RESEARCHERID
THOMSON REUTERS

[Satwinder * 6(5): May, 2019] ISSN 2349-4506
Impact Factor: 3.799

Global Journal of Engineering Science and Research Management

A FRAMEWORK FOR IMPROVING SECURITY IN CLOUD COMPUTING FOR SMES (FISCCS) USING SECURITY INDEX

Satwinder Singh Rupra*, Dr. Amos Omamo

* (MSc. IT Security & Audit, BSc. Information Technology, Authorized Telecommunications Contractor (CAK Kenya) Authorized Siemon and Giganet Network Installer, CCNSP, MTCNA, MTCWE)

DOI: 10.5281/zenodo.2703162

KEYWORDS: Benefits of Cloud Computing, Review of Existing Frameworks, ENISA Cloud Framework.

ABSTRACT

Cloud computing plays a very important role in the development of business and competitive edge for many organizations including SMEs. Cloud computing is considered to be a very capable and able internet-based computing platform which offers numerous benefits like mobility, flexibility, reliability and cost effectiveness. Every cloud user continues to expect maximum service, and a critical aspect is cloud security which is one among other specific challenges hindering adoption of the cloud technologies. The absence of appropriate, standardized and self-assessing security frameworks of the cloud world becomes an endless problem in developing countries and can expose the cloud computing model to major security risks which threaten its potential success within the country. It is further noted that security issues arise from either human error (people), lack of implementing appropriate technology or external factors like cloud providers or legislation. Security metrics can be seen as tools for providing information about the security status of a certain environment. With that in mind, this paper presents a security framework for assessing security in the cloud environment based on the Goal Question Metrics methodology. The framework named as Framework for Improving Security in Cloud Computing for SMEs (FISCCS) produces a security index that describes the security level accomplished by an evaluated cloud computing environment thereby providing the first line of defense.

INTRODUCTION

Business applications have always been very complicated and expensive; the amount and variety of hardware and software required to run them are overwhelming. Businesses need a whole team of experts to install, configure, test, run, secure, and update them, which most SMEs are unable to afford (Velte, Velte, Elsenpeter & Elsenpeter, 2010). With the introduction of cloud computing for businesses, most of the SMEs are able to avoid headaches that come with storing their own data, because they are not managing hardware and software - that becomes the responsibility of cloud computing provider. The shared infrastructure means cloud computing works like a utility, where SME only pay for what they need, upgrades are automatic and scaling up or down is easy (Fox et al, 2009). It is a model that enables on-demand access to shared configurable computing resources which can then be configured for usage by an organization. These resources include applications and services, or the infrastructure on which the services operate. By deploying IT infrastructure through the cloud, an organization can purchase additional resources on an as-required basis and avoid the initial costs of software and hardware (E.g. networks, servers, storage, application software) (Buyya, Broberg & Goscinski, 2010).

According to Kavanagh and Johnson, (2017), organizations are now comfortable to allow their employees access their information on their mobile phones and tablets and to carry out business-critical tasks. It is clear that mobility and virtualization has helped organizations in many industries to meet their business objectives. However, since this kind of computing paradigm is fairly new, it has shortfalls that need to be addressed to make its services more convenient to use. (Vecchiola, Pandey & Buyya, 2009).

Cloud computing is known to be very promising internet-based computing platforms, but this platform could result in a loss of security over customer data. This usually happens because the enterprise IT assets are hosted on third-party cloud computing platforms (Buyya, Yeo, Venugopal, Broberg & Brandic 2009). As SMEs become more embedded in cloud computing, cyber threats on the other hand is threatening the prosperity of cloud computing in the SME sector (Sultan, 2010). The increased reliance of cloud computing and cyberspace has not

only brought numerous benefits but also exposed the SMEs to a lot of cyber threats. These cyber issues range from malware that compromises with the integrity of data and privacy of critical information to denial of service (DoS) that disrupts the provision of services according to The Center of Internet Security (2016). Whatever shape the attack takes, the overall consequences are the same; sensitive data is at stake and the trust in the cloud goes down (Harries & Yellowlees, 2013).

