.
	51	service_ hosted_ pc	C	This metric represents whether the service is hosted in the private cloud.
	52	SLA_charcteristics	A	This metric represents URL to the provider's SLA documentation and information to the end user.
	53	privacy_URL	A	This metric represents URL to the provider's privacy to the end user.
	54	agility_supported	A/C	This metric represents whether the service provider automatically updates or upgrades its business software in the cloud. This feature includes the reconfiguration of server in minutes, the reallocated of the resource to another project easily, etc. This requires a control panel or an API where the customer, the user, or the service provider, logs-in, turns on or off what is needed and the software that handles the rest.
	55	sustainability_potential	A/C	This metric indicates whether the service provider has sustainability potential. This feature can indicate whether the cloud provider is a leader in the market in which they have a long-term business strategy. For example AWS has very high long term sustainability potential because in its history, prices have reduced frequently and consistently as the cost to provide the services has reduced over time.
	56	3party_ supliers_envold	A/C	This metric represents whether the service provider works with third-party suppliers.
	57	Data_ durability	A	This metric indicates the durability of the service provider's dedicated data for a service. For example they can specify data stored in a service designed to provide 99.99999999% durability of objects over a given year. This feature requires that all objects should be redundantly stored on multiple devices across multiple facilities in a region. Once stored, service providers have to maintain the durability of objects by quickly detecting and repairing any lost redundancy. Service providers also regularly verify the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data.
Aauto scaling features	58	processBased _autoscaling _supported	A/C	This metric represents whether the service provider supports process based auto scaling. This requires an automatic increase in the number of processes when demand increases. Each process generally runs in an isolated container that provides memory, (ephemeral) storage and CPU capacity. In general there

[54] [65]

[55] [67]

[56] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/dedicated-instance.html

TECHNICAL[55]				
Category	**#**	**Metrics**	**A/C**	**Description**
				are two different types of processes on-demand or dedicated processes (may also be referred to as workers, threads or another name)
	59	VMBased_autoscaling_ _supported	A/C	This metric represents if provider supports VM based auto scaling. This metric is used by VM based platforms. Automatic scaling in case of VM based platforms refers to automatic increase in VM resource allocation.
	60	CPU_bursting_availaility	A/C	This metric represents if CPU bursting is available by the service provider. When there is a need to have more CPU cycles than is allocated to a virtual machine, this metric provides a temporary performance boost.
	61	resvrd_ procese_suport	A/C	This metric represents if provider supports reserved processes. This metric can be applicable when the provider offers auto scaling.
Freely configurable monitoring services	62	template_supported	A/C	This metric represents whether the service provider offers compute instance template types or configuration settings. The advantage of instance template is that the end user can build it once and then reuse it several times.
	63	horisontal_scaling	A/C	This metric represents whether the service provider offers horizontal scaling for the service.
	64	vertical_scaling	A/C	This metric represents whether the service provider offers vertical scaling for the service.
	65	instance_resizing	A/C	This metric represents if end user can resize the provisioned compute service instances.
	66	autoscal_JEE_ webApp	A/C	This metric represents the ways that clients can host their Java EE Application with auto scaling by the service provider.
	67	log_access	A/C	This metric represents the allowance of user access to their logs in order to monitor the system's performance to find potential issues.
	68	monit_ tools _available	A/C	This metric represents the availability of monitoring tools provided by the provider for having performance reports etc.
Available storage replication to secondary site	69	replication_models_supported		This metric represents the models of replication supported by the service provider. These models are database replication, disk storage replication, file-based replication, file system journal replication, batch replication, distributed shared memory replication, primary-backup and multi-primary replication etc.
	70	storage_replc_suported	A/C	This metric represents if service has made locally replicas of data stored within this storage service.
	71	storage_geo_replicas	A/C	This metric represents if service has made geographically disperse replicas of data stored within storage services. This metric is used for block storage services.
Fault tolerance features	72	loadBalancing_suported	A/C	This metric represents if network load balancing has been supported by the service provider. This feature aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any single resource and as a consequence high reliability through redundancy. In this case if a host goes down, the DNS service will stop sending traffic to it until it resolves the issue of that IP address.
	73	automaticFailovers_supported	A/C	T This metric represents if the automatic failover have been supported by this service. This feature shows a high degree of reliability and availability and also is required to geo redundantly. In this case when a primary target host fails a health check, DNS resolution automatically changes to a backup target host. Organizations may use automatic failover systems to protect against data loss in case of storms and natural disasters.
Number of layers on which backup service is available	74	snapshots_supported	A/C	This metric represents if any kind of snapshots for different storage types have been supported by the compute service.
	75	tape_backup_support	A/C	This metric represents if backups to tapes have been supported by service provider.
	76	use_own_backup_servc	A/C	This metric represents the allowance customers' have to perform their own backups.
	77	dataStorage_redundanc	A/C	This metric represents whether the service provider have a copy of data stored in different place by using multi-site copies of data objects.
	78	backup_mechansims	C	This metric represents the provided backup mechanisms offered by the service provider.
	78	customer_gateway_BGP	A/C	This metric represents the availability of the customer gateway configuration using Border Gateway Protocol. This metric is used by customers who want to use an IPsec hardware VPN with their virtual private cloud (VPC).
Security feature	79	VPN_conect_VPC_suprt	A/C	This metric represents if VPN connectivity to VPC networks are supported by this cloud service provider.

TECHNICAL[55]				
Category	**#**	**Metrics**	**A/C**	**Description**
	80	network_link_shared	A/C	This metric represents if this service provider if this service provider supports shared network links (share with other VMs on the same host) for the compute instance.
	81	integrity_algorithm	C	This metric indicates whether the service provider offers any kind of confidentiality and integrity checking algorithms as a means of security in order to secure data flow.
	82	network_link_dedicated	A/C	This metric represents if this service provider supports the dedicated network link for the compute instance.
	83	SSL_certif_suported	A/C	This metric represents if the standard SSL certificate has been supported by the service provider. SSL is used to secure credit card transactions, data transfers and logins.
	84	SNI_SSL_certificate	A/C	This metric represents if the SNI SSL certificate is supported by the service provider. SNI certificates allow multiple custom domains to be hosted from a single IP address. This is a more complete certificate than SSL. [57]
	85	SSLcontent_delvy_Media	A/C	This metric represents how SSL content is delivered by the service provider. For instance by using dedicated IPv4, SNI based, generic domain name
	86	SSH_supported	A/C	This metric represents if the SSH has been supported by the service provider. SSH provides a secure channel over an insecure network in a client-server architecture.
	87	use_own_encryption	A/C	This metric indicates whether customers can use their own encryption mechanisms for the services.
	88	serverSide_encryp_tech	A/C	This metric represents whether the service provider offers server side encryption technology as an option for customers.
	89	3Party_encryp_ tech	A/C	This metric represents whether the service provider offers third-party encryption technology as an option for customers.
	90	physical_ sec_suported	A/C	This metric represents whether the provider meets high levels of physical security.
	91	internal _cntrl_suported	A/C	This metric represents whether the provider meets high levels of internal control.
	92	firewall_types_suported	A/C	This metric represents the types of firewalls and detection systems which are in operation to guard against malicious network activity or system attacks.
	93	data_encpt_tequniques	C	This metric indicates whether encryption approaches have been used to ensure data confidentiality by this cloud service provider.
	94	IAM_ supported	A/C	This metric represents whether the service provider offers Identity and Access Management for the services. This will protect against possible threat sources such as entering any unknown user to the virtual machines.
	95	incident _response_ plan	A/C	This metric represents whether the service provider offers Incident response plan to customers or not. This feature is used for avoiding any security breaches, in this case provider are able to handle the situation in a way that limits damage and reduces recovery time and costs.
	96	own_ sec_ artichecture	A/C	This metric represents whether the service provider allows customers to implement their own security architecture.
	97	access_client_media	A/C	This metric represents whether the service provider allows customers to secure and manage access from clients' device (e.g. PC, mobile) to their own requirements.
	98	where_data_encripted	A/C	This metric represents whether the service provider encrypts data while in storage and when being transmitted over the Internet.
Service Availability	99	average _service_downtime	A/C	This metric represents an average service downtime dedicated by service provider for the designated time interval in seconds. This can be done through the service provider or some third part companies. For example Panopta provides network and server availability monitoring in order to check constantly servers and other devices to ensure they are online and performing properly. Also they offer to monitor resource utilization for general server health and application metrics.
	100	average _service _outge	A/C	This metric represents average service outages that occurred during the designated time period. This feature normally dedicates by the service provider.
	101	service_status	A/C	This metric represents what a current service status is.

[57] http://www.networking4all.com/en/ssl+certificates/faq/server+name+indication/

TECHNICAL[55]				
Category	**#**	**Metrics**	**A/C**	**Description**
	102	geo_endpoint_ region	A/C	This metric represents where data end point is and data goes through bandwidth. This feature can have a direct effect on price. Sometimes prices are defined based on this feature. This is applicable for CDN or DNS where services are distributed.
	103	service_provisioned_location	A/C	This metric represent where service is provisioned. This feature is applicable where not all cloud services are available in all the regions and some services can only be available in some data centres.
	104	recovery_ time_estimated	A/C	This metric represents the recovery time dedicated by the service provider. Provider should test the disaster recovery plan and iron out any obvious deficiencies.
	105	annu _uptime _percet	A/C	This metric represents the percentage of the annual uptime of the service indicated by the provider.
data compatibility	106	businss _app_compatble	C	This metric represents whether the cloud solutions offered by provider supports the specific business application, such as accounting package.
	107	busins_ envrmt_compatbe	C	This metric represents whether the cloud solutions offered by provider is compatible with customer business environments.
	108	browser_compatibility	C	This metric represents whether the service runs in the same browser that customer need to use or if it requires multiple browsers for their users.
	109	busne_continuity_supp	A /C	This metric represents whether the service provider operates a business continuity program.
Data portability	110	export _data_supported	A/C	This metric represents whether the service provider supports exporting data and moving data to out of the service.
	111	import _data_supported	A/C	This metric represents whether the service provider supports importing data and moving data into provider's services.
	112	data_movement_media	A/C	This metric represents the list of the devices which are available to move data on and off storage.
	113	max _import_capacity	A/C	This metric represents the maximum amounts of data being moved as import into provider's services.
	114	max _export_capacity	A/C	This metric represents the maximum amounts of data being moved as export out of the provider's services.
	115	import_export_velocity	A/C	This metric represents the speed of importing and exporting data into/out of the provider's services.
JMS compatible message queuing service	116	data_pattern_types	C	This metric represents the different types of data exchange which service subscribers access queues and or topics to do that. They can use point-to-point or publish and subscribe patterns. One example of this feature is that a Call Centre can carry on servicing requests for bills to be presented when the billing system is unavailable. This feature is provided by e.g. by Amazon Simple Queue Service.
	117	availability_ msg_queuing	A/C	This metric represents the availability of message queuing service by the provider.
	118	java_message _service	C	This metric represents the availability of Java Message Service which is used for sending messages between two or more clients. [58]

[58] https://en.wikipedia.org/wiki/Java_Message_Service

APPENDIX C (COMPUTE INSTANCE)[59]

COMPUTE INSTANCE				
Category	**#**	**Metrics**	**A/C**	**Description**
General information	119	name	A	This metric represents the name of compute instances offered by the service provider.
	120	description	A	This metric represents the description of each compute instance.
	121	instane_type_suportd	A	This metric represents the types of the instances supported by this compute service.
	122	instane_type_location	A/C	This metric represents the variety of locations for a compute instance by the cloud provider.
	123	multiple_IP_suported	A/C	This metric represents the assignment of multiple IP addresses to a single compute instance supported by this compute instance. This metric is used for high availability and load balancing.
	124	VPC_supported	A/C	This metric represents whether the virtual private cloud (VPC) has been supported by the compute service. VPC allows users to create and deploy compute instances to logically or physically isolated networks.
Technical features	125	CPU_model	A	This metric represents the CPU model allocated for each compute instance. For example Intel Xeon E5-2620.
	126	number_CPU_sockets	A	This metric represents the number of cores per CPU allocated for each compute instance.
	127	CPU_clock	A	This metric represents the amount of CPU clock allocated for each instance type.
	128	CPU_sockets	A	This metric represents the number of CPU sockets allocated for this compute instance.
	129	CPU_cores	A	This metric represents the number of CPU cores allocated for this compute instance.
	130	CPU_quantity	A	This metric represents the quantity of CPU allocated to each compute instance.
	131	RAM_quantity	A	This metric represents the quantity of RAM allocated to each compute instance.
	132	local_disk_ raid	A	This metric represents the hardware raid level allocated for the local disks .The instance type should include the hardware raid controller.
	133	local_disk_RPM	A/C	This metric represents the spindle RPM for local disks.
	134	local_disk_type	A	This metric represents the types of local disk. It includes SATA, SAS or SSD, etc.
	135	supported_OS	A	This metric represents the operating systems supported by each compute instance.
	136	number_localStorage Disks	A/C	This metric represents the number of local storage disks allocated to each compute instance.
	137	amount_localStorage	A	This metric represents the amount of local storage across all disks in gigabytes allocated to each compute instance.
	138	max_ storage_volume	A/C	This metric represents the maximum number of storage volumes. Sometimes multiple storage volumes are attached to a compute instance. This volume is important for the end user.
	139	max_CPU_cores_temp late	A/C	This metric represents the maximum CPU cores for a compute instance template.
	140	max_memory_templa te	A/C	This metric represents the maximum memory for a compute instance template.
	141	max_storage_size	A	This metric represents the maximum size per storage for a compute instance in terabytes.
	142	IPv6_supported	A/C	This metric represents if the IPv6 networking has been supported by this compute instance.
	143	extra_IPv4_supported		This metric indicates whether the extra IPv4 networking has been supported by this compute instance.
	144	free_ IPv4_available	A/C	This metric represents at least one free IPv4 address per compute instance that has been supported by this service provider.
	145	free_ IPv6_available	A/C	This metric represents at least one free IPv6 address per compute instance that has been supported by provider.
	146	low_spec_ characteristics	A	This metric represents the low specification that has been allocated for each compute instance.

