Scientific Research Publishing

Journal of Information Security, 2020, 11, 201-224
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Cloud Computing Security Assessment Framework for Small and Medium Enterprises

Satwinder Singh Rupra*, Amos Omamo

Kabarak University, Nakuru, Kenya
Email: *satwinder@sumocomputers.net

How to cite this paper: Rupra, S.S. and Omamo, A. (2020) A Cloud Computing Security Assessment Framework for Small and Medium Enterprises. *Journal of Information Security*, **11**, 201-224.
https://doi.org/10.4236/jis.2020.114014

Received: June 30, 2020
Accepted: September 20, 2020
Published: September 23, 2020

Abstract

Cloud computing plays a very important role in the development of business and competitive edge for many organisations including SMEs (Small and Medium Enterprises). Every cloud user continues to expect maximum service, and a critical aspect to this is cloud security which is one among other specific challenges hindering adoption of the cloud technologies. The absence of appropriate, standardised and self-assessing security frameworks of the cloud world for SMEs 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. This research presents a security framework for assessing security in the cloud environment based on the Goal Question Metrics methodology. The developed framework produces a security index that describes the security level accomplished by an evaluated cloud computing environment thereby providing the first line of defence. This research has concluded with an eight-step framework that could be employed by SMEs to assess the information security in the cloud. The most important feature of the developed security framework is to devise a mechanism through which SMEs can have a path of improvement along with understanding of the current security level and defining desired state in terms of security metric value.

Keywords

Cloud Computing, Framework, SME, Security, Standards

1. Background of the Study

In the Kenyan market, an SME is defined by researchers as a company that has a yearly turnover of between KES 70 million and 1 billion and is not listed in the stock exchange [1]. Under the Micro and Small Enterprises Act of 2002, micro enterprises have a maximum annual turnover of KES 500,000 ($5000) and em-

ploy less than 10 people. Small enterprises have between $5000 to $50,000 annual turnovers and employ 10 - 49 people. Medium enterprises—while not covered by the Act have a turnover of between $50,000 and $8 million and employ 50 - 99 people (Kenya Gazette Supplement No. 219, 2013). A recent National Economic Survey report by the Central Bank of Kenya [2] shows that, SMEs constitute 98 percent of all businesses in Kenya and create 30 percent of the jobs annually as well as contribute 3 percent of the GDP. Despite their immense contribution to the economy, Kenya's SMEs are faced with numerous challenges and one of the main challenges has been information technology related costs [3]. 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 [4]. 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 SMEs only pay for what they need, upgrades are automatic and scaling up or down is easy [5].

1.1. Introduction

Cloud computing is a means of data storage whereby the data is stored and accessed over the network, mostly through the internet. The data is stored on multiple servers (and often locations), and the environment is controlled and managed by a hosting company called cloud storage providers [6]. It is a kind of outsourcing of computer programs where users are able to access software and applications from wherever they are. In other words, the computer programs are hosted by an outside party and reside in the cloud and the users do not have to worry about things such as storage and power, they simply enjoy the end result [6]. The providers always keep the data available and accessible wherever and whenever the owner or users require [7]. Put differently, cloud computing is the provisioning of IT resources including hardware, software, or services from third parties over a network, usually the internet. It is the delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally [8].

Researchers [9] assert that cloud computing is a web-service that comprises provision of storage capacity and virtualised computing resources. The virtual computing resource (email, software, data storage) are managed through remote servers by cloud providers. The cloud providers manage the cloud platform to offer their services and the end users access these services through normal browsers on computing devices such as; PC, iPad and Mobile Phones, among others [4] [9]. Therefore, end users do not have to manage or scale the IT infrastructure resources and instead focus on their core businesses. This leads to re-

duced running/capital costs, increased productivity, mobility, collaboration and profitability of businesses [10]. It is a model that enables on-demand access to shared configurable computing resources which can then be configured for usage by an organisation.

Where cloud computing can help organisations 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 [11].

The rate of cyber-attacks has increased in recent times and experts believe that if nothing is done about it, the severity of future attacks could be much greater than what has been observed currently [12]. Cloud hackers have become innovative and have the capacity to cause harm with catastrophic impact from anywhere in the world, while equipped with only a computer and the knowledge needed to identify and exploit vulnerabilities [13]. It is noted that mid-sized businesses which include SMEs, focus their investment on customer satisfaction and mechanisms of reducing operating costs and therefore tend to disregard necessary investment towards securing their cloud infrastructure [14].

1.2. Problem Statement

As more SMEs today continue to use cloud computing as a vital business tool and to store their data online, the need for security of information assets of an organisation cannot be over-emphasised. SMEs are utilising the opportunities offered by cloud to adopt innovative business operations, to increase business efficiency, to develop customer-centric strategies, and to stay competitive with the use of technology. It is therefore imperative to ensure that the information stored in the cloud is protected against any kind of failures or attacks. Although, cloud computing offers several benefits for achieving business success, if the cloud service used is not sufficiently available, reliable, and secure, the business justification for moving to the cloud will be significantly reduced. And, unfortunately, the concentration of the data and applications in the cloud can create a more attractive target for potential attackers.

Therefore, it is absolutely essential to have a comprehensive, end-to-end standardised security framework based on industry standards, but tailored to the specific requirements of SMEs. The authors developed a standardised cloud security framework for SMEs that would aid SMEs to self-assess and index challenges in cloud computing and therefore improving their overall security.

2. Review of Existing Frameworks

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 behaviours in order to monitor data and transactions that are extended to where data utilization occurs, thereby providing end-to-end security [14]. **Table 1** shows various security frameworks and their pros and cons.

Table 1. Review of existing frameworks.

Existing Framework	Pros	Cons
CSF	1) Focuses on defense 2) Relevant to current threats	1) Very complex 2) Not readily fitting into the SME environment or cloud security environment
ENISA	1) Stresses on the critical aspect of monitoring and auditing 2) Plans for exits, including how data will be deleted and how services continuity will be maintained	1) 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. 2) The framework does not account for challenges encountered by developing country SMEs.
ISO 27001	1) 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	1) 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.
COSO Framework	1) Effectiveness and efficiency of operations 2) Reliability of financial reporting 3) Compliance with applicable laws and regulations	1) The COSO framework individually does not solve the issues arising from security in the cloud.

Source: Research Data (2019).

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.

3. Basics of the Framework for Cloud Security

As any company risk, the risk of data in the cloud cannot be eliminated (or minimized to an accepted level) and therefore requires a series of coordinated actions to be taken in order to manage it. Such actions involve the organisation 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 the developing country systems (state, enterprises and citizens) it is necessary to define a common ground, a Framework, in which the various production sectors, government agencies and regulated sectors can recognise 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.

The 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 well help an SME to plan a cloud risk management strategy, developed over the time according to their business, size and other distinguishing and specific elements of the SMEs.

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; and was developed according to the characteristics of the social and economic system of our country, reaching a cross-sector framework that can be contextualised 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.

Framework Building through Metrics

Security metrics are measurements from which to monitor and compare the level of security and privacy attained, as well as the current security status of a computing environment. The use of security metrics promotes transparency, decision making, predictability and proactive planning [15]. Metric is a measurement standard, defining both what is being measured (the attribute) and how it is measured (the unit of measure) [16].

