

**Strategy for Developing Effective Cyber Security on Cloud for
SMEs**



Supervisor
Dr. Anna Shillabeer

Submitted to the School of Computer Science, Engineering, and Mathematics
in the Faculty of Science and Engineering in partial fulfilment of the
requirements for the Master's degree program of Computer Science at
Flinders University South Australia, Australia

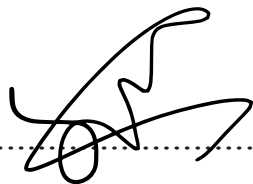
By Rayan Omar Abuhasha
Abuh0009
2132653

2017

Academic Integrity Declaration

I certify that this work does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university and that, to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where due reference is made in the text.

Signature.....

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke.

Date.....

7/3/2017

ACKNOWLEDGEMENTS

Foremost, I would like to express my sincere gratitude to my thesis supervisor Dr. Anna Shillabeer for her guidance, background knowledge, patience and editing skills in the completion of this thesis. Besides my advisor, I would like to thank Ms. Romana Challans for her advice and the information she has provided. A special appreciation and gratitude goes out to my twin for her support and encouragement during my study. Last but not least, I must express my very profound gratitude to my mother, aunts, brothers, sisters, my friends for their support, inspiration and patience during my years of study. This accomplishment would not have been possible without them. Thank you.

ABSTRACT

Cloud computing is a relatively new paradigm that presents significant business benefits and enormous opportunities for small and micro enterprises. As the information technology (IT) landscape evolves, SMEs need to find effective strategies for meeting business demands. However, many SMEs are reluctant to adopt cloud computing technology due to the inherent security, privacy, and trust issues, as well as regulatory risks and compliance implications. Preliminary studies show increasing numbers of cybersecurity attacks targeting SMEs in cloud environments (Symantec, 2016; U.S. State of Cybercrime Survey, 2013; Verizon.com, 2016). To address the security threats, there is need to establish best practices, standards, and guidelines that SMEs can follow. The aim of this study is to develop effective cloud security strategies for SMEs. The study addresses two research objectives: (i) to identify the security threats and challenges facing SMEs in cloud environments and determine the best mitigation strategies and, (ii) to develop a security strategy framework for SMEs in the context of cloud computing. The study followed the design research paradigm incorporating an extensive literature review which informed the development of the proposed model for SME security in the cloud. The overarching contribution of this study is the proposed model, which integrates four strategic components: Cloud Model, Security Model, Compliance Model, and Security Major Component. Although there is no single path for business success with cloud computing, the proposed model can serve as a guide for best practices and strategies for SMEs when deploying cloud-based solutions. It is recommended that SMEs use the conceptual model as a guide for migrating to the hyper-cloud solution.

Table of contents

ABSTRACT	4
CHAPTER 1: INTRODUCTION	8
1.1 Background	8
1.2 Significance of the Study	9
1.3 Research Questions	9
1.4 Objectives of the Study	10
CHAPTER 2: LITERATURE REVIEW	11
2.1 Cybersecurity Issues	11
2.1.1 Cybersecurity and the Nature of Cyberspace	11
2.1.2 Cybersecurity Risks and Threats Facing Businesses	11
2.1.3 Security Models	12
2.1.4 Emerging Trends in Cybersecurity	13
2.1.5 Current Cybersecurity Practices, Measures, and Standards	14
2.2 Security Issues in the Context of SMEs	15
2.2.1 Definition of SME	15
2.2.2 IT Security Threats Facing SMEs	16
2.3 Security Issues in the Context of Cloud Computing	21
2.3.1 Overview of Cloud Computing	21
2.3.2 Cloud Security Issues and Challenges	22
2.3.3 Cloud Computing Security Threats and Mitigation Techniques	22
2.3.4 Summary	24
2.4 Studies that Explicitly Address Security in SMEs that use Cloud Computing	24
2.4.1 Cloud Adoption Strategies used by SMEs and Security Implications	24
2.4.2 Security Opportunities for SME's Adopting Cloud Computing	25
2.5 Security Risk Management Strategies for SMEs in Cloud Computing	29
2.5.1 Cloud Computing Risks Affecting SMEs	29
2.5.2 SME's Approaches to Cloud Security Risk Management	30
CHAPTER 3: PROPOSED FRAMEWORK	33
3.1 Introduction	33
3.2 Methodology	33
3.3 Proposed Model	34
3.4 Discussion of the Proposed Framework	35
CHAPTER 4: FINDINGS AND DISCUSSION	38
4.1 Objective 1: SME Cloud Security Threats and Risks	38
4.2 Objective 2: Mitigation Measures for Security Threats	39
4.3 Objective 3: Developing Conceptual Cloud Security Model for SMEs	40
CHAPTER 5: CONCLUSION AND CONTRIBUTIONS	42
5.1 Conclusion	42
5.2 Contributions	42
5.2.1 Theoretical Contributions	42
5.2.2 Practical Contributions	43
5.3 Study Limitations and Directions for Future Research	43
APPENDICES	53
Appendix 1: SME Cloud Security Risk Matrix Template	53
Appendix 2: Control Domain Matrix Template	54

List of Figures

FIGURE 1. RISK MANAGEMENT MATRIX (FEN ET AL., 2012)..... 31
FIGURE 2. THE SABSA MODEL FOR SECURITY ARCHITECTURE (SHERHOOD ET AL., 2009)..... 34
FIGURE 3. THE PROPOSED SECURITY MODEL FOR SME CLOUD COMPUTING 35

List of Tables

TABLE 1. COMMON SECURITY METHODS USED BY ORGANIZATIONS (STEFFANI, 20016)14
TABLE 2. TOP SECURITY THREATS TO SME DATA, TARGET INFORMATION ASSETS, AND PREVENTION ACTIONS.....20
TABLE 3. CLOUD SECURITY ISSUES AND THEMES.....24

CHAPTER 1: INTRODUCTION

1.1 Background

With globalization and increased competition in the business context, organizations need to leverage their core competencies and continue to evolve to withstand growing competitive pressure. Factors such as budget constraints and cost saving measures are forcing enterprises to look for alternative solutions to meet business requirements and goals. For Small and Micro Enterprises (SMEs), achieving business success remains a challenge (Hashemi & Hesarlo, 2014). In order for SMEs to satisfy customer needs and deliver better services, they need to deploy IT services. However, traditional IT computing technology has typically proven costly for many SMEs as they lack the resources and the capability to integrate and manage these technologies even though, the relationship between SMEs and IT innovation is typically a mutual one. SMEs form an integral element of a country's economy as they serve as sources of employment and drivers of technological development. Advances in technology and the development of new technological solutions support this function and provide enormous business opportunities and benefits for SMEs (Wang *et al.*, 2011). The general understanding is that advances in IT provide important benefits and opportunities for SMEs to achieve competitiveness based on faster customer responsiveness, efficiency gains in business processes, and cheap, broad scale marketing.

One of the relatively new information technologies that has brought additional opportunities for enterprises, is cloud computing. According to the United States National Institute of Standards and Technology, cloud computing is a computing paradigm that involves ubiquitous and on-demand access to shared resources (Mell & Grance). This definition espouses five key features of cloud computing: broadband network access, resource sharing, on-demand access, service elasticity, and measured service. According to Mell and Grance (2011), the building blocks of cloud computing are software and hardware architectures that enable infrastructure scaling and virtualization and a cloud provider that delivers services. This simplified overview masks the complexities of this underlying technology infrastructure from the end users perspective. With cloud computing, SMEs do not need to maintain software and servers on their enterprise premises or even employ technical personnel to maintain the IT infrastructure (Mohabbattalab, Heidt, and Mohabbattalab, 2014). The attractiveness of cloud computing lies in its ability to provide SMEs with an opportunity to reduce costs, increase productivity, and improve business responsiveness (Javaid, 2014).

While cloud computing provides significant business benefits and opportunities, it also presents security, privacy, and trust challenges, particularly for SMEs (Hashemi & Hesarlo, 2014). Preliminary studies show increasing number and size of cyber-attacks targeting SMEs (Symantec, 2016; U.S. State of Cybercrime Survey, 2013; Verizon.com, 2016). The

security threats and attacks are diverse in terms of motivation and technological exploits ranging from insider attacks motivated by malice, to accidental misconfiguration of enterprise networks, lack of contingency planning, to automated exploit of known security vulnerabilities. The problem is that addressing the privacy, trust, and security challenges in cloud environments remains a challenge because it requires a combination of organizational, technological, and legal approaches that often lie beyond the control of an enterprise.

The focus of this paper is to examine effective security strategies for SMEs in the cloud. Currently, the available research focuses on security strategies for large organizations. Even the traditional approaches of security risk assessments tend to focus on methods that do not suit the unique profile of SMEs in terms of resource availability and technical capability. This indicates the need for extensive investigation to explore the best strategies for SMEs to deploy cloud services.

1.2 Significance of the Study

The main aim of this study is to contribute to the research discourse on cloud computing, by examining the security threats to SMEs, the mitigation measures, and the best strategies for effective security in cloud environments. Part of the rationale for dedicating this effort is the paucity of information about the specific security threats and risks that SMEs face in cloud environments and the strategies to use. Moreover, this area of study has not reached the level of clarity of more mature areas of business computing but the demand for information and potential for wide scale benefit cannot be overstated.

1.3 Research Questions

The primary research question is what strategies can SMEs use to ensure security in cloud computing? This overarching research question is divided into three specific research questions:

i. **Research Question 1:**

What is the effect of cloud computing on SME security?

H01: Cloud computing has no correlation with the security of SMEs

Ha1: Cloud computing has negative correlation with the security of SMEs

ii. **Research Question 2:**

What are the cloud security threats and challenges for SMEs?

Ho2: SMEs face the same security threats and challenges as large enterprises in cloud environments

Ha2: SMEs face different security threats and challenges compared to large enterprises in cloud environments

iii. **Research Question 3:**

What is the best security strategy for SMEs to adopt around cloud computing?

Ho3: There is no sure path to secure cloud computing for SMEs

Ha3: A security model for cloud computing can guide SMEs to achieve security in the cloud

1.4 Objectives of the Study

The main objective of this study is to investigate the strategies for SMEs to achieve effective security in the cloud.

The objective is divided into three sub-objectives:

- i. To identify the security threats and challenges facing SMEs in cloud computing
- ii. To determine the best mitigation measures for common security threats in cloud computing
- iii. To develop a security strategy framework for SME in the context of cloud computing.

CHAPTER 2: LITERATURE REVIEW

2.1 Cybersecurity Issues

2.1.1 Cybersecurity and the Nature of Cyberspace

With the recent advances in information technology (IT) such as the Internet and the mobile cloud computing (MCC) paradigm, focus has been directed towards protecting information systems from cyber-attacks. Consequently, cybersecurity continues to elicit heightened scholarly attention as industry experts expect the number of cyber-attacks and their severity to increase in the future (Symantec, 2016; Verizon.com, 2016). While information technology has become an indispensable aspect of the modern society, it also brings important security implications (Goutam, 2015). In the modern business environment, disruptive technologies such as cloud computing, mobile computing, and social computing are dramatically changing how enterprises use IT for conducting commerce online and sharing information. In order to safeguard the confidentiality, integrity, and availability of information, organizations invest heavily in technology resources and person hours to create countermeasures (Vinnakota, 2013).

Currently, there is no universally accepted definition of the term ‘cybersecurity’, which explains its multidimensionality. For instance, Goutam (2015) defines cybersecurity as the technologies and processes devised to protect computers and computer networks from unauthorized access. Similarly, the International Telecommunications Union (ITU) defines cybersecurity as the “*collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurances, and technologies used to protect the cyber environment*” (ITU, n.d).

According to Goutam (2015), cyberspace is a borderless virtual environment that allows people and systems to exchange information. The borderless and ubiquitous nature of cyberspace creates a platform that encourages anonymity and facilitates criminal behaviours including various forms of cyber-attacks, cyber bullying, intellectual property (IP) theft, and identity theft (Fischer, 2016). According to Bendovschi (2015), the key characteristics of a modern enterprise include pervasive usage of social networks, big data, online transactions, and vast information stored and managed via automated processes. Information security and data privacy are permanent and constantly evolving risks within such an environment (Nojeim, 2010).