[59] [68]

COMPUTE INSTANCE				
Category	**#**	**Metrics**	**A/C**	**Description**
	147	high_spec _characteristics	A	This metric represents the high specification that has been allocated for each compute instance.
Finance	148	purchase_ options	A	This metric represents the predefined purchase options by the service provider.

APPENDIX D (PAAS METRICS)

PLATFORM AS A SERVICE [60]				
Category	**#**	**Metrics**	**A/C**	**Description**
General information	149	instance_types_supported	A	This metric represents instance types supported by PaaS. This metric is used for VM based platforms only.
	150	name	A	This metric represents the name of the PaaS provider.
	151	description	A	This metric represents the description of the PaaS provider.
	152	link	A	This metric represents the link of the PaaS provider.
Support	156	customer_support	A/C	This metric represents the different types of the customer supports provided by the PaaS provider. Customer service is really important between PaaS providers because PaaS vendors build layers between and around various services such as application to database transactions and this necessitates a much closer relationship between developer and provider.
platform properties	153	supported_programming_Languages	A	This metric represents the list of the programming languages supported by the PaaS provider.
	154	dataBase_supported	A	This metric represents the list of the data bases supported by the PaaS provider.
	155	additional _services_supported	A	This metric represents the list of the additional services supported by the PaaS provider. Some examples are logging services, monitoring services, emailing services, queuing services, DNS services, payment services etc.
	157	security_regulation_types	A/C	This metric represents the types of the security and regulatory compliance taken by the PaaS provider.
	158	PaaS_availability		This metric represents the PaaS availability which is dedicated by the service provider. For example data stored in a service is designed to provide 99.99% availability of objects over a given year.
	159	unauthorize_access_checking	A/C	This metric indicates if the unauthorized access has been checked by the PaaS provider. This metric refers to the leak of customers' information and proprietary information.
	160	data_recovery_supported	A/C	This metric represents the ability of data recovery if the provider fails by the PaaS provider.
	161	application _performance	C	This metric represents how customers can manage the application performance.
	168	service_access_media	A/C	This metric represents the different medias which customer can access to the PaaS services. It can be both directly and through add-ons from the provider.
	169	automated_ failover_supported	A/C	This metric represents the availability of automated failover by the PaaS provider.
	170	backup_supported	A/C	This metric represents the availability of back up options by the PaaS provider.
	171	automated_ scaling_supported	A/C	This metric represents the availability of automated scaling by the PaaS provider.
	172	add_on_ supported	A/C	This metric indicates if the PaaS provider supports add-ons in order to access to services.
	173	free _trials_ supported	A/C	This metric represents the availability of free trials by the PaaS provider.
	174	cache_ servers_supported		This metric represents weather or not the company offers cash servers to the customers.
	175	integrated_supported	A/C	This metric represents if the PaaS provider offers integrated support for some additional services like performance issues and if it is essential to run cache servers, like Mem cached or Redis. The vendor should provide integrated support for this.

[60] [68]

PLATFORM AS A SERVICE [60]				
Category	**#**	**Metrics**	**A/C**	**Description**
Business continuity	162	businessContinuity _readiness	C	This metric represents the readiness of policies and procedures to operate business continuity by the PaaS provider.
	163	disasterRecovery_readiness	C	This metric represents the readiness of policies and procedures to operate DR (disaster recovery) by the PaaS provider.
Subjective features for PaaS	165	buisiness_viabilty	C	This metric represents the level of the customer satisfaction and loyalty of the PaaS provider.
	166	vendor_lockin	C	This metric represents the level of vendor lock-in" by this provider. This metric is really important when a vendor attempts to keep its clients by making it difficult for them to leave. [61]- [62]
	167	technology_ maturity_features	C	This metric represents the features and general maturity of technology used by the PaaS provider.
	164	legacy_integration_problem	C	This metric represents how the cloud data can be integrated with customer internal systems.
Finance	176	purchase_ option	A	This metric represents the predefined purchase options by the service provider.

[61] http://www.cetrom.net/blog/paas-vendor-lock/#sthash.NsyDJSpc.dpuf

[62] http://iamondemand.com/blog/the-cloud-lock-in-part-2-the-great-lock-in-of-paas/#sthash.GAkpC6Gk.dpbs

APPENDIX E (STORAGE METRICS)[63]

STROAGE SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
General information	177	storage_name	A	This metric represents the name of the storage service.
	178	storage_description	A	This metric represents the description of the storage service.
Storage properties	179	storage_type_supported	A	This metric represents the types of storage service such as block storage, object storage and archive storage.
	180	type_of_volume_supported	A	This metric represents the standard volume types have been supported by this provider such as SSD volumes.
	181	data_ durability	A/C	This metric represents the percentage of data durability which the service provide indicated for storage service.
	182	data_ availability	A/C	This metric indicates whether the data availability of the service has been mentioned by the cloud service provider.
	183	accessLevel_ storage_supported	A/C	This metric represents the level of access to the storage that can be an object level access or block level access, etc. supported by this provider. The difference in the way the data can be stored as multiple copies of data over a distributed system.
	184	compute_throughput _storage	A/C	This metric represents the throughput capacity in megabits/sec between compute instances and storage platform. This metric depends on the type of the storage service. It means that it can be used with some types such as block storage service.
	185	disk _RPM	A	This metric represents the spindle RPM speed of the hard disks have been used by the provider for this storage service.
	186	hardDisks_ type	A	This metric represents types of hard disks have been used by the provider for this storage service.
	187	provisionedIOPS_supported	A	This metric represents the availability of the pre-provisioning/allocation of IOPS by this storage service which can be used normally with block storage services.
	188	IOPS_block_ size	A	This metric represents the block size in kilobytes that the IOPS values are based on. (E.g. 16KB). This metric uses for block storage services.
	189	max_Iops _supported	A	This metric represents the maximum number of IOPS has been supported for the storage. This metric is used for block storage services.
	190	max_volume_size	A	This metric represents the maximum size per volume in terabytes. It is used for block storage services.
	191	max_ volume	A	This metric represents the maximum number of distinct volumes. It uses for block storage services.
	192	max_volumes_windows	A	This metric represents the maximum number of distinct volumes that can be allocated specifically to Windows compute instances. It is used for block storage services. This metric can be different for Windows compared to other operating systems.
	193	allocated_computeInstance_storage	A	This metric indicates whether or not this storage service is limited to a subset of the compute instance types. It is used for block storage services associated with a compute service.
	194	storage_raid_level	A	This metric represents the raid level has been used by the provider for this storage service.
	195	storage_size_limits	A	This metric represents the volume limitation for this storage service.
	196	IO_performance	A/C	This metric represents the input/output performance indicated in the benchmarking.
	197	max_upload_size	A/C	This metric represents the volume of data can that be stored by storage service.
	198	free_ retrieval _limits	A/C	This metric represents the allowance of free retrieval supported by this provide. For example, if up to 7% of your data stored in storage can be retrieved for free each month.
	199	low_spec_ characteristics	A/C	This metric indicates whether or not the low specification has been allocated for each storage service.

[63] [70]

STROAGE SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
	200	high_spec_ characteristics	A/C	This metric represents the high level specification that has been allocated for each storage service.
	201	data_storage_redundancy	A/C	This metric represents whether the cloud provider has considered the data storage redundancy.
Finance	202	purchase_ options	A	This metric represents the predefined purchase options by the service provider.

APPENDIX F (DBAAS)[64]

DATA BASE AS A SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
General information	203	name	A	This metric represents the names of data bases offered by the service provider.
	204	description	A	This metric represents the descriptions of each service.
	205	link	A	This metric represents the links to each service.
Database features	206	relational_ database_services_supported	A/C	This metric indicates whether the relational data base has been supported by the service provider.
	207	NoSQL_ database_ services	A/C	This metric indicates whether the NOSQL data base is supported by the service provider.
	208	low_spec_ characteristics	A/C	This metric represents the minimum specification necessary to run the data base.
	209	high_spec_ characteristics	A/C	This metric represents the maximum specification necessary to run the data base.
	210	storage_ size_ limits	A/C	This metric represents the limit of the storage volume used for a specific data base.
	211	throughput _limits	A/C	This metric represents the limitation of throughput supported by this data base. For instance this can be up to 20,000 queries per day.
	212	instance_type_supported	A/C	This metric represents the variety of instance types or classes which data base services can run in top of them. This instance types are helpful for supporting the different types of workloads.
	213	self-adapting_NoSql _sharding	A/C	This metric represents the distribution of data across multiple partitions called shards. This metric is used when data grows and the size of clusters change considerably. This metric helps to balance the data in such situation along with the hardware limitations.
	214	Relational_ database _replication	A/C	This metric represents the availability of the relational data base replication by the service provider.
	215	RAM_quantity	A	This metric represents the quantity of RAM supported by a data base.
	216	CPU_quantity	A	This metric represents the quantity of CPU supported by a data base.
	217	CPU_ model	A	This metric represents the model of CPU supported by a data base.
Finance	218	purchase_ option	A	This metric represents the predefined purchase options by the service provider.

[64] [69]

APPENDIX G (CDN MATRICS)[46 47]

CDN SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
CDN technical Properties	219	limiting_access_ content_supported	A/C	This metric represents the limiting of access to content supported by provider.
	220	content_pull_supported	A/C	This metric represents the availability of the CDN content pull method in order to serve customer content. This is an important option where the CDN edge pulls content from an HTTP accessible origin or Reverse Proxy. The Pull method CDN will then cache that file until it expires.
	221	content_push_supported	A/C	This metric represents the availability of the CDN content Push method in order to serve customer content. This is similar to Poll method, the difference is that in content push, the CDN provides a means of FTP, SCP, rsync, etc. for customers to upload content to a storage repository. In this case, clients are responsible for providing content to the CDN, pushing it to the network, specifying the content that is uploaded, when it expires and when is updated.
	222	access_federatedServerLogs _supported	A/C	This metric represents the availability of access to federated server access logs by CDN provider. These logs include the history of CDN edge servers where customer content was accessed and stored on a user accessible storage platform.
	223	routing_method	A/C	This metric represents the routing methods that have been implemented in the CDN provider. A CDN may employ multiple methods such as 'edge-anycast', 'dns-anycast', 'dns', 'edns', 'proprietary' etc. These methods are used to improve performance. However, the prices differ according to the complexity of installation.
	224	edge_purging_supported	A/C	This metric indicates whether the CDN allows customers to manually remove or replace cached content before it expires. Edge purge is useful when you need to quickly remove or replace cached content from all CDN edge servers.
	225	network_speed	A/C	This metric represents whether the service provider has assessed the physical speed of the network and delivery service for the end users.
	226	network_outage	A/C	This metric represents whether the service provider has measured the network outages for the end users.
	227	outage_compensation	A/C	This metric represents whether the service provider has been compensated in case of an outage of the network or any portion of its hardware that has affected him.
	228	data _accessibility	A/C	This metric represents whether the service provider allow customer to access and upload contents at all times.
	229	CDN_monitoring	A/C	This metric represents whether the service provider allows monitor of the network uptime by the end user.
	230	multipleSite_low latency_ highBW	C	This metric represents the Availability of multiple site infrastructures with low latency, high BW LAN interconnect by this provider.
Finance	231	purchase_ options	A	This metric represents the predefined purchase options by the service provider.

APPENDIX H (DNS METRICS)[48]

DNS SERVICE				
Category	**#**	**Metrics**	**A/C**	**Description**
DNS technical properties	232	routing_locationBased_Edns	**A/C**	This metric represents if the location based routing support EDNS (IP forwarding from the name server) is available by this provider. IP forwarding helps to determine over which path a packet or datagram can be sent in multiple networks.
	233	DNS_ sync_method	**A/C**	This metric represents which methods for DNS synchronisation are operated by this provider. These methods are standard master/slave DNS synchronization including support for NOTIFY (ability to send or receive), AXFR (full zone transfer), IXFR (incremental zone transfer) and TSIG (Transaction Signature).
	234	DNSSEC_mngmnt _suported	**A/C**	This metric represents the availability of the domain Name System Security Extensions by the service provider. DNSSEC is used to protect clients from forged DNS responses by digitally signing DNS responses. By checking the digital signature, DNS clients can verify the authenticity of those responses.
	235	core _competency	A/C	This metric represents whether this provider offers DNS as main core business or just as an add-on service. This feature shows that, if customers are looking for a specific service, then it is better to go for those providers that provide such a service as their main core. [65]
	236	DNS_media	**C**	This metric represents whether this service from which medias or devices deliver DNS.
	237	monitoring_supported	**A**	This metric represents whether this service provider allow tracking of the record of uptime and availability to the end user.
	238	multiple_ nameServerClusters_ supported	A/C	This metric represents whether the service provider operates multiple name server clusters.
	239	anycast_supported	**C**	This metric represents whether the service provider employs anycast. This feature is used for Enhanced Availability, Increased Reliability, Load Balancing, Increased Performance and Attack Mitigation.[66]
	240	deliver_DNS_resolving	**C**	This metric represents whether the service provider dedicates how fast it is to deliver resolving DNS.
	241	BIND_supported	**C**	This metric represents whether the service provider use BIND or similar server technology that has known security issues.
	242	DNS_ failover_ supported	A/C	This metric represents whether the service provider supports DNS failover.
	243	GEO_ DNS _supported	A/C	This metric represents whether the service provider supports GEO DNS.
	244	DNS_performance	**C**	This metric represents whether the service provider estimates DNS performance. Performance means that the provider's ability to resolve DNS queries quickly for users around the globe.[67]
	245	total_ uptime_DNS	A/C	This metric represents whether the service provider has estimated the total Uptime in DNS.
	246	DNSSEC_management _supp orted	A/C	This metric represents whether the service provider has provided domain Name System Security Extensions.
Finance	247	purchase_options	A	This metric represents the pre-defined purchase's options by the service provider.

