University of Nairobi

SCHOOL OF COMPUTING AND INFORMATICS.

FACTORS HINDERING INTEGRATION OF PHYSICAL ACCESS CONTROL AND CYBER SECURITY IN THE BANKING SECTOR IN KENYA.

BY

ISABELLA NJUMBI GITAU.

ADMISSION NUMBER: P54/85624/2016

SUPERVISOR: DR ANDREW KAHONGE

A research Dissertation submitted in partial fulfillment of the requirements for the award of Masters of Science Degree in Information Technology Management

DECLARATION

I certify that this research project entitled "Factors hindering integration of physical access control and cyber security in the banking sector in Kenya" is my own work. The work has not been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged.

SIGNED -------------------- DATE --------------------

Isabella Njumbi Gitau

Registration No: P54/85624/2016

This research project has been submitted for examination towards fulfilment for the award of Masters of Science in Information Technology Management with my approval as the university supervisor.

SIGNED -------------------- DATE -------------------------

Dr. Andrew Mwaura Kahonge

ACKNOWLEDGEMENTS.

I would like to express my deep appreciation to my supervisor Dr Andrew Mwaura Kahonge for his support, guidance and encouragement during the entire period of this research. Special thanks to all other lecturers who were involved for their support and recommendations, which helped improve this thesis.

I would also like to thank all financial institutions who participated in this research, for their help and co-operation; without them I would not have been able to complete my research.

Last but not least, I am forever indebted to my parents John Gitau and Hannah Gitau for their endless support.

Thank you all.

Isabella Njumbi Gitau

Registration No. P54\85624\2016

ABSTRACT.

Over the last few years, many industrial control systems, including security solutions, have adopted digital technology. Components of these systems, which were physically separated are now linked together over network, making them remotely accessible and thus open to cyber threats. As part of the technological transformation made globally, physical access control and cyber security have been integrated so as to mitigate the risk of the existing cyber threats. However, in the Kenyan banking sector, financial institutions are reluctant to adopt the integrated security model despite its renown benefits.

This research focused on determining the factors that hinder integration of physical access control and cyber security in the Kenyan banking sector. A descriptive research design was used in the study with the questionnaire being used as the primary data collection tool. The study targeted employees who work in both the physical access control and cyber security units in the 43 banks in Kenya. Data analysis was done using descriptive and inferential statistics. The study established that banks’ attitude towards integration of the two security functions is determined by the banks’ commitment to security reforms, the ability of the integrated approach to resolve existing vulnerabilities and also reduce the firms’ risk exposure. In addition, the managements’ willingness to reorganize the current security model and the reduction of operational costs also determine the banks’ attitude towards the integrated security model.

The study established that the banks’ intention to integrate their security functions is determined by: the need for detective controls, the need to enhance coordination of security functions, the urge to improve accountability during security breaches, the need to improve internal monitoring by detecting security breaches before they occur and the need to prevent insider fraud by gagging any fraud loopholes. The study identified internal and external sources of pressure that would push the financial institutions to integrate physical access control and cyber security. The sources identified include: persistent security threats, the need for efficiency in security procedures, incorrect response during security breaches, legal requirements, industry regulations, integration motivated by competitors and continued global changes. Factors identified as hindrances to the integration of the physical access control and cyber security units in financial institutions include: absence of organizations which financial institutions can benchmark with, absence of industrial regulations that support integration of the security units, unknown cost implications, organizational culture and lack of road map that would guide the integration process. The findings of the study were then used to develop a conceptual framework that is recommended as a guide for all financial institutions that wish to integrate their security functions.

Keywords

Physical access control, cyber security, network, security solutions, banks.

TABLE OF CONTENTS

Table of Figures

List of Tables

ABBREVIATIONS AND ACRONYMS

CISO- Chief Information Security officer.

CSO- Chief Security Officer.

AERSRM- Alliance for Enterprise Security Risk Management

ISACA- Information System Audit Control Association.

ISSA- Information Systems Security Association.

SIEM- Security Information and Event Management.

US- United States.

TCP/IP- Transmission Control Protocol/Internet Protocol.

PCI- Payment Card Industry.

IT- Information Technology.

CIO- Chief Information Officer.

CFO- Chief Finance Officer.

LAN- Local Area Network.

IMS- Information Management System.

PDA- Personal Digital Assistant.

PL- Physical logical security.

VPN- Virtual Private Network.

DEFINITION OF TERMS.

Cyber security/ IT security/ Logical security: Security function that focuses on protection of information, information processing facilities, network resources and communication systems.

Physical access control: Security function that focuses on protection of facility structures, physical assets and personnel with the purpose of limiting access to authorized personnel.

Integrate/ converge: Combining two to form one whole unit.

Security breach: Incidents that lead to the unauthorized access and unauthorized modification of data, applications, services, networks and/or devices as a result bypassing underlying security controls.

Forensics: Procedures used to investigate and unveil fraudulent activities done in information systems.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

Shoulder surfing: The practice of spying on a user of a computer, or any other electronic device in order to obtain their personal access information.

Tail gating: The practice of authorized users assisting unauthorized users to gain access to a secured premise.

Middleware: A software that acts as a bridge between two systems that are interfaced.

Vault: A section of the bank where money and other valuables are stored to protect them from unauthorized access, theft, fir and natural disasters.

Keystroke logging: Recording of keys struck on a keyboard by a user for the sole purpose of getting information from the user without their consent.

Security control center: This is the section of the organization where all information security activities are conducted.

TCP/ IP protocol: Network protocol that governs the interconnection between computing devices and the internet.

PCI standards: These are information security best practices that credit cards must adhere to

CHAPTER ONE

1.1 INTRODUCTION

For several decades, it has been clear that the subjective division of security related activities into physical access control, IT security, information security and other disciplines has not been favorable to achieving optimal results. The increasing dire consequences of nonintegrated security efforts has caused this separation to, increasingly, be reconsidered by professionals and management. It is becoming more common to see CISOs (Chief Information Security officers) elevated to CSOs (Chief Security Officers) or both functions combined to better integrate the main security elements. Financial sector report by Raytheon (2015) revealed the importance of integration of commercial banks security components, as the financial sector experienced persistent exposure to numerous security risks.

A good example being the recent hiring of Kirsten Davies who is to serve as the group chief security officer for the Barclays Africa Group. She was previously working for Hewlett Packard Enterprise where she was the Vice president and deputy chief information security officer. One of her main tasks will be to bring together Cyber security, Information Security, Fraud Strategy, Physical access control and Forensics (amongst other security functions) into a single functional area.

Physical access control for many organizations has become fairly routine and is more easily integrated into information security or information systems security than the other way round (Tarimo, 2006; Raytheon, 2015). The creation of the Alliance for Enterprise Security Risk Management (AESRM) BY ASIS International, *Information Systems Audit and Control Association* (ISACA) and the Information Systems Security Association (ISSA) is an indication of the trend in this direction. According to Ula, Ismail and Sidek (2015) the access control and information systems security is vital to the overall success of the commercial bank in its operations.

Given that it is not possible to effectively deliver information security without a number of physical considerations, the evolution is natural. It is sensible to expect that convergence of many security activities will center around information security and information systems security in the coming decade as it’s also an organizational component (Van Niekerk & Von

Solms, 2010). As a result, integration of physical access control and cyber security will increasingly be relevant for management in the banking sector to consider.

Current corporate practices and future trends commissioned by the AESRM provide significant insight into the convergence or security integration issue.

1.2 BACKGROUND

This research is based on the importance of integrating physical access control and cyber security in the banking sector in Kenya. Over the past few years, many systems, including security solutions, have implemented digital technology. Modules of these systems, which were physically separated a few years ago, are now linked thorough networks, making them remotely accessible and thus exposed to cyber threats. Symantec (2012) identified the numerous security risks, which interconnected networks face in the digital purview. This research focuses on the importance of integrating the two, examines the specific threats and opportunities, proposes viable, affordable and readily available solutions and develops a conceptual framework that is to guide the implementation of the proposed solutions.

Banking and Technology are inseparable. The banking industry highly depends on technology to contribute to its great improvement and propagation. Technology enhances and supports the execution of all round tasks in the banking sector (Baffour, 2015). Given that most of the banks' functions are mainly accomplished through exchange of sensitive information, there arises a need to have the integrity of the data exchanged protected. This gives more reason as to why security has to be included in service delivery. More efficient security can be achieved by having a holistic view of security which would include integration of physical access control and cyber security (Kurt, 2015).