2.1.2 Cybersecurity Risks and Threats Facing Businesses

Information systems are exposed to a wide range of cybersecurity threats. Currently, organizations struggle with understanding what threats exist for their information assets and how to combat them. According to Fischer (2016), the

risks associated with a cyber-attack depend on three interrelated factors: threats, vulnerabilities, and impacts. The threats are the people or systems who initiate cyber-attacks. The cyber threats fall into five categories based on their motivations (Fischer, 2016). The first category is cybercriminals, usually motivated by monetary gain. The second category comprises of spies motivated to steal proprietary or classified information. The third category of threats is nation-state warriors who use their capabilities to support or disrupt a nation's strategic objectives. The fourth category comprises of hackers who perform cyber-attacks for reasons based on personal beliefs or political leanings. Lastly are terrorists who engage in organised cyber-attacks for various reasons. In terms of vulnerabilities, cybersecurity is characteristically an arms race between attackers and defenders. Vulnerabilities consist of system weaknesses, which are open to exploitation by attackers. A threat manifests when vulnerability exists in a system (Fischer, 2016).

2.1.3 Security Models

Jouini, Rabai, and Aissa (2014) presents a hybrid model for classifying security threats to information systems. The model combines threat classification and impacts as tools to identify the threats to organizations and to determine which assets or areas they could affect. The threat classification model considers criteria of five primary factors: source, agent, motivation, intention, and impacts (Jouini *et al.*, 2014). In general, threats fall into two basic categories: internal threats and external threats. Internal threats fall into three categories: human threats, environmental threats, and technological threats. Human threats can take the form of accidental or intentional malicious actions or non-malicious actions. Both technological and environmental threats are non-malicious (Jouini *et al.*, 2014).

In a previous study, Geric and Hutinski proposed a model of security threat classification called C³ Model. The C³ Model uses a classification criteria based on three primary factors: frequency of security threat, area of security threat activity, and source of security threat (Geric & Hutinski, 2007). Similarly, Alhabeeb, Almuhaideb, and Srinivasan (2010), propose a classification method for information security threats based on three factors: attacker's prior knowledge about a system, criticality of system parts, and losses can occur because of a successful attack.

Other classification methods focus on security threat impact such as the STRIDE Model, which is an abbreviation for *Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service and Elevation of privileges* (Microsoft Corporation, 2003). This model characterizes known security threats based on the specific motivations, goals, and purposes of attacks (Microsoft Corporation, 2003). The International Standards Organization (ISO) lists five major security threats as a reference model: destruction of information resources, corruption, and modification of information, theft, removal, or loss of information, resources, disclosure of information, and interruption of services

(ISO/IEC 7498-1, 1994). The reference model provides common basis for coordinating existing standards for system interconnection.

2.1.4 Emerging Trends in Cybersecurity

The scope of today's cyber security issues extends to the security of IT systems deployed in enterprises as well as to the broader digital networks including critical national infrastructures (Sharma, 2012). Unfortunately, preliminary security surveys by industry players such as Symantec (2016) and Verizon.com (2016) show an increasing number of cyber-attacks targeting enterprises, but with paucity of information about the characteristics of the attacks and their possible impacts.

Reddy and Reddy (2014) identified six major trends that characterize the changing cybersecurity landscape. The first trend is the persistence of attacks targeting Web applications by exploiting legitimate Web servers to extract data and distribute malicious codes (Reddy & Reddy, 2014). For businesses involved in e-commerce, this is a major of concern as cyber criminals use their Web servers to steal data. Another defining trend is the pervasive deployment of cloud computing services. As the clouds evolve, the security concerns increase. Other trends of notable significance in cybersecurity are the growth in mobile networks, evolution from IPv4 to the new Internet protocol (IPv6), and the emergence of Advanced Persistent Threat (APT) and targeted attacks (Reddy & Reddy, 2014). Security is a major challenge as business rely more on wireless communications and mobile devices connected to their internal networks.

According to Symantec Security Threat Report for 2016, over 430 million unique malware threats were discovered in 2015, representing a 36% increase from the previous year (Symantec, 2016). The report suggests that attacks targeting organizations and businesses in general continue to rise. However, the most notable insight from the available data is the evolution of Web attacks, toolkits, and exploitation of vulnerabilities online. According to Symantec (2016), attackers are exploiting any vulnerability they find and compromise websites in order to commandeer host servers. These trends indicate the broadening vulnerability of businesses to various security attacks and data breaches with significant economic implications. According to the report, most of the current attacks target mobile devices and the Internet of Things (IoT), web threats, social media and email threats, cloud services and infrastructure, as well as targeted attacks, spear phishing, and intellectual property theft among other forms of data breaches and privacy violations (Symantec, 2016).

The Information Security Breaches Surveys conducted by Price Waterhouse (PwC) shows similar trends with 91% of large organizations reporting security breaches compared to 81% in 2014, and over three-quarters of small businesses reporting security breaches (PwC, 2015). In addition, the report shows that the average cost of a single breach suffered by

organizations increased sharply for all types and sizes of businesses. According to the report, the human factor accounted for over three-quarters of security-related breaches, most of them related to insider threats (PwC, 2015).

2.1.5 Current Cybersecurity Practices, Measures, and Standards

The threat to cybersecurity is growing as enterprises increasingly rely on information infrastructure in an interconnected cyberspace. For this reason, security measures are crucial to safeguard the confidentiality, integrity, and availability of information. However, Vinnakota (2013) notes that most of the approaches designed to address cybersecurity issues are fragmented in nature due to poor understanding of cyberspace.

In a previous study, Steffani (2006) found that the most common security methods used in organizations include firewalls, role-based access, physical separation, data encryption, identity management, and monitoring backup data.

Table 1. Common Security Methods used by Organizations (Steffani, 20016)

Security method used	Organizations
Firewalls	94%
Role-based access	86%
Physical network separation	83%
Data encryption on HD	69%
Identity management	69%
Encryption of data backup	63%
Monitoring usage of backup media	36%

The survey findings showed that most organizations use security technologies and tools such as firewall technologies, advanced perimeter controls, security intelligence systems, data-loss prevention tools, access governance tools, and automated policy management tools (Steffani, 2006).

Although there is no sure success for enterprises regarding cybersecurity, the security practices are maturing with best practices and various standards designed to guide enterprises. The United States federal government agencies have released various standards and guidelines that can help the private sector as well as government agencies to improve information security such as the National Institute of Standards and Technology (NIST) (2014) and the Centre for Internet Security (CIS, 2016). The U.S. NIST developed a “Framework for Improving Critical Infrastructure Cybersecurity” for all types of organizations (NIST, 2014). The core of the NIST Framework comprises of five functions that reflect the entire

cycle of cybersecurity risk management: identify, protect, detect, respond, and recover (NIST, 2014). The comprehensive framework decomposes the five functions into 22 categories and 98 sub-categories, which map into various informative cybersecurity references such as the Critical Security Controls (CSC).

According to the Centre for Internet Security (CIS), an effective cyber defence system consists of five critical tenets or principles that espouse CSC: offense informs defence, prioritization, metrics, continuous diagnoses and mitigation, and automation of defences (CIS, 2016). The CIS Critical Security Controls represent the prioritized security actions that organizations need to assess and improve their security posture (CIS, 2016).

Similarly, the ISO/IEC 27000 standards describes requirements for information security management, which serve as guidelines for helping organizations keep information systems secure (ISO/IEC 27000, 2014). The requirements apply to all types of businesses including both small and large enterprises in any sector. According to ISO's Joint Technical Committee (2009), the committee responsible for ISO 27000 and other related standards, the standard suits different types of use including formulation of security requirements, managing security risks, ensuring compliance, and definition of information security management processes. In addition, the NIST security guidance gives an extensive set of baseline security controls (Joint Task Force Transformative Initiative, 2013).

2.2 Security Issues in the Context of SMEs

2.2.1 Definition of SME

Currently, there is no specific definition of the term SME that may be taken as a reference for all economies. As a result, different countries have different criteria for defining the SME. However, despite the lack of a universal definition, the importance of such a definition is unassailable. According to Lucky (2012), the common criteria for defining SMEs include the size of an organization, the number of employees, the size of the industry, and asset value. Similarly, the U.S. International Trade Commission (2010) recognizes the number of employees and the annual revenue as the basic classification criteria.

The U.S. Small Business Administration (SBA) (2017) provides yet the most straightforward definition of SME as it includes all businesses with less than 500 employees. This definition will apply for the rest of this study. Generally, the SME sector comprises of three categories of enterprises: micro enterprises, small enterprises, and medium enterprises or businesses. The micro enterprises are the smallest of the three categories, comprising of up to nine employees. The medium businesses are the largest among the SME categories in terms of number of employees, and capital investment. The three categories fall within the description of SBA and will be part of the definition used in this study.

2.2.2 IT Security Threats Facing SMEs

The U.S. State of Cybercrime Survey (2013) shows increasing cyber-attack threats to SMEs. The report shows that the most common IT vulnerabilities affecting SMEs include social collaboration, embracing workforce mobility and increased usage of mobile devices, growing deployment of cloud storage, and digitization of privacy-sensitive information. Watchguard.com (2008), an agency that focuses on issues that affect SMEs has published a list of the most common IT security threats facing businesses in the U.S. There are other valid sources of IT security threats such as the Verizon Data Breach Report for 2016. Verizon.com (2016) gives incident report for different types of business including SMEs and large enterprises. Similarly, Symantec (2016) Internet Security Threat Report provides an insightful overview and analysis of the global security threat activities for all types of businesses.

To gain a complete picture of the threats facing SMEs, it is important to analyse existing cybersecurity reports and come up with a comprehensive view of the security posture of enterprises. The discussion of each of the security threats consists of a definition, the IT assets under threats, and the possible mitigation measures that SMEs can adopt. The most common security threats facing SMEs according to these reports are insider threats, lack of contingency planning, poor network configuration, and reckless usage of Wi-Fi networks, portable devices, web server compromise, HTML email, and exploitation of known vulnerabilities (WatchGuard 2008; Verizon 2016; Symantec, 2016).

i. Insider Attacks

According to WatchGuard (2008), insider threat is a common security threat to SMEs than in large organizations. Perhaps this can be attributed to the fact that SMEs have fewer employees than large organizations and their structure allows for illegal practices related to their IT operations. Furthermore, due to the smaller number of employees, SMEs often entrust a single person to a lot of control over information assets. This presents a significant ability for such an employee to harm the business as an insider. Similarly, Verizon Data Breach Report (2016) considers insider and privilege misuse a common security threat for businesses. According to Verizon, this category includes insider-only misuse as well as outsiders and partners that collude with employees or have access privileges granted for IT resources.

Assets Targeted: Insider attacks target the entire IT infrastructure.

Mitigation Measures: WatchGuard (2008) proposes three measures to mitigate the threat of insider attacks: implementing the principle of dual control, formalizing hiring practices, and reducing the opportunity for mischief. Implementing dual control principles means that SMEs need to establish fallback measures for each key resource.

According to Balakrishnan (2015), SMEs can develop programs for mitigating insider threats by tailoring specific elements of their organization to the NIST Cybersecurity Framework, the CERT Insider Threat program components, and the Intelligence and National Security Alliance (INSA) Roadmap. The NIST Cybersecurity Framework provides a guide on how to mitigate security threats using the core elements. However, each component in a mitigation program for insider threat has a distinct human element, unlike in a general cybersecurity program. The INSA Roadmap envisions 13 essential elements that require iteration and coordination starting from Initial Planning to Feedback and Lessons Learned (INSA, 2016).