Where cloud computing can help organizations accomplish more by paying less and breaking the physical boundaries between IT infrastructure and its users, heightened security threats must be overcome in order to benefit fully from this new computing exemplar (Palmer, 2015).

PROBLEM STATEMENT

A baseline survey of cloud computing in Kenya in 2013 reveals that security is one among other specific challenges hindering adoption of the cloud technologies in Kenya (Omwansa, Waema & Omwenga, 2014). Every cloud user continues to expect maximum service, and a critical aspect is cloud security which is one among other specific challenges hindering adoption of the cloud technologies. The absence of appropriate, standardized and self-assessing security frameworks of the cloud world becomes an endless problem in developing countries and can expose the cloud computing model to major security risks which threaten its potential success within the country. Although there are a number of standard Security Framework/guidelines like ISO 27001, Cyber Security Framework and others, all these standards are in evolving stages for the Cloud computing environment and do not provide methods to guide the SMEs. Apart from this, the security requirements of SMEs vary based on their specific security risks. Therefore it is absolutely essential to have a comprehensive, end-to-end standardized Security Framework based on industry standards, but tailored to the specific requirements of SMEs.

There are six crucial areas in the cloud that require protection to be able to suffice against the threats. These six areas are as below:

1. Security of data at rest – This means data should be secure when it is stored in the cloud server(s). This is usually achieved by providing encryption for all data stored.
2. Security of data in transit – Means that data should be secure when being transferred from the cloud to the user computers and vice versa. This can be achieved by providing TLS/SSL security.
3. Authentication of users – Users who have access to data should pass some sort of access control to be able to keep off unwanted users. These include strong passwords and biometrics among others.
4. Robust isolation between data belonging to different customers – Although not applicable to private clouds, however for public clouds each customers data is isolated using different VMs.
5. Cloud legal/regulatory issues – All customers should usually have their legal and regulatory experts inspect cloud provider policies and practices especially for things like data retention, deletion and security.
6. Incident response – Customers should understand how incidents and disasters will affect their data and should therefore implement relevant recovery procedures for the same.

LITERATURE REVIEW

Cloud computing is believed to have been introduced as early as 1969 by J.C.R. Licklider, who was in charge of the development of Advanced Research Projects Agency Network (ARPANET). His vision was to create a platform for accessing data and programs from anywhere and at any site. This vision is quite similar to the modern cloud computing. Since those days, cloud computing and storage has evolved a long way Buyya, Broberg, & Goscinski, (2010). However, since in the early years the internet was not able to offer bandwidth capacities like today, cloud computing for the masses has been adopted and widely used much later (Mohamed, 2009).

For a paradigm to be classified as a cloud computing, it usually possesses the following characteristics as indicated by NIST:

- Elasticity: Cloud users can at their convenience downsize/upsize computing resources, as and when need arises, without human interaction. This means that to add or reduce resources on the cloud, one will not need to buy additional hardware, users can do this by the use of controlled software.

- Access on multiple devices: Users of the cloud are not limited to the number or type of devices they use. Mostly, if devices can access internet and have the relevant cloud applications, a user can connect to the cloud from any device.
- Accessible anywhere: Cloud customers may be able to access their data and service irrespective of the geographical location. Therefore, the cloud user has no control or whereabouts of the location of the assets. Similarly, the cloud vendor does not have restrictions over the location of its users.
- Reliability: Clouds are usually backed up on multiple redundant sites sometimes even offshore, therefore all data saved on the cloud has disaster recovery catered for.
- Economies of scale and cost effectiveness. Cloud implementations, regardless of the deployment model, tend to be as large as possible in order to take advantage of economies of scale. Therefore, cloud vendors can be located in areas where electricity and real estate prices are lower eventually lowering their start-up and running costs.