Physical access control and cyber security commonly referred to as logical security are detached functions in most banking institutions. In fact, cyber security and physical access control units have a tendency to mix like oil and water. The irony is that investment is being made in physical access control and IT security separately, yet the connection between the two is being ignored. According to Gustafson, Andersons and Walden (2008), physical security offers first line defense for commercial banks, and forms a critical deterrent to physical security risks which a bank is exposed to, thus valuable to integrate it with cyber platforms to enhance congruence in responding to all kind security threats.

The need for integrated banking security systems is informed by the complexity and benefits of congruent socio-technical security infrastructure (Tarimo, 2006).

Integrating the two security structures can accrue great benefits. One of the benefits is that it heightens efficiency as employee access to physical and network resources are streamlined. Employees experience the ease of access to both physical premises and IT resources through a single device. Enhanced access management leads to better-quality security and better compliance with various legal requirements. This is because access to resources by users is role-based and thus users can only access authorized resources and no more.

This research is meant to show the importance of integrating the cyber security and physical access control, analyzes the specific threats and opportunities, propose viable, affordable and readily available solutions and develops a conceptual framework that is to guide the implementation of the proposed solutions.

Security Gap Scenario.

The CFO of a commercial bank travels abroad and hasn't badged into the premises using his smart access card in the London branch. He has, however, checked into the branch in Geneva where he will be handling his assignments from in the coming 4 weeks. The physical access control system in London is not the same as the one in the Geneva branch. The two systems are totally independent systems. The employees in charge of the physical access control system in London are not aware that the CFO is away.

In the meantime, a trustworthy employee has been shoulder surfing as the CFO logs into the network and has acquired his login details basically his user name and password. Knowing he is away for 4 weeks, and not in the same time zone, she logs on to the network, during regular office hours, and gains access to confidential information, which she has the intention of sharing it with the firm's competitors in exchange for a fee.

In this case, no alarm will be annunciated.

This is due to the fact that no violation has occurred in neither the physical access control system nor the IT access system, which are currently functioning independent of each other.

The user committing the violation is authorized to access the premises during UK, EST working hours, which means no alarm will be raised in the physical access system since no abnormal behavior has been captured.

The Network security system captures the CFO logging in and gaining access to the confidential documents that he is authorized to access at a time that is normal for him. Thus, an alarm will not be signaled as a sign of a security breech.

Efficient management of security by converging both logical security and physical access controls could result in structurally and functionally synchronized security.

If the physical access control systems in London and Geneva were interlinked, the guards in charge of the premises would have been informed that the CFO was entering the office in Geneva and not in London.

If the physical access control system was integrated with the network access system, the CFO's authorization details may only grant him access to the network resources if he has been flagged as having entered the premises by the physical access control system.

If the physical access control system was integrated with the network access system, an alarm should be flagged indicating that the CFO is trying to access the network in London whereas he has been captured by the physical access control system as being at the Geneva office.

This would have prevented the unauthorized employee from accessing the confidential information using the CFO’s log in details.

If the physical access control unit had policies and standards implemented to identify and flag abnormal events, the violation would have been captured by the network access system which would have notified the cyber security team on a probable security incident.

If the authorization details required by the CFO to gain access to the office in Geneva were the same as those used to log on to the network, no one would manage to use his credentials to gain access.

If a firm fails to keenly review its security policies and standards, gaps in the protection systems will definitely be present (Ula, 2011; Symantech, 2012). Usually, the bigger the firm, the more the security gaps, and overlapping security efforts and thus more opportunity for them to reduce the costs incurred in enhancing efficiency in physical access control and cyber security.

1.3 PROBLEM STATEMENT

In nearly every large financial institution, the physical access control and logical security units are run independently. Both are uninformed of each other’s strengths and weaknesses, the dangers of operating and being managed separately, and the benefits that would be reaped if the management of the two security functions is integrated. The independent handling of the two security disciplines leads to creation of gaps and overlapping efforts in security.

As new and advanced technologies are introduced to the institutions, the threats become more complex and unpredictable thus giving more reason as to why we should recognize and embrace the need to integrate the two security disciplines considering the new unique security risks facing financial institutions (Mulwa, 2012).

A common example for a security coordination breakdown between physical access control and cyber security a security breach that was estimated to have cost Société Générale an estimated USD 7 Billion (Damenu & Beaumont, 2017). Further, a security breach once occurred at the Sumitomo Mitsui bank in London, England in which hackers succeeded in stealing 220 million euros. Despite the bank having strong cyber security measures, a physical access control hitch occurred. Adversaries posing as custodians mounted keystroke logging devices on the computer keyboards that allowed them to capture confidential login credentials. In addition, its strategic pre-planning and vital deterrence to put in place measures that thwart insider attacks and deliberate human errors that can be effected by exploring on the gaps between physical access and cyber security (Lacey, 2009; Mulwa,2012).

This highlights and supports the need integrate all security functions in an organization. This approach should reach across the organizations structure, policies and procedures that guide the security team, the people forming the security functions, their skills and expertise and the systems and technology in use. This will enable the organization to prevent, detect, respond to and recuperate from any kind of security breach. In addition to the costs that firms have to face when dealing with the direct consequences of security breaches, costly and protracted harm such as damage to reputation and brand are also experienced.

Previous research.

Previous studies on security in banking institutions largely have focused on specific components of cyber security such as data exchange and transmission risks for commercial banks, products that will aid the convergence process, challenges faced in the integration process and importance of converging the two security disciplines. Below is some of the existing research on integration of physical access control and cyber security:

1. In 2003, Yahya Mehdizadeh focused on the importance and challenges faced in convergence of logical and physical security.
2. In 2003, IBM wrote a technical report on a solution that they developed in collaboration with GE.

3. In 2005, Christopher Michael Connor wrote a research paper on how Integration of IT and physical security can be achieved by using Microsoft active directory.
4. In 2006, Edward Stead came up with a conceptual model for a product that integrated physical access control and IT security using Microsoft Active Directory.
5. In 2006, Sun Microsystems came up with a conceptual model for a product called Sun and Actividentity which was to help customers in solving the convergence challenge.

There has been no attempt to explore on the factors that hinder integration of security infrastructure in commercial banks. The main aim of the study will be to determine the factors that hinder the integration of physical access control and cyber security in financial institutions in Kenya and develop a conceptual framework that will guide the banks in the process of integration.

1.4 RESEARCH OBJECTIVES

The study is guided by the following objectives;

i) To establish the factors that determine the attitude of banking institutions towards integration of physical access control and cyber security.

ii) To establish the factors that determine the intention of banking institutions to integrate the two security functions.

iii) To determine the sources of pressure that would influence integration of the two security functions.

iv) To establish the factors hindering integration of physical access control and cyber security in banking institutions in Kenya.

v) To develop a conceptual framework that will guide the implementation of existing security integration solutions.

1.5 SIGNIFICANCE AND PURPOSE OF THE STUDY

This study focuses on identifying factors that hinder integration of physical access control and cyber security in financial institutions in Kenya. The study also determines factors that determine bank's attitude towards adopting the integrated security model, factors that determines the intention of the banks' to integrate physical access control and cyber security and the possible sources of pressure that would push financial institutions to converge their security functions. In addition, the study also develops a conceptual framework that can be used as a guide by financial institutions during the implementation of the integrated security framework.

1.6 HOW RESEARCH OBJECTIVES WILL BE ACHIEVED

Table 1 how objectives will be achieved

Objectives	**How to achieve the objectives.**
To establish the factors that determine the attitude of banking institutions towards integration of physical access control and cyber security.	Assessment of the physical access control and cyber security in banks.
To establish the factors that determine the intention of banking institutions to integrate the two security functions.	Assessment of the physical access control and cyber security in banks.
To determine the sources of pressure that would influence integration of the two security functions.	Assessment of the physical access control and cyber security in banks.
To establish the factors hindering integration of physical access control and cyber security in banking institutions in Kenya.	Assessment of the physical access control and cyber security in banks.
To develop a conceptual framework that will guide the implementation of existing security integration solutions.	Proposed conceptual framework

CHAPTER TWO

LITERATURE REVIEW

In spite of physical access control and logical security depending on each other, a big number of organizations still treat the two as separate functions. This was justifiable since the technology needed to converge the two was not available. Until recently when a variety of readily available products that will aid the integration were developed. Most companies have three security control centers i.e. network security which manages the security of all network operations, information Security which is in charge of security of both stored data and that which is in transit and physical security whose function involves CCTV control and access control. The problem trickles down to the governance structure, which should make prioritize creating one unit for security procedures, guidelines, policies, processes and deployment.