The CERT Insider Threat Centre (2015) provides key components for effective insider threat program focusing on enterprise-wide participation and communication, oversight, reporting mechanisms, response planning, and protection of employee civil rights and liberties among others. Further, the Securities Industry and Financial Markets Association (SIFMA) (2014) has developed a comprehensive guide of best practices that provide a framework for creating programs to mitigate insider threats.

ii. **Lack of Contingency Planning**

According to WatchGuard IT Security Report (2008), lack of effective contingency planning is a major security threat facing SMEs. Indeed, the survey report found that most SMEs lack Business Continuity Plans (BCP), Disaster Recovery Plans (DRP), and Intrusion Response Plans (IRP) that would help the businesses to restore their operations in the event of data failure or compromise. These plans form essential components of best practices for all types of businesses.

Assets Targeted: poor contingency planning can affect the entire IT infrastructure of an SME.

Mitigation Measures: According to WatchGuard (2008), the mitigation measure is to develop BCP, DRP, and IRP. In addition, ISO standards form an essential component as the building blocks of Business Continuity Management (BCM). In particular, the ISO/IEC 22301:2012 standard specifies generic requires for planning, establishing, implementing and maintaining management systems to protect against disruptive incidents. Indeed, the ISO/IEC 27031 standard proposes a framework for all types of organizations and identifies relevant aspects such as performance criteria and implementation details.

The NIST SP 800-34 publication provides guidelines and considerations for IT contingency planning (Swanson *et al.*, 2010). The guidelines include BCP, DRP, Crisis Communications Plan, Cyber Incident Response Plan, and Continuity Operations (COOP) Plan. Although the recommendations target federal systems, they can guide SMEs in designing their contingency plans.

iii. **Poor Configuration Leading to Compromise**

According to WatchGuard (2008), SMEs often make poor network configurations due to their inexperience in installing switches, routers, and other networking equipment. Some of the SMEs lack the resources to employ competent IT security personnel. This is consistent with the Verizon (2016) report, which states that 62% of data breaches occurred because of misconfiguration of IT equipment and information networks.

Target Assets: SME's entire information network.

Mitigation Measures: WatchGuard (2008) proposes four major mitigation measures for misconfiguration security threats: changing default passwords and usernames, performing automated audit scans, employing qualified experts to check the network configuration, and selecting solutions that employees can use with ease.

NIST provides guidelines and best practices for configuration management from a security perspective in SP-800-14 (Swanson & Guttman, 1996). In addition, NIST gives guidelines and best practices for understanding the capabilities of firewall technologies and policies including standard configuration practices (Scarfone & Hoffman, 2009).

iv. **Reckless Usage of Hotel Networks and Kiosks**

According WatchGuard (2008), hotel and kiosk networks tend to provide free Wi-Fi, which presents a security threat because they can infect connected devices with various forms of malware besides attacks such as DoS and eavesdropping. Essentially, the greatest threat is to laptops and other devices that connect to the network connections without appropriate antivirus software and later connect to their own company network.

Target Assets: the main target is an employee's device and the company's entire IT network.

Mitigation Measures: WatchGuard (2008) suggests three forms of mitigation measures: ensuring comprehensive defences for mobile devices, enforcing policies to forbid employees from turning off the defences, and installing client integrity checks at company headquarters.

v. **Reckless use of Wi-Fi Hotspots**

According to WatchGuard (2008), public wireless hotspots possess the same level of risk as hotel and kiosk Wi-Fi networks. This is especially important because attackers can establish unsecured wireless access points (APs) that broadcast as free public networks. Such attackers can enable packet sniffers and access privacy-sensitive data.

Target Assets: the main target for these attacks include privacy-sensitive company data.

Mitigation Measures: to mitigate reckless usage of Wi-Fi connection, WatchGuard (2008) advises enhanced user training and awareness on the need to encrypt connections, encouraging users to select reputable hotspots and encourage wired connections.

vi. **Data Loss on Portable Devices**

This type of vulnerability commonly occurs due to the usage of stolen portable devices such as laptops, tablets, and mobile phones. The loss of such devices can lead to unauthorized access to sensitive data (WatchGuard, 2008).

Target Assets: this attack targets portable devices that may contain sensitive data.

Mitigation Measures: to mitigate potential data loss in portable devices, WatchGuard (2008) recommends training users and creating awareness on the need for proactive physical defence, enforcing password policies, centralized management of mobile devices, and overall training on data security.

vii. **Web Server Compromise**

According to WatchGuard (2008), most SMEs have websites and application code customized to run the site. Consequently, most of the common botnet attacks target vulnerabilities in web servers and web applications at the higher level.

Target Assets: the main target of this vulnerability is company websites and Web servers

Mitigation Measures: the best mitigation measures against Web server compromises include auditing of web application code and using firewalls to filter HTTP and HTTPS traffic.

viii. **Reckless Web Surfing by Employees**

According to WatchGuard (2008), the sites that spread the most malware are celebrity fan sites, gaming sites, and porn sites. Employees who surf to such kinds of sites are highly vulnerable to different types of malware.

Target Assets: the target assets are devices connected to company networks such as PCs, laptops, tablets and mobile phones.

Mitigation Measures: WatchGuard (2008) proposes three types of mitigation measures; gathering data about a company's Web habits, adopting a strict Acceptable Use Policy, and implementing Web content filtering.

ix. **Malicious HTML Email**

Most of the attackers who exploit emails as an attack vector now use HTML email with malicious links and not the conventional email attachments. SMEs are particularly vulnerable to this kind of attack because they may likely not implement necessary security controls.

Target Asset: the main target of HTML email is the computers, mobile phones, or any other equipment used to view or open the malicious emails.

Mitigation Measures: WatchGuard (2008) recommends three mitigation measures against email HTML: spam filtering, implementing outbound Web proxy, and user awareness about email security.

x. **Automated Exploit of Known Vulnerabilities**

According to Verizon (2016), 73% of data breaches occur due to known security vulnerabilities. Similarly, WatchGuard (2008) reports that the most common threats to SMEs come from automated attacks that scan the Internet to find vulnerabilities in connected systems. These kinds of non-targeted attacks seek to exploit security vulnerabilities, especially in Windows operating systems.

Target Assets: Operating Systems of computers and mobile phones

Mitigation Measures: to mitigate automated exploits, WatchGuard (2008) recommends investing in patch management, building test networks, minimizing and controlling the devices installed on the network, and emphasizing on thoroughness.

Table 2. Top Security Threats to SME Data, Target Information Assets, and Prevention Actions

Security Threat	Target Asset	Prevent Action for SME
Insider attacks	Entire IT infrastructure	Implement precaution policy Individual employees should not have full authority over IT assets Perform background check when recruiting new employees
Lack of contingency planning	Entire SME IT infrastructure	Implementing preventive policies Developing policies based on business needs
Poor configuration leading to security compromise	Entire SME network	Implementing password policy Implementing preventive policies Using firewalls Using updated anti-virus programs
Reckless use of hotel networks and kiosks	Employee's devices	Use firewalls Use updated antivirus software
Reckless usage of Wi-Fi hotspots	Company data	Using encryption technology
Data loss on portable devices	Portable device and data	Mobile device management software Data encryption on devices
Web server compromise	SME website and server	Using firewall to filter malicious traffic Auditing web application code to eliminate security vulnerabilities
Malicious HTML email	Devices used to view email	Implementing spam filtering Employee security training and awareness Implementing prevention policies
Reckless web surfing by SME employees	Employee laptops, computers	Using firewall Enforcing Acceptable Use Policy Using web filtering solutions
Automated exploits of vulnerabilities	Computer OS	Using patch management software Training employees on security to increase awareness

2.3 Security Issues in the Context of Cloud Computing

2.3.1 Overview of Cloud Computing

Attempts to define the term ‘cloud computing’ come from different perspectives in academia and practice, which explains the variations in definition. Buyya *et al.* (2009) describes cloud computing as the ‘fifth utility’ along with water, gas, electricity, and telephone. Based on this description, cloud computing encompasses readily available and on-demand access to computing services just like the other utilities. However, Kim (2009) disputes this definition and describes it as inaccurate because utility computing is merely a form of service cloud computing. NIST provides the most straightforward definition of cloud computing by describing it as, “*A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources*” (Mell & Grance, 2011). This study will use this definition as it describes a cloud model using five essential characteristics, three service models, and four types of deployment models.

Essentially, the NIST definition of cloud computing distinguishes five key characteristics of the cloud model: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell & Grance, 2011). Any cloud computing service needs to espouse these key characteristics. On the other hand, NIST identifies three types of cloud service models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). According to Mell and Grance (2011), SaaS describes the capability for the consumer to use applications provided by a cloud provider from various client devices and program interfaces. PaaS describes the capability for the consumer to deploy applications acquired or created using various programming languages, tools, and services onto the cloud infrastructure (Mell & Grance, 2011). Lastly, IaaS describes the capability for the consumer to provision storage, processing, networks, and other computing resources in order to deploy and run software including OS and applications. Apart from the three main cloud service models, additional models have been described in literature including Desktop-as-a-Service (DaaS), and Database-as-a-Service (DBaaS), both are subsets of PaaS that describe the capability for users to request database services using a self-service portal (Khurana & Verma, 2013).

NIST describes four types of deployment models depending on the relationship between the cloud service provider and the consumer: private cloud, community cloud, public cloud, and hybrid cloud (Mell & Grance, 2011). The security and privacy of these models varies with their deployments.

2.3.2 Cloud Security Issues and Challenges

For businesses, cloud computing comes with enormous possibilities and challenges as well. Besides availability and trust, security and privacy remain the most significant challenge for enterprises. Indeed, various flaws in the cloud architecture create vulnerabilities to security and privacy threats. According to Nazir and Rashid (2013), each of the three cloud deployment models presents its unique advantages and disadvantages in terms of security and privacy. The key security issues in a public cloud include lack of control over data lifecycle, lack of surety of system availability and data back-up, and multi-tenancy applications, which increase vulnerability (Nazir and Rashid, 2013). A private cloud model allows customers to establish control over the network but the common usage of virtualization techniques introduces additional vulnerabilities.

Besides the regular threats to network security, Sharma & Trivedi (2014) identifies seven top issues associated with cloud computing: data loss, data breaches, malicious insiders, insecure interfaces, data location, service hacking, and DoS.

2.3.3 Cloud Computing Security Threats and Mitigation Techniques

Existing literature distinguishes three categories of general security threats that also manifest in cloud environments: threats to confidentiality, threats to integrity, and threats to availability; that is, threats to the CIA-triad (Sharma & Trivedi, 2014; Aldossary & Allen, 2016). In the context of cloud computing, confidentiality refers to established rules or agreement on the access and restriction of different types of information in the cloud. The idea is to ensure that user's information remains confidential. Data integrity refers to the completeness of information in the cloud. In cloud environments, data integrity proofs the consistency, validity, and regularity of data in the cloud. Lastly, availability refers to the ability to access the data and operate systems (Sharma & Trivedi, 2014).

i. Attacks on Confidentiality

In the cloud, clients want to protect their data from potential attacks as well as to prevent access by the cloud service providers. According to Alani (2014), confidentiality is a priority target for security attacks. Some of the dangerous attacks in private clouds target encryption keys, OS information, and Virtual Machine (VM) locations. Attackers can also use social engineering techniques in which they trick clients to give access to their cloud accounts (Alani 2014). Other attacks can be executed via side-channel attacks. Ristenpart *et al.*, (2009) describes a common attack method in which an adversary maps the internal cloud infrastructure and identifies the location of VM to launch cross-VM side channel attacks and extract information from target VMs that reside on the physical machine. In another study, Zhang and Juels (2012)

demonstrated the first type of a successful side channel attack in which a malicious VM extracted information from a modern symmetric multi-processing Xen-based VM running on the same physical computer.

ii. **Attacks of Integrity**

Data stored in the cloud presents significant integrity issues due to potential damage when transmitting it to or from cloud data storage. According to Aldossary and Allen (2016), cloud computing presents two major data integrity issues: data loss or manipulation, and the risk of untrusted remote server performing computation on behalf of users. The risk of data loss or manipulation occurs as users lose control over their data in cloud environments besides the many administrative errors that can lead to accidental modification of data. To reduce threats to data integrity in the cloud, Al-Saiyd and Sail (2013) recommends using secure hash mathematical functions, using digital signatures, as well as cloud data tokenization at the field level, data backup, standard API, and tiered access control lists (ACLs).

iii. **Threats to Availability**

According to Alani (2014), threats to availability exist in virtually all networking services. Generally, the threats aim to prevent legitimate users from accessing or using the systems. In cloud computing environments, the attacks can be particularly severe due to the high demand for additional computing power. One of the notable attacks that render cloud services unavailable are DoS and DDoS attacks (Deshmukh & Dvadkar, 2015). Given that cloud service providers charge clients based on the amount of resources they use, adversaries can attack the cloud infrastructure and cause huge increment in bills even without compromising the client's system. Indeed, heavy DoS attacks can breakdown the entire cloud. The DoS threat affects all types of cloud service models including SaaS, IaaS, and PaaS (Alani, 2014). Chawla *et al.* (2015) classifies DDoS attacks into three categories: network layer/transport layer attacks, application layer attacks, and DDoS attacks against web services. These variations indicate the variability of DoS and DDoS attacks as well as the challenge in dealing with the different attack techniques. Currently, there are no clear mitigation measures for DoS and DDoS attacks, but service providers use various security techniques including intrusion detection systems and firewalls to reduce the risk and ensure early detection. Tian and Wu (2014), proposes a strategy for allocating cloud resources dynamically for clients who experience DDoS attacks. Devi and Subbulakshmi (2016) compare various DDoS mitigation techniques and measures including for cloud-based computing environments, but none shows the capability to ensure sufficient level of protection for all cloud environments.