[65] http://totaluptime.com/the-top-5-things-to-look-for-in-a-dns-service-provider/

[66] http://totaluptime.com/what-is-ip-anycast-and-how-does-it-work-in-the-cloud/

[67] http://totaluptime.com/the-top-5-things-to-look-for-in-a-dns-service-provider/

APPENDIX I (GENERIC SURVEY QUESTIONNAIRE 1)

Map Q with metrics	#	End Users Questions Generic Survey Questioner (Part one)
107	1	**How satisfied are you with the way which the data in the cloud is integrated with your company data?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
8	2	**How satisfied are you with the quality of non-technical support in this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
1-2	3	**How satisfied are you with this cloud provider´s certifications?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
1-2	4	**How satisfied are you with the way the cloud provider´s certification meets your needs?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
8-9	5	**How satisfied are you with the quality of support in this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
8	6	**How satisfied are you with the technical support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
9	7	**How satisfied are you with the non-technical support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
10	8	**How satisfied are you with the ticket system support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
11	9	**How satisfied are you with the phone support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
12	10	**How satisfied are you with the email response time of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
13	11	**How satisfied are you with the live chat support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
22	12	**How satisfied are you with the quality of document translation in this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
16	13	**How satisfied are you with the community support provided by this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
16	14	**How satisfied are you with the quality of self service support in this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
18	15	**How satisfied are you with the premium support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
17	16	**How satisfied are you with the remote support of this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
19	17	**How satisfied are you with the pilot solution?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
52	18	**How satisfied are you with the actual response time as compared to the response time indicated in the SLA?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
20	19	**How satisfied are you with the quality of response from this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
21	20	**How satisfied are you with the tutorial videos provided by company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
24	21	**How satisfied are you with the quality of user manual provided by company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
22	22	**How satisfied are you with the quality of documentation provided by company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
24	23	**How satisfied are you with the quality of user interface translation?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
26	2	**How satisfied are you with the cost calculator offered by this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
27	25	**How satisfied are you with the discount calculator provided by this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
34	26	**How satisfied are you with the audited financial statements provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
52	27	**How satisfied are you with the ease of termination of the contract should the company not fulfil its contractual obligations?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
39	28	**How satisfied are you with the discount percentage provided?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

Map Q with metrics	#	End Users Questions Generic Survey Questioner (Part one)
60	29	**How satisfied are you with the provided CPU bursting?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
61	30	**How satisfied are you with the reserved process provided by provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
64	31	**How satisfied are you with the provided vertical scaling?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
63	32	**How satisfied are you with the provided horizontal scaling?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
65	33	**How satisfied are you with the provided instance resizing?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
116-117	34	**How satisfied are you with the message queuing service?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
68	35	**How satisfied are you with the monitoring services offered?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
213	36	**How satisfied are you with the supported NoSql database sharding?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
230	37	**How satisfied are you with low latency, high BW LAN interconnect and BGP routing of multiple site infrastructure?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
72-73	38	**How satisfied are you with the provided health Checks mechanism?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
72	39	**How satisfied are you with the provided load balancing mechanism?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
73	40	**How satisfied are you with the provided automatic failovers mechanism?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
78	41	**How satisfied are you with the provided backup mechanism?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
74	42	**How satisfied are you with snapshot mechanism offered by this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
100	43	**How satisfied are you with the estimated total average service downtime indicated by this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
102	44	**How satisfied are you with the locations of provided service?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
105	45	**How satisfied are you with the annual uptime percentage indicated by the provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
113-114	46	**How satisfied are you with the ease of migration from this provider to another provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
155	47	**How satisfied are you with the additional services (such as monitoring services, monitor application performance, emailing services, queuing services...)?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
156	48	**How satisfied are you with the PaaS customer support?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
159	49	**How satisfied are you with the protection of sensitive data provided in PaaS company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
162-163	50	**How satisfied are you with the business continuity and disaster recovery provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
167	51	**How satisfied are you with the level of maturity of the technology of this PaaS provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
169	52	**How satisfied are you with automated failover provided by PaaS company** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
170	53	**How satisfied are you with supported backup strategies by the cloud provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
171	54	**How satisfied are you with automated scaling provided by PaaS company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
172	55	**How satisfied are you with supported add-ons in order to access specific service?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
173	56	**How satisfied are you with free trials provided by company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
174	57	**How satisfied are you with the cash server provided by this company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

Map Q with metrics	#	End Users Questions Generic Survey Questioner (Part one)
206	58	**How satisfied are you with relational database services provided in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
207	59	**How satisfied are you with NoSQL database services provided in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
206-207	60	**How satisfied are you with the provided data base software in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
210	61	**How satisfied are you with the allocated storage limit for database in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
215	62	**How satisfied are you with the allocated RAM quantity for database in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
216	63	**How satisfied are you with the allocated CPU quantity for database in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
217	64	**How satisfied are you with the allocated CPU model for database in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
31	65	**How satisfied are you with the manageable Firewall provided by the company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
124	66	**How satisfied are you with the virtual private cloud service of compute instance for this cloud provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
125	67	**How satisfied are you with the CPU model of compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
128	68	**How satisfied are you with the allocated number of CPU sockets for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
127	69	**How satisfied are you with the allocated CPU clock for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
129	70	**How satisfied are you with the allocated CPU core for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
130	71	**How satisfied are you with the allocated CPU quantity for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
131	72	**How satisfied are you with the allocated RAM quantity for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
132	73	**How satisfied are you with the allocated local disk raid for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
133	74	**How satisfied are you with the allocated local disk RPM for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
134	75	**How satisfied are you with the allocated local disk type for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
135	76	**How satisfied are you with the allocated operating system for each compute instance in this cloud company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
122	77	**How satisfied are you with locations of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
136	78	**How satisfied are you with the number of local storage disks of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
137	79	**How satisfied are you with the amount of local storage of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
138	80	**How satisfied are you with the maximum storage volume of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
139	81	**How satisfied are you with the maximum CPU Cores template of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
140	82	**How satisfied are you with the maximum memory template of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
141	83	**How satisfied are you with the maximum storage size of each compute instance type?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
144	84	**How satisfied are you with the number of free IPV4s?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
145	85	**How satisfied are you with the number of free IPV6?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
179	86	**How satisfied are you with the supported storage types offered by this cloud provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
183	87	**How satisfied are you with the supported access level of storage offered by this cloud provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

Map Q with metrics	#	End Users Questions Generic Survey Questioner (Part one)
133-185	88	**How satisfied are you with the RPM speed of the hard disks used by this provider?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
187	89	**How satisfied are you with the pre-provisioning/allocation IOPS for block storage services?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
188	90	**How satisfied are you with IOPS block size of block storage services?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
189	91	**How satisfied are you with the maximum number of IOPS supported for block storage services?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
194	92	**How satisfied are you with storage raid level used by this provider for this storage service?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
196	93	**How satisfied are you with IO performance for the block storage services?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
244	94	**How satisfied are you with this DNS's service performance?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
245	95	**How satisfied are you with this DNS's service uptime time?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
234	96	**How satisfied are you with provided domain name system security extensions of this DNS company?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide

APPENDIX J (GENERIC SURVETY END USER QUESTIONNAIRE 2)

Map Q with metrics	#	End users Questions Generic Survey Questioner (Part two)
107	1	**Is your current business environment compatible with this cloud service?** Yes/No/Don't know
113-114	2	**Does the provider allow customers to move data on and off storage as needed?** Yes/No/Don't know
115	3	**Can the data stored by this service provider be exported at your request?** Yes/No/Don't know
5	4	**Have you had any bad experiences regarding authorization access to your data?** Yes/No/Don't know **If Yes give a brief summary**
1-2	5	**Does this cloud provider's certifications fulfil your needs?** Yes/No/Don't know
13	6	**Does this provider offer live chats in the languages with which you are familiar?** Yes/No/Don't know
15	7	**Does this provider offer support in the languages with which you are familiar?** Yes/No/Don't know
21	8	**Does the provider offer video tutorials?** Yes/No/Don't know **If yes How satisfied are you with the quality of video tutorials?** 1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide
24	9	**Is the interface available in your preferred language?** Yes/No/Don't know
33	10	**Does this cloud provider have long term sustainability potential for its service?** Yes/No/Don't know
87	11	**Do you prefer to use your own encryption mechanism?** Yes/No/Don't know
67	12	**Can you access the system logs?** Yes/No/Don't know
214	13	**Does this cloud provider use replication techniques for the relational database?** Yes/No/Don't know
72-73	14	**Does this cloud provider support health Checks?** Yes/No/Don't know
72	15	**Does this cloud provider support load Balancing?** Yes/No/Don't know
73	16	**Does this cloud provider support automatic failovers?** Yes/No/Don't know
70	17	**Does this cloud provider support storage replicas?** Yes/No/Don't know
71	18	**Does this cloud provider support storage geographic replicas?** Yes/No/Don't know
74	19	**Does this cloud provider support snapshots?** Yes/No/Don't know
75	20	**Does this service provider offer backups to tapes?** Yes/No/Don't know
76	21	**Does this cloud provider allow you to perform your own backups?** Yes/No/Don't know **If yes, How satisfied are you with this option?** **1.Very Satisfied 2.Moderately Satisfied 3.Satisfied 4.Dissatisfied 5.Very Dissatisfied 6.Doesn´t provide**
101	22	**Have you ever experienced service status for specific regions different from those indicated by the cloud provider?** Yes/No/Don't know
156	23	**Do you feel a close relationship between yourself and this company?** Yes/No/Don't know
142	2	**Does this cloud provider support IPV6 addresses?** Yes/No/Don't know
193	25	**Do you know what the allocated compute instances to the storage service are?** Yes/No/Don't know
201	26	**Does this provider support data storage redundancy?** Yes/No/Don't know

Map Q with metrics	#	End users Questions Generic Survey Questioner (Part two)
219	27	**Are streaming media delivery services written in the SLA?** Yes/No/Don't know
228	28	**Are you able to access and upload your content at all times?** Yes/No/Don't know
225	29	**Have you experienced any problems with the physical speed of the network and delivery service with this CDN provider?** Yes/No/Don't know
226	30	**Have you experienced any network outages with this CDN provider?** Yes/No/Don't know
229	31	**Does this provider allow to monitor network uptime?** Yes/No/Don't know
231	32	**Does the provider charge for "bursting overages"?** Yes/No/Don't know
237	33	**Does this company allow to track records for uptime and availability to the end user?** Yes/No/Don't know
241	34	**Does this provider allow you to define different roles or levels of access to the DNS management interface?** Yes/No/Don't know

APPENDIX K (GENERIC PROVIDER QUESTIONNAIRE)

Map Q with metrics	#	Generic Cloud Provider Questions Generic Provider Questioner
5	1	**Apart from your company, can anyone else access the customer data?** Yes/No **If Yes, Who? Under what conditions? At what level are they allowed access?**
52	2	**Are there Service Level Agreements (SLAs) that back everything up?** Yes/No
56	3	**Does your organization work with third-party suppliers?** Yes/No
7	4	**Does your company provide a data processing agreement with customers?** Yes/No
9	5	**Does your organization provide sales/ financial supports for free?** Yes/No
10	6	**Does your organization support ticket systems?** Yes/No
16	7	**Does your organization provide any kind of community support for the customers?** Yes/No
17	8	**Does your organization provide remote support for all the customers?** Yes/No
19	9	**Does your organization provide any pilot solutions for the customers?** Yes/No
21	10	**Does your organization provide videos to enhance your documentation?** Yes/No
26	11	**Does your organization provide cost calculator for the customers?** Yes/No
27	12	**Does your organization provide a discount calculator for the customer?** Yes/No
34-35	13	**Can your company ensure financial stability to the customers?** Yes/No
33	14	**Does your organization provide an agreement for the stability of price during contract time?** Yes/No
34	15	**Does your company provide audited financial statements to their customers?** Yes/No
60	16	**Does your organization support CPU bursting?** Yes/No
61	17	**Does your organization support reserved process?** Yes/No
63-64	18	**Does your organization support vertical/horizontal scaling?** Yes/No
65	19	**Does your organization support instance resizing?** Yes/No
116-117	20	**Does your organization support message queuing services?** Yes/No
67	21	**Does your organization enable customers to access logs?** Yes/No
68	22	**Does your organization allow customers to monitor services?** Yes/No
213	23	**Does your organization support NoSql database sharding?** Yes/No
230	2	**Does your organization permit multiple site infrastructure with low latency, high BW LAN interconnect and BGP routing?** Yes/No
214	25	**Does your organization use replication techniques for the relational database?** Yes/No
70	26	**Does your organization support storage replicas?** Yes/No
71	27	**Does your organization support storage geographic replicas?** Yes/No
78	28	**Does your organization support any types of backup?** Yes/No

Map Q with metrics	#	Generic Cloud Provider Questions Generic Provider Questioner
74	29	**Does your organization support snapshots?** Yes/No
75	30	**Does your organisation offer backups to tapes?** Yes/No
76	31	**Does your company allow customers to perform their own backups?** Yes/No
103	32	**Are all the cloud services available in all regions?** Yes/No **If no, please list those unavailable?**
156	33	**Does your company provide closer support and relationship between developer and company for PaaS services?** Yes/No
162-163	34	**Does your company provide business continuity and disaster recovery?** Yes/No
166	35	**Does your company present stronger company lock-in in compared with the other companies?** Yes/No **If yes, how flexible and standard is this cloud provider?**
169	36	**Does your company provide automated failover for the customers?** Yes/No
171	37	**Does your company provide automated scaling to the customers for the PaaS service?** Yes/No
172	38	**Does your company provide access to services through add-ons from other companies?** Yes/No
173	39	**Does your company provide any free trials for end users?** Yes/No
174	40	**Does your company offer cash servers to the customers?** Yes/No
206	41	**Does your organization provide relational database services?** Yes/No
207	42	**Does your organization provide NoSQL database services?** Yes/No
123	43	**Does your company provide multiple IP addresses to a single compute instance?** Yes/No
31	44	**Does your organization provide a manageable Firewall for the customer?** Yes/No
124	45	**Does your company support virtual private cloud for the logically or physically isolated networks?** Yes/No
142	46	**Does your company support IPV6?** Yes/No
144	47	**Does your company support free IPV4?** Yes/No
145	48	**Does your company support free IPV6 in your company?** Yes/No
187	49	**Does your company support the pre-provisioning/allocation of IOPS for block storage services?** Yes/No
201	50	**Does your organization support data storage redundancy?** Yes/No
219	51	**Does your company support limited access to content?** Yes/No
228	52	**Does your company allow customers to access and upload content at all times?** Yes/No
220	53	**Does your organization support CDN content pull?** Yes/No
225	54	**Does your organization assess the physical speed of the network and delivery service for the end users?** Yes/No
221	55	**Does your organization support CDN content push?** Yes/No
226	56	**Does your organization measure network outages for the end users?** Yes/No
222	57	**Does your company support access to federated server access logs?** Yes/No