As long as companies manage their physical access control and IT security functions independently, very little hope is left of securing them. The convergence of logical and physical access security has already been implemented at the functional level. It just might be the right time to implement the convergence at the structural level. Physical access control and cyber security technologies have grown to the extent that they can now be converged (Scott Borg, 2010).

The evolution of the legacy sensor appliances from the IP network to TCP/IP has helped to drive this transformation. Security cameras and access card readers now use network protocols and policies, procedures and access lists are now saved by computers which means they can be generated when need be. PCI (Payment Card Industry) is amongst the latest innovative security policies available. Both physical access control and cyber security are included as part of the policy.

Logical security greatly depends on physical security. Attackers always take advantage of physical access gained to any computing equipment which always assists them to further their attempts.

Gaining access to a physical station where a USB stick can be inserted is adequate for the attackers to launch an attack. Any device linked to the network must be secured to ensure that attackers do not manage to turn it into an aiding tool in an attack.

The following are challenges that emerge as a result of lack of convergence between physical access control and IT security:

I. No single system to ascertain an individual's identity. This is because each security division has its own independent identity system and database.

II. Increase in potential for theft and attacks.

III. Inadequate IT management and implementation of standards applied to physical access control systems, or not implementing the standards consistently across all units in the organization.

IV. Inadequate physical monitoring of IT security gadgets that can sense tampering. This would help attackers in gaining unauthorized access to a cyber-security gadget console.

2.1 OVERVIEW

In the present day, security can be referring to either IT security (also known as cyber / logical security) which involves prevention of unauthorized network access and virus detection or physical security that mainly involves access control. The units that manage the operations and technology for the two security disciplines are completely separate, and more often than not never work together. The growth of IP integration on the network can have a great effect on the units, safety and security of an enterprise.

The purpose of this research is to describe the history and upcoming developments of cyber security and physical access control management, find out the reasons behind the need for the two units to work together, and why having a concrete security foundation is critical to a strong security posture. A concrete security policy begins at the top.

Having a single, sophisticated unit responsible for an all-inclusive security policy that includes both physical access control and cyber security is essential. Getting managerial support and sponsorship from the CSO or CIO, the main governing team, is essential. Cross-departmental collaboration between the two security teams for creation of the policy and requirements analysis will ensure that the specific requirements for the two security departments are put into consideration. Formulating the security policy independently deters the ability to efficiently deploy the policies.

2.1.2 THEORIES TO BE REFERENCED TO.

In this research, I will be using the general system theory, the diffusion of innovation theory and the theory of reasoned action.

Diffusion of innovation theory

Diffusion of innovations is a theory that seeks to explain how, why, and at what rate new ideas and technology is adopted.

Rogers (2010) highlights the main components that influenced on the adoption of a new idea, which include; the innovation itself, communication channels, time, and a social system. This is largely dependent of human resources. For a new idea to gain sustainability, it needs to be extensive spread and self-sustained (Gerrard and Cunningham, 2003). Within the rate of adoption, there is a point where an innovation reaches the saturation level.

According to Rodgers (2010), there are groups of adopters classified as; innovators, early adopters, early majority, late majority, and laggards. The concept of diffusion exhibits itself in many ways and is subject to the type of adopters and innovation-decision process.

The criterion for the adopter categorization is innovativeness, defined as the degree to which an individual adopts a new idea.

The diagram below shows the different groups of adopters as derived by Rogers.

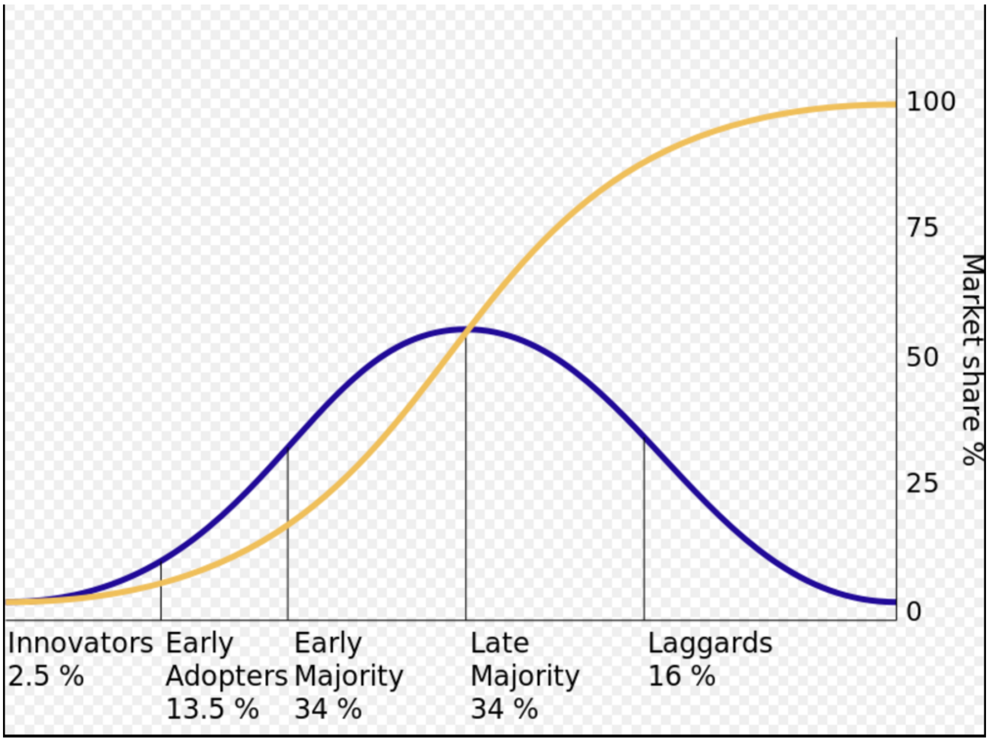


Figure 1..source: Diffusion of Innovations, fifth edition by Everett M. Rogers.

Scholars notably; Md Nor, Pearson and Ahmed (2010), Kolodinsky, Hogarth and Hilgert (2004) looked at the Innovation of Diffusion theory in the banking sector with an emphasis on the adoption and utilization of internet and mobile banking technologies.

This theory will be used later in this chapter to analyze the integration of the two security functions in the Kenya's banking sector.

The general system theory.

This theory was pitched in the 1936 by the biologist Ludwig von Bertalanffy, and further developed by Ross Ashby. Von Bertalanffy (1972) was both exploring on the reduction concept and attempting to revive the unity of science. He stressed that real systems are exposed to interaction with their environments, and that they can acquire qualitatively new properties through emergence, resulting in continual evolution.

According to Boulding (1956), instead of reducing an entity (e.g. the human body) to the properties of its numerous components (e.g. organs or cells), systems theory centers on the arrangement of and relations between the parts which connect them into a whole (cf. holism). This individual organizational setup, defines a system, which is separate of the concrete substance of the elements (e.g. particles, cells, transistors, people, etc.).

In addition, similar terminologies and philosophies of organization underlie the different disciplines (physics, biology, technology, sociology, etc.), providing a basis for their unification. Systems concepts include: system-environment boundary, input, output, process, state, hierarchy, goal-directedness, and information.

An information system is an example of the interaction of multiple elements as envisioned by the general system theory.

While borrowing from the general system theory, a system can be observed as a complete structure and not merely as the sum of its parts. The connection between systems and their components can be appreciated as the main source of complexity and interdependence. In most cases, the properties of the whole cannot be known and understood from analysis of the components in isolation. In this scenario, security is the system and physical access control and cyber security are the parts that make up the security function.

For one to get an optimized security function in an organization, you have to integrate the two into one which will then be governed by one general policy.

The concepts from this theory will be used in deriving the questions that will be included in the questionnaire with the aim of the finding out the factors hindering integration of physical access control and cyber security in banks.

Theory of reasoned action.

The theory of reasoned action was developed by Martin Fishbein and Icek Ajzen in 1967. The theory assumes that, the individual behavior of a person is driven by behavioral intentions where behavioral intentions are derived from personal attitude toward the behavior and the subjective norms that constrain the performance of the behavior (Hennessey, 2012). Attitude which forms a basis for a behavior is defined as the individual's positive or negative feelings about performing a behavior. It is determined through an assessment of one's beliefs regarding the consequences arising from a behavior and an evaluation of the desirability of these consequences.