2.3.4 Summary

The cloud security issues covered in existing literature falls under five categories or themes as shown in table 3.

Table 3. Cloud Security Issues and Themes

<i>Category of Cloud Security Issue</i>	<i>Description</i>	<i>Main Issues</i>
Network	Describes network and related attacks such as DoS & DDoS attacks, MITM attacks, DNS attacks, flooding attacks, and vulnerabilities to IP	<ul style="list-style-type: none"> - IP vulnerabilities - Network security configuration - Internet dependence
Security standards	Explores current standards required to prevent attacks against cloud infrastructure including policies to ensure confidentiality, integrity, and availability of cloud systems	<ul style="list-style-type: none"> - Lack of adequate security standards - Trust issues - Compliance issues
Cloud infrastructure	Includes security attacks specific to cloud infrastructure (SaaS, IaaS, and PaaS)	<ul style="list-style-type: none"> - Insecure API interface - Security misconfiguration - Multi-tenancy - Server location and backup
Access Control	This theme covers mainly authentication and access control mechanisms or issues that affect data storage and user privacy	<ul style="list-style-type: none"> - Malicious insiders - Authentication mechanisms - Account & service hijacking - Privileged user access
Data	Covers issues related to data related security including the CIA-triad	<ul style="list-style-type: none"> - Data protection - Data integrity - Data availability - Data loss and leakage - Data confidentiality (privacy)

2.4 Studies that Explicitly Address Security in SMEs that use Cloud Computing

2.4.1 Cloud Adoption Strategies used by SMEs and Security Implications

A growing body of research on cloud computing focuses on the strategies that small and medium businesses use to adopt this technology and the security implications inherent in those strategies. According to Javaid (2014), SMEs do not need to install software and maintain servers on their premises or employ highly technical personnel in order to benefit from cloud computing. This is especially important because the cloud computing services created by providers such as Amazon and Google rely on centralized data centres that provide economies of scale. Therefore, the providers deliver the Cloud model to end-users as oriented pay-per-use services with customized Service Level Agreements (SLAs) (Javaid, 2014). As a result, this strategy for cloud computing converts the computing power into a public utility, which SMEs can access and afford. In a study to examine the factors that affect SME adoption of cloud-based technologies, Akbari (2013) found that the

factors fall into two categories: intra-organizational factors and external factors. In particular, the study found that many SMEs use the owner/manager model in which the role of the business owner influences IT strategies and security measures adopted by an organization (Akbari, 2013).

Alshamaila *et al.* (2013) used the Technological, Organizational, and Environmental (TOE) theoretical framework to investigate the adoption process SMEs use to deploy cloud computing. The study findings indicated that the most important factors influencing SME adoption of cloud services were uncertainty, size, prior experience, relative advantage, geo-restriction, compatibility, industry, and market scope. More importantly, the study found that cloud security, privacy, and ownership were major concerns for businesses. However, SMEs would be willing to adopt cloud computing services as most rely on their perception of trust (Alshamaila *et al.*, 2013).

Carcary *et al.* (2014) found that the reasons for SME adoption of cloud computing technology are multi-fold including expected cost reduction, improved scalability, and business community. The study found that security of the cloud environment, data ownership and protection, as well as compliance issues were the most common obstacles for SME migration to the cloud. The security concerns include physical and personnel security in terms of accessing customer data, and machines, identity management in terms of accessing information and computing resources, as well as the application of security to applications that exist as a service via the cloud (Carcary *et al.*, 2014). Similarly, Doherty *et al.* (2013) found that the key driver pushing SMEs to adopt cloud computing is the perceived cost benefits and the main barrier is concern over the continuous availability of the service and security implications in general.

2.4.2 Security Opportunities for SME's Adopting Cloud Computing

SMEs can use cloud computing for a range of applications including corporate website, email, Customer Relationship Management (CRM), internal payroll processing among others. Indeed, cloud services have attractive cost structures for SMEs because they typically use the “pay-as-you-go” model. More importantly, cloud environments provide inherent network and information security opportunities. According to the European Union Agency for Network and Information Security (ENISA) (2015), one important opportunity that SMEs can exploit is the existence of large cloud computing providers that offer advanced security measures and spreads the associated costs across multiple customers. Essentially, this means that SMEs can share best practices for security settings that they would not otherwise have which is, a significant business opportunity.

ENISA (2015) identifies various network and information security opportunities that abound in cloud computing environments such as geographic spread, elasticity, physical security, standard formats and interfaces, software

development, and security-as-a-service among others. The emphasis is that cloud services come with significant geographic spread and elasticity as providers can leverage large data centres with massive spare resources. For SMEs that use shared resource requirements, cloud computing provides additional physical security including alarm systems, perimeter protection, and camera surveillance provided by cloud providers (ENISA, 2015). Moreover, cloud providers provide secure software development while spreading the high costs across multiple customers. For SMEs, it is often cheaper and feasible to outsource some security tasks to the cloud provider or third parties such as security add-ons.

ENISA (2015) identifies eleven priority security risks that SMEs should take into account in the cloud environment:

i. **Software Security Vulnerabilities**

According to ENISA (2015) software vulnerabilities such as SaaS email service that is vulnerable to SQL injection attacks have major impact on customers. These vulnerabilities could lead to breach of confidentiality and damage the reputation of a business. Khan and Al-Yasiri (2016) concurs that various service delivery models such as SaaS and PaaS present significant security issues. In the case of SaaS, providers bear the primary responsibility for preventing software vulnerabilities. ERP systems provided as a service in the cloud can have important security implications for SMEs if not well secured (Khan & Al-Yasiri, 2016). In both PaaS and IaaS, the responsibility falls on the customer to ensure the software runs securely. Unfortunately, certain types of software security vulnerabilities in the cloud can lead to customers accessing the data of another customer. These isolation failures arise due to the multi-tenancy feature of cloud computing environments. The solution according to Ghorade *et al.* (2014) is to use effective resource isolation to ensure data security during processing as well as isolating the virtual caches. Private clouds provide robust security features that can also help SMEs address this problem.

ii. **Network Attacks**

SMEs access and manage cloud computing services over Internet connections, which introduce enormous risk of network attack such as DoS, network traffic sniffing, and MITM attacks. Fu *et al.* (2014) identifies four key security challenges that confront SMEs in managing network using the cloud model. The first challenge is the problem of remote dynamic network configuration management. Secondly, certain functions of network management are unsuitable for moving to the cloud. Thirdly, most of the service-oriented network management functions become a service in the cloud environment, and lastly, cross-domain requires usage of traditional network management functions (Fu *et al.*, 2014). Consequently, Fu *et al.* (2014) presents a novel model of management architecture called Multi-Tenant Cloud-based Network Property trusteeship or MulCNeT, which focuses on monitoring, configuring, and management network using

property management as a business model. The model envisages that the most significant work in network management is self-network management, remote management, and diagnostic capabilities. Similarly, Gastermann *et al.* (2015) proposes an optimal cloud storage solution for SME purpose. The solution focuses on protecting data on client, server, and during transport as a strategy to reduce the attack surface of the cloud storage services.

iii. **Social Engineering Attacks**

According to ENISA (2015), some administrative processes in businesses such as issuing credentials happen via websites and emails. This practice increases the risk of social engineering attacks in which adversaries' attempt to fake user communications while masquerading as trusted sources, such as a cloud provider. According Mouton *et al.* (2016), social engineering attacks are similar in terms of the communications medium, goal, compliance techniques and principles as well as the steps and phases of the attacks. Essentially, an attacker using social engineering technique may attempt to impersonate a customer to initiate credential recovery impersonate the provider to obtain the credentials, or target normal users such as system administrators and software developers on both the customer side and the provider's side (ENISA, 2015).

iv. **Management GUI and API Compromise**

According to ENISA (2015), many cloud providers offer their customers management interfaces that give administrative access to multiple assets such as access to SME's employee user accounts in SaaS, or access to different VMs and applications in PaaS and IaaS. Indeed, cloud service providers often publish APIs and enable customers to design interfaces for interacting with various cloud computing services (Munir & Palaniappan, 2013). The interfaces add a layer on the framework and increase the cloud complexity. This introduces a major security risk in case an attacker gains access to the management interface with such privileged access. For this reason, ENISA (2015) recommends customers to verify that providers offer secure management interfaces with robust authentication techniques and authorization mechanisms. Moreover, ENISA (2015) recommends customers to ensure robust security for PCs and browsers used by their administrators, especially for accounts with strong administrative roles and privileges.

v. **Device Theft/Loss**

A major feature of cloud computing is accessibility from fixed PCs, and mobile laptops, tablets, smartphones, and other mobile devices. Mobile devices introduce new risks because they are vulnerable to loss and theft (ENISA, 2015). The loss of a mobile device means that attackers could access data or authentication credentials stored on the devices. A major common problem for SMEs is the trend towards Bring-Your-Own-Device (BYOD), which means that employees use their

own devices to connect to the company network. In BYOD, SMEs do not have full control over the devices. Indeed, features such as storage media encryption, screen locks among others may work differently for different devices. Downer and Bhattacharya (2015) classify BYOD security challenges into deployment, technical, human aspects, and policy and regulation challenges. The main idea is that when mobile devices access cloud-based storage, the same security threats to the device apply to the data itself.

vi. **Physical Hazards**

Natural disasters can also affect the data centres and provider's IT infrastructure. This means that natural disasters affecting the provider might affect customers. In PaaS and IaaS, customers can specify which datacentres they will use as failover. To address this problem, SMEs need to establish business continuity strategy to address the risk of physical hazards (ENISA, 2015).

vii. **Overloads**

In cloud environments, customers use the same physical infrastructure. This means that resource usage peaks may affect customers by other customers or DoS attacks on other customers. To address this risk, SMEs need to know how their cloud service addresses increased demand in cloud usage and check SLA guarantees on service availability (ENISA, 2015).

viii. **Unexpected Costs**

Most cloud services are often based on the pay-as-you-go model, which means that costs depend on usage. This indicates the risk that the costs could go unexpectedly high because users such as employees store massive data on the cloud or in case of DoS attacks. The risk of unexpected cost in the cloud is a business risk. SMEs need to check their SLAs to determine the associated costs (ENISA, 2015).

ix. **Vendor Lock-in**

Vendor lock-in describes a situation in which it is difficult for the cloud customers to migrate to a competitor provider (ENISA, 2015). For SMEs, this is both a financial and a security risk because the customer does not have the flexibility. To mitigate this problem, customers need business continuity strategies outlining their migration and exit plans in cloud computing.

x. **Administrative or Legal outages**

Administrative and legal conflicts affecting the provider can affect the availability of cloud services (ENISA, 2015). SMEs need to review the provider obligations stated in SLAs including the liability and indemnity issues.

xi. **Foreign Jurisdiction Issues**

According to Shilpa, Nagashree, Divya, and Spurthi (2014), cloud services often involve the usage of foreign cloud providers or data centres located abroad. This means that foreign jurisdiction may affect the security of the cloud services (ENISA, 2015). SMEs should be aware of applicable foreign jurisdictions.