Measurement is the process of metric collection which, through pre-established rules, will allow the interpretation of results [16]. Metrics can be composed of sub-elements that are referred to as primitive metrics or sub-metrics. Any restrictions or controls relating to the primitives are defined in the measurement process. A metric can be expressed in one of the following ways:

1) #—"Number"—expressing an absolute value of any element measured;

2) %—Percentage—expressing a percentage of an element measured in relation to the total number of elements;

3) Logic value—expressing Yes or No for an event.

Figure 1 represents the proposed life cycle of security management for cloud computing environments.

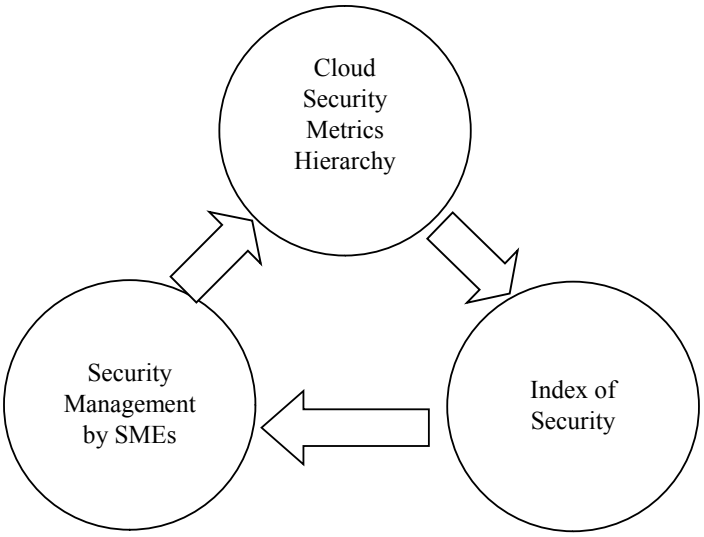

Figure 1. Life cycle of security management. Source: Author (2019).

The proposed methodology for security management in cloud computing is based on the following components:

1) Cloud security metrics hierarchy;

2) Index of Security (IndSec);

3) Security Management by SMEs.

In the 1970s, the GQM method (Goal Question Metric) [15] was designed to move testing for software defects from the qualitative and subjective state it was currently into an empirical model, in which defects would be measured against defined goals and objectives that could then be linked to results.

The GQM methodology defines a measurement model on three levels:

1) Conceptual level (goal)—a goal is defined for an object for a variety of reasons, with respect to various models of quality, from several points of view and relative to a particular environment.

2) Operational level (question)—a set of questions is used to define models of the object under study and then attention is focused on that object to characterize the assessment or achievement of a specific goal.

3) Quantitative level (metric)—a set of metrics, based on the models, is associated with every question in order to answer it in a measurable way.

The Cloud security metrics hierarchy is derived from the GQM methodology. A security index (IndSec) will be computed using the security metrics hierarchy. Finally, the SME will use the security index as a reference for improving their security. In the context of the life cycle of security management (**Figure 1**), a security metrics hierarchy is presented as a new form of visualisation of security-related information that is collected from the cloud computing environment [17].

In this research methodology, the security metrics hierarchy is generated directly from the GQM definition process, during which stage security features are mapped to corresponding security metrics. **Table 2** shows the relationship between the GQM methodology and the security metrics hierarchy (SMH).

Table 2. Relationship between the GQM methodology and SMH.

GQM Levels	SMH Levels
Conceptual level	Group Metric
Operational level	Metric
Quantitative level	Sub-Metric

Source: Security Metrics Hierarchy (2019).

For each goal statement identified in the conceptual level, a group metric was defined. The operational level identifies which objects or activities must be observed or collected to measure the individual components of the goal statement. Lastly, the quantitative level defines which metrics remains explicitly aligned with the higher-level goal statement.

The security metrics hierarchy is derived from the GQM methodology. The metrics are classified into Group metrics, Metrics and Sub-Metrics as shown in Figure 2.

The sub-metric represents a sub-part of a metric; it is used when a metric can be specialised in several ways, with each one having a different contribution to the overall metric. The importance of value conversion is to extract a meaning for the values measured by the primitive metrics. Further, value conversion helps to prevent the value domains of security metrics from having instances that are difficult to be compared with each other, and to simplify the computational model using a method to converge the values of each primitive metric measured to a common scale of values.

A metric of type logic must return a logical value measured from an event, for instance, does the cloud have a 2-factor authentication for authorising users? The conversion function is described as $y = f(x)$, where x can be a measured logic value Yes or No:

$$y = \begin{cases} 1 & \text{if } x = \text{Yes} \\ 0 & \text{if } x = \text{No} \end{cases}$$

Beginning with goals, the researcher defined the strategic objectives for cloud security based on the feedback from the SMEs. These goals naturally trigger questions that must be answered to determine whether the goal has been met. For instance, if the goal is ensuring that a cloud provider is protecting sensitive data as well as the consumer, certain questions emerge: How well does the consumer protect data today? How well does the provider protect internal data? What controls are in place in the SME? Many questions emerge, all representing the process by which the SME verifies performance against the goal. Questions in turn trigger demands for data and measurement.

4. Developed Framework

The framework developed by the researcher is as indicated in Figure 3. The author proposes an eight-stage cloud security framework divided into two sections.

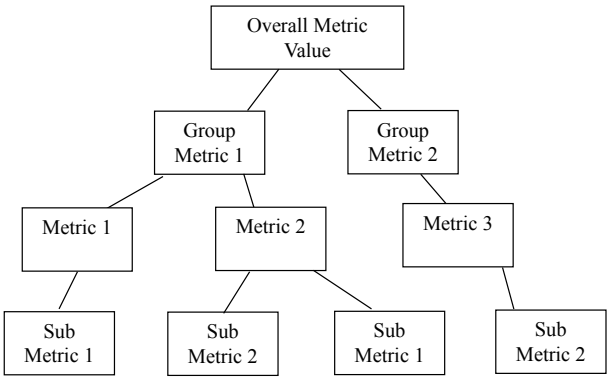

Figure 2. Metrics classification. Source: GQM Methodology (2019).