The diagram below represents the concepts that make up the theory of reasoned action.

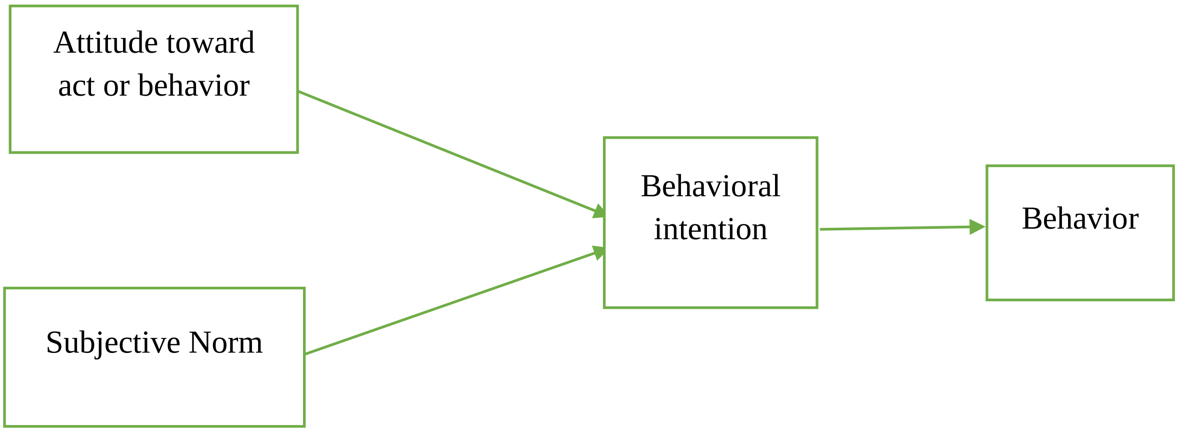


Figure 2 source: Fishbein, M., & Ajzen, I.

This theory will be used to determine the factors that hinder the integration of physical access control and cyber security in banking institutions in Kenya. This will be used to determine the attitude of the security practitioners towards integrating the two security functions and whether they intend to integrate the two security functions in the near future. It will also help in determining what strategy would be followed for the banking institutions in the case where they opted to integrate their security function.

2.2 THE IMPORTANCE OF SECURITY SYSTEMS INTEGRATION

Evidence exists to highlight the positive effect felt as a result of aligning security systems in an integrated framework (Choo, 2011).

According to Aberdeen Group (2011), integration of security systems wields numerous benefits, including; improved physical access control, improved IT security, sustained and improved compliance, faster response times during security incidents, lower total costs in managing the two security units and enhanced collaboration between their IT security and physical access control teams. The findings also showed that initiatives in converging physical access control and IT security are already assisting most companies to achieve improved and superior performance in a number of critical areas and some of the findings were listed in the table 2.

Table 2 Benefits of Security Systems integration

Outcome	**Details**
Improved physical security	83% of all the companies which have converged their security units experience a decrease in the number of actual physical access control incidents, 40% had a decrease in the average time used in handling these incidents and 27% spent less in addressing them. Companies that have their security functions as independent units experienced an increase in the physical access control incidents and the total time used in handling them which in turn lead to an increase in costs incurred.
Improved logical security	48% of all the companies that integrated their security units experienced a decrease in the number of actual physical access control incidents, 31% had a decrease in the average time used in handling these incidents and 22% spent less in addressing them. Companies that have their security functions as independent units experienced an increase in the physical access control incidents and the total time used in handling them which in turn lead to an increase in costs incurred.
Improved compliance	55% of all the companies which have converged their security units experience a decrease in the number of actual non-compliance incidents (this refers to failed audits), 59% had a decrease in the average time used in handling these incidents and 35% spent less in addressing them. Companies that have their security functions as independent units experienced an increase in the physical access control incidents and the total time used in

	handling them which in turn lead to an increase in costs incurred.
Improved collaboration	57% of all the companies which have converged their security units experienced improvement in communication between the IT security and physical access control teams, 36% improved the management of responses to security breaches by their security units.

Source (Aberdeen Group, 2010)

2.2.1 The administrative perspective of security integration

Why should the two security units converge? This truthfully reflects the opinion of most security experts. In reference to a common phrase, the above convergence question focuses on the trees rather than the forest. The convergence must start with the management of physical access control and IT security integrating. A brick wall and a database cannot be integrated. Nonetheless, the management of the people authorized to get past the wall and inside the database must be integrated, failure to which gaps will exist in the company's security function.

The convergence of physical access control and cyber security should be thought of in the line of integration of physical access control and IT security management.

Figure 3 below illustrates the concept of converged security management.

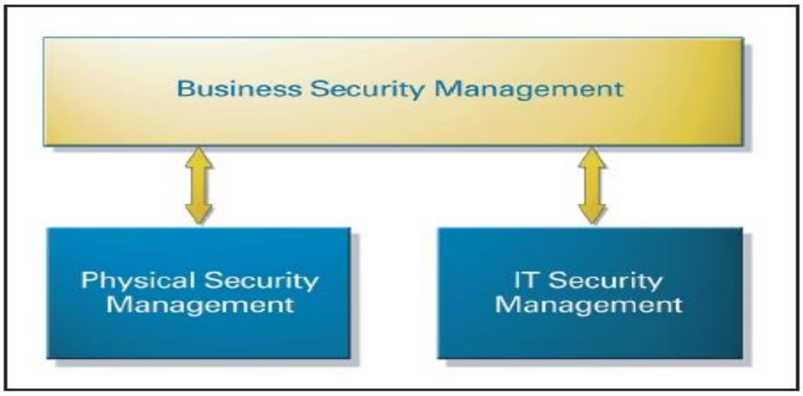


Figure 3 Source: PhysBITS document provided by the Open Security Exchange

In most banking institutions, the physical access control and logical security units function independently. They most times are uninformed of the strengths and weaknesses of one another, the dangers of their functions being independent and the benefits of converging.

Integrating Security Management.

The application of security policies, procedures and processes helps in achieving security objectives. Figure 4 below defines the key processes in security management which involves physical access control and cyber security technologies and processes.

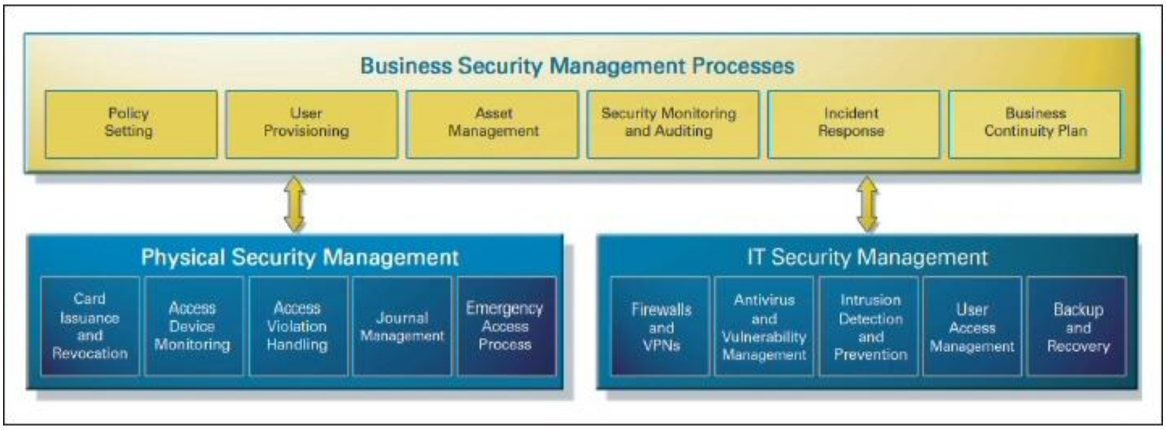


Figure 4 Source: PhysBITS document provided by the Open Security Exchange

Most of the physical access control and logical security procedures and processes need be converged at the technology level. However, the technology does not define the integration. The procedures and processes define it while it is implemented by the technology. This gives more reason as to why analysis of business requirements that are security-related and the physical access control and logical security processes and procedures that support them should be the first step in converging physical access control and cyber security.

The absence of technical convergence between cyber security and physical access control systems has caused gaps in the organization and procedures for most enterprises in the world (Faulkner, 2005). Very few companies have adopted an all-inclusive security strategy incorporating both physical access control and cyber security. Among the few that have an all-inclusive security strategy are a few government agencies.