2.5 Security Risk Management Strategies for SMEs in Cloud Computing

2.5.1 Cloud Computing Risks Affecting SMEs

Cloud computing provides SMEs with access to cloud services, software, and infrastructure that would be beyond their reach otherwise. However, cloud computing presents significant risks and challenges. In a survey conducted by the Information Systems Audit and Control Association (ISACA) (2010), it was revealed that 45% of the participants consider security risks of cloud computing as outweighing the potential benefits. The study showed that consumers worry about the security of their data, but they feel well prepared to protect against security risks. The study identified the top five things that cloud consumers fear would be misused by cybercriminals: credit card and debit card information, passwords, personal emails, national ID number, and social media usage (ISACA, 2010). As a result, the survey found that the most common protection mechanisms that cloud consumers use include regular changes in passwords, changes in privacy settings, avoiding public Wi-Fi access points, avoiding storing sensitive data on devices, and turning off Internet functions when not in use. The main security risk concerns for SMEs include information security, privileged user access, regulatory compliance and data location in cloud environments, system availability and disaster recovery, as well as provider lock-in and long-term viability (Brender & Markov, 2013).

Azarnik *et al.* (2012), categorizes the security risks associated to cloud computing into four categories: outsourcing opportunity risks, technology development risks, functional risks, political risks, technical risks, financial risks, and project risks. According to Azarnik *et al.* (2012), outsourcing risks relate to the vendor behaviour and they range from theft of intellectual property and proprietary software to client-lock-in and stealing confidential data. Functionality risks arise when vendor fails to understand what a cloud user needs, technology risks relate to technical and operational limitations, while political risks are common stakeholder conflicts. Technical risks arise when software and hardware technology become complex while financial risk arises when projects fail to meet anticipated benefits (Azarnik *et al.*, 2012).

Keung and Kwok (2012) explains that SME enterprises with inadequate resources to ensure in-house support and limited knowledge about the available cloud technologies face challenges in deciding whether to buy a private cloud or to rent a public cloud service. In order to help SMEs address this problem, the researchers present a method for assessing cloud deployment with a model called the Cloud Deployment Selection Model (CDSM). The model evaluation

demonstrates its ability to recommend the most suitable cloud deployment model for SMEs based on the relevant factors affecting such enterprises.

Prasad *et al.* (2014) agrees that SMEs need to determine the path to follow in adopting cloud computing services to ensure a sustainable presence in cloud environments. The researchers developed a model of cloud computing adoption to assist SMEs to adopt cloud-based strategy and ensure sustainable business performance. The model takes into consideration five factors affecting SMEs: strategic and incremental intent, understanding the organizational structure and culture, understanding the external factors, the human resource capacity, and understanding value expectations (Prasad *et al.*, 2014). The overarching conclusion is that SMEs need to be proactive in their cloud computing strategy focusing on awareness and understanding of internal and external circumstances before they start deploying cloud computing services (Prasad *et al.*, 2014).

2.5.2 SME's Approaches to Cloud Security Risk Management

Cloud computing will trigger some level of loss exposure. For SMEs, the level of risk exposure determines their ability to survive (Fan & Chen, 2012). However, preliminary investigations show paucity of information or evaluation of risk exposures emanating from cloud environments used by SMEs. This indicates the need to explore the best strategies that SMEs can use to manage the security risk associated with cloud environments. According to the ISO 31000 (2009), risk management is the methodical process that organizations use to treat risks related to their activities. The goal of risk management is to obtain benefits and sustainable values across organizational activities.

Based on the core sub-process, there are three primary methods of risk assessment: qualitative methods, which use simple calculations without determining the numerical value of risk, quantitative methods, which assign numerical values to both risk impact and likelihood, and the semi-quantitative or hybrid methods that combine both qualitative and quantitative (Frame, 2003). The three methods have their inherent limitations and strengths. Quantitative risk assessments have been faulted for emphasizing on reductive aspects of organization risk and diverting efforts from preventive measures (Frame, 2003). In addition, quantitative methods of risk assessments may ignore crucial qualitative risk differences while some of the calculations are tedious and no straightforward. Qualitative assessments prioritize risks and help in identifying the most important areas that need improvement. However, qualitative risk assessments are limited because they do not provide quantifiable measurements of risk probabilities and impact. On the other hand, semi-quantitative risk assessment combines the advantages of both approaches to offset their inherent weaknesses (Frame, 2003).

According to Fan *et al.* (2012), a matrix would be helpful to determine the most appropriate techniques for handling security threats. The idea is to evaluate the consequences of the risks in terms of severity of impact and cost to SMEs and to place the risks of the Risk Management Model in Fig. 1.

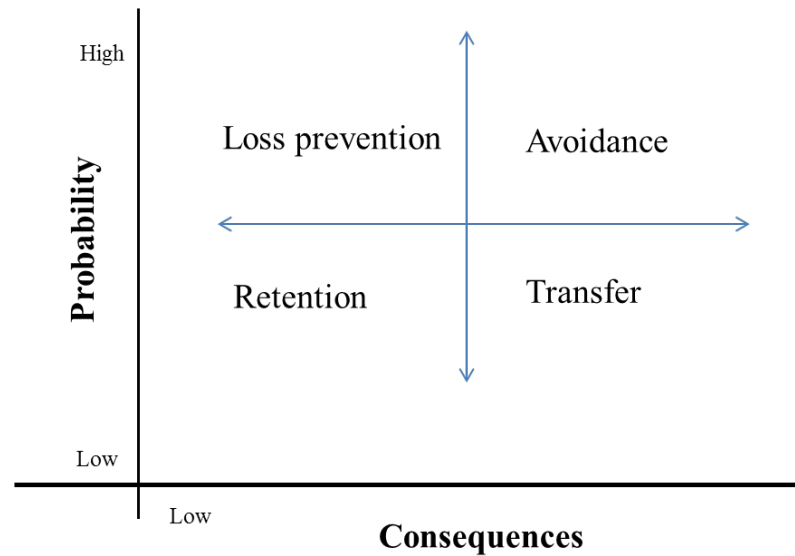


Figure 1. Risk Management Matrix (Fen *et al.*, 2012)

Various researchers have proposed many variations of the risk management matrix . Unfortunately, the available information does not address specific risk management for SMEs in the cloud. Moreover, the traditional risk management approaches tend to adopt common methodologies for all types of organizations, which usually do not suit SMEs given their unique security posture, budget and skills capacity. One solution developed specifically for assessing SME’s cloud security risk is the CloudWatch2, a methodology that helps small businesses and initiatives to capture value proposition (CloudWatch, 2016). CloudWatch provides a simplified approach to cloud risk assessment that relies on the assumption that SMEs need simple, efficient, and flexible cloud security solutions.

The CloudWatch approach encompasses three major steps:

i. Assessing the security posture of SMEs

This step entails creating profiles for SMEs to determine what information security risk management would be appropriate based on their security posture (CloudWatch, 2016). A questionnaire can help to explore the specific security threats and vulnerabilities as well as the potential impact SMEs face in relation to their IT systems and the information they utilize (See sample questionnaire in Appendix 3). The designed questions gather information about the level of exposure to

security threats, the potential impact, and the value of IT systems to a business enterprise. Processing the answers to the questionnaire can help in computing the security posture of SMEs.

ii. Selection of security controls

The second step in the CloudWatch approach takes an input from the impact level in step 1 as a strategy for recommending appropriate security controls to mitigate the identified security risks (CloudWatch, 2016). The Cloud Security Alliance (2017) has developed Cloud Controls Matrix (CCM) to provide baseline security principles that serve as a guide to assist prospective cloud customers to assess the overall security risk of a cloud provider. The CSA CCM provides a robust framework of security controls that offer detailed understanding of pertinent security principles and concepts (CSA, 2017). The CSA CCM framework provides SMEs with a structured model on how to tailor cloud deployments. For SMEs to select appropriate security controls and enterprise architecture components, they need to respond to the computed level of risk impact.

iii. Deployment and monitoring of the risk profile

The third step in the CloudWatch Approach entails deployment and monitoring the security risk profile. This includes considering the cloud security Service Level Agreements or secSLAs. The idea is that SMEs intending to use secSLA as a strategy for implementing appropriate security should start by identifying the assets that they need to protect and assess the security risks imposed when migrating to the cloud (CloudWatch, 2016). Therefore, the primary consideration for successful adoption of cloud computing based on secSLA is the comprehensive understanding of the cloud-specific characteristics, the architectural components, and the specific role of cloud actors (CloudWatch, 2016).

CHAPTER 3: PROPOSED FRAMEWORK

3.1 Introduction

Existing literature reveals that many SMEs are adopting cloud-based enterprise systems. However, businesses need to be convinced of their security as they seek to migrate to the cloud. This study has been undertaken to ensure the security of SMEs in the cloud and proposes a conceptual framework model for enhancing security in the cloud. There is a consensus among security experts, professionals, and researchers that the overall objective of information security is to safeguard the availability, integrity, and confidentiality of an enterprise's information.

3.2 Methodology

In order to achieve this objective in the context of SMEs adopting or migrating to the cloud, I followed the Architects View of SABSA Model, the Conceptual Security Architecture (Sherwood *et al.*, 2009). SABSA is a popular open-source generic method for security architecture development and management. It provides a robust methodology for developing business-driven and risk/opportunity focused business enterprise security. The primary characteristic of the SABSA Model is that every business strategy must be derived from the analysis of business requirements for security management and risk management (Sherwood *et al.*, 2009).

The risk management aspect of SABSA embraces the notion of opportunity and threat, as well as the balance that enterprises need to strike between the two concepts for their survival. Consequently, the SABSA model is layered with its top layer representing the definition of business requirements. Each lower layer encompasses the development of a new level of abstraction moving through the conceptual framework definition, logical architecture, physical architecture, and the component architecture, which represents the selection of technologies and products at the lowest layer (Sherwood *et al.*, 2009). Fig. 2 illustrates the SABSA Model for security architecture.

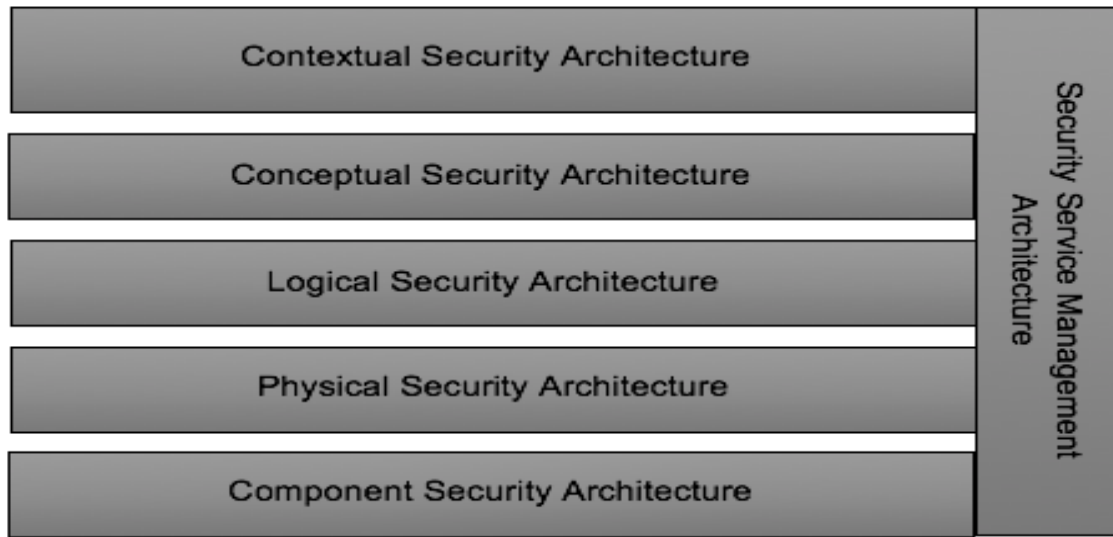


Figure 2. The SABSA Model for Security Architecture (Sherhood *et al.*, 2009)

3.3 Proposed Model

Based on the security requirements for SMEs in the cloud, a matrix of five security questions (what, who, why, where, how) are answered in the conceptual security framework (see Fig. 3). The proposed conceptual model adapts and enhances the model proposed by Alemu and Omer (2014) to incorporate additional aspects for risk management. In the model, the system that needs protection in the cloud is represented with cloud architecture and the main security item components including the Physical, Network, Storage, Computer, Data, and Application Components. In addition, the model includes Cloud Service Models (PaaS, IaaS, and SaaS), and Cloud Deployment Model (public, private, hybrid, and community), which represent the main elements of SME cloud architecture. The framework is adapted from a model proposed by Alemu and Omer (2014) specifically for the banking sector. This model has been chosen because it provides a comprehensive strategy addressing security in all cloud service models and deployment models.