Benefits of Cloud Computing

The shift from grid computing to cloud computing is getting more evident by the day. Cloud computing offers numerous benefits which could not be attained in the native computing infrastructure. The advantages of cloud computing paradigm include the following:

1. Mobility: The primary benefit of cloud computing by far would be the ability to access data from anywhere at any time. Once cloud users have registered themselves to a cloud vendor, all that is needed is an internet connection to be able to access their information and services. This feature lets users move beyond time zone and geographical boundary issues.
2. Flexibility: Users only have to pay for services and capacity which they are really using. So if they need less they pay less and if they need more they can simply acquire additional storage and services, which of course leads to higher costs, but it is still much more flexible than adding another server to the company internal IT resources. The addition or removal of processing units or storage space does only take seconds to minutes and not days like it would in a company internal data center using physical servers.
3. Reliability: Cloud computing also adds to reliability of data in case the user loses their device. If a laptop or mobile phone is stolen, the user's data cannot be lost since it is stored in the cloud; the user can simply buy another device and connect it to the internet to access their data.
4. Reduction of cost: Many cloud services are provided for free and offer enough functionality for most of the users. Therefore, users can save much money by using cloud services.
5. Allow IT people to concentrate on other areas by taking the load of data storage, application control and update from off their work.

Review of Existing Frameworks

As new threats emerge, regulations and standards continue to increase in number and complexity. Now, many laws carry penalties for data breaches and for not meeting timely notification of those affected. These areas of concern are addressed as the cloud environment continues to evolve with the utilization of encryption methods are incorporated as organizations define their strategy for cloud control. The benefits of security frameworks are to protect vital processes and the systems that provide those operations. A security framework is a coordinated system of tools and behaviors in order to monitor data and transactions that are extended to where data utilization occurs, thereby providing end-to-end security (Vahradsky, 2012).

Cyber Security Framework

The National Institute of Standards and Framework's Cyber Security Framework (CSF) was published in February 2014 in which the president called for a standardized security framework for critical infrastructure in the United States. The NIST CSF is recognized by many as a resource to help improve the security operations and governance for public and private organizations. While the NIST CSF is a vital guideline for transforming the organizational security posture and risk management from a reactive to proactive approach, it is a difficult framework to understand and implement due to its complexity. The CSF has two primary advantages:

1. Risk-based approach. Since the beginning of cyber security, the focus has been on defense. CSF shifts the primary focus to risks as the outcome as opposed to just controls.

2. Relevance to Current Threats. The CSF framework includes important updates that make more relevant today, including authentication and identity, self-assessing cyber security risk, managing cyber security within the supply chain and vulnerability disclosure.

Similarly, the CSF has some shortcomings as mentioned below:

1. Complexity. There is not much information provided on how companies can automate some of the implementation steps for this framework (Pleshakova, 2018) As the cyber security world continues to evolve and change, automation is key for resource allocation and, as a result, a better security posture.
2. Developed for Critical Infrastructures. The CSF was developed for critical infrastructure community and is not readily fitting into the SME environment or cloud security environment. CSF would be yet another security checklist that smaller organizations would ignore due to its complexity (Hayden, 2010). By following this framework, organizations are assumed to have less risk but this framework still does not help to measure cloud risks in tangible terms. According to Shackelford, Russell and Haut, (2015) the functions, categories or sub categories in the latest NIST CSF draft do not specifically call out or even attempt to address cloud related risks.

ENISA Cloud Framework

The Cloud Security Alliance and European Union Agency for Network and Information Security (ENISA) have compiled a set of recommendations in a cloud security framework for European Union (EU) governments. The recommendations discuss some EU- and government-specific topics, such as the possibility of a European Government Cloud and an assessment of EU member cloud maturity, but most of the report is generally applicable to cloud security across application domains.