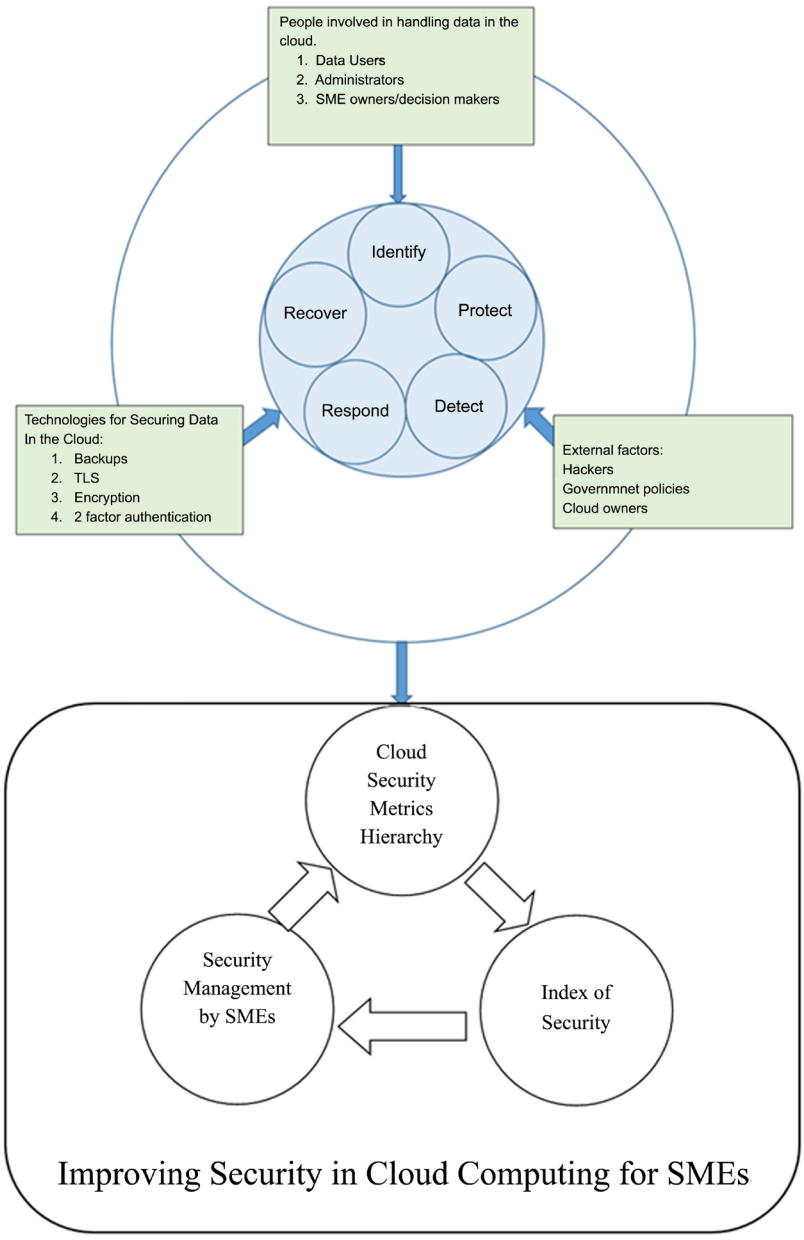

Figure 3. Framework for improving security in cloud computing. Source: Author (2019).

The first five stages are Identify, Protect, Detect, Respond and Recover. The second section includes Metric Hierarchy, Index of Security and finally Implementation of a Secure Cloud [18].

The developed framework has considered factors from results of the data collected, previous studies and frameworks that are in place. It was evident that SMEs need a cloud security framework with the ability to guide them on the three core factors that cause compromise on security (people, lack of technologies and external factors).

Several key references were employed to gather the information required for building these categories, including CSA's security guidance and top threats analysis, ENISA's security assessment and the cloud computing definitions from NIST.

4.1. Implementation of the Framework

The framework core represents the life cycle structure of the management process of cyber security, both from a technical and organisational 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 priority levels help to support organisations and companies in the preliminary identification of sub metrics to be implemented in order to further reduce their risk levels, while balancing the effort to implement them. The priority levels aid to:

1) Simplify the identification of essential sub metrics to be immediately implemented;

2) Support the organisations in their risk analysis and management process.

The identification of priority levels assigned to Subcategories has been performed according to two specific criteria:

1) Ability to reduce cyber risk, by working on one or more key factors for the identification, that is, exposure to threats, intended as the set of factors that increase or diminish the threat probability; Occurrence Probability, that is the frequency of the possible event of a threat over the time; impact on business operations and company assets, intended as the amount of damage resulting from the threat occurrence;

2) Ease of sub metric implementation, considering the technical and organisational maturity usually required to put in place specific countermeasures.

The framework suggests the use of a priority scale of three levels among sub metrics. The combination of these two criteria allows the definition of three different priority levels:

1) High Priority: Actions that enable the slight reduction of one of the three key factors of cyber risk. Such actions are prioritised and must be implemented

irrespective of their implementation complexity;

2) Medium Priority: Actions that enable the reduction of one of the three key factors of cloud security risk, that is generally easily implementable.

3) Low Priority: Actions that make possible to reduce one of the three key factors of the cloud security risk and that are generally considered as hard to be implemented (Require significant organisational and/or infrastructural changes).

Further, the framework core structure shows validation references that link the single sub metric to a number of known security practices by using internationally recognised security standards like ISO, SP800-53r4, COBIT-5, SANS20 and others [19] [20].

The classification of the sub-levels advises the SME on the rules and procedures that all individuals accessing and using the organisation's IT assets and resources must follow. The goal of the classifications is to provide details on which aspect of the security needs attention and also who is in charge of doing so.

Appendix 1 shows details of the framework, its levels, priority, validation reference, which group it applies to, the metric type and the metric classification. 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 indicator of how secure the SME's cloud data is.

4.2. Testing the Framework Functionality

The Security Index (IndSec) is defined as the highest value in a set of security items:

IndSec = max(Met_1, Met_2, Met_3, Met_4, Met_5)

Example 1, max(Met_1, Met_2, Met_3, Met_4, Met_5) = max(1, 1, 1, 1, 1) = 1.

Therefore, IndSec = 1, meaning the cloud environment is secure.

Example 2, max(Met_1, Met_2, Met_3, Met_4, Met_5) = max(1, 0, 1, 0, 0) = 0.

Therefore, IndSec = 0, meaning the cloud environment is not secure.

The use of the function max at each level of hierarchy causes the largest measured metric value to be passed on to the level. Immediately above, *i.e.* the highest measured value will be the only significant one.

The value of a metric group (Met_x) is defined as the highest value from a set of metrics:

Met_x = max($Met_{x.1}$, $Met_{x.2}$, ..., $Met_{x.n}$). For instance, Met_1 = max($Met_{1.1}$, $Met_{1.2}$, $Met_{1.3}$).

An example for a best-case scenario is as below:

Met_1 = max($Met_{1.1}$, $Met_{1.2}$, $Met_{1.3}$).

Met_1 = max(1, 1, 1).

Met_1 = 1

Met_2 = max($Met_{2.1}$, $Met_{2.2}$, $Met_{2.3}$, $Met_{2.4}$, $Met_{2.5}$).

Met_2 = max(1, 1, 1, 1, 1).

Met_2 = 1

$Met_3 = \max(Met_{3.1}, Met_{3.2}, Met_{3.3})$.

$Met_3 = \max(1, 1, 1)$.

$Met_3 = 1$

$Met_4 = \max(Met_{4.1}, Met_{4.2}, Met_{4.3}, Met_{4.4}, Met_{4.5})$.

$Met_4 = \max(1, 1, 1, 1, 1)$.

$Met_4 = 1$

$Met_5 = \max(Met_{5.1}, Met_{5.2}, Met_{5.3})$.

$Met_5 = \max(1, 1, 1)$.

$Met_5 = 1$

On the flip side, a non-secure scenario result is represented below:

$Met_1 = \max(Met_{1.1}, Met_{1.2}, Met_{1.3})$.

$Met_1 = \max(1, 0, 0)$.

$Met_1 = 0$

$Met_2 = \max(Met_{2.1}, Met_{2.2}, Met_{2.3}, Met_{2.4}, Met_{2.5})$.

$Met_2 = \max(1, 1, 0, 0, 0)$.

$Met_2 = 0$

$Met_3 = \max(Met_{3.1}, Met_{3.2}, Met_{3.3})$.

$Met_3 = \max(0, 0, 0)$.

$Met_3 = 0$

$Met_4 = \max(Met_{4.1}, Met_{4.2}, Met_{4.3}, Met_{4.4}, Met_{4.5})$.

$Met_4 = \max(0, 1, 0, 0, 0)$.