From a structural view, very few companies have approved processes and procedures implemented in the different units handling physical access control and logical security. This has resulted in extreme risk exposure due to the absence of manageability.

2.2.2 Market drivers.

A number of market drivers are causing a substantial instance of convergence.

These include:

1. According to the ("HSPD-12) the homeland security presidential directive 12, it is compulsory for all US federal agencies to issue a PIV (personal identity) card to all staff. It is expected that the PIV cards are to be adopted by additional large user organizations.

   Tim Gower, an expert from Datamonitor, a London research company, predicts significant growth in the total number of PIV's issued by large organizations to their staff. According to Tim, it is likely that this category will increase to 36 million in 2006 from 14 million in 2002. NEC, IBM, Microsoft, shell, Sun Microsystems, Nissan and Schlumberger are examples of organizations that have issued the identification cards to their staff.

   Boeing, Procter & Gamble and Pfizer are among firms that are embarking on a pilot Project to substitute company badges with PIV smart cards. Government organizations have also helped in boosting PIV smart card through a rollout of 4 million smart access cards that the US unit of defense has issued to its military and civilian personnel.

   In 2009, the secretary of defense gave directions that Military Services should implement Common Access Card (CAC) which are smart cards. The cards have numerous functions such as combining a number of cards into one (Lacey, 2009).

   Besides replacing the existing identification cards, the CAC grants physical access to premises and restricted areas, gives access to network resources and organizational systems as well as serve as the platform for the PKI (Public Key Infrastructure) token.

   The main benefit of this deployment is the automation of processes that were paper-based before the implementation of CAC. Processes that took days to do now take hours.

   The card issued to military employees is being used to get into the military premises, to access network resources in the defense domain, verify eligibility of their medical benefits and access the dining privileges in their premises.

   The implementation of the cards and the PKI not only contributes to increasing personal security, but also to enhanced national security (NCSC, 2014)

Although indirectly motivated by the HSPD-12 compliance directive, many profitable companies worldwide are also implementing solutions that converge physical access control management and cyber security on a standardized smart card based credential.

2. In the back-end, most of the emerging cases of integration are encouraged by improvements in risk management and visibility through correlation of both IT security and physical access control information and events. This is achieved with the help of normalization, consolidated collection and the Security information and event management (SIEM) solution.

   The use of the E-SSO (enterprise single sign-on) solution has also made a major contribution in the discovering of new and innovative use cases in cyber security/ physical access control integration (NCSC,2014; Aberdeen Group, 2017).

3. Integration examples are also being compelled by new network-enabled physical access control solutions in areas such as building automation, building access, video surveillance, video analytics, data acquisition systems and supervisory control.

   Planning, policy, processes and organizational politics also play a major role in the effective convergence. Aberdeen's research done in 2007 on risk management and security governance indicated that by taking an all-inclusive view of risk, most leading companies have proven their ability to improve security as a whole, be in line with their compliance expectations, benefit the most from IT resources in use, make faster and better decisions, enhance business processes and improve visibility across the organization (Aberdeen Group, 2017).

2.2.3 Before and after review

Before the integration of devices, applications and services on the IP network, security processes were completely detached:

- Video surveillance mainly covered the dedicated analog connections.
- Physical access to the premises was managed across a completely isolated network instead of LAN, as it is done today
- Firewalls were in charge of Intrusion prevention.
- Intrusion detection and virus scanning was done on the user's desktops.
- E-mail and web security acceptable use policies were set only for internal users. This exposed the network to the threat of computer viruses and worms coming from external parties who are in communication with internal staff.

The integration of voice/video/data has caused changes to each of the above areas as described below:

- Voice: In addition to traffic formed by setting up VoIP services (voice-over-IP), voice is now used to refer to audio sources such as monitoring of a crowd, a gunshot in a high crime area or detection of noise in an office block that is meant to be vacant at a given time.
- Video: Video now refers to traffic cameras, video surveillance, streaming video, and digital signage.
- Data: The rampant use of cloud services means that data is not only accessed through the intranet. One can access it from anywhere through a device as long as you are connected to the internet. Most devices are now heterogeneous since you can connect to the network and the device will serve more than one purpose.

  Enterprise collaboration through Social media also plays a big role in the timely reporting of security incidents. According to the IMS Research, whose main aim was to find out the number of devices that have internet connectivity ability, the devices that are connected to the internet were over 5 billion in 2010. This figure is likely to get to 22 billion by 2020. This trend shows the outburst of personal devices which include tablets, laptops, smart-phones. This is inclusive of all the cameras, sensors and devices used in security operations that are now IP-enabled due to their integration into the IP network (Kurt, 2015; Raytheon, 2015).

This massive integration can have an undesirable impact on the network's performance. This will occur if the network has not been accurately designed and deployed in such a way that it can handle the increase in traffic (Symantec, 2012; Aberdeen Group, 2017). Despite presenting new challenges in security, the integration of devices inter-connected through the Internet, video, voice and data also provides ways to converge cyber security and physical access control which was not possible a few years ago.

2.2.4 Emerging vulnerabilities.

A security system for a seaport would include gate access control, smart fences, cameras and an SMS (security management system) which would all be networked and monitored over a PC.

Networking in this scenario could be done either over dedicated networks or traditionally. The dedicated network could be over a standard network with TCP/IP routers, switches, servers, and PCs. The network may also incorporate wireless or cellular elements (Kurt, 2015).

The network described above is vulnerable and exposed to cyber threats. This is due to the following reasons:

- Physical exposure – The security devices are physically accessible. This is because they are installed outdoors and close to perimeter walls.

- Lack of awareness – Most network security practitioners trust that their networks are safe since they are separated.

- Lack of skills – Most traditional physical security practitioners lack skills and knowledge in IT technology, let alone logical security.

- Division of responsibility – In many companies, logical security and physical access control are separately managed, meaning that no one sees the holistic picture.

- Market fragmentation – The market for the security equipment market is exceedingly fragmented.

This means that most of the industry players are small and less likely to invest in strengthening their systems which would make them less vulnerable the emerging cyber threats.

The Hybrid Cyber/ Physical Threat

Experience from the past, shows that intruders chose to execute logical or a mixed logical/physical intrusion, other than a pure physical or pure logical one (NCSC, 2014).

As an alternative, hackers take on a number of actions that are as effective instead of taking the great risk of actively gaining access through a gate or a fence. The actions are described below:

- Neutralizing alerts – This is achieved by saturating or blocking alarms on the smart fence.

- Generating false perceptions – This is done by freezing of video on IP cameras or streaming recorded surveillance footage to the physical guard’s monitor.

• Making fake identities – This involves the remote creation of an access card.

• Hacking onsite systems – This is done by creating an outage or power black-out which will affect the fire alarms, elevators and even cause damage to the production systems.

In the above mentioned situations, the cyber-attacks will go totally undetected. No one will be aware that an attack has occurred since no flag is raised during the attack.

This means that no measures will be taken to further strengthen the security of the systems hence the systems vulnerability will remain (NCSC, 2015).

The way forward.

Below are a number of the solutions that can solve the problem described above:

1. **Converged PSIM (Physical Security Information Management) with CMS (Card management System).**

Convergence of PSIM (Physical Security Information Management) and card management systems is the expected change which will ensure better state awareness and effective use of security resources (cameras, 24/7 guards, communication and escalation processes).

Despite IT security attacks posing a new kind of threat to industrial security control systems, an all-inclusive strategy that considers both logical security and physical access control is achievable.

2. **Common Authenticator.**

The integration typically puts into use a common credential to authenticate. The most commonly used authenticator is the smart card (Miller, 2009; Kurt, 2015). The card made of two interfaces. These include the contact and contactless interfaces which use the same storage which provides superior functionality. The contactless interface is used for physical access control. Users place the card near a door reader when using the contactless part of the card. The physical access control system only opens the door when the authentication process is successful. This authentication process and subsequent access is referred to as badging.
The contact interface of the smart card is used to grant users' access to their PC's. Most of these cards have separate storage mechanisms for the contact and contactless interfaces (Kurt, 2015). The other type of authenticator that is commonly used is biometrics. In collation to the

access cards, biometric devices are mainly fingerprint scanners that are rarely used for physical access control. However, a few high security environs use them.

The fingerprint readers are normally used to authenticate in the contact interface of the cards which grants the users IT access.

The use of the common authenticator can be implemented as a solution to converging physical access control and IT security. This will help in enhancing user lifecycle management, contextual authorization and information security management and as described below.