The framework outlines a four-stage lifecycle for developing and deploying clouds, which includes planning, implementing, review and evaluation, and remediation. The ENISA framework has two primary advantages:

1. Monitoring and Logging: The framework stresses on this as a critical aspect since monitoring and auditing may detect weaknesses in current practices and implementations.
2. Exit management: Exit management is especially important to manage transitions when a government or enterprise terminates a cloud contract. A number of critical areas should be addressed when planning for exits, including how data will be deleted, how access control and identity information will be protected, and how services continuity will be maintained. The framework encompasses this aspect soundly.

The ENISA framework has some shortcomings as mentioned below:

1. Relevance: The framework is less relevant to enterprise cloud users due to its complexity and also the fact that it is more significant to government clouds. The framework does not account for challenges encountered by developing country SMEs. For example, the challenges of availability due to internet outages. The framework is aligned for the EU countries.

International Standards Organization (ISO) 27001

The ISO 27001 is one of the most widely known security standards and is a mature framework focused on information security. It's very comprehensive and broad, and can be used across a wide range of types and sizes of businesses.

Because it's tried and tested, countries often use it as a basis on which to create a manual about security and what to do. However, like many of the ISO standards, it can be a bit daunting, and many smaller organizations are put off by the effort required to gain accreditation and the perception that it can be difficult to implement. According to a research conducted by Muthee (2013), only 5% of organizations in Kenya have certified with ISO 27001 and the number is less than 1% for SME. This is due to the fact that organizations see it as both technically and procedurally challenging, adding additional overhead to their business.

Based on the studies on cloud security and existing frameworks reviewed above, it is noted that a suitable framework for SMEs to self-assess their cloud security is not available either due to their complex nature in adopting them or because they do not cover the cloud aspect effectively.

COSO Framework

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognized as the definitive standard against which organizations measure the effectiveness of their systems of internal control. The COSO model defines internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives in the following categories:

1) Effectiveness and efficiency of operations
2) Reliability of financial reporting
3) Compliance with applicable laws and regulations

In an effective internal control system, the five components work to support the achievement of an entity's mission, strategies and related business objectives. The five functions are Control Environment, risk assessment, control activities, Information and Communication and finally monitoring.

The COSO framework individually does not solve the issues arising from security in the cloud. This is because the framework is focused on just one area of the organization of the internal controls and therefore might not be cloud ready.

As indicated in the above section, framework and guidelines like ISO 27001, NIST 800-53, ENISA and COSO have been reviewed, but all these standards are in evolving stages for the Cloud computing environment. Although ISO/IEC 27001 provides generic guidance in developing the security objectives and metrics, but it still does not provide methods to guide SMEs and is very general. Apart from this, the security requirements of SMEs vary based on their specific security risks. Therefore it is vital to have a standardized security framework based on industry standards, but tailored to the specific requirement of SMEs. While reviewing industry security framework and guidelines, it was found out that there are no cloud security frameworks, best practices and guidelines aligned towards the challenges faced by SMEs either due to their complex nature in adopting them or because they do not cover the cloud aspect effectively.

PROPOSED FRAMEWORK

Typically, the security objective for any cloud framework is to deter, prevent, detect, recover from, and respond to threats arising from the usage of cloud computing. Cloud security is to safeguard these information assets, the information systems and networks that deliver the information to and from the cloud, from damage or compromise resulting from failures of confidentiality, integrity and availability. Security is multifaceted and it includes information technology, procedures and practices, laws and regulations, people and organizations; these areas are said to be interrelated and impact each other (Denning, 2003).

To ensure business continuity, SMEs require a means that enables them to proactively analyze the various imperative factors critical to the security and business operations.

The proposed Framework for Improving Security in Cloud Computing for SMEs (FISCCS), as defined in this paper is based on the Cyber-security Framework (CSF). This choice is based on the fact that the Framework, deriving from the NIST, provides a full coverage and is at the state of the art of the life-cycle of information and system security, however, because it has been created from Critical Infrastructures made up of 21 Categories and 98 Subcategories, it introduces a complexity level which is not suitable for most SMEs of the developing nation and therefore Kenyan context.