$Met_4 = 0$

$Met_5 = \max(Met_{5.1}, Met_{5.2}, Met_{5.3})$.

$Met_5 = \max(1, 0, 0)$.

$Met_5 = 0$

The value of a metric ($Met_{x.y}$) is defined as the highest value from a set of sub-metrics:

$Met_{x.y} = \max(Met_{x.y.1}, Met_{x.y.2}, ..., Met_{x.y.n})$. For instance, $Met_{1.1} = \max(Met_{1.1.1}, Met_{1.1.2}, Met_{1.1.3}, Met_{1.1.4}, Met_{1.1.5})$.

An example for a best-case scenario is as below:

$Met_{1.1} = \max(Met_{1.1.1}, Met_{1.1.2}, Met_{1.1.3}, Met_{1.1.4}, Met_{1.1.5})$.

$Met_{1.1} = \max(1, 1, 1, 1, 1)$.

$Met_{1.1} = 1$

$Met_{1.2} = \max(Met_{1.2.1}, Met_{1.2.2}, Met_{1.2.3}, Met_{1.2.4})$.

$Met_{1.2} = \max(1, 1, 1, 1)$.

$Met_{1.2} = 1$

$Met_{1.3} = \max(Met_{1.3.1}, Met_{1.3.2}, Met_{1.3.3}, Met_{1.3.4}, Met_{1.3.5})$.

$Met_{1.3} = \max(1, 1, 1, 1, 1)$.

$Met_{1.3} = 1$

On the flip side, a non-secure scenario result is represented below:

$Met_{1.1} = \max(Met_{1.1.1}, Met_{1.1.2}, Met_{1.1.3}, Met_{1.1.4}, Met_{1.1.5})$.

$Met_{1.1} = \max(1, 0, 0, 0, 1)$.

$Met_{1.1} = 0$

$Met_{1.2}$ = max($Met_{1.2.1}$, $Met_{1.2.2}$, $Met_{1.2.3}$, $Met_{1.2.4}$).

$Met_{1.2}$ = max(0, 0, 0, 1).

$Met_{1.2}$ = 0

$Met_{1.3}$ = max($Met_{1.3.1}$, $Met_{1.3.2}$, $Met_{1.3.3}$, $Met_{1.3.4}$, $Met_{1.3.5}$).

$Met_{1.3}$ = max(0, 0, 0, 0, 0).

$Met_{1.3}$ = 0

The sub-metric $Met_{x.y.n}$ either yields a 1 (based on a yes) or a 0 (based on a no). For example, $Met_{2.3.2}$—*Is the Data protected while in transit* (*upload/download from the cloud*)? *Yes.*

Then $Met_{2.3.2}$ = 1

$Met_{2.3.2}$—*Is the Data protected while in transit (upload/download from the cloud)? No.*

Then, $Met_{2.3.2}$ = 0

4.3. Using the Framework

The implementation of the Framework by an SME should be performed in five steps, as showed in Figure 4.

The steps are explained as follows:

1) Understand the Framework and the Metrics. The SME has to understand

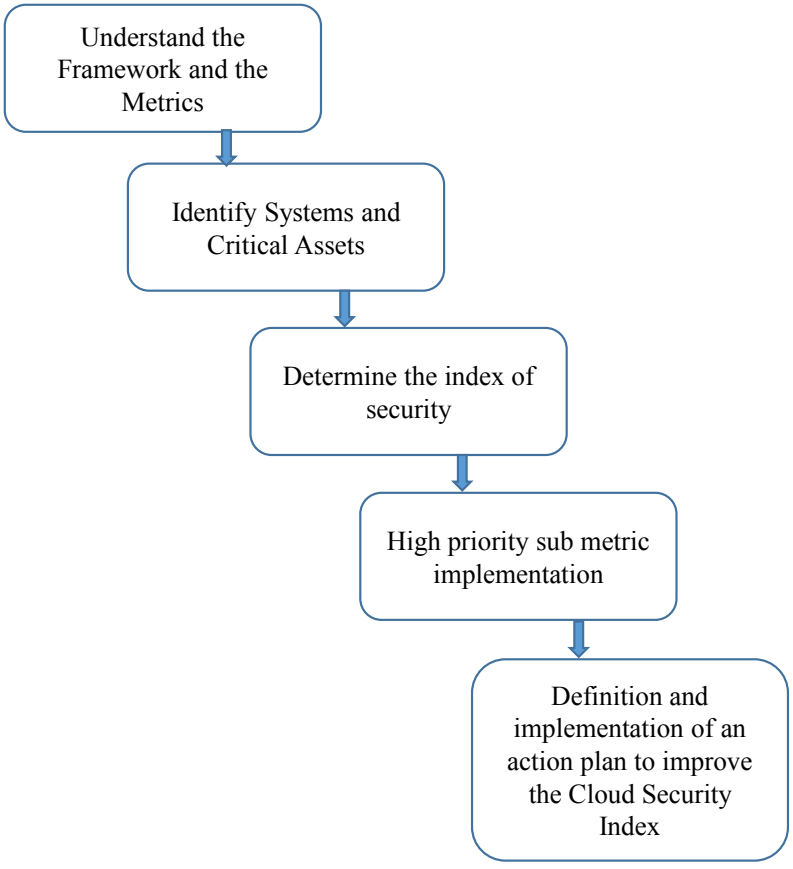

Figure 4. Using the framework for improving security in cloud computing. Source: Author (2019).

the framework and its sub-components for its business objectives and its security pertaining to the cloud. This activity can be performed also starting from a publicly available contextualisation and adjusting it to the specific business context of the SME. The questions representing the contextualisation are structured in a logical manner with a yes or no as an answer.

2) Identify Systems and Critical Assets. The identification of ICT systems and information is considered crucial or anyway critical by the SME to ensure its operations. This step is important especially for the following stages, as it makes it possible to properly evaluate the impacts during risk analysis and it makes it easier to understand the actual needed protection. It should be noted that within SMEs it is important to also identify the ones who are responsible for the implementation of the Framework steps for each sub metric.

3) Determine the Index of Security. Once the sub metric questions have been answered, the answers are subjected to the GQM metrics to be able to determine the index of security which can be either *secure* or *not secure*.

4) High Priority Sub-Metric Implementation. The SME should start to use the Framework by implementing the high priority sub metrics. This is a critical step in the Framework implementation and it makes it possible to reach a degree of preparedness and awareness of the cloud security risk. The target (turning all sub metrics into positive responses) represents the reference to compare the current profile, thus establishing the existing gaps within the cybersecurity management.

5) Definition and Implementation of an Action Plan to Improve the Cloud Security Index. The last step of the process of Framework endorsement consists of defining the set of activities needed to reach a secure security index. This means to establish a specific plan to implement the Framework security practices, according to a schedule, that varies upon the actual identified risks and specific conditions of the SME business.

Clearly it is preferable to have a continuous evolution of the Framework implementation, even after having reached the target profile, in line with the cyclic risk assessment staged and following actions of steady improvement.

5. Conclusions

Cloud computing offers many opportunities to SMEs, but risks and challenges as well [21]. 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 [22]. 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.

Standardised 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 as well as increase their trust in the cloud and the cloud provider. It is important to note that as stated by Becker and Bailey (2014), no one framework or model encompasses all of the possible IT controls, collectively they cover the—what, how, and scope of IT Governance.