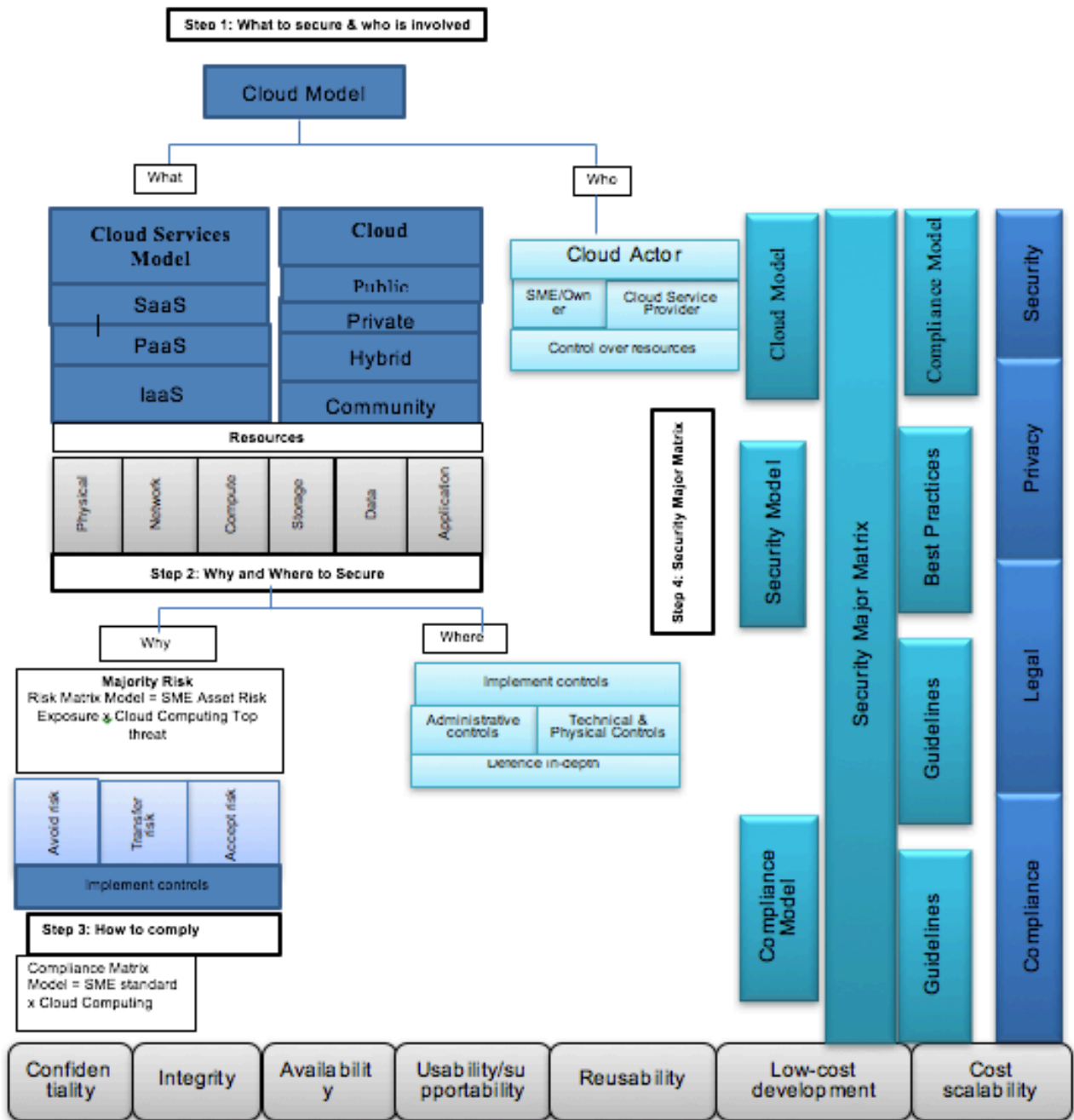


Figure 3. The Proposed Security Model for SME Cloud Computing

3.4 Discussion of the Proposed Framework

The proposed framework entails four basic components as follows:

Component 1: Cloud Model (Step 1: What and Who)

From a business view, the first question to ask in order to ensure SME security in the cloud is what type of system to deploy and who will use it consistent with the SABSA Model (Sherwood *et al.*, 2009). The question of ‘What’ represents the assets to be protected and the business needs for SME information security. In terms of high-level of the information architecture, this question is expressed as business decisions along with the business goals and objectives (Sherwood *et al.*, 2009).

On the other hand, the question of ‘Who’ addresses the owners of the business processes that require security such as business transactions and communications. The SABSA Model expresses this question in relation to the business attributes, the relevant business requirements or needs, the roles and responsibilities and the level of business trust that exists between the business owners, customers, data custodians, and service providers. More importantly, when developing a cloud security infrastructure, it is always advisable to consider the cloud reference model to deploy in order to map the cloud services against the cloud model. For SMEs, this ensures robust security architecture as well as compliance to regulatory requirements. Based on these two founding factors, the proposed Conceptual Framework for SME security in the cloud envisages the first step to involve determining what system to secure and who would be involved. The answer to this question is addressed via the Cloud Model component (See Figure 3). The parties (who) involved with cloud systems are represented as Cloud Actor, a component that includes the SME/Business Owner and Cloud Service Provider. In addition, the model addresses the type of cloud services including the three basic Cloud Service Models: IaaS, SaaS, and SaaS. It also addresses the nature of computing resources at each service physical, network, computer, storage, application, and data resources.

Component 2: Security Model (Step 2: Why and Where)

Component 2 of the Conceptual Model represents the ‘Why’ and ‘Where’ question in the SABSA Model (Sherwood *et al.*, 2009). The question of ‘Why’ represents the business risks expressed as business opportunities and threats to the business assets. Similarly, ‘Where’ depicts the organizational aspects of business geography and general location-related issues that affect business security such as remote working sites (Sherwood *et al.*, 2009) and the physical locations of infrastructure and data. In order to address the ‘Why’ security question in cloud computing, SMEs have to focus on addressing the risk of deploying each application, function, asset, or data for cloud deployment and services. As illustrated in Figure 3, the idea is to specify the Risk Matrix Model represented as Risk Matrix Model = SME Asset Risk Exposure x Cloud Computing Top Threat (Alemu & Omer, 2014).

In order to perform risk assessment, SMEs need to identify specific assets and priority cloud computing threats as well as compute the probability of risk impact. The Risk Matrix Template in Appendix 1 illustrates the framework of addressing the security threats based on the Security Model and the Cloud Model. According to Alemu & Omer (2014), SMEs should determine the probability of risk occurrence in deploying an asset across the cloud environment. Both the SME and its Cloud Service Provider can decide to Avoid the risk, Accept the risk, Transfer the risk, or to Implement the risk (Appendix 1).

Component 3: Compliance Model (How)

The third component is the Compliance Model, which addresses the ‘How’ question in SME cloud computing. The ‘How’ question relates to the business processes that require security such as enterprise transactions and communications (Sherwood *et al.*, 2009). The SABSA Model expresses this question in relation to high-level technical and cloud management security strategies. The Compliance Model addresses this question based on a Compliance Matrix defined by four main components in cloud computing environments: Compliance, Legal, Privacy, and Security. Previously, Alemu & Omer (2014) identified the four components as crucial for compliance.

Component 4: Security Major Matrix

Component 4 represents Security Major Matrix in the proposed Conceptual Model. The model envisages that SMEs need to comply with security, privacy, legal and overall compliance requirements to ensure adequate protection in cloud environments. The Matrix illustrates the integration of three the three models: Cloud Model, Security Model, and the Compliance Model. Appendix 2 shows the template for Control Domain Matrix for establishing specific security major that addresses specific tools, products, guidelines, and best practices (Alemu & Omer, 2014).

CHAPTER 4: FINDINGS AND DISCUSSION

The aim of this study was to examine strategies for effective cyber security for SMEs in the cloud. While cloud computing is considered a vital IT innovation with enormous operational and strategic benefits, SMEs still lag behind in the adoption rates. Therefore, there is a need to understand the security threats to SMEs in cloud environments, the target information assets, and the mitigation measures. Based on the SABSA Model, this study has developed a cloud computing conceptual security model for SMEs (Sherwood *et al.*, 2009).

The study demonstrated various key findings that have implications on SMEs that seek to adopt cloud computing. In particular, the study findings show that SME's adoption of cloud computing depends on factors such as organizational context, technological context, and environmental context. New technologies would be expected to bring additional benefits and value to businesses. However, SMEs may likely postpone the adoption of new technologies due to perceived risks such as security and privacy threats, loss of control, and poor understanding of the potential benefits.

4.1 Objective 1: SME Cloud Security Threats and Risks

From the onset, the study has established that the global and borderless nature of cyberspace presents significant challenges to enterprises that rely on information systems embedded to the Internet. The security threats affect all manner of businesses, but the risks to SMEs may differ from large corporations because of the unique contexts. The study found that the major security issues in the context of SMEs include the risk of insider threat, lack of contingency planning, network misconfiguration, portable device, Web server compromise, malicious HTML emails, automated exploits among others. In the context of cloud computing, the major security threats are categorized into three categories: threats to confidentiality, threats to integrity, and threats to availability. The common threats to confidentiality target OS information, encryption keys, and VM locations and exploit methods such as social engineering. The risks of data loss and untrusted remote server manipulation are real for SMEs operating in the cloud environment, and threaten data integrity. DoS and DDoS present significant threats to the availability of information and information systems in the cloud and the cost of using the technology.

Overall, the security issues facing SMEs in cloud environments fall under five categories or themes: network issues, security standards issues, cloud infrastructure issues, access control issues, and data issues. Network-related issues include threats posed by DoS and DDoS attacks, MITM attacks, flooding attacks, DNS attacks, and IP vulnerabilities. There are also concerns about dependence on the Internet and network security configuration. Security issues include lack of adequate security standards to ensure robust security for enterprises, trust issues when working over the Internet, and

compliance issues. Existing literature focuses more on the available standards required to mitigate cyber-attacks in the cloud infrastructure and the policies that can safeguard the CIA triad of cloud systems. For the cloud infrastructure, the major security issues for SMEs include insecure API interfaces, security misconfiguration, server location and data backup, as well as the multi-tenancy characteristics of the cloud environment. Access control themes allude to various security issues such as malicious insiders, authentication mechanisms, account and service hijacking, and privileged user access. These impact are unique to each business. Lastly, SMEs also have generic security issues concerning data protection, integrity, availability, and the risk of data loss and privacy issues hence a multi-level solution is required.