The proposed Framework for Improving Security in Cloud Computing for SMEs (FISCCS) borrows some concepts from the Cyber-security Framework (CSF) represented in Figure 1 below:

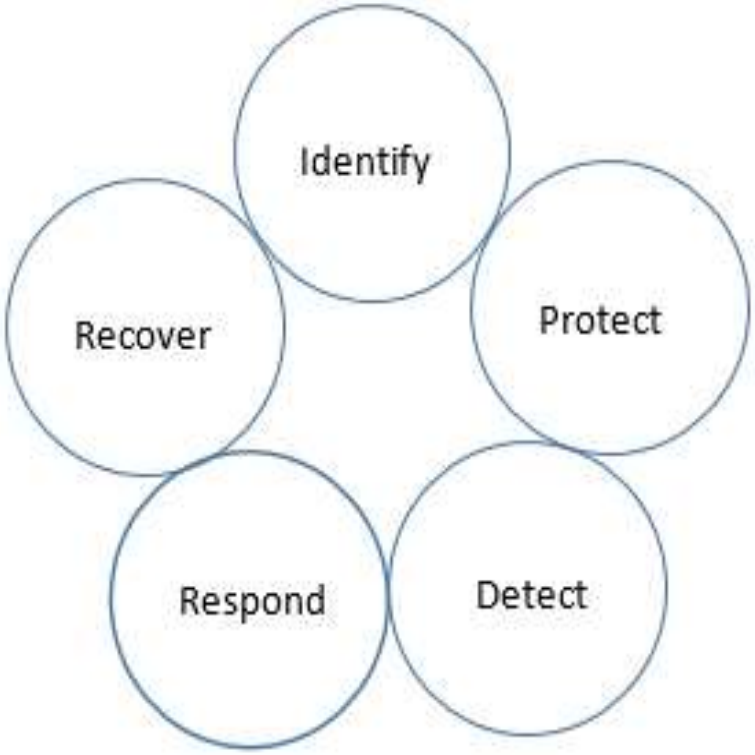

Figure 1: Cyber-Security Framework
Source: The National Institute of Standards and Technology (2014)

The 5 Functions are briefly described below:
Identify: The Identify Function is linked to the understanding of the company context, of assets that support the critical business processes and relevant associated risks. Such understanding enables the SME to define resources and investments according to the risk management strategy and company objectives. The Categories within this Function are: Asset Management; Business environment; Governance; Risk analysis; Risk management strategy.
Protect: The Protect Function is linked to the implementation of measures aimed at protecting the data and its movement, regardless of their IT nature. Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

Detect: The Detect Function is linked to the definition and implementation of appropriate activities aimed at identifying IT security accidents on time. Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Respond: The Respond Function is linked to the definition and implementation of appropriate activities in order to take action in case of detection of a cyber-security event or attack. The aim is to reduce the impact of a potential cyber security event. Categories within this Function include: Planning; Communications; Analysis; Mitigation; and Improvements.

Recover: The Recover Function is linked to the definition and implementation of activities aimed at the management of plans and activities to restore processes and services impaired due to a cyber-security event. The aim is to ensure the resilience of systems and facilities and, in case of accident, to support the timely recovery of business operations. Categories within this Function include: Recovery Planning; Improvements; and Communications.

As any company risk, the risk of data in the cloud cannot be eliminated and therefore requires a series of coordinated actions to be taken in order manage it. Such actions involve the organization and technology departments of the company, in addition to the financial management of the risk, also through the establishment of a residual risk management strategy and a strategy to protect the company balance. Furthermore, the cyber risk is intrinsically highly dynamic. It changes as threats, technology and regulations change. To start approaching this issue in a way which is useful for SMEs, it is necessary to define a common ground, a Framework, in which the various production sectors, government agencies and regulated sectors can recognize their business, so to align their cyber security policies in a steadily developing process. To reach this aim a common Framework should be first of all neutral both in terms of business risk management policies and in terms of technology, so that each player could keep on using its own risk management tools, managing its technology assets while monitoring at the same time the compliance with sector standards.