The framework further gives a guiding strategy and procedure to SMEs who wish to develop a cloud security policy by telling them what to secure at which stage and how to do it. It further also gives IT technicians a better idea of how processes flow in the cloud, thereby allowing them to solve security related problems in an informed manner.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Adeyeye, A. (2016) Challenges to SME Growth in Kenya. In Africa Business Insight: Academic Conferences.

[2] Kenya Gazette Supplement No. 54 (Acts No. 11) (2017) Kenya Gazette Supplement.

[3] Bowen, M., Morara, M. and Mureithi, M. (2009) Management of Business Challenges among Small and Micro Enterprises in Nairobi-Kenya. *KCA Journal of Business Management*, **2**, 16-31. https://doi.org/10.4314/kjbm.v2i1.44408

[4] Velte, A.T., Velte, T.J., Elsenpeter, R.C. and Elsenpeter, R.C. (2010) Cloud Computing: A Practical Approach. McGraw-Hill, New York, 44.

[5] Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Stoica, I., *et al.* (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).

[6] Sultan, N.A. (2011) Reaching for the "Cloud": How SMEs Can Manage. *International Journal of Information Management*, **31**, 272-278. https://doi.org/10.1016/j.ijinfomgt.2010.08.001

[7] Daniel, W.K. (2014) Challenges on Privacy and Reliability in Cloud Computing Security. 2014 *International Conference on Information Science, Electronics and Electrical Engineering*, Vol. 2, 1181-1187. https://doi.org/10.1109/InfoSEEE.2014.6947857

[8] Seccombe, A., Hutton, A., Meisel, A., Windel, A., Mohammed, A. and Licciardi, A. (2009) Security Guidance for Critical Areas of Focus in Cloud Computing. *Cloud Security Alliance*, **2**, 2-70.

[9] Bhardwaj, S., Jain, L. and Jain, S. (2010) An Approach for Investigating Perspective of Cloud Software-as-a-Service (SaaS). *International Journal of Computer Applications*, **10**, 40-43. https://doi.org/10.5120/1450-1962

[10] Li, Y. and Liu, Z. (2011) The ICT Industrial Interaction between Mainland China and Taiwan: Empirical Analysis and Policy Implications. 2011 *IEEE* 2*nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce*, Dengfeng, 8-10 August 2011, 3478-3484.

[11] Palmer, S.A. (2015) U.S. Patent No. 9,172,918. U.S. Patent and Trademark Office,

Washington DC.

[12] Cashell, B., Jackson, W.D., Jickling, M. and Webel, B. (2004) The Economic Impact of Cyber-Attacks. Congressional Research Service Documents, CRS RL32331, Washington DC, 2.

[13] Reveron, D.S. (2012) Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press, Washington DC.

[14] Khajeh-Hosseini, A., Greenwood, D., Smith, J.W. and Sommerville, I. (2012) The Cloud Adoption Toolkit: Supporting Cloud Adoption Decisions in the Enterprise. *Software*: *Practice and Experience*, **42**, 447-465. https://doi.org/10.1002/spe.1072

[15] Hayden, L. (2010) IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education Group, New York.

[16] Herrmann, D.S. (2007) Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI. Auerbach Publications, New York. https://doi.org/10.1201/9781420013283

[17] Caldiera, V.R.B.G. and Rombach, H.D. (1994) The Goal Question Metric Approach. In: Marciniak, J.J., Ed., *Encyclopedia of Software Engineering*, 528-532.

[18] National Institute of Standards and Technology (2017). https://www.nist.gov

[19] Muthee, J.W. (2016) A Data Security Implementation Model for Cloud Computing in Government Parastatals. University of Nairobi, Nairobi.

[20] Padgett, D.K. (2016) Qualitative Methods in Social Work Research (Vol. 36). Sage Publications, Thousand Oaks.

[21] Rittinghouse, J.W. and Ransome, J.F. (2016) Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton. https://doi.org/10.1201/9781439806814

[22] Denning, D.E. (2003) Information Technology and Security.

Appendix 1: Framework Details

Level	DESCRIPTION	Priority	Validation References	Classification	Type	Metric
1	**IDENTIFY RISKS IN CLOUD**				Group Metric	Met_1
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.				Metric	$Met_{1.1}$
1.1.1	**ID.AM-1**: Are all physical IT equipment (computers, laptops, BYOD) within the SME inventoried?	**HIGH**	· COBIT 5 BAI09.01, BAI09.02 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4CM-8	SME Administrators need to comply	Sub Metric	$Met_{1.1.1}$
1.1.2	**ID.AM-2:** Are all system and application software within the SME inventoried?	**HIGH**	· COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4CM-8	SME Administrators need to comply	Sub Metric	$Met_{1.1.2}$
1.1.3	**ID.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?	**LOW**	· COBIT 5DSS05.02 · ISA 62443-2-1:20094.2.3.4 · ISO/IEC 27001:2013A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	Cloud providers need to provide information	Sub Metric	$Met_{1.1.3}$
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?	**HIGH**	· COBIT 5APO02.02 · ISO/IEC 27001:2013A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9	SME Administrators need to comply	Sub Metric	$Met_{1.1.4}$
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)?	**MEDIUM**	· ISO/IEC 27001:2013A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 · COBIT 5 APO03.03, · APO03.04, BAI09.02	Cloud providers need to provide information	Sub Metric	$Met_{1.1.5}$
1.2	**Governance (1.2):** The guidelines, policies and methods to manage and monitor the SME's regulatory, legal, risk, environmental, and operational requirements are understood and inform the SME owner(s) of cyber security risk.				Metric	$Met_{1.2}$
1.2.1	**ID.GV-1:** Has the cloud provider established and communicated a well-informed security policy in relation to the data stored on the cloud?	MEDIUM	· COBIT 5 APO01.03, EDM01.01, EDM01.02 · ISA 62443-2-1:2009 4.3.2.6 · ISO/IEC 27001:2013 A.5.1.1 · NIST SP 800-53 Rev. 4 -1 controls	Cloud providers need to provide information	Sub Metric	$Met_{1.2.1}$
1.2.2	**ID.GV-2:** Are the staff trained regularly on Information security roles & responsibilities including third party providers?	MEDIUM	· COBIT 5 APO13.12 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 · NIST SP 800-53 Rev. 4 PM-1, PS-7	SME Owner/Admin/Users need to be regularly trained	Sub Metric	$Met_{1.2.2}$
1.2.3	**ID.GV-3:** Are legal and regulatory requirements regarding cloud security understood and managed by the SME and explained well by the cloud provider?	HIGH	· COBIT 5 MEA03.01, MEA03.04 · ISO/IEC 27001:2013 A.18.1 · ISA 62443-2-1:2009 4.4.3.7	SME Owner/Admin/ Users	Sub Metric	$Met_{1.2.3}$