Further analysis of existing literature identifies 11 priority security threats facing SMEs in the cloud. The first security threat is software security vulnerabilities such as SaaS email service, which is vulnerable to SQL injections. The multi-tenancy features of cloud environments expose customers to attacks that seek to exploit isolation failures. This implies that SMEs need to use effective resource isolation and isolation of virtual caches. Even though, private cloud would be appropriate for SMEs because they provide robust security features despite their cost implications. The second priority threat for SMEs is network attacks. Using Internet connections exposes SMEs to enormous risks associated with MITM, network traffic sniffing, and DoS attacks. Combined with the network configuration issues associated with SME networks, the risk become ever apparent. For SMEs, this implies the need to focus on protecting data on the server-side, client-side, and reduce the attack surfaces that expose cloud storage services. The other priority security risks include social engineering attacks. API compromise and vulnerabilities to management GUI, device theft, overloads, vendor lock-in, as well as unexpected costs, jurisdictional issues, administrative outages.

4.2 Objective 2: Mitigation Measures for Security Threats

To address the second research objective, the study examined the current cybersecurity practices standards, and measures, the threat mitigation techniques against security issues in cloud computing contexts, and approaches for cloud security risk management. From the onset, the study findings suggest that the most common security methods used by enterprises include firewalls, physical network separation, role-based access control mechanisms, data encryption, and identity management, as well as backup media monitoring. The study found that that SMEs use security tools such as firewall technologies, security intelligence systems, access governance tools, perimeter controls, and tools for automated policy management. While there is no sure path for success in the deployment of security measures, the findings indicate maturity in terms of security practices and standards designed to guide enterprises. Examples of best practices and guides include the NIST Cybersecurity Framework, the ISO/IEC 27000 standards, and the CIS Critical Security Controls.

To mitigate the security threats in the cloud, the study established the need for SMEs to focus on risk management. The study established that SMEs are increasingly aware of the importance of risk management, but effective risk management remains a challenge for many businesses. The problem is that the traditional approach to risk management tends to focus on adopting common methodologies that address risks to all types of organizations. Given the unique nature of SMEs in terms of their security posture, these methodologies would be too complex and unsuitable. However, further analysis has identified CloudWatch2 methodology as an appropriate tool for SMEs. CloudWatch is justified because it provides a simplified and straightforward approach to risk assessment in the cloud. For SMEs, this implies the suitability of CloudWatch to enable them assess their security posture, select appropriate security controls, as well as deploy and monitor the risk profile.

4.3 Objective 3: Developing Conceptual Cloud Security Model for SMEs

After understanding the security threats, risks, and general challenges for SMEs in the cloud and mapping the security mitigation measures, the next step for this study was to develop a strategy for effective and secure cloud deployment for SMEs. The strategy is represented as a conceptual framework modelled using the SABSA Conceptual Security Architecture (Sherwood *et al.*, 2009). The proposed conceptual model integrates four components: Cloud Model, Security Model, Compliance Model, and Security Major. The Cloud Model is the first step in the overall security strategy for SMEs, and it addresses the question of “**What**” to protect and “**Who**” would be involved in the firm’s security management. For SMEs that seek to deploy cloud-computing technology, the first step in the cloud deployment strategy envisaged under this model would be to identify the type of systems to use and determine who will use the systems. This approach makes it possible for SMEs to map security architecture and determine the business, regulatory, and compliance requirements. The model identifies various threat sources in cloud computing including the cloud actors, the cloud deployment model, and the cloud services model.

The second component in the proposed cloud model is the Security Model, which corresponds to the second step of the SME cloud strategy. This step addresses the question of “**Why**” the protection would be needed in cloud environments and “**Where**” SMEs would like to achieve the protection. For SMEs to address the “**Why**” question, they need to focus on the risks of deploying their information assets, data, and applications at each cloud-computing model and deployment model. The Security Model provides a Risk Matrix Model represented as “Risk Matrix Model = Bank Asset Risk Exposure X Cloud Computing Top Threat”, following the ISO-27001 definition of risk exposure. This means that business owners need to identify specific assets and the top security threats to cloud computing to perform the risk

measurement. After measuring the security risks, parties need to determine where to implement the controls. The most important concepts to consider here include the logical and physical security domains and the associated domain boundaries. The model envisages three types of control domains: technical, administrative, and physical. In addition, the model maps these controls to each cloud computing resource component.

The third component is the Compliance Model and it addresses the question of **how** SMEs want to achieve the protection they need in cloud environments. The last component is the Security Architecture. For SMEs to achieve effective security in cloud computing, they need to consider the cloud architectural component and controls that meet internal standards.

CHAPTER 5: CONCLUSION AND CONTRIBUTIONS

5.1 Conclusion

This study has explored effective strategies for SME security in cloud computing. The study has investigated the security challenges facing SMEs in the cloud including the major security threats and risks, as well as their mitigation measures, best practices, and standards. By adopting the conceptual framework, the findings of this research support the notion that various factors influence the strategies that SMEs use to adopt cloud computing. More importantly, the proposed framework is borne of the idea there exists no single path to success for SME cloud security. Rather, the framework envisages different contexts in terms of security threats, vulnerabilities, and general risk posture. As such, the model anticipates variations in the strategies that SMEs adopt to secure their assets in the cloud. The model provides a flexible framework that can guide SMEs to select the best security measures, policies, and strategies based on their unique security circumstances in the cloud. In conclusion, it is recommended that SMEs use the proposed model as a guide to securing information and other assets when moving to any-cloud solution.

5.2 Contributions

The overarching significance of the study finding is the contributions it makes to the current research discourse exploring better ways for improving the security of cloud computing at the SME level. The study findings have both theoretical and practical contributions.

5.2.1 Theoretical Contributions

From a theoretical perspective, the study contributes to the IT adoption literature, by examining the range of strategies that SMEs can use when deploying cloud computing. Examining SME's adoption of new IT innovations can enrich the understanding of the innovation process, especially in an era characterized by constant technological advances and emerging security threats. The theoretical model builds on the existing literature on enterprise information security in the context of cloud computing. This is a pioneering research in terms of looking at strategies that SMEs can use when deploying cloud services. The nature of cloud computing offers enough scope to generalize the study findings to both small and medium-sized enterprises. Furthermore, the security threats and vulnerabilities as well as the opportunities would be expected to apply to the majority of SMEs so the work is extensible. The study adds to the growing body of literature on security threats and risks to enterprises in cloud environments by examining the priority threats unique to SMEs. The conceptual model takes into consideration virtually all the key elements cited in the existing literature to explain the best approach to cloud security.

5.2.2 Practical Contributions

At the practical level, the study has important implications for SME owners, cloud software vendors, and technology consultants. For business owners, the study provides an overview of the security risks and provides a model for finding the best countermeasures. As SMEs represent the majority of businesses in many economies, it also represents an important economic segment for service providers and software vendors. Much of the existing uncertainty surrounding cloud computing for SMEs has been how data is handled in a cloud environment without regard for the other critical business assets.

5.3 Study Limitations and Directions for Future Research

This study aimed to expand our knowledge about strategies that SMEs can use to improve security in the cloud. While the study has fulfilled the research aims and objectives, there are various areas for additional research given the limitations of the study. Admittedly, the study represents a small fraction of the vast literature about security strategies for SME success in cloud computing. However, as noted earlier, there is paucity of research on the specific security strategies that SMEs can use to achieve success in cloud computing despite the well documented security threats. Future research could extend the study findings by validating the proposed model and examining appropriate strategies for cloud computing in different sectors, industries, or countries.

REFERENCES

- Akbari M 2013, 'Cloud computing adoption for SMEs: challenges, barriers, and outcomes'. Masters Dissertation. Dublin Institute of Technology. Available from:
<http://arrow.dit.ie/cgi/viewcontent.cgi?article=1053&context=scschcomdis>. [29 January 2017].
- Alani MM 2014, 'Securing the cloud: threats, attacks, and mitigation techniques', *Journal of Advanced Computer Science and Technology*, vol. 3, no. 2, pp. 203-213.
- Aldossary, S & Allen W 2016, 'Data security, privacy, availability, and integrity in cloud computing: issues and current solutions', *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 4, pp. 485-498.
- Alemu, M & Omer, A 2014, 'Cloud computing conceptual security framework for banking industry', *Journal of Emerging Trends in Computing and Information Sciences*, vol. 5, no. 12, 921-930.
- Alhabeeb, M. Almuhaideb, A. Le, PG & Srinivasan, B 2010, 'Information security threats classification pyramid', In *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, pp. 208-213.
- Al-Saiyd, N & Sail, D, 2013, 'Data integrity in cloud computing security', *Journal of Theoretical and Applied Information Technology*, vol. 58, no. 3, pp. 570-581.
- Alshamaila, Y Papagiannidis, S & Li, F 2013, 'Cloud computing adoption by SMEs in the northeast of England: A multi-perspective framework', *Journal of Enterprise Information Management*, vol. 36, no. 3, pp. 250-275.
- Azarnik, A. Shayan, J. Alizadeh, M. & Karamizadeh, S 2012, 'Associated risks of cloud computing for SMEs', *Open International Journal of Informatics*, vol. 1, 37-45.
- Balakrishnan, B 2015, 'Insider threat mitigation guidance', The SANS Institute. Available from:
<https://www.sans.org/reading-room/whitepapers/monitoring/insider-threat-mitigation-guidance-36307>. [25 January 2017].
- Bendovschi, A 2015, 'Cyber-attacks: trends, patterns, and security countermeasures' *7th International Conference on Financial Criminology*, *Procedia Economics and Finance*, vol. 28, pp. 24-31.

- Brender, N & Markov, I 2013, 'Risk perception and risk management in cloud computing: results from a case study of Swiss companies', *International Journal of Information Management*, vol. 33, no. 5, pp. 726-733.
- Buyya, R. Yeo, CS. 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*, vol. 25, no. 6, pp. 599-616.
- Carcary, M. Doherty, E & Conway, G 2014, 'The adoption of cloud computing by Irish SMEs: an exploratory study', *The Electronic Journal of Information Systems Evaluation*, vol. 17, no. 1, pp. 3-14.
- Centre for Internet Security 2016, 'The CIS Critical Security Controls for Effective Cyber Defence (Version 6.1)' Available from: <https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf>. [24 January 2017].
- CERT. Insider Threat Centre 2015, 'InTP Series: Protection of Employee Civil Rights and Privacy Rights. Available from: <https://insights.sei.cmu.edu/insider-threat/2015/06/-intp-series-protection-of-employee-civil-liberties-and-privacy-rights-part-15-of-18.html>. [25 January 2017].
- Chawla, I. Luthra, P & Kaur, D 2015, 'DDoS attacks in the cloud and mitigation techniques', *International Journal of Innovative Science, Engineering, & Technology*, vo. 2, no. 7, pp. 596-600.
- Cloud Security Alliance 2017, 'Cloud Controls Matrix Working Group. Available from: <https://cloudsecurityalliance.org/group/cloud-controls-matrix/>. [6th February 2017].
- CloudWatch 2016, 'D3.2 Risk-Based Decision Making Mechanisms for Cloud Service in the Public Sector'. Available from: http://www.cloudwatchhub.eu/sites/default/files/D3.2_Risk-Based-Decision-Making-Mechanisms-For-Cloud-Service-In-The-Public-Sector.pdf. [6th February 2017].
- Deshmukh, RV & Dvadkar, KK 2015, 'Understanding DDoS attack & its effect in cloud environment', *In Proceedings of the 4th Conference on Advances in Computing, Communications, and Control*, vol. 49, pp. 202-210.
- Devi, BS & Subbulakshmi, T 2016, 'A comparative analysis of security methods for DDoS attacks in the cloud computing environment', *Indian Journal of Science and Technology*, vol. 9, no. 34, 1-7.