Map Q with metrics	#	Generic Cloud Provider Questions Generic Provider Questioner
229	58	**Does your organization allow the end user to monitor network uptime to?** Yes/No
224	59	**Does your company allow the end user to manually remove or replace cached content before it expires?** Yes/No
231	60	**Does your company charge for 'bursting overages'?** Yes/No
235	61	**Does your organisation offer DNS as main core business or as an add-on service?** Yes/No
237	62	**Does your organization allow the end user to track records for uptime and availability?** Yes/No
232	63	**Does your organization support EDNS for location based routing?** Yes/No
239	64	**Does your organisation employ anycast?** Yes/No
241	65	**Does your organisation use BIND or a similar server technology with experience of security issues?** Yes/No
241	66	**Does your organisation have servers around the globe?** Yes/No
242	67	**Does your organisation support DNS failover?** Yes/No
243	68	**Does your organisation support GEO DNS?** Yes/No
234	69	**Does your company provide domain name system security extensions?** Yes/No

APPENDIX M - Terremark-CAIQ-v1.1-2014-03-31.xlsx

Consensus Assessments Initiative Questionnaire v1.1					CCMv1.1 Compliance Mapping							
Control Group	**CGID**	**CID**	**Consensus Assessment Questions**	**Comments and Notes**	**COBIT**	**HIPAA**	**ISO27001**	**SP800_53**	**FedRAMP**	**PCI_DSS**	**BITS**	**GAPP**
Compliance												
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	Yes - Our cloud infrastructure is assessed annually for PCI compliance and also goes through an annual SSAE 16 audit.	COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.3 e) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PL-6	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PL-6	PCI DSS v2.0 2.1.2.b	SIG v6.0: L.1, L.2, L.7, L.9, L.11	GAPP Ref 10.2.5
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?	2.1 - Yes, with a current NDA on file, clients can view our PCI AoC, SAS 70/SSAE 16 report. 2.2 - Yes, per PCI guidelines. 2.3 - Yes, per PCI guidelines. 2.4 - Yes 2.5 - Yes 2.6 - No. The results of these tests are not released outside of the company. 2.7 - Yes, with a current NDA on file, clients can view our PCI AoC, SAS 70/SSAE 16 report.	COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5 NIST SP800-53 R3 RA-5 (1) NIST SP800-53 R3 RA-5 (2) NIST SP800-53 R3 RA-5 (3) NIST SP800-53 R3 RA-5 (9) NIST SP800-53 R3 RA-5 (6)	PCI DSS v2.0 11.2 PCI DSS v2.0 11.3 PCI DSS v2.0 6.6 PCI DSS v2.0 12.1.2.b	SIG v6.0: L.2, L.4, L.7, L.9, L.11	GAPP Ref 1.2.5 GAPP Ref 1.2.7 GAPP Ref 4.2.1 GAPP Ref 8.2.7 GAPP Ref 10.2.3 GAPP Ref 10.2.5
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?									
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?									
		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?									
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?									
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?									
		CO-02.7	Are the results of internal and external audits available to tenants at their request?									
Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?	3.1 - Yes, for tenant environment virtual machines only. 3.2 - Yes	COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1) (New) 45 CFR 164.308 (b)(4)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SC-7		PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4 Appendix A	AUP v5.0 C.2 SIG v6.0: C.2.4,C.2.6, G.4.1, G.4.2, L.2, L.4, L.7, L.11	GAPP Ref 1.2.11 GAPP Ref 4.2.3 GAPP Ref 7.2.4 GAPP Ref 10.2.3 GAPP Ref 10.2.4
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?									

Contact / Authority Maintenance	CO-04	CO-04.1	Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations?	Yes	COBIT 4.1 ME 3.1		A.6.1.6 A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-6 (1) NIST SP800-53 R3 SI-5	PCI DSS v2 11.1.e PCI PCI DSS v2 12.5.3 PCI DSS v2 12.9	SIG v6.0: L1	GAPP Ref 1.2.7 GAPP Ref 10.1.1 GAPP Ref 10.2.4
Information System Regulatory Mapping	CO-05	CO-05.1	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	5.1 - Yes 5.2 - Yes	COBIT 4.1 ME 3.1		ISO/IEC 27001:2005 Clause 4.2.1 b) 2) Clause 4.2.1 c) 1) Clause 4.2.1 g) Clause 4.2.3 d) 6) Clause 4.3.3 Clause 5.2.1 a - f Clause 7.3 c) 4) A.7.2.1 A.15.1.1 A.15.1.3 A.15.1.4 A.15.1.6			PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.1	SIG v6.0: L.1, L.2, L.4, L.7, L.9	GAPP Ref 1.2.2 GAPP Ref 1.2.4 GAPP Ref 1.2.6 GAPP Ref 1.2.11 GAPP Ref 3.2.4 GAPP Ref 5.2.1
		CO-05.2	Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss?									
Intellectual Property	CO-06	CO-06.1	Do you have policies and procedures in place describing what controls you have in place to protect tenants' intellectual property?	Yes			Clause 4.2.1 A.6.1.5 A.7.1.3 A.10.8.2 A.12.4.3 A.15.1.2	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5	NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 PM-5		SIG v6.0: L.4	
Intellectual Property	CO-07	CO-07.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved?	Yes								
Intellectual Property	CO-08	CO-08.1	If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to opt-out?	Yes								
Data Governance												
Ownership / Stewardship	DG-01	DG-01.1	Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)?	Yes	COBIT 4.1 DS5.1, PO 2.3	45 CFR 164.308 (a)(2)	A.6.1.3 A.7.1.2 A.15.1.4	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 SA-2	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PS-2 NIST SP800-53 R3 RA-2		SIG v6.0: C.2.5.1, C.2.5.2, D.1.3, L.7	GAPP Ref 6.2.1

									NIST SP800-53 R3 SA-2			
Classification	DG-02	DG-02.1	Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)?	2.1 - Yes 2.2 - Yes 2.3 - No 2.4 - Yes 2.5 - Yes	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.1	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	NIST SP800-53 R3 RA-2 NIST SP800-53 R3 AC-4	PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.10 PCI DSS v2.0 12.3	SIG v6.0: D.1.3, D.2.2	GAPP Ref 1.2.3 GAPP Ref 1.2.6 GAPP Ref 4.1.2 GAPP Ref 8.2.1 GAPP Ref 8.2.5 GAPP Ref 8.2.6
		DG-02.2	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)?									
		DG-02.3	Do you have a capability to use system geographic location as an authentication factor?									
		DG-02.4	Can you provide the physical location/geography of storage of a tenant's data upon request?									
		DG-02.5	Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation?									
Handling / Labeling / Security Policy	DG-03	DG-03.1	Are Policies and procedures established for labeling, handling and security of data and objects which contain data?	3.1 - Yes 3.2 - Yes	COBIT 4.1 PO 2.3, DS 11.6		A.7.2.2 A.10.7.1 A.10.7.3 A.10.8.1	NIST SP800-53 R3 AC-16 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 SC-9	NIST SP800-53 R3 AC-16 NIST SP800-53 R3 MP-1 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-9 (1)	PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.7.1 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.10	AUP v5.0 G.13 SIG v6.0: D.2.2	GAPP Ref 1.1.2 GAPP Ref 5.1.0 GAPP Ref 7.1.2 GAPP Ref 8.1.0 GAPP Ref 8.2.5 GAPP Ref 8.2.6
		DG-03.2	Are mechanisms for label inheritance implemented for objects that acts as aggregate containers for data?									
Retention Policy	DG-04	DG-04.1	Do you have technical control capabilities to enforce tenant data retention policies?	4.1 - Yes, this is an additional service. 4.2 - Yes.	COBIT 4.1 DS 4.1, DS 4.2, DS 4.5, DS 4.9, DS 11.6	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) (New) 45 CFR 164.316(b)(2)(i) (New)	Clause 4.3.3 A.10.5.1 A.10.7.3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-8 NIST SP800-53		PCI DSS v2.0 3.1 PCI DSS v2.0 3.1.1 PCI DSS v2.0 3.2 PCI DSS v2.0 9.9.1 PCI DSS v2.0	SIG v6.0: D.2.2.9	GAPP Ref 5.1.0 GAPP Ref 5.1.1 GAPP Ref 5.2.2 GAPP Ref 8.2.6
		DG-04.2	Do you have a documented procedure for responding to requests for tenant data from governments or third parties?									

								R3 CP-9 NIST SP800-53 R3 SI-12 NIST SP800-53 R3 AU-11		9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 10.7		
Secure Disposal	DG-05	DG-05.1 DG-05.2	Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant? Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource?	5.1 - Yes, as optional service degaussing and wiping is a part of Verizon Terremark's normal procedure and available in dedicated data solutions. 5.2 – Verizon Terremark has a a published process documenting the customer exit from the Cloud service, however the current process does not include assurances that Verizon Terremark has sanitized all compute resources upon exit. Verizon Terremark is evaluating a technical solution to sanitize tenant data during the service lifecycle.	COBIT 4.1 DS 11.4	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.9.2.6 A.10.7.2	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 PE-1	NIST SP800-53 R3 MP-6 NIST SP800-53 R3 MP-6 (4) NIST SP800-53 R3 PE-1	PCI DSS v2.0 3.1.1 PCI DSS v2.0 9.10 PCI DSS v2.0 9.10.1 PCI DSS v2.0 9.10.2 PCI DSS v2.0 3.1	SIG v6.0: D.2.2.10, D.2.2.11, D.2.2.14,	GAPP Ref 5.1.0 GAPP Ref 5.2.3
Nonproduction Data	DG-06	DG-06.1	Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments?	Yes		45 CFR 164.308(a)(4)(ii)(B)	A.7.1.3 A.10.1.4 A.12.4.2 A.12.5.1	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 CM-04	NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-11 (1) NIST SP800-53 R3 CM-04	PCI DSS v2.0 6.4.3	SIG v6.0: I.2.18	GAPP Ref 1.2.6
Information Leakage	DG-07	DG-07.1 DG-07.2	Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment? Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?	7.1 - Yes 7.2 - Yes	COBIT 4.1 DS 11.6		A.10.6.2 A.12.5.4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AU-13 NIST SP800-53 R3 PE-19 NIST SP800-53 R3 SC-28 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SI-7		PCI DSS v2.0 1.2 PCI DSS v2.0 6.5.5 PCI DSS v2.0 11.1 PCI DSS v2.0 11.2 PCI DSS v2.0 11.3 PCI DSS v2.0 11.4 PCI DSS v2.0 A.1	SIG v6.0: I.2.18	GAPP Ref 7.2.1 GAPP Ref 8.1.0 GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.5 GAPP Ref 8.2.6

Risk Assessments	DG-08	DG-08.1	Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?)	Yes. Some audit/logging capabilities are built in and optional security monitoring services can be purchased.	COBIT 4.1 PO 9.1, PO 9.2, PO 9.4, DS 5.7	45 CFR 164.308(a)(1)(ii)(A) (New) 45 CFR 164.308(a)(8) (New)	Clause 4.2.1 c) & g) Clause 4.2.3 d) Clause 4.3.1 & 4.3.3 Clause 7.2 & 7.3 A.7.2 A.15.1.1 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3 NIST SP800-53 R3 MP-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 SI-12	PCI DSS v2.0 12.1 PCI DSS v2.0 12.1.2	SIG v6.0: L.4, L.5, L.6, L.7	GAPP Ref 1.2.4 GAPP Ref 8.2.1
Facility Security												
Policy	FS-01	FS-01.1	Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?	Yes	COBIT 4.1 DS5.7, DS 12.1, DS 12.4 DS 4.9	45 CFR 164.310 (a)(1) 45 CFR 164.310 (a)(2)(ii) 45 CFR 164.308(a)(3)(ii)(A) (New) 45 CFR 164.310 (a)(2)(iii) (New)	A.5.1.1 A.9.1.3 A.9.1.5	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-8	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8	PCI DSS v2.0 9.1 PCI DSS v2.0 9.2 PCI DSS v2.0 9.3 PCI DSS v2.0 9.4	AUP v5.0 F.2 SIG v6.0: F.1.1, F.1.2 F.1.3, F.1.4, F1.5, F.1.6, F.1.7, F.1.8, F.1.9, F.2.1, F.2.2, F.2.3, F.2.4, F.2.5, F2.6, F.2.7, F.2.8, F.2.9, F.2.10, F.2.11, F.2.12, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18,F.2.19, F.2.20	GAPP Ref 8.1.0 GAPP Ref 8.1.1 GAPP Ref 8.2.1
User Access	FS-02	FS-02.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes - employment candidates, contractors, and preferred vendors.		45 CFR 164.310(a)(1) (New) 45 CFR 164.310(a)(2)(ii) (New) 45 CFR 164.310(b) (New) 45 CFR 164.310 (c) (New)	A.9.1.1 A.9.1.2	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1)	PCI DSS v2.0 9.1	AUP v5.0 H.6 SIG v6.0: F.1.2.3, F.1.2.4, F.1.2.5, F.1.2.6, F.1.2.8, F.1.2.9, F.1.2.10, F.1.2.11, F.1.2.12, F.1.2.13, F.1.2.14, F.1.2.15, F.1.2.24, F.1.4.2, F1.4.6, F.1.4.7, F.1.7, F.1.8, F.2.13, F.2.14, F.2.15, F.2.16, F.2.17, F.2.18	GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.3