Continued

1.2.4	**ID.GV-4:** Does the cloud provider update the SME on any change pertaining to risk management processes?	LOW	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, · 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 PM-9, PM-11	Cloud Provider need to confirm	Sub Metric	$Met_{1.2.4}$
1.3	**Risk Assessment (1.3):** The SME understands the cyber security risk to their operations including their operations, image and reputation, assets, and staff.				Metric	$Met_{1.3}$
1.3.1	**ID.RA-1:** Does the SME update and patch their operating systems and carry out vulnerability scans on their systems regularly?	MEDIUM	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	SME Administrators need to comply	Sub Metric	$Met_{1.3.1}$
1.3.2	**ID.RA-3:** Does the SME perform a continuous risk assessment process to identify, evaluate and mitigate risks across their company?	LOW	· COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	SME Administrators need to comply	Sub Metric	$Met_{1.3.2}$
1.3.3	**ID.RA-4:** Does the SME identify potential business impacts and likelihoods related to the cloud?	LOW	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	SME Owner/Admin/Users need to get trained	Sub Metric	$Met_{1.3.3}$
1.3.4	**ID.RA-5**: Threats, vulnerabilities, likelihoods, and impacts in cloud computing are understood well by the SME?	LOW	· COBIT 5 APO12.02 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	SME Owner/Admin/Users need to get trained	Sub Metric	$Met_{1.3.4}$
1.3.5	**ID.RA-6:** Are cloud Risk responses identified and prioritised?	LOW	· COBIT 5 APO12.05, APO13.02 · NIST SP 800-53 Rev. 4 PM-4, PM-9	SME Owner/Admin/Users need to get trained	Sub Metric	$Met_{1.3.5}$
2	**PROTECT DATA IN THE CLOUD**				Group Metric	Met_{1}
2.1	**Access Control (2.1):** Access to IT and related equipment, facilities and systems is limited to only authorised personnel and devices and to carry out only authorised actions and transactions.				Metric	$Met_{2.1}$
2.1.1	**PR.AC-1:** Does the SMEs user credentials for the cloud issued, managed, verified, revoked, and audited for authorised devices, users and processes only?	HIGH	· COBIT 5 DSS05.04, DSS06.03 · ISA 62443-2-1:2009 4.3.3.5.1 · NIST SP 800-53 Rev. 4 AC-2, IA Family	SME Administrator/ Implement authentication technologies	Sub Metric	$Met_{2.1.1}$
2.1.2	**PR.AC-2:** Are physical assets protected and access to assets in the SMEs premises managed?		· COBIT 5 DSS01.04, DSS05.05 · ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8	SME Owners/Users. Implement physical controls.	Sub Metric	$Met_{2.1.2}$

Continued

		MEDIUM	· ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3			
2.1.3	**PR.AC-3:** Are SMEs establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed to their systems in accordance with their access control policy?	**HIGH**	· COBIT 5 APO13.01, DSS01.04, DSS05.03 · ISA 62443-2-1:2009 4.3.3.6.6 · ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1	SME Administrator/ Logging all activities.	Sub Metric	$Met_{2.1.3}$
2.1.4	**PR.AC-4:** Is access to systems by users |managed in terms of permissions, implementing the use of least privilege?		· CCS CSC 12, 15 · ISA 62443-2-1:2009 4.3.3.7.3 · SA I62443-3-3:2013 SR 2.1 · NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	SME Administrator to avoid giving access to unauthorised users.	Sub Metric	$Met_{2.1.4}$
		HIGH				
2.1.5	**PR.AC-5:** Is the SMEsLAN and WAN well protected, including network segregation if applicable?	**MEDIUM**	· ISA 62443-2-1:2009 4.3.3.4 · ISA 62443-3-3:2013 SR 3.1, SR 3.8 · ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1	SME Administrator t ensure network is secure	Sub Metric	$Met_{2.1.5}$
2.1.6	**PR.AC-7:** Does the cloud provider use appropriate technology like single-factor, multi-factor to ensure that SME users, devices, and other assets are authenticated?	**MEDIUM**	· COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03 · ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4	Cloud Provider	Sub Metric	$Met_{2.1.6}$
2.2	**Awareness and Training (2.2):** The SME's users and staff are provided regular security awareness trainings and are sufficiently trained to perform their work whilst ensuring that security is paramount and tasks are performed as outlined in the policies, procedures, and agreements.				Metric	$Met_{2.2}$
2.2.1	**PR.AT-1:** All users are informed and trained on the security aspects pertaining to their cloud usage?	HIGH	· ISO/IEC 27001:2013 A.7.2.2 · NIST SP 800-53 Rev. 4 AT-2, PM-13 · COBIT 5 APO07.03, BAI05.07 · ISA 62443-2-1:2009 4.3.2.4.2	SME Users/Admin/ Owners be trained well	Sub Metric	$Met_{2.2.1}$
2.2.2	**PR.AT-2:** Do the SME's Privileged users like admins and super users understand their privileges & responsibilities pertaining to the cloud?	HIGH	· CCS CSC 9 · COBIT 5 APO07.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/Admin/ Owners be trained well	Sub Metric	$Met_{2.2.2}$
2.2.4	**PR.AT-4:** Do the SME's owners and senior personnel understand their privileges & responsibilities pertaining to the cloud?	HIGH	· COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/ Admin/ Owners be trained well	Sub Metric	$Met_{2.2.4}$
2.2.5	**PR.AT-5:** Do information security personnel understand their privileges & responsibilities pertaining to the cloud?	MEDIUM	· CCS CSC 9 · COBIT 5 APO07.03 · ISA 62443-2-1:2009 4.3.2.4.2 · ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, · NIST SP 800-53 Rev. 4 AT-3, PM-13	SME Users/Admin	Sub Metric	$Met_{2.2.5}$

Continued

2.3	**Data Security (2.3):** Information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information.				Metric	$Met_{2.3}$
2.3.1	**PR.DS-1:** Is the Data protected while at rest in the cloud?	HIGH	· CCS CSC 17 · COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 · ISA 62443-3-3:2013 SR 3.4, SR 4.1 · ISO/IEC 27001:2013 A.8.2.3 · NIST SP 800-53 Rev. 4 SC-28	Cloud Provider/Use of Encryption	Sub Metric	$Met_{2.3.1}$
2.3.2	**PR.DS-2:** Is the Data protected while in transit (upload/download from the cloud)?	HIGH	· ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 · CCS CSC 17 · ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	Cloud Provider/Use of TLS	Sub Metric	$Met_{2.3.2}$
2.3.4	**PR.DS-4:** Does the SME have Adequate bandwidth capacity to ensure availability is maintained for data in the cloud?	HIGH	· COBIT 5 APO13.01 · ISA 62443-3-3:2013 SR 7.1, SR 7.2 · ISO/IEC 27001:2013 A.12.3.1	Administrators/Use of secondary link	Sub Metric	$Met_{2.3.4}$
2.3.5	**PR.DS-5:** Does the cloud provider have approved firewall rule sets and access control lists between network fabrics to restrict the flow of information to specific information system services and counter for multi-tenancy?	MEDIUM	· ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	Cloud Provider	Sub Metric	$Met_{2.3.5}$
2.3.6	**PR.DS-6:** Does the SME or cloud provider employ integrity verification tools to monitor and detect unauthorised changes to organisation's software and information?	LOW	· ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8 · ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3 · NIST SP 800-53 Rev. 4 SI-7	Cloud Provider, use of monitoring tools	Sub Metric	$Met_{2.3.6}$
2.4	**Information Protection Processes and Procedures (2.4):** Security policies addressing roles, responsibilities, and scope, processes, and procedures are maintained and used to manage protection of information systems and assets.				Metric	$Met_{2.4}$
2.4.1	**PR.IP-1:** Does the SME create and maintain configuration of IT control systems for the cloud as well as internal systems?	HIGH	· COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 · ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · CCS CSC 3, 10	Cloud Provider	Sub Metric	$Met_{2.4.1}$
2.4.2	**PR.IP-2:** Does the SME have a System Development Life Cycle to manage cloud and internal systems implemented?	MEDIUM	· COBIT 5 APO13.01 · ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	SME users	Sub Metric	$Met_{2.4.2}$