3. User lifecycle management.

This helps in improving efficiency and boosting compliance benefits and security. The improved efficiency is more evident when the CMS is converged with the systems (Lacey, 2009). New staff are granted access to IT and physical resources in an appropriate way. When a user resigns from the firm or is terminated by the firm, their access is promptly and timely terminated in both the IT and physical resources. This procedure provides a framework that supports role based access which thus enhances the compliance efforts (Miller, 2009).

4. Security information management.

SIM (Security information management) systems are becoming a necessity in most organizations. This is because they consolidate and associate user activity which helps in providing an all-inclusive view of activities by the users across the network (Tarino, 2009).

This in return enhances compliance and simplifies the forensic processes when need be. While the convergence of cyber security audit events into security information management systems is fairly direct, inclusion of security events from physical access control systems is a move which highly depends on the maturity level of the physical access control system (Kurt, 2015). However, convergence can be implemented and will be necessary for raising an alarm in the case of potential security incidents.

The security information management system can link security events from a physical access control system with the UNIX system and manage to detect when an employee has left the building but makes an attempt to log in to the UNIX system console within the disaster recovery site (Raytheon, 2015). Likewise, the SIM system can link events from physical access control system to those of Microsoft Windows.

This will enable the system to identify an employee who has accessed the physical premises the New York campus but has authenticated to the active directory through a computer in Los Angeles.

5. Contextual authorization.

The main goal of Physical access control and IT security contextual authorization is to prevent an employee from authenticating through a New York workstation where as she has badged into the Chicago office. A good example of an existing product that applies contextual authorization is Imprivata's One Sign which has the ability to deny a user access to the active directory and other IT network resources and platforms based on whether the employee has badged into the physical premises (Miller, 2009).

2.2.5 Organizations that are already integrating their security functions

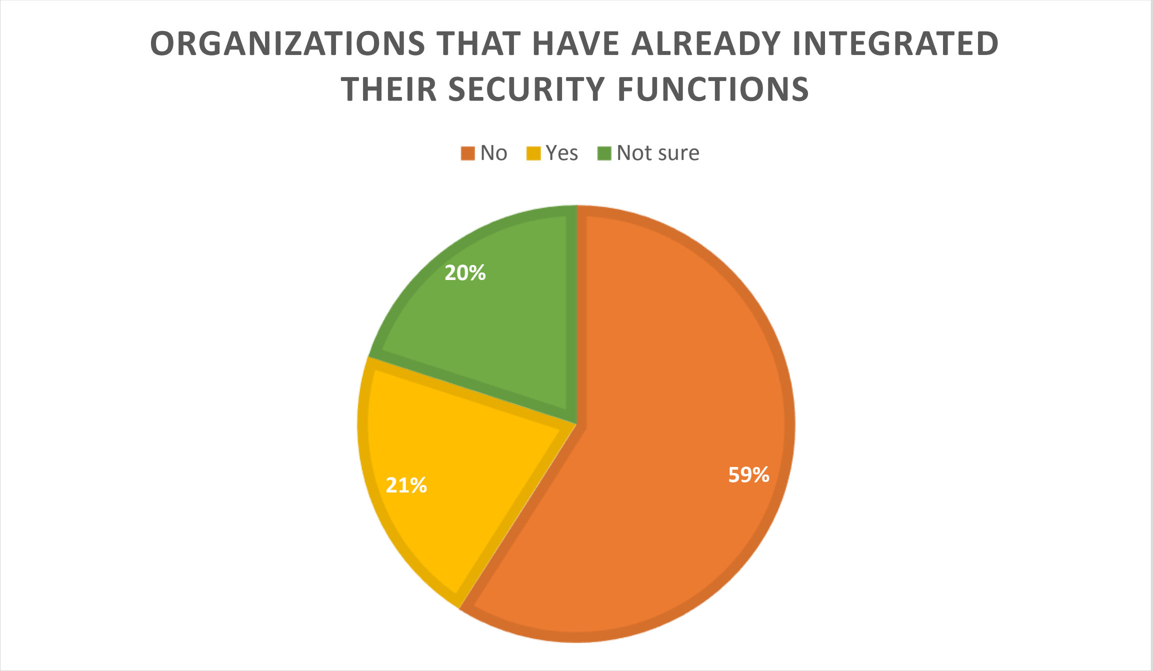


Figure 5 Source: Aladdin Knowledge systems 2002

The figure above shows the percentage of organizations that have converged their security functions (21%), those that haven’t converged (20%) and those that are not sure whether their security teams are integrated (59%). This was an analysis that was carried out by the Aladdin knowledge system.

The New York State is one of the government agencies that has integrated their security units**.** This has been done through the formation of a new department known as the Center for

Internet Security which mainly deals with merging cyber security and physical access control. This will help the government in dealing with emerging threats (NCSC, 2014).

The Integrated Intelligence Center, which is the new department, has implemented a converged approach which is making a major contribution in creating a trustworthy relationship between the government and organizations in the private sector. This has helped the government in developing and circulating critical information.

The main aim of the new department is to leverage the information that the CIS has obtained from the Multi-State Information Sharing and Analysis Center. This in combination with the information availed by participating partners will offer reliable intelligence products.

The unit intends to put into good use the information gathered. Physical access control and cybersecurity can no longer be viewed separately as an attack on a firm's systems can cause failure of physical infrastructure.

Rich Licht, the executive director stated that the convergence process was initiated in 2009. The process began by having monthly meetings whose main agenda was to analyze the risks and threats that they were exposed to. They also tried to brain storm on the best ways of securing the environment so as to ensure that the risks are mitigated. After holding many meetings, the convergence was implemented. This was successful due to the help received from their partners who include the FBI (Federal Bureau of Investigation) and the department of homeland security (Kurt, 2015).

In the African continent, no organizations have made public their intention to integrate the two security disciplines. However recommendations on the same have been made by IT security professionals who recognize the need for the convergence. One such professional is Sanjay Vaid who is the director, cyber security and risk at Wipro Limited which is a global IT consulting and outsourcing company. He states that new and emerging technologies such as internet of things (IOT) opens up organizations in the African continent to major risks and threats. He insists that it is essential for companies to have an all-inclusive approach as it will help in tightly securing everything from networks, to data centers, Identity & Access to infrastructure, endpoints and more (Sanjay Vaid, 2009).

To reinforce all this, it will be important to focus on converged security so as to get a clear understanding of the various attacks that the firms are vulnerable to.

As a way of preparing for the future, he suggests that a company's IT partner must have an all-encompassing cyber-security practice which must cover every part of the threat landscape. It is also essential to involve the best experts in the security disciplines. He also states that it is important for these IT organizations to include a converged security practice which should include Global security & risk intelligence centers monitoring the risk and threat landscape (Sanjay Vaid, 2009).

This can only be accomplished with the help of expert engineers who have diverse experience in deployment, monitoring, detection and prevention experience.

He recommends that reviewing the current information technology environment and breaking down the security disciplines should be the starting point.

The security environment should be analyzed in terms of infrastructure, endpoint, network, physical and IT security (Kurt, 2015). The tools used to secure the components of the security environment should also be thoroughly analyzed.

This would then be followed by reviewing the IT and security environments in the line of the company's strategy, government and industrial compliances. The broad analysis and audit for the tools and architecture would be the next step, followed by recommendations, a roadmap and policies to guide the process would be used by the organization. By designing, implementing, and managing the new policies and procedures in the best way, Sanjay is certain that the companies can be assured that potential risks and threats are reduced (Sanjay Vaid, 2009). This will help the organizations to stay one step ahead of attackers.

As per the 2013 Norton report, South Africa was ranked as the third highest among the countries with the highest cybercrime victims. Despite this, no integration efforts have been made so far.

An incident once occurred in a bank in South Africa where R11 million was stolen. The break in involved more than five people who stormed the financial institution's depot in Midrand where they first disconnected the alarm. This allowed them to get access to the physical premises without raising a flag to the physical access control system. They then were able to open the vault and escape with the money.

The burglars committed a mixed cyber/physical invasion which involved deactivating alerts by saturating alarms from the physical access control system and making forged identities through remote creation of a smart access card. Similar incidents can be stopped by centralizing security management (Miller, 2009). The burglars could not have gained access to the vault since only the authorized staff could access it and they had not been flagged as having entered the premises. Thus the physical access control that gives access to the vault would have denied them access.

In Kenya, no organizations have made public their intention to integrate the two security disciplines. However discussions on the same have been held.