Controlled Access Points	FS-03	FS-03.1	Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?	Yes	COBIT 4.1 DS 12.3		A.9.1.1	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1		GAPP Ref 8.2.3
Secure Area Authorization	FS-04	FS-04.1	Do you allow tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?	Yes	DS 12.2, DS 12.3		A.9.1.1 A.9.1.2	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-2 NIST SP800-53 R3 PE-2 (1) NIST SP800-53 R3 PE-3 NIST SP800-53 R3 PE-6 NIST SP800-53 R3 PE-6 (1) NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-8 NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.2		GAPP Ref 8.2.3
Unauthorized Persons Entry	FS-05	FS-05.1	Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?	Yes	COBIT 4.1 DS 12.3		A.9.1.6	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-7 NIST SP800-53 R3 PE-7 (1) NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-18			GAPP Ref 8.2.3
Offsite Authorization	FS-06	FS-06.1	Do you provide tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication)	Yes, if such optional services are purchased by the tenant.		45 CFR 164.310 (d)(1) (New)	A.9.2.7 A.10.1.2	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 PE-16	NIST SP800-53 R3 MA-1 NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-2 (1)	PCI DSS v2.0 9.8 PCI DSS v2.0 9.9	AUP v5.0 G.21 SIG v6.0:F.2.18	GAPP Ref 8.2.5 GAPP Ref 8.2.6

									NIST SP800-53 R3 PE-16			
Offsite equipment	FS-07	FS-07.1	Do you provide tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment?	Yes, upon request.		45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) (New) 45 CFR 164.310 (d)(2)(i) (New)	A.9.2.5 A.9.2.6	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 MA-1 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-16 NIST SP800-53 R3 PE-17		PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 9.10	SIG v6.0:F.2.18, F.2.19,	
Asset Management	FS-08	FS-08.1	Do you maintain a complete inventory of all of your critical assets which includes ownership of the asset?	Yes Yes		45 CFR 164.310 (d)(2)(iii)	A.7.1.1 A.7.1.2	NIST SP800-53 R3 CM-8	NIST SP800-53 R3 CM-8 NIST SP800-53 R3 CM-8 (1) NIST SP800-53 R3 CM-8 (3) NIST SP800-53 R3 CM-8 (5)	PCI DSS v2.0 9.9.1 PCI DSS v2.0 12.3.3 PCI DSS v2.0 12.3.4	AUP v5.0 D.1 SIG v6.0: D.1.1, D.2.1. D.2.2,	
		FS-08.2	Do you maintain a complete inventory of all of your critical supplier relationships?									
Human Resources Security												
Background Screening	HR-01	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?	Yes - employment candidates, contractors, and preferred vendors.	COBIT 4.1 PO 7.6		A.8.1.2	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	NIST SP800-53 R3 PS-2 NIST SP800-53 R3 PS-3	PCI DSS v2.0 12.7 PCI DSS v2.0 12.8.3	AUP v5.0 E.2 SIG v6.0: E.2	GAPP Ref 1.2.9
Employment Agreements	HR-02	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?	2.1 - Yes 2.2 - Yes	COBIT DS 2.1	45 CFR 164.310(a)(1) (New) 45 CFR 164.308(a)(4)(i) (New)	A.6.1.5 A.8.1.3	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	PCI DSS v2.0 12.4 PCI DSS v2.0 12.8.2	AUP v5.0 C.1 SIG v6.0: E.3.5	GAPP Ref 1.2.9 GAPP Ref 8.2.6
		HR-02.2	Do you document employee acknowledgment of training they have completed?									
Employment Termination	HR-03	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?	Yes	COBIT 4.1 PO 7.8	45 CFR 164.308 (a)(3)(ii)(C)	A.8.3.1	NIST SP800-53 R3 PS-4 NIST SP800-53 R2 PS-5	NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5		SIG v6.0: E.6	GAPP Ref 8.2.2 GAPP Ref 10.2.5
Information Security												

Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?	Yes	COBIT 4.1 R2 DS5.2 COBIT 4.1 R2 DS5.5	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.306(a) (New)	Clause 4.2 Clause 5 A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.1.6 A.6.1.7 A.6.1.8	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-2 NIST SP800-53 R3 PM-3 NIST SP800-53 R3 PM-4 NIST SP800-53 R3 PM-5 NIST SP800-53 R3 PM-6 NIST SP800-53 R3 PM-7 NIST SP800-53 R3 PM-8 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0: A.1, B.1	GAPP Ref 8.2.1
Management Support / Involvement	IS-02	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?	Yes	COBIT 4.1 DS5.1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	Clause 5 A.6.1.1	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 PM-1 NIST SP800-53 R3 PM-11	PCI DSS v2.0 12.5	SIG v6.0: C.1	GAPP Ref 8.2.1
Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?	3.1 - Yes 3.2 - Yes 3.3 - Yes	COBIT 4.1 DS5.2	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2) (New)	Clause 4.2.1 Clause 5 A.5.1.1 A.8.2.2			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2	SIG v6.0:B.1	GAPP Ref 8.1.0 GAPP Ref 8.1.1
		IS-03.2	Do you have agreements which ensure your providers adhere to your information security and privacy policies?									
		IS-03.3	Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?									
Baseline Requirements	IS-04	IS-04.1	Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?	4.1 - Yes 4.2 - Yes 4.3 - Yes	COBIT 4.1 AI2.1 COBIT 4.1 AI2.2 COBIT 4.1 AI3.3 COBIT 4.1 DS2.3 COBIT 4.1 DS11.6		A.12.1.1 A.15.2.2	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4	NIST SP800-53 R3 CM-2 NIST SP800-53 R3 CM-2 (1) NIST SP800-53 R3 CM-2 (3) NIST SP800-53 R3 CM-2 (5)	PCI DSS v1.2 1.1 PCI DSS v1.2 1.1.1 PCI DSS v1.2 1.1.2 PCI DSS v1.2 1.1.3 PCI DSS v1.2 1.1.4 PCI DSS v1.2 1.1.5	AUP v5.0 L.2 SIG v6.0: L.2, L.5, L.7 L.8, L.9, L.10	GAPP Ref 1.2.6 GAPP Ref 8.2.1 GAPP Ref 8.2.7
		IS-04.2	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?									

		IS-04.3	Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?						NIST SP800-53 R3 SA-2 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)	PCI DSS v1.2 1.1.6 PCI DSS v1.2 2.2 PCI DSS v1.2 2.2.1 PCI DSS v1.2 2.2.2 PCI DSS v1.2 2.2.3 PCI DSS v1.2 2.2.4		
Policy Reviews	IS-05	IS-05.1	Do you notify your tenants when you make material changes to your information security and/or privacy policies?	No. Our privacy policies are made publicly available on our website at all times. Information security policies can be provided upon request.	COBIT 4.1 DS 5.2 DS 5.4	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306(e) (New)	Clause 4.2.3 f) A.5.1.2			PCI DSS v2.0 12.1.3	AUP v5.0 B.2 SIG v6.0: B.1.33. B.1.34,	GAPP Ref 1.2.1 GAPP Ref 8.2.7 GAPP Ref 10.2.3
Policy Enforcement	IS-06	IS-06.1	Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	6.1 - Yes 6.2 - Yes	COBIT 4.1 PO 7.7	45 CFR 164.308 (a)(1)(ii)(C)	A.8.2.3	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-8	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-8		SIG v6.0:B.1.5	GAPP Ref 10.2.4
		IS-06.2	Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?									
User Access Policy	IS-07	IS-07.1	Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes?	7.1 - Yes 7.2 - No	COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) (New) 45 CFR 164.308(a)(4)(ii)(c) (New)	A.11.1.1 A.11.2.1 A.11.2.4 A.11.4.1 A.11.5.2 A.11.6.1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 IA-1	PCI DSS v2.0 3.5.1 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	AUP v5.0 B.1 SIG v6.0: B.1.8, B.1.21, B.1.28, E.6.2, H.1.1, K.1.4.5,	GAPP Ref 8.1.0
		IS-07.2	Do you provide metrics which track the speed with which you are able to remove systems access which is no longer required for business purposes?									
User Access Restriction / Authorization	IS-08	IS-08.1	Do you document how you grant and approve access to tenant data?	8.1 - Not applicable. Verizon Terremark employees do not have access to our cloud tenant data. Customers have the ability to authorize Verizon Terremark to assist with virtual machine issues if needed. 8.2 - Verizon Terremark does not control tenant access control policies. Customer in control of access control for their virtual machines.	COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.11.2.1 A.11.2.2 A.11.4.1 A 11.4.2 A.11.6.1	NIST SP800-53 R3 AC-3 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-5 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-9		PCI DSS v2.0 7.1 PCI DSS v2.0 7.1.1 PCI DSS v2.0 7.1.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 7.2.1 PCI DSS v2.0 7.2.2 PCI DSS v2.0 8.5.1 PCI DSS v2.0 12.5.4	SIG v6.0: H.2.4, H.2.5,	GAPP Ref 8.2.2
		IS-08.2	Do you have a method of aligning provider and tenant data classification methodologies for access control purposes?									

User Access Revocation	IS-09	IS-09.1	Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?	9.1 - Yes 9.2 - Yes	COBIT 4.1 DS 5.4	45 CFR 164.308(a)(3)(ii)(C)	ISO/IEC 27001:2005 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.2	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-2 (1) NIST SP800-53 R3 AC-2 (2) NIST SP800-53 R3 AC-2 (3) NIST SP800-53 R3 AC-2 (4) NIST SP800-53 R3 AC-2 (7) NIST SP800-53 R3 PS-4 NIST SP800-53 R3 PS-5	PCI DSS v2.0 8.5.4 PCI DSS v2.0 8.5.5	AUP v5.0 H.2 SIG v6.0: E.6.2, E.6.3	GAPP Ref 8.2.1
		IS-09.2	Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization?									
User Access Reviews	IS-10	IS-10.1	Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)?	10.1 - Yes 10.2 - Yes 10.3 - No. Verizon Terremark employees do not have access to our cloud tenant data.	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.11.2.4	NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7			SIG v6.0:H.2.6, H.2.7, H.2.9,	GAPP Ref 8.2.1 GAPP Ref 8.2.7
		IS-10.2	If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?									
		IS-10.3	Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data?									
Training / Awareness	IS-11	IS-11.1	Do you provide or make available a formal security awareness training program for cloud related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data?	11.1 - Not applicable. Verizon Terremark employees do not have access to our cloud tenant data. Customers have the ability to authorize Verizon Terremark to assist with virtual machine issues if needed. 11.2 - Yes	COBIT 4.1 PO 7.4	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 5.2.2 A.8.2.2	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	NIST SP800-53 R3 AT-1 NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	PCI DSS v2.0 12.6 PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0:E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1
		IS-11.2	Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity?									
Industry Knowledge / Benchmarking	IS-12	IS-12.1	Do you participate in industry groups and professional associations related to information security?	12.1 - Yes 12.2 - Yes			A.6.1.7	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 SI-5	NIST SP800-53 R3 AT-5 NIST SP800-53 R3 SI-5		SIG v6.0:C.1.8	
		IS-12.2	Do you benchmark your security controls against industry standards?									

Roles / Responsibilities	IS-13	IS-13.1	Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant?	Yes	COBIT 4.1 DS5.1		Clause 5.1 c) A.6.1.2 A.6.1.3 A.8.1.1	NIST SP800-53 R3 AT-3 NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7	NIST SP800-53 R3 AT-3 NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PM-10 NIST SP800-53 R3 PS-1 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 PS-7		AUP v5.0 B.1 SIG v6.0: B.1.5, D.1.1,D.1.3.3, E.1, F.1.1, H.1.1, K.1.2	GAPP Ref 1.2.9 GAPP Ref 8.2.1
Management Oversight	IS-14	IS-14.1	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility?	Yes	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4 COBIT 4.1 DS5.5		Clause 5.2.2 A.8.2.1 A.8.2.2 A 11.2.4 A.15.2.1	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PM-10	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 CA-7 (2) NIST SP800-53 R3 PM-10	PCI DSS v2.0 12.6.1 PCI DSS v2.0 12.6.2	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.1.2 GAPP Ref 8.2.1
Segregation of Duties	IS-15	IS-15.1	Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering?	Yes	COBIT 4.1 DS 5.4	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) (New) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.3	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-2 NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-6 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-4		PCI DSS v2.0 6.4.2	SIG v6.0:G.2.13. G.3, G.20.1, G.20.2, G.20.5	GAPP Ref 8.2.2
User Responsibility	IS-16	IS-16.1	Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements?	16.1 - Yes 16.2 - Yes 16.3 - Yes	COBIT 4.1 PO 4.6	45 CFR 164.308 (a)(5)(ii)(D)	Clause 5.2.2 A.8.2.2 A.11.3.1 A.11.3.2	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3 NIST SP800-53 R3 AT-4	NIST SP800-53 R3 AT-2 NIST SP800-53 R3 AT-3	PCI DSS v2.0 8.5.7 PCI DSS v2.0 12.6.1	AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 1.2.10 GAPP Ref 8.2.1