This study presents a Framework for Improving Security in Cloud Computing for SMEs (FISCCS) aimed at creating a common language to compare the implementation of these systems risks. The Framework may help an SME to plan a cyber-risk management strategy, developed over the time according to its business, size and other distinguishing and specific elements of the enterprise.

The choice to develop the Framework is based on the idea that the answer to threat management should provide an alignment at international level, not only at national level. The Framework offers high flexibility, which is mostly targeted at SME facilities; we developed it according to the characteristics of the social and economic system of our country, reaching a cross-sector framework that can be contextualized in implementation of secure cloud for SMEs. This allows the transfer of practices and knowledge from one sector to another in an easy and efficient way.

In this sense, this study introduces three important concepts in the FISCCS Framework:

1) People involved in handling the data in the cloud, the cloud users, the administrators as well as the owners of the SME who make decisions and invest into IT security. The people element represents the human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. It is critical for the IT administrators or IT managers to work with the human resources and legal departments to address employment issues including access to tools and data, training and awareness, privileges within the enterprise and its IT assets. Other issues that may need to be addressed include recruitment strategies (access, background checks, interviews, roles and responsibilities) and termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees).
2) Technologies for securing data in the cloud available to the SMEs, these include two factor authentication for logging into the cloud, use of encryption for data at rest, transport later security (TLS) for data during transport over the network, secondary link for failover to prevent lockout. As an evolving element that experiences frequent changes, it has its own dynamic risks. Given the typical enterprise's dependence on technology, technology constitutes a core part of any SMEs infrastructure and a critical component in accomplishing its mission. Technology is often seen by the enterprise's management team as a way to resolve security threats and risks. While technical controls are helpful in mitigating some types of risks, technology should not be viewed as an information security solution.
3) External factors affecting the usage of cloud including government laws, cloud owner data retention policies, offshore backups by cloud providers.

This is represented in framework in Figure 2:

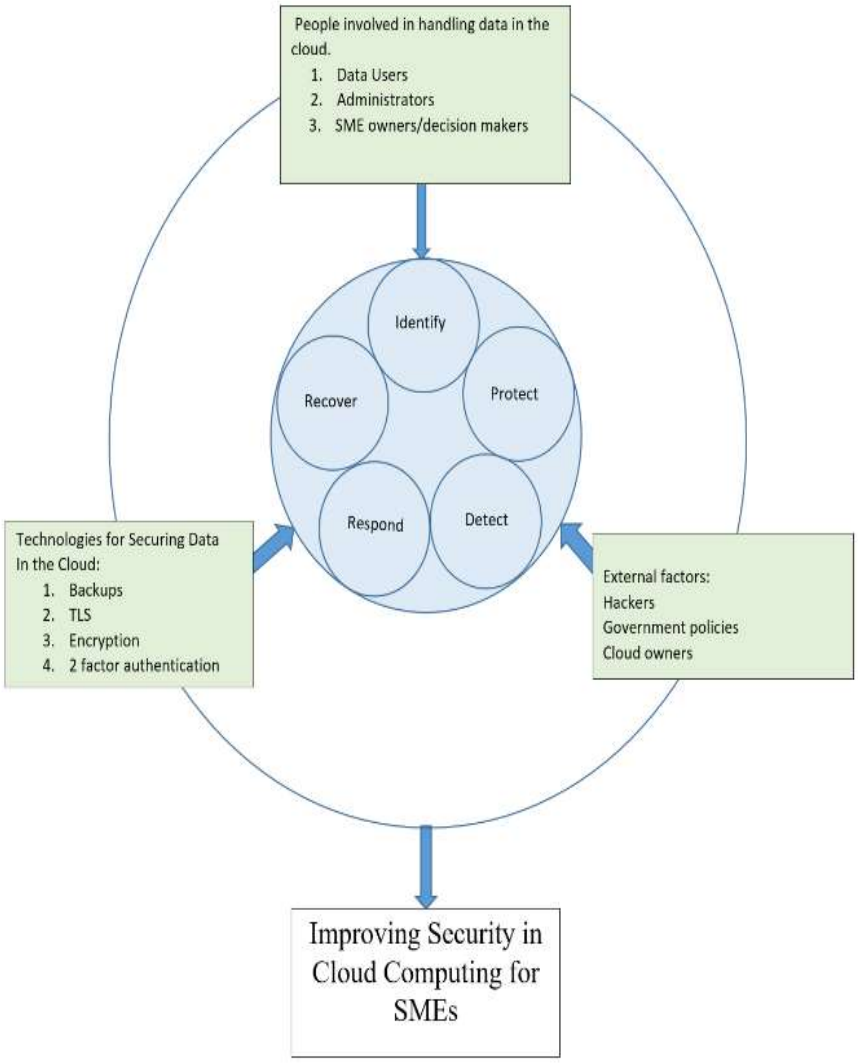

Figure 2: Building the Framework
Source: Author

The framework core represents the life cycle structure of the management process of cyber security, both from a technical and organizational point of view. The core is structured hierarchically into group metrics, metrics and sub metrics. The group metrics are: Identify, Protect, Detect, Respond, Recover and they represent the main topics to deal with in order to strategically secure data in the cloud. Thus, the Framework, for each group metrics, metrics and sub metrics, will provide information in terms of specific questions, defines the categories and technologies to be put in place in order to manage the single Function.

The research suggests a score of one (1) point if the answer is yes and score of zero (0) if the answer is no. The total scored subjected to the GQM formula will enable one to work out the indicative of how secure the SME's cloud data is.

Examples of the security questions are as below and can be formulated based on the SMEs personal scenario.

1	**IDENTIFY RISKS IN CLOUD**
1.1	**Asset Administration (1.1):** The information, employees, equipment, structures, and services that allow the SME to achieve business processes are identified and managed consistent with their relative importance to business objectives and the SME's risk strategy.
1.1.1	**ID.AM-1**: Are all physical IT equipment (computers, laptops, BYOD) within the SME inventoried?
1.1.2	**ID.AM-2:** Are all system and application software within the SME inventoried?
1.1.3	**).AM-3:** Cloud Providers allow the SME to determine where their content will be stored, how it will be secured in transit or at rest, and managed?
1.1.4	**ID.AM-4:** Does the SME ensure that providers of external information system services comply with the SME's information security requirements like applicable laws, directives, policies, regulations, standards, and guidance?
1.1.5	**ID.AM-5:** Does the cloud provider specify what sort of resilience to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)?

CONCLUSION

Cloud computing offers many opportunities to SMEs, but risks and challenges as well. For an SME to succeed, they must critically examine available data, create policies especially security policies, follow existing standards and develop adequate procedures of ensuring adherence. This research offers a means for SMEs to implement cloud solutions in a more secure way, by an approach that is oriented on most of the stages that an organisation must go through to achieve a relatively secure cloud environment.

Frameworks such as FISCCS make a significant impact and create healthy competition among Cloud providers to satisfy their Service Level Agreement (SLA) and improve their Quality of Services (QoS) as well as give SMEs an opportunity to store data in the cloud in a more secure manner. It is important to note that as stated by Becker and Elana (2014), no one framework or model encompasses all of the possible IT controls, collectively they cover the ―what, how, and scope of IT Governance.