One such discussion was held on 28th May 2015 in a meeting where IT leaders in the country were present. The IT leaders recognized the need to integrate physical access control and cyber security. They pinpointed that in top performing companies, the union between Physical access control, Information Security and information technology is achieved through integration that is followed by an all-inclusive risk management and strategy at top levels. Strategic collaboration in relevant ongoing operations and projects and are a few methods that can help in achieving the integration. However, most companies are still tussling with organizational and technical integration challenges.

This is due to the scanty knowledge that the practitioners have, thus prompting them to work re-actively which involves handling problems as they arise. This is done without trying to transform their firm into a stronger position and without understanding the whole integration setting (Kurt, 2015).

In reference to the diffusion of innovation theory, Kenya is not in a position to be analyzed in terms of the different classes of adopters. This is because the idea of integrating the two security functions is yet to be fully embraced and implemented in the Kenyan banking sector as explained above.

2.2.6 Benefits of centralized management.

Managing staff, their approved rights on the systems and their access credentials—a process known as user provisioning—is amongst some of the greatest challenges that companies are facing. Usually the human resources department creates the first record entry for a new employee. This is meant to facilitate payroll processing and other staff-related functions. This is followed by the security department making a second entry which is meant to grant the user access to the physical premises with the help of an access control card also known as an ID badge (Ula et al., 2011). The IT department then makes the final entry which grants the user access to the approved information systems. The separate entries result in inconsistencies amongst the three units. The inconsistencies range from user's inconvenience such as a user being denied access to the computer network or parking, to substantial organizational risk such as failure to deactivate network and physical access rights instantly upon termination (Miller, 2009).

The above discrepancies motivate former employees to circumvent security by affording access to the physical premises mainly done through tail gating or sharing access credentials used to gain access to the network and system resources.

This more often than not enables the former employee to gain access to information, systems and areas that they are not authorized to. Such access violations more often than not are never documented.

The lack of centralized user provisioning management makes it difficult to answer questions such as “Who has access to what resources”. The above question cannot be responded to fast enough to offer perfect response time in the case of a security breach.

Decreasing the staff provisioning stages down to one from three will not only do away with the security weaknesses and implement consistent role-based access across the company. This in the long run will significantly decrease the cost of user management.

Integrating physical access to the premises and network access also makes it easier for companies to get rid of a user's access rights in the security system simultaneously (Lacey, 2009; Murari & Tater, 2014). This will be essential when a user is fired or resigns. In most cases, there is always a gap of weeks or at times even months between the last day of employment and when access to the physical premises or the network and IT access is deactivated. The likelihood of a security breach at such a time is very high. This is because security can easily be compromised as resentful former staff could remotely access the network, or in other cases, gain access to the premises and steal sensitive and confidential information. Integration prevents this by enabling companies to disable all physical and system access concurrently (NCSC, 2014).

NCSC (2014) and Raytheon (2015) list other benefits of integrating physical access control and logical security including;

- Having one system that manages all cyber security and physical access control which includes an efficient workflow for adding, deactivating and amending employees’ identities. The integration of user authentication and identity management technologies such as biometrics, tokens, with physical access control technologies, such as proximity or magnetic readers and cards will enable companies to create and manage one consolidated database for all authentication credentials. This will also help by having a centralized way of granting access rights for both IT and physical resources.

- A combined network strategy and policy for local and remote network access that gets status information and location from physical access control systems.

  The convergence of physical premises access with IT and network security enables the two technologies to compliment and fortify each other.

  Synchronized management of the two functions creates a robust, more converged security, as integration enables companies to manage logical security and physical access as one.

  A good example of this practice is where organizations allow their staff to access network resources only after accessing the physical premises using their employee smart cards.

  This stops people from accessing the IT/ network resources when out of the office. The system will know that the user in this case is in the building and ought not to be accessing the network remotely.

- Enhances employees access and assists in solving privacy issues; In addition, a converged security also helps in preventing tailgating. This is when a worker follows another worker into the premises without swiping their access card; or when an unauthorized individual closely follows an employee in without getting authorized access or signing in as a visitor. By interlinking IT access to physical access, the staff are forced to badge in everyday so that they can access IT resources. To enhance this further, a rule can be set up to alert the physical access control unit whenever an employee or an unauthorized person who has not badged in attempts to access IT or network resources.
- An affordable and practical dual authentication method; another advantage of integrating security functions is that it enables organizations to implement dual authentication. This refers to a security system that involves combining use of complex passwords with a second type of identification. By converging cyber security and physical access control, existing tools can be put to use instead of forcing firms to spend more money so as to substitute staff badges with biometric readers.

- This practice has a greater return on investment as compared to the existing infrastructure.
- Improved management of security resources in emergency situations; with cyber security and physical access control systems fully converged, immediate response to network alarms during emergency situations has now been made possible.

  This is due the fact that integration makes it possible to consolidate logs from the two security systems with those of access records.

  This thus makes it easier for organizations to maintain an upto date occupancy record, knowing precisely where their staff are in case of a crisis.

- Simplify forensic investigations; integrated security solutions are also essential tools for IT auditors.

  It is exceedingly hard to recreate a timeline of access to the premises and network. This is due to the fact that the log that maintains the record of employees who access a building is kept within the physical access control system; the network access log is locked in the network access list. The two security systems maintain their own independent logs of each time an employee gains access to the systems. An integrated system supports forensic timelines by supporting converged event and report creation. The integration gateway gathers information from all systems, thus enabling it to recreate the entire log of events. This includes how the employee badged into the building, logged onto the network, the authentication mode used, the network user identity used and how long the employee was active on the network.

- In cases where single sign-on is in use, the system is also able to track applications that the employee accessed, either through the local network or remotely.
- Assists with organizational compliance efforts. Currently, there are many government restrictions and regulations being placed on firms in respect to releasing financial information, reporting the company’s performance and protecting customer/employee information. This has led to most organizations implementing security solutions that will enhance their compliance efforts (Kurt, 2015). Integrated security solutions enable companies to conform to data collection and data protection laws like the GLBA (the Gramm-Leach-Bliley Act), HIPAA (Health Insurance Portability and

Accountability Act), HSPD-12 (Homeland Security Presidential Directive), Sarbanes-Oxley among others. The integrated security can help in preventing unauthorized access to information by granting access only to authorized people.

2.2.7 Challenges of integration

Despite having ready solution systems to the issue of integrating physical and cyber security, it is rare to find firms that have their security levers converged.

This is as a result of challenges that have slowed down their intention to converge the two security functions. The challenges include:

- Companies are focusing on technology concerns instead of prioritizing security management issues
- Lack of standards
- Physical security resources in most companies are reluctant to embrace IT.
- Firms luck a roadmap to guide them for the integration of the two security levers.
- The physical access control and logical security units are totally independent and separated in terms of the organization structure. This is a challenge as the two teams have different work cultures and reporting structures. The division is evident even in their recognition by the rest of the units. Physical security personnel are merely referred to as the security staff while the cyber security staff are commonly referred to as geeks.
- Apart from having structural challenges, some physical issues also exist. As a result of mergers and acquisitions, most blue chip firms have patchworks of physical access control systems at the different phases of the of maturity.

  For example, a firm that has multiple locations worldwide might have old physical access technology implemented (such as the commonly used lock and key technology). When such a firm is merged to another that uses access cards, a patchwork issue will arise. This is due to the fact that their lacks an interface to integrate the two physical security technologies. This thus hinders the physical security and logical security integration. Another issue arises due to the multiple locations of the firm which all have different physical access control systems. This thus means that there is no common authenticator for employees who move between locations.

- Most companies do not have the technology that supports egress badging. Egress badging refers to a physical security setting where employees have to badge out on leaving the physical premises. Lack of this technologies makes it difficult for the firm to correlate events across physical and IT systems due to the uncertainty of the precise location of their employees.

  This is hindered by the IT challenges. For the convergence technology to be implemented, the firm has to deploy an access card middleware to all terminals. The middleware acts as a link between the operating system and applications (such as email clients, Web browsers and VPN clients) thus allowing communication with the access card. The middleware in some instances replaces the workstation's interactive logon component, commonly referred to as the GINA for Windows operating systems. Operating systems companies such as Microsoft have made integration possible by enhancing windows to easen smart access card deployment.