		IS-16.2	Are users made aware of their responsibilities for maintaining a safe and secure working environment?					NIST SP800-53 R3 PL-4	NIST SP800-53 R3 AT-4 NIST SP800-53 R3 PL-4			
		IS-16.3	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?									
Workspace	IS-17	IS-17.1	Do your data management policies and procedures address tenant and service level conflicts of interests?	17.1 - Yes 17.2 - Yes 17.3 - Yes			Clause 5.2.2 A.8.2.2 A.9.1.5 A.11.3.1 A.11.3.2 A.11.3.3	NIST SP800-53 R3 AC-11 NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-3 NIST SP800-53 R3 MP-4	NIST SP800-53 R3 AC-11 NIST SP800-53 R3 AC-11 (1) NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-2 (1) NIST SP800-53 R3 MP-3 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-4 (1)		AUP v5.0 E.1 SIG v6.0: E.4	GAPP Ref 8.2.3
		IS-17.2	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data?									
		IS-17.3	Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?									
Encryption	IS-18	IS-18.1	Do you have a capability to allow creation of unique encryption keys per tenant?	18.1 -Yes, for Linux SSH admin access and API user access. 18.2 -No - customer responsibility.	COBIT 4.1 DS5.8 COBIT 4.1 DS5.10 COBIT 4.1 DS5.11	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.10.6.1 A.10.8.3 A.10.8.4 A.10.9.2 A.10.9.3 A.12.3.1 A.15.1.3 A.15.1.4	NIST SP800-53 R3 AC-18 NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-7 NIST SP800-53 R3 SC-7 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-16 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SI-8		PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 3.4 PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2		GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5
		IS-18.2	Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?									
Encryption Key Management	IS-19	IS-19.1	Do you encrypt tenant data at rest (on disk/storage) within your environment?	19.1 - Yes, Verizon Terremark offers encryption capabilities through the use of CloudSwitch software. 19.2 - Yes, Verizon Terremark offers encryption capabilities through the use of CloudSwitch software. 19.3 - Yes, Verizon Terremark offers encryption capabilities through the use of CloudSwitch software. 19.4 - Yes, Verizon Terremark offers encryption capabilities through the use of CloudSwitch software.	COBIT 4.1 DS5.8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1) (New)	Clause 4.3.3 A.10.7.3 A.12.3.2 A.15.1.6	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-17 NIST SP800-53 R3 SC-28	NIST SP800-53 R3 SC-12 NIST SP800-53 R3 SC-12 (2) NIST SP800-53 R3 SC-12 (5) NIST SP800-53 R3 SC-13 NIST SP800-53 R3 SC-13 (1) NIST SP800-53 R3 SC-17 NIST SP800-53	PCI-DSS v2.0 3.4.1 PCI-DSS v2.0 3.5 PCI-DSS v2.0 3.5.1 PCI-DSS v2.0 3.5.2 PCI-DSS v2.0 3.6 PCI-DSS v2.0 3.6.1 PCI-DSS v2.0 3.6.2 PCI-DSS v2.0 3.6.3 PCI-DSS v2.0 3.6.4 PCI-DSS v2.0	SIG v6.0: L.6	GAPP Ref 8.1.1 GAPP Ref 8.2.1 GAPP Ref 8.2.5
		IS-19.2	Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?									
		IS-19.3	Do you have a capability to manage encryption keys on behalf of tenants?									
		IS-19.4	Do you maintain key management procedures?									

									R3 SC-28 NIST SP800-53 R3 SC-28 (1)	3.6.5 PCI-DSS v2.0 3.6.6 PCI-DSS v2.0 3.6.7 PCI-DSS v2.0 3.6.8		
Vulnerability / Patch Management	IS-20	IS-21.1	Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices?	21.1 - Yes, per PCI guidelines 20.2 - Yes, per PCI guidelines 20.3 - Yes, per PCI guidelines 20.4 - These results are not released outside of the company. 20.5 - Yes 20.6 - Yes	COBIT 4.1 AI6.1 COBIT 4.1 AI3.3 COBIT 4.1 DS5.9	45 CFR 164.308 (a)(1)(i)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)	A.12.5.1 A.12.5.2 A.12.6.1	NIST SP800-53 R3 CM-3 NIST SP800-53 R3 CM-4 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 RA-5 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SI-1 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-5		PCI-DSS v2.0 2.2 PCI-DSS v2.0 6.1 PCI-DSS v2.0 6.2 PCI-DSS v2.0 6.3.2 PCI-DSS v2.0 6.4.5 PCI-DSS v2.0 6.5.X PCI-DSS v2.0 6.6 PCI-DSS v2.0 11.2 PCI-DSS v2.0 11.2.1 PCI-DSS v2.0 11.2.2 PCI-DSS v2.0 11.2.3	AUP v5.0 I.4 SIG v6.0: G.15.2, I.3	GAPP Ref 1.2.6 GAPP Ref 8.2.7
		IS-20.2	Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices?									
		IS-20.3	Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices?									
		IS-20.4	Will you make the results of vulnerability scans available to tenants at their request?									
		IS-20.5	Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?									
		IS-20.6	Will you provide your risk-based systems patching timeframes to your tenants upon request?									
Antivirus / Malicious Software	IS-21	IS-21.1	Do you have anti-malware programs installed on all systems which support your cloud service offerings?	21.1 - Yes 21.2 - Yes	COBIT 4.1 DS5.9	45 CFR 164.308 (a)(5)(ii)(B)	A.10.4.1	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-5 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-8	NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SC-5 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-3 (1) NIST SP800-53 R3 SI-3 (2) NIST SP800-53 R3 SI-3 (3) NIST SP800-53 R3 SI-5 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-7 (1) NIST SP800-53 R3 SI-8	PCI-DSS v2.0 5.1 PCI-DSS v2.0 5.1.1 PCI-DSS v2.0 5.2	SIG v6.0:G.7	GAPP Ref 8.2.2
		IS-21.2	Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes?									
Incident Management	IS-22	IS-22.1	Do you have a documented security incident response plan?	22.1 - Yes 22.2 - No 22.3 - Yes	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 4.3.3 A.13.1.1 A.13.2.1	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-3	NIST SP800-53 R3 IR-1 NIST SP800-53 R3 IR-2	PCI-DSS v2.0 12.9 PCI-DSS v2.0 12.9.1 PCI-DSS v2.0 12.9.2	AUP v5.0 J.1 SIG v6.0: J.1.1, J.1.2	GAPP Ref 1.2.4 GAPP Ref 1.2.7 GAPP Ref 7.1.2
		IS-22.2	Do you integrate customized tenant requirements into your security incident response plans?									

		IS-22.3	Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents?					NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-8	NIST SP800-53 R3 IR-3 NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-7 (1) NIST SP800-53 R3 IR-7 (2) NIST SP800-53 R3 IR-8	PCI-DSS v2.0 12.9.3 PCI-DSS v2.0 12.9.4 PCI-DSS v2.0 12.9.5 PCI-DSS v2.0 12.9.6		GAPP Ref 7.2.2 GAPP Ref 7.2.4 GAPP Ref 10.2.1 GAPP Ref 10.2.4
Incident Reporting	IS-23	IS-23.1	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?	23.1 - Yes. This is an optional service for our tenants. 23.2 - Yes	COBIT 4.1 DS5.6	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) (New) 16 CFR 318.5 (a) (New) 45 CFR 160.410 (a)(1) (New)	Clause 4.3.3 Clause 5.2.2 A.6.1.3 A.8.2.1 A.8.2.2 A.13.1.1 A.13.1.2 A.13.2.1	NIST SP800-53 R3 IR-2 NIST SP800-53 R3 IR-6 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-5		PCI-DSS v2.0 12.5.2 PCI-DSS v2.0 12.5.3	AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1, E.4	GAPP Ref 1.2.7 GAPP Ref 1.2.10 GAPP Ref 7.1.2 GAPP Ref 7.2.2 GAPP Ref 7.2.4 GAPP Ref 10.2.4
		IS-23.2	Does your logging and monitoring framework allow isolation of an incident to specific tenants?									
Incident Response Legal Preparation	IS-24	IS-24.1	Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?	24.1 - Yes 24.2 -Yes 24.3 - Yes 24.4 - Yes	COBIT 4.1 DS5.6	45 CFR 164.308 (a)(6)(ii)	Clause 4.3.3 Clause 5.2.2 A.8.2.2 A.8.2.3 A.13.2.3 A.15.1.3	NIST SP800-53 R3 AU-6 NIST SP800-53 R3 AU-7 NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-7 NIST SP800-53 R3 IR-8			AUP v5.0 J.1 AUP v5.0 E.1 SIG v6.0: J.1.1, J.1.2, E.4	GAPP Ref 1.2.7
		IS-24.2	Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?									
		IS-24.3	Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data?									
		IS-24.4	Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas?									
Incident Response Metrics	IS-25	IS-25.1	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?	25.1 - Yes 25.2 - No	COBIT 4.1 DS 4.9	45 CFR 164.308 (a)(1)(ii)(D)	A.13.2.2	NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-5 NIST SP800-53 R3 IR-8	NIST SP800-53 R3 IR-4 NIST SP800-53 R3 IR-4 (1) NIST SP800-53 R3 IR-5	PCI DSS v2.0 12.9.6	SIG v6.0: J.1.2,	GAPP Ref 1.2.7 GAPP Ref 1.2.10
		IS-25.2	Will you share statistical information security incident data with your tenants upon request?									

									NIST SP800-53 R3 IR-8			
Acceptable Use	IS-26	IS-26.1	Do you provide documentation regarding how you may utilize or access tenant data and/or metadata?	26.1 - Yes 26.2 - No 26.3 - No	COBIT 4.1 DS 5.3	45 CFR 164.310 (b)	A.7.1.3	NIST SP800-53 R3 AC-8 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 PL-4	NIST SP800-53 R3 AC-8 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 AC-20 (1) NIST SP800-53 R3 AC-20 (2) NIST SP800-53 R3 PL-4	PCI-DSS v2.0 12.3.5	AUP v5.0 B.3. SIG v6.0: B.1.7, D.1.3.3, E.3.2, E.3.5.1, E.3.5.2	GAPP Ref 8.1.0
		IS-26.2	Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)?									
		IS-26.3	Do you allow tenants to opt-out of having their data/metadata accessed via inspection technologies?									
Asset Returns	IS-27	IS-27.1	Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data?	27.1 - Yes 27.2 - Yes		45 CFR 164.308 (a)(3)(ii)(C)	A.7.1.1 A.7.1.2 A.8.3.2	NIST SP800-53 R3 PS-4	NIST SP800-53 R3 PS-4		AUP v5.0 D.1 SIG v6.0: E.6.4	GAPP Ref 5.2.3 GAPP Ref 7.2.2 GAPP Ref 8.2.1 GAPP Ref 8.2.6
		IS-27.2	Is your Privacy Policy aligned with industry standards?									
eCommerce Transactions	IS-28	IS-28.1	Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)	28.1 - Yes, when router network terminations are established. All other forms of internet encryption are the customer's responsibility. 28.2 - Yes	COBIT 4.1 DS 5.10 5.11	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.7.2.1 A.10.6.1 A.10.6.2 A.10.9.1 A.10.9.2 A.15.1.4	NIST SP800-53 R3 AC-14 NIST SP800-53 R3 AC-21 NIST SP800-53 R3 AC-22 NIST SP800-53 R3 IA-8 NIST SP800-53 R3 AU-10 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-8 NIST SP800-53 R3 SC-9		PCI-DSS v2.0 2.1.1 PCI-DSS v2.0 4.1 PCI-DSS v2.0 4.1.1 PCI DSS v2.0 4.2		GAPP Ref 3.2.4 GAPP Ref 4.2.3 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 8.2.1 GAPP Ref 8.2.5
		IS-28.2	Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?									
Audit Tools Access	IS-29	IS-29.1	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)	29.1 - Yes	COBIT 4.1 DS 5.7		A.15.3.2	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	NIST SP800-53 R3 AU-9 NIST SP800-53 R3 AU-9 (2) NIST SP800-53 R3 AU-11 NIST SP800-53 R3 AU-14	PCI DSS v2.0 10.5.5		GAPP Ref 8.2.1

Diagnostic / Configuration Ports Access	IS-30	IS-30.1	Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure?	Yes	COBIT 4.1 DS5.7		A.10.6.1 A.11.1.1 A.11.4.4 A.11.5.4	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5	NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-3 (1) NIST SP800-53 R3 MA-3 (2) NIST SP800-53 R3 MA-3 (3) NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 MA-5	PCI-DSS v2.0 9.1.2	SIG v6.0: H1.1, H1.2, G.9.15	
Network / Infrastructure Services	IS-31	IS-31.1 IS-31.2	Do you collect capacity and utilization data for all relevant components of your cloud service offering? Do you provide tenants with capacity planning and utilization reports?	31.1 - Yes 31.2 - Yes	COBIT 4.1 DS5.10		A.6.2.3 A.10.6.2	NIST SP800-53 R3 SC-20 NIST SP800-53 R3 SC-21 NIST SP800-53 R3 SC-22 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SC-24	NIST SP800-53 R3 SC-20 NIST SP800-53 R3 SC-20 (1) NIST SP800-53 R3 SC-21 NIST SP800-53 R3 SC-22 NIST SP800-53 R3 SC-23 NIST SP800-53 R3 SC-24		AUP v5.0 C.2 SIG v6.0:C.2.6, G.9.9	GAPP Ref 8.2.2 GAPP Ref 8.2.5
Portable / Mobile Devices	IS-32	IS-32.1	Are Policies and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)?	Yes	COBIT 4.1 DS5.11 COBIT 4.1 DS5.5	45 CFR 164.310 (d)(1)	A.7.2.1 A.10.7.1 A.10.7.2 A.10.8.3 A.11.7.1 A.11.7.2 A.15.1.4	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 AC-19 NIST SP800-53 R3 MP-2 NIST SP800-53 R3 MP-4 NIST SP800-53 R3 MP-6		PCI DSS v2.0 9.7 PCI DSS v2.0 9.7.2 PCI DSS v2.0 9.8 PCI DSS v2.0 9.9 PCI DSS v2.0 11.1 PCI DSS v2.0 12.3	SIG v6.0:G.11, G12, G.20.13, G.20.14	GAPP Ref 1.2.6 GAPP Ref 3.2.4 GAPP Ref 8.2.6
Source Code Access Restriction	IS-33	IS-33.1	Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?	33.1 - Yes 33.2 - Not applicable. Verizon Terremark employees do not have access to our cloud tenant			Clause 4.3.3 A.12.4.3 A.15.1.3	NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-6	NIST SP800-53 R3 CM-5 NIST SP800-53 R3 CM-5 (1)	PCI-DSS v2.0 6.4.1 PCI-DSS v2.0 6.4.2	SIG v6.0: I.2.7.2, I.2.9, I.2.10, I.2.15,	GAPP Ref 1.2.6 GAPP Ref 6.2.1