REFERENCES

1. Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 693-702). IEEE.
2. Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2(1), 60-63.
3. Behl, A. (2011, December). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Information and communication technologies (WICT), 2011 world congress on (pp. 217-222). IEEE.
4. Jansen, W. A. (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.
5. Buyya, R., Broberg, J., & Goscinski, A. M. (Eds.). (2010). Cloud computing: Principles and paradigms (Vol. 87). John Wiley & Sons.
6. Computing, C. (2010). Security–A Natural Match. Trusted Computing Group (TCG) http://www. trustedcomputinggroup. org.
7. Velte, A. T., Velte, T. J., Elsenpeter, R. C., & Elsenpeter, R. C. (2010). Cloud computing: a practical approach (pp. 1-55). New York: McGraw-Hill.
8. Xu, Y., Yang, Y., Li, T., Ju, J., & Wang, Q. (2017, November). Review on cyber vulnerabilities of communication protocols in industrial control systems. In Energy Internet and Energy System Integration (EI2), 2017 IEEE Conference on (pp. 1-6). IEEE.
9. Pearson, S. (2013). Privacy, security and trust in cloud computing. In Privacy and Security for Cloud Computing (pp. 3-42). Springer London.
10. Jahdali, H., Albatli, A., Garraghan, P., Townend, P., Lau, L., & Xu, J. (2014, April). Multi-tenancy in cloud computing. In Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on (pp. 344-351). IEEE.
11. Saripalli, P., & Walters, B. (2010). QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. Paper presented at 2010 IEEE 3rd International Conference on Cloud Computing, Miami, Florida.
12. Sen, J. (2013). Security and privacy issues in cloud computing. Architectures and Protocols for Secure Information Technology Infrastructures, 1-45.
13. Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., ... & Stoica, I. (2009). Above the clouds: A berkeley view of cloud computing. Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, 28(13), 2009.
14. Kavanagh, M. J., & Johnson, R. D. (Eds.). (2017). Human resource information systems: Basics, applications, and future directions. Sage Publications.
15. Vecchiola, C., Pandey, S., & Buyya, R. (2009, December). High-performance cloud computing: A view of scientific applications. In 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks (pp. 4-16). IEEE.
16. Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), 599-616.
17. Sultan, N. (2010). Cloud computing for education: A new dawn?. International Journal of Information Management, 30(2), 109-116.
18. Center of Internet Security (2016). Retrieved from https://www.cisecurity.org/
19. Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the US healthcare system safe?. Telemedicine and e-Health, 19(1), 61-66.
20. Palmer, S. A. (2015). U.S. Patent No. 9,172,918. Washington, DC: U.S. Patent and Trademark Office.
21. Omwansa, K. T., Waema, M. T., & Omwenga, B. (2014). Cloud Computing in Kenya. Baseline survey.
22. Buyya, R., Broberg, J., & Goscinski, A. M. (Eds.). (2010). Cloud computing: Principles and paradigms (Vol. 87). John Wiley & Sons.
23. Mohamed, A. (2009, March 01). A history of cloud computing. Retrieved March 12, 2016, from http://www.computerweekly.com/feature/A-history-of-cloud-computing
24. Vahradsky, D. (2012). Cloud risk: 10 principals and a framework for assessment. *ISACA*, *5*, 1-12.

25. Pleshakova, A. (2018, November 08). 3 Winners & 2 Losers: NIST Cybersecurity Framework 1.1. Retrieved from https://nehemiahsecurity.com/blog/nist-framework/
26. Hayden, L. (2010). IT security metrics: A practical framework for measuring security & protecting data (Vol. 396). New York: McGraw Hill.
27. Shackelford, S. J., Russell, S., & Haut, J. (2015). Bottoms up: a comparison of voluntary cybersecurity frameworks. UC Davis Bus. LJ, 16, 217.
28. Muthee Josephine W. (2016). *A Data Security Implementation Model for Cloud Computing In Government Parastatals*.
29. Denning, D. E. (2003). Information technology and security.