Continued

2.4.3	**PR.IP-3:** Does the SME have change control processes in place to track changes in the cloud provider's functionality?	MEDIUM	· COBIT 5 BAI06.01, BAI01.06 · ISA 62443-3-3:2013 SR 7.6 · ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · NIST SP 800-53 Rev. 4 CM-3, CM-4	Cloud Provider to communicate	Sub Metric	$Met_{2.4.3}$
2.4.4	**PR.IP-4:** Does the cloud provider regularly create, test and validate backups of data stored in the cloud?	HIGH	· COBIT 5 APO13.01 · ISA 62443-2-1:2009 4.3.4.3.9 · ISA 62443-3-3:2013 SR 7.3, SR 7.4 · ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 · NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	Cloud Provider/Use of offshore backup	Sub Metric	$Met_{2.4.4}$
2.4.6	**PR.IP-6:** Is data in the cloud destroyed according to policy and no copies retained without the SMEs knowledge?	HIGH	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.4.4.4 · NIST SP 800-53 Rev. 4 MP-6	Cloud Provider to ensure	Sub Metric	$Met_{2.4.6}$
2.4.8	**PR.IP-8:** Does the cloud provider share effectiveness of protection technologies with the SME?	LOW	· ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4	Cloud Provider	Sub Metric	$Met_{2.4.8}$
2.4.9	**PR.IP-9:** Are Incident Response, Business Continuity and disaster/incident recovery plans) in place and managed well by the cloud provider?	MEDIUM	· COBIT 5 DSS04.03 · ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 · NIST SP 800-53 Rev. 4 CP-2, IR-8	SME Owners	Sub Metric	$Met_{2.4.9}$
2.4.10	**PR.IP-10:** Are the above-mentioned BC and DR plans tested and validated periodically?	LOW	· ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 · ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.17.1.3 · NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	SME Owners/Admin/Cloud Provider	Sub Metric	$Met_{2.4.10}$
2.4.12	**PR.IP-12:** Does the SME have a vulnerability management plan in place?	MEDIUM	· ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 · NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	SME Owners/ Admin/Cloud Provider	Sub Metric	$Met_{2.4.12}$
2.4.13	**PR.MA-1:** Does the SME maintain and repair their IT assets in a timely manner and are these repair and maintenance activities approved and logged?	LOW	· COBIT 5 BAI09.03 · ISA 62443-2-1:2009 4.3.3.3.7 · ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 · NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	Admins	Sub Metric	$Met_{2.4.13}$
2.4.14	**PR.MA-2:** Is Remote maintenance of the SME's IT assets is approved, logged, and performed in a manner that prevents unauthorised access?	HIGH	· COBIT 5 DSS05.04 · ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 · NIST SP 800-53 Rev. 4 MA-4	Admins	Sub Metric	$Met_{2.4.14}$
2.5	**Protective Technology (2.5):** Technical security solutions are managed in a manner that ensures the security and resilience of all IT assets, equipment and systems. Also ensures that the management confers with appropriate policies, procedures, and agreements.				Metric	$Met_{2.5}$

Continued

2.5.1	**PR.PT-1:** Are all records pertaining to audits and logs of cloud usage documented and reviewed in accordance with the SME's internal policy?	MEDIUM	· CCS CSC 14 · COBIT 5 APO11.04 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · NIST SP 800-53 Rev. 4 AU Family	Admins to administer logging software or tools	Sub Metric	$Met_{2.5.1}$
2.5.2	**PR.PT-2:** Are any removable media used in the SME's premises protected and its use restricted according to the SME's policy?	MEDIUM	· COBIT 5 DSS05.02, APO13.01 · ISA 62443-3-3:2013 SR 2.3 · ISO/IEC 27001:2013 A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7	Administrator to enforce rules	Sub Metric	$Met_{2.5.2}$
2.5.3	**PR.PT-3:** Is Access to equipment, systems and IT assets controlled in a manner that enforces the least functionality principle?	MEDIUM	· COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, · ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, · ISO/IEC 27001:2013 A.9.1.2 · NIST SP 800-53 Rev. 4 AC-3, CM-7	Administrator to enforce rules	Sub Metric	$Met_{2.5.3}$
3	**DETECT SECURITY INCIDENTS IN THE CLOUD**				Group Metric	Met_3
3.1	**Anomalies and Events (3.1):** Unusual or irregular activity is detected in a timely manner and the potential impact of events is understood.				Metric	$Met_{3.1}$
3.1.1	**DE.AE-1:** Does the SME manage network operations and data flow for users through the cloud?	LOW	· COBIT 5 DSS03.01 · ISA 62443-2-1:2009 4.4.3.3 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	Administrator	Sub Metric	$Met_{3.1.1}$
3.1.2	**DE.AE-2:** Does the SME have measures to detect events and analyse attacks and methods?	LOW	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR · 2.12, SR 3.9, SR 6.1, SR 6.2 · ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4	Administrator. Use of IPD/IDS	Sub Metric	$Met_{3.1.2}$
3.1.4	**DE.AE-4:** Does the cloud provider give means of determining the impact of events in the cloud?	MEDIUM	· COBIT 5 APO12.06 · NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI -4	Cloud Provider	Sub Metric	$Met_{3.1.4}$
3.1.5	**DE.AE-5:** Are incident alert thresholds established by the cloud provider for their cloud services?	MEDIUM	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.2.3.10 · NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	Cloud Provider	Sub Metric	$Met_{3.1.5}$
3.2	**Security Continuous Monitoring (3.2):** The IT systems and assets are monitored at appropriate intervals to identify any security events and to verify the effectiveness of security controls.				Metric	$Met_{3.2}$
3.2.1	**DE.CM-1:** Is the LAN and WAN monitored to detect potential cloud security events?	MEDIUM	· CCS CSC 14, 16 · COBIT 5 DSS05.07 · NIST SP 800-53 Rev. 4 AC-2, AU-12,	Administrator. Use network monitoring tools.	Sub Metric	$Met_{3.2.1}$