		IS-33.2	Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only?	data. Customers have the ability to authorize Verizon Terremark to assist with virtual machine issues if needed.					NIST SP800-53 R3 CM-5 (5) NIST SP800-53 R3 CM-6 NIST SP800-53 R3 CM-6 (1) NIST SP800-53 R3 CM-6 (3)			
Utility Programs Access	IS-34	IS-34.1	Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?	34.1 - Yes 34.2 - Yes 34.3 - Yes	COBIT 4.1 DS5.7		A.11.4.1 A 11.4.4 A.11.5.4	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 CM-7 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-19	NIST SP800-53 R3 AC-5 NIST SP800-53 R3 AC-6 NIST SP800-53 R3 AC-6 (1) NIST SP800-53 R3 AC-6 (2) NIST SP800-53 R3 CM-7 NIST SP800-53 R3 CM-7 (1) NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-19	PCI DSS v2.0 7.1.2	SIG v6.0:H.2.16	
		IS-34.2	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?									
		IS-34.3	Are attacks which target the virtual infrastructure prevented with technical controls?									
Legal													
Nondisclosure Agreements	LG-01	LG-01.1	Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals?	Yes			ISO/IEC 27001:2005 Annex A.6.1.5	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9	NIST SP800-53 R3 PL-4 NIST SP800-53 R3 PS-6 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)	PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	SIG v6.0:C.2.5	GAPP Ref 1.2.5
Third Party Agreements	LG-02	LG-02.1	Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted?	2.1 - Yes 2.2 - Yes 2.3 - Yes	COBIT 4.1 DS5.11		A.6.2.3 A10.2.1 A.10.8.2 A.11.4.6 A.11.6.1 A.12.3.1 A.12.5.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MP-5 NIST SP800-53 R3 PS-7 NIST SP800-53 R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MP-5 NIST SP800-53 R3 MP-5 (2) NIST SP800-53 R3 MP-5 (4) NIST SP800-53 R3 PS-7 NIST SP800-53	PCI DSS v2.0 2.4 PCI DSS v2.0 12.8.2	AUP v5.0 C.2 SIG v6.0: C.2.4, C.2.6, G.4.1, G.16.3,	GAPP Ref 1.2.5
		LG-02.2	Do you select and monitor outsourced providers in compliance with laws in the country where the data originates?									
		LG-02.3	Does legal counsel review all third party agreements?									

									R3 SA-6 NIST SP800-53 R3 SA-7 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-9 (1)			
Operations Management												
Policy	OP-01	OP-01.1	Are policies and procedures established and made available for all personnel to adequately support services operations roles?	Yes	COBIT 4.1 DS13.1		Clause 5.1 A 8.1.1 A.8.2.1 A 8.2.2 A.10.1.1			PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 8.2.1
Documentation	OP-02	OP-02.1	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?	Yes	COBIT 4.1 DS 9, DS 13.1		Clause 4.3.3 A.10.7.4	NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11		PCI DSS v2.0 12.1 PCI DSS v2.0 12.2 PCI DSS v2.0 12.3 PCI DSS v2.0 12.4	SIG v6.0: G.1.1	GAPP Ref 1.2.6
Capacity / Resource Planning	OP-03	OP-03.1	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?	3.1 - Yes 3.2 - Yes	COBIT 4.1 DS 3		A.10.3.1	NIST SP800-53 R3 SA-4	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-4 (1) NIST SP800-53 R3 SA-4 (4) NIST SP800-53 R3 SA-4 (7)		SIG v6.0:G.5	GAPP Ref 1.2.4
		OP-03.2	Do you restrict use of the memory oversubscription capabilities present in the hypervisor?									
Equipment Maintenance	OP-04	OP-04.1	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities?	4.1 - Yes for data restore. Yes for hardware restore if hardware is compatible. 4.2 - Yes, but just data, not the full VM 4.3 - Yes, customers who leverage Verizon Terremark's CloudSwitch software on top of the Enterprise Cloud have the ability to move their virtual machines to an internal cloud or other provider which is supported by the CloudSwitch software technology. 4.4 - Yes. Application	COBIT 4.1 A13.3	45 CFR 164.310 (a)(2)(iv)	A.9.2.4	NIST SP800-53 R3 MA-2 NIST SP800-53 R3 MA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-5 NIST SP800-53 R3 MA-6			SIG v6.0:F.2.19	GAPP Ref 5.2.3 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.4 GAPP Ref 8.2.5 GAPP Ref 8.2.6 GAPP Ref 8.2.7
		OP-04.2	If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?									
		OP-04.3	If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?									
		OP-04.4	If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?									

		OP-04.5	Does your cloud solution include software / provider independent restore and recovery capabilities?	replication can be used. 4.5 - Yes								
Risk Management												
Program	RI-01	RI-01.1	Is your organization insured by a 3rd party for losses?	1.1 - Yes 1.2 - Yes	COBIT 4.1 PO 9.1	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(B) (New)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.6.1 A.14.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 RA-1	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-6 NIST SP800-53 R3 PM-9 NIST SP800-53 R3 RA-1	PCI DSS v2.0 12.1.2	AUP v5.0 L.2 SIG v6.0: A.1, L.1	GAPP Ref 1.2.4
		RI-01.2	Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure?									
Assessments	RI-02	RI-02.1	Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?	2.1 - Yes 2.2 - Yes	COBIT 4.1 PO 9.4	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2.1 c) through g) Clause 4.2.3 d) Clause 5.1 f) Clause 7.2 & 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.14.1.2 A.15.1.1 A.15.2.1 A.15.2.2	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 PL-5 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.1.2	AUP v5.0 I.1 AUP v5.0 I.4 SIG v6.0: C.2.1, I.4.1, I.5, G.15.1.3, I.3	GAPP Ref 1.2.4 GAPP Ref 1.2.5
		RI-02.2	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?									
Mitigation / Acceptance	RI-03	RI-03.1	Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?	Yes	COBIT 4.1 PO 9.5	45 CFR 164.308 (a)(1)(ii)(B)	Clause 4.2.1 c) through g) Clause 4.2.2 b) Clause 4.3.1 Clause 5.1 f) Clause 7.3 A.6.2.1 A.12.5.2 A.12.6.1 A.15.1.1 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4	NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CM-4		AUP v5.0I.4 AUP v5.0 L.2 SIG v6.0: I.3, L.9, L.10	
	RI-03	RI-03.2	Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?	Yes								

Business / Policy Change Impacts	RI-04	RI-04.1	Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?	Yes	COBIT 4.1 PO 9.6		Clause 4.2.3 Clause 4.2.4 Clause 4.3.1 Clause 5 Clause 7 A.5.1.2 A.10.1.2 A.10.2.3 A.14.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 RA-2 NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.1.3	AUP v5.0 B.2 AUP v5.0 G.21 AUP v5.0 L.2 SIG v6.0: B.1.1, B.1.2, B.1.6, B.1.7.2, G.2, L.9, L.10	
Third Party Access	RI-05	RI-05.1	Do you provide multi-failure disaster recovery capability?	5.1 - Yes, this is an optional service. 5.2 - Yes 5.3 - Yes 5.4 - No 5.5 - Yes, this is an optional service. 5.6 - Yes, this is an optional service. 5.7 - No.	COBIT 4.1 DS 2.3		A.6.2.1 A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.4	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 RA-3	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 MA-4 NIST SP800-53 R3 MA-4 (1) NIST SP800-53 R3 MA-4 (2) NIST SP800-53 R3 RA-3	PCI DSS v2.0 12.8.1 PCI DSS v2.0 12.8.2 PCI DSS v2.0 12.8.3 PCI DSS v2.0 12.8.4	AUP v5.0 B.1 AUP v5.0 H.2 SIG v6.0: B.1.1, B.1.2, D.1.1, E.1, F.1.1, H.1.1, K.1.1, E.6.2, E.6.3	GAPP Ref 7.1.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 7.2.3 GAPP Ref 7.2.4
		RI-05.2	Do you monitor service continuity with upstream providers in the event of provider failure?									
		RI-05.3	Do you have more than one provider for each service you depend on?									
		RI-05.4	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?									
		RI-05.5	Do you provide the tenant the ability to declare a disaster?									
		RI-05.6	Do you provided a tenant triggered failover option?									
		RI-05.7	Do you share your business continuity and redundancy plans with your tenants?									
Release Management												
New Development / Acquisition	RM-01	RM-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	Yes	COBIT 4.1 A12, A 16.1		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-9 NIST SP800-53 R3 PL-1 NIST SP800-53 R3 PL-2 NIST SP800-53 R3 SA-1 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4		PCI DSS v2.0 6.3.2	AUP v5.0 I.2 SIG v6.0: I.1.1, I.1.2, I.2. 7.2, I.2.8, I.2.9, I.2.10, I.2.13, I.2.14, I.2.15, I.2.18, I.2.22.6, L.5,	GAPP Ref 1.2.6

Production Changes	RM-02	RM-02.1	Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	Yes	COBIT 4.1 A16.1, A17.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2			PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.3.2 PCI DSS v2.0 6.4 PCI DSS v2.0 6.1	SIG v6.0: I.2.17, I.2.20, I.2.22	GAPP Ref 1.2.6
Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?	Verizon Terremark can provide a description upon request.	COBIT 4.1 PO 8.1		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.6.1 A.13.1.2 A.15.2.1 A.15.2.2	NIST SP800-53 R3 CM-1 NIST SP800-53 R3 CM-2 NIST SP800-53 R3 SA-3 NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-13		PCI DSS v2.0 1.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.4	C.1.7, G.1, G.6, I.1, I.4.5, I.2.18, , I.22.1, I.22.3, I.22.6, I.2.23, I.2.22.2, I.2.22.4, I.2.22.7. I.2.22.8, I.2.22.9, I.2.22.10, I.2.22.11, I.2.22.12, I.2.22.13, I.2.22.14,I.2.20, I.2.17, I.2.7.1, I.3, J.2.10, L.9	GAPP Ref 9.1.0 GAPP Ref 9.1.1 GAPP Ref 9.2.1 GAPP Ref 9.2.2
Outsourced Development	RM-04	RM-04.1	Do you have controls in place to ensure that standards of quality are being met for all software development?	4.1 - Yes 4.2 - N/A			A.6.1.8 A.6.2.1 A.6.2.3 A.10.1.4 A.10.2.1 A.10.2.2 A.10.2.3 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.1 A.12.5.2 A.12.5.3 A.12.5.5 A.12.6.1 A.13.1.2	NIST SP800-53 R3 SA-4 NIST SP800-53 R3 SA-5 NIST SP800-53 R3 SA-8 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-10 NIST SP800-53 R3 SA-11 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SA-13		PCI DSS v2.0 3.6.7 PCI DSS v2.0 6.4.5.2 PCI DSS v2.0 7.1.3 PCI DSS v2.0 8.5.1 PCI DSS v2.0 9.1 PCI DSS v2.0 9.1.2 PCI DSS v2.0 9.2b PCI DSS v2.0 9.3.1 PCI DSS v2.0 10.5.2 PCI DSS v2.0 11.5 PCI DSS v2.0 12.3.1		
		RM-04.2	Do you have controls in place to detect source code security defects for any outsourced software development activities?									

							A.15.2.1 A.15.2.2			PCI DSS v2.0 12.3.3		
Unauthorized Software Installations	RM-05	RM-05.1	Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?	Yes			A.10.1.3 A.10.4.1 A.11.5.4 A.11.6.1 A.12.4.1 A.12.5.3				AUP v5.0 G.1 AUP v5.0 I.2 SIG v6.0: G.2.13, G.20.2,G.20.4, G.20.5, G.7, G.7.1, G.12.11, H.2.16, I.2.22.1, I.2.22.3, I.2.22.6, I.2.23,	GAPP Ref 3.2.4 GAPP Ref 8.2.2
Resiliency												
Management Program	RS-01	RS-01.1	Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants?	Yes	COBIT 4.1 PO 9.1 PO 9.2 DS 4.2	45 CFR 164.308 (a)(7)(i) (New) 45 CFR 164.308 (a)(7)(ii)(C)	Clause 4.3.2 A.14.1.1 A 14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2)	PCI DSS v2.0 12.9.1	SIG v6.0: K.1.2.9, K.1.2.10, K.3.1	
Impact Analysis	RS-02	RS-02.1	Do you provide tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance?	2.1 - No. Only available upon request. 2.2 - No 2.3 - No. Only available upon request.		45 CFR 164.308 (a)(7)(ii)(E)	ISO/IEC 27001:2005 A.14.1.2 A 14.1.4	NIST SP800-53 R3 RA-3	NIST SP800-53 R3 RA-3		SIG v6.0:K.2	
		RS-02.2	Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?									
		RS-02.3	Do you provide customers with ongoing visibility and reporting into your SLA performance?									
Business Continuity Planning	RS-03	RS-03.1	Do you provide tenants with geographically resilient hosting options?	3.1 - Yes 3.2 - No		45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	Clause 5.1 A.6.1.2 A.14.1.3 A.14.1.4	NIST SP800-53 R3 CP-1 NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-6 NIST SP800-53 R3 CP-7 NIST SP800-53 R3 CP-8 NIST SP800-53 R3 CP-9 NIST SP800-53 R3 CP-10 NIST SP800-53 R3 PE-17		PCI DSS v2.0 12.9.1 PCI DSS v2.0 12.9.3 PCI DSS v2.0 12.9.4 PCI DSS v2.0 12.9.6	SIG v6.0: K.1.2.3. K.1.2.4, K.1.2.5, K.1.2.6, K.1.2.7, K.1.2.11, K.1.2.13, K.1.2.15,	
		RS-03.2	Do you provide tenants with infrastructure service failover capability to other providers?									