- Doherty, E. Carcary, M & Conway, G. 2013, 'Migrating to the cloud: examining the drivers and barriers to adoption of cloud computing by SMEs in Ireland: an exploratory study', *Journal of Small Business and Enterprise Development*, vol. 22, no. 3, pp. 512-527.
- Downer, K & Bhattacharya, 2015, 'BYOD security: a new business challenge'. In *Proceedings of the 5th International Symposium on Cloud and Service Computing*, IEEE CS Press, pp. 1128-1133.
- European Union Agency for Network and Information Security 2015, April, 'Cloud security guide for SMEs: cloud computing security risks and opportunities for SMEs'. ENISA. Available from: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes/at_download/fullReport. [29 January 2017].
- Fan, CK & Chen, TC 2012, 'The risk management strategy of applying cloud computing', *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 9, pp. 18-27.
- Fan, CK, Chiang, CM & Kao, TL 2012, 'Risk management strategies for the use of cloud computing', *International Journal of Computer Network and Information Security*, vol. 12, pp. 50-58.
- Fischer, EA 2016, 'Cybersecurity issues and challenges: In brief. Congressional Research Service (7-5700 R43831)'. Available from: <https://fas.org/sgp/crs/misc/R43831.pdf>. [24 January 2017].
- Frame, JD, 2003, *Managing Risk in Organizations: A Guide for Managers*, New York, John Wiley & Sons.
- Fu, C, Jia-hai, Y & Shaobin, Z 2014, 'MulCNet: Network management cloud', *International Journal of Grid and Distribution Computing*, vol. 7, no. 2, pp. 139-150.
- Gastermann, B, Stopper, M, Kossik, A. & Katalinic, B 2015, 'Secure implementation of an on-premise cloud storage service for small and medium-sized enterprises', *Procedia Engineering*, vol. 100, pp. 574-583.
- Geric, S & Hutinski, Z 2007, 'Information system security threats classification', *Journal of Information and Organizational Sciences*, vol. 31, no. 1, pp. 51-61.

- Ghorade, VL, Surendrananu, MS & Basapur, SB 2014, 'Securing software as a service model of cloud computing: issues and solutions', *International Journal of Scientific Engineering and Technology Research*, vol. 3, no. 9, pp. 1874-1879.
- Goutam, RK 2015, 'Importance of cybersecurity', *International Journal of Computer Applications*, vol. 111, no.7, pp. 14-17.
- Hashemi, SY & Hesarlo, PS 2014, 'Security, privacy, and trust challenges in cloud computing and solutions', *International Journal of Computer Network and Information Security*, vol. 8, pp. 34-40.
- Information Systems Audit and Control Association (2010). 2010 ISACA IT risk/reward barometer. Available from: <https://www.isaca.org/SiteCollectionDocuments/2015-risk-reward-survey/2015-it-risk-reward-barometer-report.pdf>. [6 February 2017].
- Intelligence and National Security Alliance 2016, 'Insider Threat Resource Directory'. Available from: <http://www.insaonline.org/InsiderThreat>. [25 January 2017].
- International Standards Organization (ISO/IEC 7498-1) 1994, Information technology: open systems interconnection: basic reference model. Available from: <http://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf>. [24 January 2017].
- International Telecommunication Union, n.d, 'Data networks, open system communications and security'. Available from: <https://ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf>. [24 January 2017].
- ISO 31000 2009, 'Risk management – Principles and guidelines'. Available from http://www.iso.org/iso/catalogue_detail?csnumber=43170. [2 February 2017].
- ISO/IEC 22301: 2012, 'Societal Security, business Continuity Management Systems, Requirements'. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=50038. [25 January 2017].
- ISO/IEC 27000 2014, 'ISO/IEC Information Technology, Security Techniques, Information Security Management Systems, Overview, and Vocabulary'. Available from: http://www.iso.org/iso/catalogue_detail?csnumber=63411. [24 January 2017].

- Javaid, MA 2014, 'Implementation of cloud computing for SMEs. *World Journal of Computer Application and Technology*, vol. 2, no. 3, pp. 66-72.
- Joint Task Force Transformative Initiative 2013, 'Security, and privacy controls for federal information systems and organizations', (NIST Special Publication 800-53). Available from:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>. [24 January 2017].
- Joint Technical Committee 2009, 'ISO Standards – JTC 1/sc27 – IT Security Techniques'. Available from:
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on. [24 January 2017].
- Jouini, M. Rabai, LBA & Aissa, AB 2014, 'Classification of security threats in information systems', *5th International Conference on Ambient Systems, Networks, and Technologies; Procedia Computer Science*, vol. 32, pp. 489-496.
- Keung, J & Kwok, F 2012, 'Cloud deployment model selection assessment for SMEs: renting or buying cloud', *IEEE International Conference on Utility and Cloud Computing*, doi:101109/UCC.2012.29.
- Khan, N & Al-Yasiri, A 2016, 'Identifying cloud security threats to strengthen cloud computing adoption framework', *The 2nd International Workshop on Internet of Thing: networking Applications and Technologies, Procedia Computer Science*, vol. 94, pp. 485-490.
- Khurana, S & Verma, AG 2013, 'Comparison of cloud computing service models: SaaS, PaaS, IaaS', *International Journal of Electronics & Communication Technology*, vol. 4, no. 3, pp. 29-32.
- Kim, W 2009, 'Cloud computing: today and tomorrow', *Journal of Object Technology*, vol. 8, no. 1, 65-72.
- Lucky, EO 2012, 'Is Small and Medium Enterprise (SME) an entrepreneurship', *International Journal of Academic Research in Business and Social Sciences*, vol. 2, no. 1, pp. 341-352.
- Mell, P & Grance, T 2011, September, 'The NIST definition of cloud computing', NIST Special Publication 800-145. Available from: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- Microsoft Corporation 2003, 'Improving Web application security: threats and countermeasures'. Microsoft Press.
Available from: http://download.microsoft.com/download/d/8/c/d8c02f31-64af-438c-a9f4-e31acb8e3333/threats_countermeasures.pdf. [24 January 2017].
- Mohabbattalab, E. Heidt, T & Mohabbattalab, B 2014, 'The perceived advantages of cloud computing for SMEs', *GSTF Journal on Computing*, vol. 4, no. 1, pp. 61-65.
- Mouton, F. Leenen, L & Venter, HS 2016, 'Social engineering attack examples, templates and scenarios', *Journal of Computers and Security*, vol. 59, pp. 186-209.
- Munir, K & Palaniappan, S 2013, 'Secure cloud architecture', *Advanced Computing: An International Journal*, vol. 4, no. 1, pp. 9-22.
- National Institute of Standards and Technology, 2014, 'Framework for improving critical infrastructure cybersecurity'.
Available from: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. [24 January 2017].
- Nazir, M & Rashid, MS 2013, 'Security threats with associated mitigation techniques in cloud computing', *International Journal of Applied Information Systems*, vol. 5, no. 7, pp. 16-27.
- Nojeim, GT 2010, 'Cybersecurity and freedom on the Internet', *Journal of National Security Law & Policy*, vol. 4, pp. 119-137.
- Prasad, A. Green, P. Heales, J & Finau, G 2014, 'Towards a model of cloud computing services for SMEs. In *Proceedings of the 25th Australasian Conference on Information Systems*, 8-10 December, Auckland, New Zealand.
- Pricewaterhouse Coopers 2015, 'Information Security Breaches Survey'. Available from:
<http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf>. [24 January 2017].
- Reddy, GN. & Reddy, G. JU 2014, 'A study of cybersecurity challenges and its emerging trends on latest technologies', *International Journal of Engineering and Technology*, vol. 4, no. 1, pp. 48-51.

- Ristenpart, T. Tromer, E. Shacham, H & Savage, S 2009, 'Hey, you, get off my cloud: exploring information leakage in third-party computer clouds', In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp. 199-212.
- Scarfone, K & Hoffman, P 2009, September, 'Guidelines on firewalls and firewall policy'. NIST Special Publication 800-41. Available from: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>. [25 January 2017].
- Securities Industry and Financial Markets Association 2014, 'SIFMA Cybersecurity: Insider Threats Best Practices'. Available from: http://www.sifma.org/uploadedfiles/issues/technology_and_operations/cyber_security/sifma-cybersecurity-insider-threat-best-practices.pdf. [25 January 2017].
- Sharma, R & Trivedi, RK 2014, 'Literature review: cloud computing; security issues, solutions, and technologies,' *International Journal of Engineering Research*, vol. 3, no. 4, pp. 221-225.
- Sharma, R 2012, 'Study of latest emerging trends on cyber security and its challenges to society', *International Journal of Scientific & Engineering Research*, vol. 3, no. 6, pp 1-4.
- Sherwood, J. Clark, A & Lynas, D 2009, 'SABSA: Enterprise security architecture', SABSA, White Paper, Sabsa Limited. Available from: http://www.mitsconsulting.com/images/SABSA_White_Paper_2009.pdf. [6 February 2017].
- Shilpa, D. Nagashree, C. Divya, C. & Spurthi, G. S 2014, 'Survey on security attacks and solutions in cloud infrastructure', *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 8, 7757-7761.
- Steffani, AB 2006, 'The impact of information security in academic institutions on public safety and security: assessing the impact and developing solutions for policy practices'. National Criminal Justice Reference Service. Available from: <https://www.ncjrs.gov/pdffiles1/nij/grants/215953.pdf>. [24 January 2017].
- Swanson, M & Guttman, B 1996, September, 'Generally accepted principles and practices for securing information technology systems'. NIST Special Publication 800-14. Available from: <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>. [25 January 2017].

- Swanson, M. Bowen, P. Phillips, AW, Gallup, D & Lynes, D 2010, May, 'Contingency planning guide for federal information systems', NIST Special Publication 800-34 Rev. 1. Available from:
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>. [25 January 2017].
- Symantec, 2016, 'Internet Security Threat Report'. Available from:
<https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>. [24 January 2017].
- Tian, Y & Wu, DO 2014, 'Can we beat DDoS attacks in clouds?', *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2245-2254.
- U.S. International Trade Commission 2010, 'Small and medium-sized enterprises: overview of participation in the U.S. exports'. Available from: <https://www.usitc.gov/publications/332/pub4125.pdf>. [24 January 2017].
- U.S. Small Business Administration 2017, 'Am I a small business? Available from:
<https://www.sba.gov/contracting/getting-started-contractor/make-sure-you-meet-sba-size-standards/small-business-size-regulations>. [24 January 2017].
- U.S. State of Cybercrime Survey 2013, CSO Magazine. Carnegie Mellon University. Available from:
http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf. [24 January 2017].
- Verizon.com, 2016 'Data Breach Investigations Report'. Available from:
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf. [25 January 2017].
- Vinnakota, T 2013, 'Understanding of cyberspace using cybernetics: an imperative need for cybersecurity of enterprises', *IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM)*, pp. 107-111.
- Wang, R. Von, G. Younge, A. He, X. Kunze, M. Tao, J & Fu, C 2010, 'Cloud computing: a perspective study', *New Generation Computing*, vol. 28, no. 2, pp. 137-146.
- WatchGuard.com, 2008, 'Top 10 Threats to SME Data Security'. Available from:
https://www.watchguard.com/docs/whitepaper/wg_top10threats_wp.pdf. [25 January 2017].

Zhang Y & Juels, A 2012, 'Cross-VM side channels and their use to extract private keys', In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, pp. 305-316.

APPENDICES

Appendix 1 : SME Cloud Security Risk Matrix Template

Security Model	SME Asset	Top Threats to SME Cloud Computing	Cloud Model										Cloud Actors		
			Cloud Architecture			Cloud Service Models				Cloud Service Model					
			Physical	Network	Computer	Storage	App	SaaS	PaaS	Private	Public	Hybrid	Community	SM	Service
			Risk Likelihood Score												
Customer & Sales serving	Insider attacks														
Customer information & CRM	Data Loss														
External interfaces	Insecure Wi-Fi hotspots														
Functional & transaction processing systems	Insecure apps														
Enterprise common services	DOS														
Application infrastructure	Insider threat														

Appendix 2: Control Domain Matrix Template

Control Domain Matrix Template		Cloud Model										Cloud Actors		
SME Asset	Top Threats to SME Cloud Computing	Cloud Architecture	Cloud Service Models										Cloud Actors	
		Physical	Network	Computer	Storage	App	SaaS	Paas	Private	Public	Hybrid	Community	SME	
													Service	
Administrative Control	Policy													
	Personal security													
	Third party													
	Business continuity													
	Network and VM security													
Technical Control	Application security													
	Identity and access management													
	Incident management													
	Data security													