Continued

3.2.2	**DE.CM-2:** Is the physical IT equipment monitored to detect potential cloud security?	LOW	· ISA 62443-2-1:2009 4.3.3.3.8 · NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20	Cloud Provider/ Administrator/ Logging	Sub Metric	$Met_{3.2.2}$
3.2.3	**DE.CM-3:** Personnel activity is monitored to detect any breaches and non-repudiation activities?	LOW	· ISA 62443-3-3:2013 SR 6.2 · NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	Administrator/ Logging	Sub Metric	$Met_{3.2.3}$
3.2.7	**DE.CM-7:** Is the cloud environment monitored for unauthorised users or connections?	MEDIUM	· NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	Administrator/ Logging	Sub Metric	$Met_{3.2.7}$
3.2.8	**DE.CM-8:** Are vulnerability scans regularly performed on the cloud environment?	MEDIUM	· COBIT 5 BAI03.10 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 · ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 RA-5	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.2.8}$
3.3	**Detection Processes (3.3):** Threat detection methods and procedures are maintained and tested to ensure timely and adequate awareness of unusual or irregular events.				Metric	$Met_{3.3}$
3.3.1	**DE.DP-1:** Does the SME and cloud provider define the roles and responsibilities for all the users to enable accountability for their actions?	**LOW**	· CCS CSC 5 · COBIT 5 DSS05.01 · ISA 62443-2-1:2009 4.4.3.1 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.3.1}$
3.3.2	**DE.DP-2:** Do the threat detection measures conform to all relevant requirements?	**MEDIUM**	· ISA 62443-2-1:2009 4.4.3.2 · ISO/IEC 27001:2013 A.18.1.4 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.3.2}$
3.3.3	**DE.DP-3:** Are the above-mentioned measures tested?	**LOW**	· ISA 62443-3-3:2013 SR 3.3 · ISO/IEC 27001:2013 A.14.2.8 · NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.3.3}$
3.3.4	**DE.DP-4:** Are the above-mentioned measures communicated to the SME personnel?	**MEDIUM**	· COBIT 5 APO12.06 · ISA 62443-2-1:2009 4.3.4.5.9 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.3.4}$
3.3.5	**DE.DP-5:** Are the above-mentioned measures and processes continuously improved?	**LOW**	· COBIT 5 APO11.06, DSS04.05 · ISA 62443-2-1:2009 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	Cloud Provider/ Administrator/	Sub Metric	$Met_{3.3.5}$
4	**RESPOND TO SECURITY EVENTS IN THE CLOUD**				Group Metric	Met_{4}
4.1	**Response Planning (4.1):** Response procedures and measures are executed and maintained, to ensure timely response to detected cloud security incidents.				Metric	$Met_{4.1}$

Continued

4.1.1	**RS.RP-1:** Is a valid response plan executed in case of an event?	**LOW**	· COBIT 5 BAI01.10 · CCS CSC 18 · ISA 62443-2-1:2009 4.3.4.5.1 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8	Cloud Provider/ Administrator/	Sub Metric	$Met_{4.1.1}$
4.2	**Communications (4.2):** Response activities are coordinated with the SME, to include external support from law enforcement agencies if applicable.				Metric	$Met_{4.2}$
4.2.1	**RS.CO-1:** Do all the staff of the SME know their roles and directive of procedures when a response is required?	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 · NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	Cloud Provider	Sub Metric	$Met_{4.2.1}$
4.2.2	**RS.CO-2:** Are all events reported in accordance with the established criteria?	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.5 · ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 · NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	Cloud Provider/ Administrator	Sub Metric	$Met_{4.2.2}$
4.2.3	**RS.CO-3:** Is information shared between the SME and the cloud provider in accordance with response plans?	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.2 · ISO/IEC 27001:2013 A.16.1.2 · NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	Cloud Provider/ Administrator	Sub Metric	$Met_{4.2.3}$
4.2.4	**RS.CO-4:** Coordination between the SME and the cloud provider occurs in accordance to the response plans?	**LOW**	· ISA 62443-2-1:2009 4.3.4.5.5 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider/ Administrator	Sub Metric	$Met_{4.2.4}$
4.3	**Analysis (4.3):** Proper analysis is done to confirm sufficient response and recovery |undertakings.				Metric	$Met_{4.3}$
4.3.1	**RS.AN-1:** Are notifications from detection systems investigated appropriately by the cloud providers and administrators?	LOW	· COBIT 5 DSS02.07 · ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISA 62443-3-3:2013 SR 6.1 · ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5 · NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4	Cloud Provider/ Administrator/ Logging	Sub Metric	$Met_{4.3.1}$
4.3.2	**RS.AN-2:** Is the impact of any potential incident understood by the SME?	MEDIUM	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4	Users/ Administrator/SME Owners	Sub Metric	$Met_{4.3.2}$
4.3.3	**RS.AN-3:** Are forensics for any potential security incident performed?	LOW	· ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR · 2.12, SR 3.9, SR 6.1 · ISO/IEC 27001:2013 A.16.1.7 · NIST SP 800-53 Rev. 4 AU-7, IR-4	Cloud Provider	Sub Metric	$Met_{4.3.3}$
4.3.4	**RS.AN-4:** Are incidents categorised based on the response plans?	LOW	· ISA 62443-2-1:2009 4.3.4.5.6 · ISO/IEC 27001:2013 A.16.1.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8	Cloud Provider	Sub Metric	$Met_{4.3.4}$

Continued

4.4	**Mitigation (4.4):** Strategic activities are performed to prevent further escalation of a security incident, and measures to mitigate and eliminate the threat.				Metric	$Met_{4.4}$
4.4.1	**RS.MI-1:** Incidents in the cloud are contained when they occur as per previous reports?	HIGH	· ISA 62443-2-1:2009 4.3.4.5.6 · ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4	Cloud Provider	Sub Metric	$Met_{4.4.1}$
4.4.2	**RS.MI-2: I**ncidents in the cloud are mitigated when they occur as per previous reports?	HIGH	· ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 · ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 · NIST SP 800-53 Rev. 4 IR-4	Cloud Provider	Sub Metric	$Met_{4.4.2}$
4.4.3	**RS.MI-3:** Are any new vulnerabilities mitigated or documented as accepted risks?	HIGH	· ISO/IEC 27001:2013 A.12.6.1 · NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	Cloud Provider	Sub Metric	$Met_{4.4.3}$
4.5	**Improvements (4.5):** SME's response activities are improved by incorporating lessons learned from current and previous detection/response activities.				Metric	$Met_{4.5}$
4.5.1	**RS.IM-1:** Are response plans updates to include lessons learned?	LOW	· COBIT 5 BAI01.13 · ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4 · ISO/IEC 27001:2013 A.16.1.6 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider/ Admin	Sub Metric	$Met_{4.5.1}$
4.5.2	**RS.IM-2:** Are response strategies updated accordingly?	LOW	· NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider/ Admin	Sub Metric	$Met_{4.5.2}$
5	**RECOVER FROM BREACHES IN THE CLOUD**				Group Metric	Met_{5}
5.1	**Recovery Planning (5.1):** Recovery procedures and techniques are performed and continued to make sure apt restoration of IT systems or assets that may be affected by the security events.				Metric	$Met_{5.1}$
5.1.1	**RC.RP-1:** Is the recovery plan effected in case of an event?	MEDIUM	· CCS CSC 8 · COBIT 5 DSS02.05, DSS03.04 · ISO/IEC 27001:2013 A.16.1.5 · NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	Cloud Provider	Sub Metric	$Met_{5.1.1}$
5.2	**Improvements (5.2):** Recovery planning and techniques are continuously upgraded by including lessons learned.				Metric	$Met_{5.2}$
5.2.1	**RC.IM-1:** Do all recovery documents include lessons learned?	LOW	· COBIT 5 BAI05.07 · ISA 62443-2-1 4.4.3.4 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider/ Admin	Sub Metric	$Met_{5.2.1}$
5.2.2	**RC.IM-2:** Are all the recovery strategies updated?	LOW	· COBIT 5 BAI07.08 · NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	Cloud Provider/ Admin	Sub Metric	$Met_{5.2.2}$
5.3	**Communications (5.3):** Restoration activities are coordinated with the SMEs				Metric	$Met_{5.3}$
5.3.3	**RC.CO-3:** Restoration accomplishments are communicated to SME teams.	MEDIUM	· NIST SP 800-53 Rev. 4 CP-2, IR-4	Cloud Provider	Sub Metric	$Met_{5.3.3}$