Business Continuity Testing	RS-04	RS-04.1	Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Yes		45 CFR 164.308 (a)(7)(ii)(D)	A.14.1.5	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4	NIST SP800-53 R3 CP-2 NIST SP800-53 R3 CP-2 (1) NIST SP800-53 R3 CP-2 (2) NIST SP800-53 R3 CP-3 NIST SP800-53 R3 CP-4 NIST SP800-53 R3 CP-4 (1)	PCI DSS v2.0 12.9.2	SIG v6.0: K.1.3, K.1.4.3, K.1.4.6, K.1.4.7, K.1.4.8, K.1.4.9, K.1.4.10, K.1.4.11, K.1.4.12	
Environmental Risks	RS-05	RS-05.1	Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?	Yes		45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii) (New)	A.9.1.4 A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3) NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18		AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	GAPP Ref 8.2.4
Equipment Location	RS-06	RS-06.1	Are any of your datacenters located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	Yes		45 CFR 164.310 (c)	A.9.2.1	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-5 NIST SP800-53 R3 PE-14 NIST SP800-53 R3 PE-14 (1) NIST SP800-53 R3 PE-15 NIST SP800-53 R3 PE-18	PCI DSS v2.0 9.1.3 PCI DSS v2.0 9.5 PCI DSS v2.0 9.6 PCI DSS v2.0 9.9 PCI DSS v2.0 9.9.1	AUP v5.0 F.1 SIG v6.0: F.2.9, F.1.2.21, F.5.1, F.1.5.2, F.2.1, F.2.7, F.2.8,	

Equipment Power Failures	RS-07	RS-07.1	Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	Yes			A.9.2.2 A.9.2.3 A 9.2.4	NIST SP800-53 R3 CP-8 NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-9 NIST SP800-53 R3 PE-10 NIST SP800-53 R3 PE-11 NIST SP800-53 R3 PE-12 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-14			AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12,	
Power / Telecommunications	RS-08	RS-08.1	Do you provide tenants with documentation showing the transport route of their data between your systems?	8.1 - No 8.2 -Yes, customers have the ability to provision dedicated connectivity from any network provider within the data center. This allows customers complete control over their connectivity.			A.9.2.2 A.9.2.3	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13	NIST SP800-53 R3 PE-1 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 PE-13 NIST SP800-53 R3 PE-13 (1) NIST SP800-53 R3 PE-13 (2) NIST SP800-53 R3 PE-13 (3)		AUP v5.0 F.1 SIG v6.0: F.1.6, F.1.6.1, F.1.6.2, F.1.9.2, F.2.10, F.2.11, F.2.12,	
		RS-08.2	Can Tenants define how their data is transported and through which legal jurisdiction?									
Security Architecture												
Customer Access Requirements	SA-01	SA-01.1	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?	No			A.6.2.1 A.6.2.2 A.11.1.1	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-2 (1) NIST SP800-53 R3 CA-5 NIST SP800-53 R3 CA-6		SIG v6.0: C.2.1, C.2.3, C.2.4, C.2.6.1, H.1	GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 6.2.1 GAPP Ref 6.2.2
User ID Credentials	SA-02	SA-02.1	Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service?	2.1 - No 2.2 - No 2.3 - No 2.4 - No 2.5 - Yes 2.6 - Yes 2.7 - No	COBIT 4.1 DS5.3 COBIT 4.1 DS5.4	45 CFR 164.308(a)(5)(ii)(c) (New) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.8.3.3 A.11.1.1 A.11.2.1 A.11.2.3 A.11.2.4 A.11.5.5			PCI DSS v2.0 8.1 PCI DSS v2.0 8.2, PCI DSS v2.0 8.3 PCI DSS v2.0 8.4 PCI DSS v2.0 8.5 PCI DSS v2.0 10.1, PCI DSS v2.0 12.2, PCI DSS v2.0 12.3.8	AUP v5.0 B.1 AUP v5.0 H.5 SIG v6.0: E.6.2, E.6.3, H.1.1, H.1.2, H.2, H.3.2, H.4, H.4.1, H.4.5, H.4.8,	
		SA-02.2	Do you use open standards to delegate authentication capabilities to your tenants?									
		SA-02.3	Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?									
		SA-02.4	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?									

		SA-02.5	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)?									
		SA-02.6	Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access?									
		SA-02.7	Do you allow tenants to use third party identity assurance services?									
Data Security / Integrity	SA-03	SA-03.1	Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP CAESARS)	Yes	COBIT 4.1 DS5.11		A.10.8.1 A.10.8.2 A.11.1.1 A.11.6.1 A.11.4.6 A.12.3.1 A.12.5.4 A.15.1.4	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-1 NIST SP800-53 R3 SC-16	PCI DSS v2.0 2.3 PCI DSS v2.0 3.4.1, PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.0 6.1 PCI DSS v2.0 6.3.2a PCI DSS v2.0 6.5c PCI DSS v2.0 8.3 PCI DSS v2.0 10.5.5 PCI DSS v2.0 11.5	AUP v5.0 B.1 SIG v6.0: G.8.2.0.2, G.8.2.0.3, G.12.1, G.12.4, G.12.9, G.12.10, G.16.2, G.19.2.1, G.19.3.2, G.9.4, G.17.2, G.17.3, G.17.4, G.20.1,	GAPP Ref 1.1.0 GAPP Ref 1.2.2 GAPP Ref 1.2.6 GAPP Ref 4.2.3 GAPP Ref 5.2.1 GAPP Ref 7.1.2 GAPP Ref 7.2.1 GAPP Ref 7.2.2 GAPP Ref 7.2.3 GAPP Ref 7.2.4 GAPP Ref 8.2.1 GAPP Ref 8.2.2 GAPP Ref 8.2.3 GAPP Ref 8.2.5 GAPP Ref 9.2.1
Application Security	SA-04	SA-04.1	Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)?	4.1 - Yes 4.2 - Yes 4.3 - Yes	COBIT 4.1 AI2.4	45 CFR 164.312(e)(2)(i)	A.11.5.6 A.11.6.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.5.2 A.12.5.4 A.12.5.5 A.12.6.1 A.15.2.1			PCI DSS v2.0 6.5	AUP v5.0 I.4 SIG v6.0: G.16.3, I.3	GAPP Ref 1.2.6
		SA-04.2	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?									
		SA-04.3	Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?									

Data Integrity	SA-05	SA-05.1	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	5.1 - Yes		45 CFR 164.312 (c)(1) (New) 45 CFR 164.312 (c)(2)(New) 45 CFR 164.312(e)(2)(i)(New)	A.10.9.2 A.10.9.3 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4 A.12.6.1 A.15.2.1	NIST SP800-53 R3 SI-10 NIST SP800-53 R3 SI-11 NIST SP800-53 R3 SI-2 NIST SP800-53 R3 SI-3 NIST SP800-53 R3 SI-4 NIST SP800-53 R3 SI-6 NIST SP800-53 R3 SI-7 NIST SP800-53 R3 SI-9		PCI DSS v2.0 6.3.1 PCI DSS v2.0 6.3.2	AUP v5.0 I.4 SIG v6.0: G.16.3, I.3	GAPP Ref 1.2.6
Production / Nonproduction Environments	SA-06	SA-06.1	For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes?	6.1 - N/A 6.2 - Yes	COBIT 4.1 DS5.7		A.10.1.4 A.10.3.2 A.11.1.1 A.12.5.1 A.12.5.2 A.12.5.3	NIST SP800-53 R3 SC-2	NIST SP800-53 R3 SC-2	PCI DSS v2.0 6.4.1 PCI DSS v2.0 6.4.2	AUP v5.0 B.1 SIG v6.0: I.2.7.1, I.2.20, I.2.17,I.2.22.2, I.2.22.4,I.2.22.10-14, H.1.1	GAPP Ref 1.2.6
		SA-06.2	For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments?									
Remote User Multifactor Authentication	SA-07	SA-07.1	Is multi-factor authentication required for all remote user access?	Yes			A.11.1.1 A.11.4.1 A.11.4.2 A.11.4.6 A.11.7.1	NIST SP800-53 R3 AC-17 NIST SP800-53 R3 AC-20 NIST SP800-53 R3 IA-1 NIST SP800-53 R3 IA-2 NIST SP800-53 R3 MA-4		PCI DSS v2.0 8.3	AUP v5.0 B.1 SIG v6.0: H.1.1, G.9.13, G.9.20, G.9.21,	GAPP Ref 8.2.2
Network Security	SA-08	SA-08.1	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?	Yes			A.10.6.1 A.10.6.2 A.10.9.1 A.10.10.2 A.11.4.1 A.11.4.5 A.11.4.6 A.11.4.7 A.15.1.4	NIST SP800-53 R3 SC-7		PCI DSS v2.0 1.1 PCI DSS v2.0 1.1.2 PCI DSS v2.0 1.1.3 PCI DSS v2.0 1.1.5 PCI DSS v2.0 1.1.6 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 2.2.2, PCI DSS v2.0 2.2.3		GAPP Ref 8.2.5
Segmentation	SA-09	SA-09.1	Are system and network environments logically separated to ensure Business and customer security requirements?	9.1 - Yes 9.2 - Yes 9.3 - Yes 9.4 - Yes	COBIT 4.1 DS5.10	45 CFR 164.308 (a)(4)(ii)(A)	A.11.4.5 A.11.6.1 A.11.6.2 A.15.1.4	NIST SP800-53 R3 AC-4 NIST SP800-53 R3 SC-2 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7		PCI DSS v2.0 1.1 PCI DSS v2.0 1.2 PCI DSS v2.0 1.2.1 PCI DSS v2.0 1.3 PCI DSS v2.0 1.4	AUP v5.0 G.17 SIG v6.0: G.9.2, G.9.3, G.9.13	
		SA-09.2	Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements?									
		SA-09.3	Are system and network environments logically separated to ensure separation of production and non-production environments?									

		SA-09.4	Are system and network environments logically separated to ensure protection and isolation of sensitive data?									
Wireless Security	SA-10	SA-10.1	Are policies and procedures established and mechanisms implemented to protect network environment peremeter and configured to restrict unauthorized traffic?	10.1 - Yes 10.2 - Yes 10.3 - Yes	COBIT 4.1 DS5.5 COBIT 4.1 DS5.7 COBIT 4.1 DS5.8 COBIT 4.1 DS5.10	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) (New) 45 CFR 164.312(e)(1) (New) 45 CFR 164.312(e)(2)(ii) (New)	A.7.1.1 A.7.1.2 A.7.1.3 A.9.2.1 A.9.2.4 A.10.6.1 A.10.6.2 A.10.8.1 A.10.8.3 A.10.8.5 A.10.10.2 A.11.2.1 A.11.4.3 A.11.4.5 A.11.4.6 A.11.4.7 A.12.3.1 A.12.3.2	NIST SP800-53 R3 AC-1 NIST SP800-53 R3 AC-18 NIST SP800-53 R3 CM-6 NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-3 NIST SP800-53 R3 SC-7		PCI DSS v2.0 1.2.3 PCI DSS v2.0 2.1.1 PCI DSS v2.0 4.1 PCI DSS v2.0 4.1.1 PCI DSS v2.011.1 PCI DSS v2.0 9.1.3		GAPP Ref 8.2.5
		SA-10.2	Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)									
		SA-10.3	Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?									
Shared Networks	SA-11	SA-11.1	Is access to systems with shared network infrastructure restricted to authorize personnel in accordance with security policies, procedures and standards? Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?	11.1 - Yes		45 CFR 164.312 (a)(1) (New)	A.10.8.1 A.11.1.1 A.11.6.2 A.11.4.6	NIST SP800-53 R3 PE-4 NIST SP800-53 R3 SC-4 NIST SP800-53 R3 SC-7		PCI DSS v2.0 1.3.5 PCI DSS v2.0 2.4	AUP v5.0 B.1 SIG v6.0: D.1.1, E.1, F.1.1, H.1.1,	GAPP Ref 8.2.5
Clock Synchronization	SA-12	SA-12.1	Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?	Yes	COBIT 4.1 DS5.7		A.10.10.1 A.10.10.6	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8	NIST SP800-53 R3 AU-1 NIST SP800-53 R3 AU-8 NIST SP800-53 R3 AU-8 (1)	PCI DSS v2.0 10.4	AUP v5.0 G.7 AUP v5.0 G.8 SIG v6.0: G.13, G.14.8, G.15.5, G.16.8, G.17.6, G.18.3, G.19.2.6, G.19.3.1,	
Equipment Identification	SA-13	SA-13.1	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?	Yes	COBIT 4.1 DS5.7		A.11.4.3	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4	NIST SP800-53 R3 IA-3 NIST SP800-53 R3 IA-4 NIST SP800-53 R3 IA-4 (4)		AUP v5.0 D.1 SIG v6.0: D.1.1, D.1.3	
Audit Logging / Intrusion Detection	SA-14	SA-14.1	Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?	14.1 - Yes 14.2 - Yes 14.3 - Yes	COBIT 4.1 DS5.5 COBIT 4.1 DS5.6 COBIT 4.1 DS9.2	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)(c) (New)	A.10.10.1 A.10.10.2 A.10.10.3 A.10.10.4 A.10.10.5 A.11.2.2			PCI DSS v2.0 10.1 PCI DSS v2.0 10.2 PCI DSS v2.010.3 PCI DSS v2.0		GAPP Ref 8.2.1 GAPP Ref 8.2.2

		SA-14.2	Is Physical and logical user access to audit logs restricted to authorized personnel?				A.11.5.4 A.11.6.1 A.13.1.1 A.13.2.3 A.15.2.2 A.15.1.3			10.5 PCI DSS v2.010.6 PCI DSS v2.0 10.7 PCI DSS v2.0 11.4 PCI DSS v2.0 12.5.2 PCI DSS v2.0 12.9.5		
		SA-14.3	Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done?									
Mobile Code	SA-15	SA-15.1	Is mobile code authorized before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?	15.1 - N/A - Mobile code is not used. 15.2 - Yes			A.10.4.2 A.12.2.2	NIST SP800-53 R3 SC-18	NIST SP800-53 R3 SC-18 NIST SP800-53 R3 SC-18 (4)		SIG v6.0:G.20.12, I.2.5	
		SA-15.2	Is all unauthorized mobile code prevented from executing?									