  This was made possible in the windows 2000 and other later versions of the windows operating system. This however still needs the deployment of the middleware which links the smart card to the operating system.
- Correlating the employee's physical and network locations is also a challenge. Network technology that includes wireless access points, VPNs, proxy servers, and network address translation makes it easy to find the employee’s exact network location. The physical access control systems also show the physical location of the employee. However, the lack of a link between the two systems makes it impossible to correlate physical and network locations.

2.2.8 Building for the Future

Organizations should start thinking of the benefits that could be drawn from implementing the integration solutions.

Many integration solutions are available in the market. For firms to implement the existing solutions, they need to review their security function and find out what their current security situation is and what security improvements are needed. This will help them determine what solution best suits them. (Aberdeen Group, 2017). During the review of the current security situation, firms should seek to find out if their existing security technology can be retained and interfaced with the existing integration solutions. If interfacing is possible, the firm will be saved the agony of having to replace the entire security technology that is currently implemented. This thus saves them from financial implications and disruption of work that comes with replacement of a system. Not only should firms think of the technology but also equipment interoperability. Organizations should also recognize the fact that the physical access control and cyber security functions have different work cultures, ideologies and views.

The integration process would work best if the existing integration technology is interfaced to what the organization has already invested in for both the physical access control and logical security (Staal, 2015). The integration should also not affect user's practices (other than tailgating) (Tarimo, 2006).

2.3 JUSTIFICATIONS FOR A FRAMEWORK APPROPRIATE FOR INTEGRATION OF SECURITY FUNCTIONS IN THE BANKING SECTOR

As stated earlier, no frameworks have been developed for the purpose of guiding organizations that wish to integrate their security departments. Previous research mainly dwelled around developing design models for products that will aid the convergence process, challenges faced in the integration process and importance of converging the two security disciplines.

Based on the above, it is necessary to develop a framework that will guide organizations that wish to implement existing integration solutions.

2.3.1 The conceptual framework.

In this section, a conceptual framework for convergence of physical access control and cyber security in Kenya is proposed. This has been developed by applying the industry best practice recommendations and guidelines as suggested in various standards, guidelines and literature by security researchers and practitioners.

2.3.2 Theories to be referenced to.

In this research, I will be using the general system theory, the diffusion of innovation theory and the theory of reasoned action.

Diffusion of innovation theory

This theory was used in the literature review to analyze the integration of the two security functions in the Kenya's banking sector. As gathered from the research, Kenya is still at the infant stage in the integration of physical access control and cyber security. This thus makes it difficult to categorize the adopters of the integration technology into the different adopter classes as described by Rodgers. The theory cannot also be used in developing the conceptual framework as the main intention of the research does not entail finding out the number of banking institutions belonging to the different adopter classes.

The general system theory.

An information system is a good example of many elements that interact as envisioned by the general system theory.

In reference to the general system theory, a system should be viewed holistically and not merely as the sum of its parts.

The connection between systems and their parts can be appreciated as the main source of complexity and interdependence. In most cases, the properties of the whole cannot be known and understood from analysis of the components in isolation. In this scenario, security is the system and physical access control and cyber security are the parts that make up the security function. For one to get an optimized security function in an organization, you have to integrate the two into one which will then be governed by one general policy.

The concepts from this theory will be used in deriving the questions that will be included in the questionnaire with the aim of the finding out the factors hindering integration of physical access control and cyber security in banks. The systems concepts include: system-environment boundary, input, output, process, state, hierarchy, goal-directedness, and information.

Theory of reasoned action.

The diagram below represents the concepts that make up the theory of reasoned action.

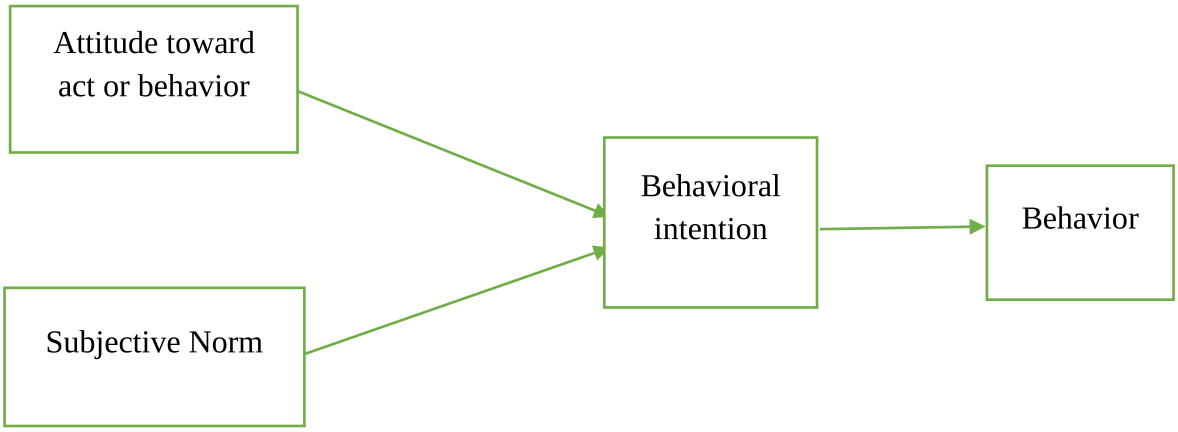


Figure 6 source: Fishbein, M., & Ajzen, I.

This theory will be used to determine the factors that hinder the integration of physical access control and cyber security in banking institutions in Kenya. This will be used to determine the attitude of the security practitioners towards integrating the two security functions, whether they intend to integrate the two security functions in the near future and if there are any forces that are putting pressure on the financial institutions to integrate the two security functions.

It will also help in determining what strategy would be followed for the banking institutions in the case where they opted to integrate their security function.

The conceptual framework has mainly been developed based on the independent and dependent variables that have been derived from the theory of reasoned action concepts that had been described in the literature review.

As explained earlier, the diffusion of innovation theory will not be a suitable theory given the fact that Kenya is still getting to understand the new innovation of integrating the two security functions.

This thus makes it challenging to classify the banking institutions in the different adopter classes as described by Rodgers. The theory cannot also be used in developing the conceptual framework as the main intention of the research does not entail finding out the number of banking institutions belonging to the different adopter classes.

The system theory will be used in deriving the questions that will be included in the questionnaire with the aim of the finding out the factors hindering integration of physical access control and cyber security in banks.

The conceptual framework will also be guided by the research objectives which include:

i. To establish the factors that determine the attitude of banking institutions towards integration of physical access control and cyber security.

ii. To establish the factors that determine the intention of banking institutions to integrate the two security functions.

iii. To determine the sources of pressure that would influence integration of the two security functions.

iv. To establish the factors hindering integration of physical access control and cyber security in banking institutions in Kenya.

v. To develop a conceptual framework that will guide the implementation of existing security integration solutions.

The above research objectives will be mapped to the relevant variables that will be included in the conceptual framework. The proposed framework will serve as a guide to the data collection process. It will be used to develop the data collection instrument that will be discussed in chapter three.

2.3.3 Independent and dependent variables.

The dependent variable in this research is the integrated cyber security and physical access control. The independent variables will be derived from the theory of reasoned action. Below are the independent variables as derived from the aforementioned theory:

Theory of reasoned action independent variables

The below variables have been derived from the 4 concepts of the theory of reasoned action which include: attitude towards an act/ behavior, subjective norm, behavioral intention, and behavior.

1. Attitude towards an act/ behavior: This refers to a mental state involving beliefs, feelings, values, and dispositions to act in certain ways. In this study, it will refer to the **attitude of the banking institutions towards integrating the two security functions**. In the research design, this will be used to find out what factors determine the attitude of banks towards integration of the security functions
2. Subjective norm: This is an individual's perception of social norms or his/her peers' beliefs about a behavior. It is a function of an individual's normative beliefs and motivation to comply with beliefs. In this study, it will refer to **pressure to the banks to integrate their security functions.** This will be used in the research design to find out what sources of pressure would push banks to integrate the security functions.
3. Behavioral intention: This refers to an indication of an individual's readiness to perform the behavior. In this study, it will refer to the **intention of the**

banking institutions to integrate the two security functions. This will be used in the research methodology to establish the factors that determine the financial institutions intention to integrate the two security functions.

4. Behavior: This refers to an individual’s observable response in a given situation with respect to a given target. In the integration context, this refers to the **integration of the two security functions**. This will be used in the research design to find out how best the banks can integrate the two security functions. This will be relevant only to banking institutions that have the intention to integrate the two security functions.

Below is the proposed conceptual framework:

Independent Variables **Dependent Variable**

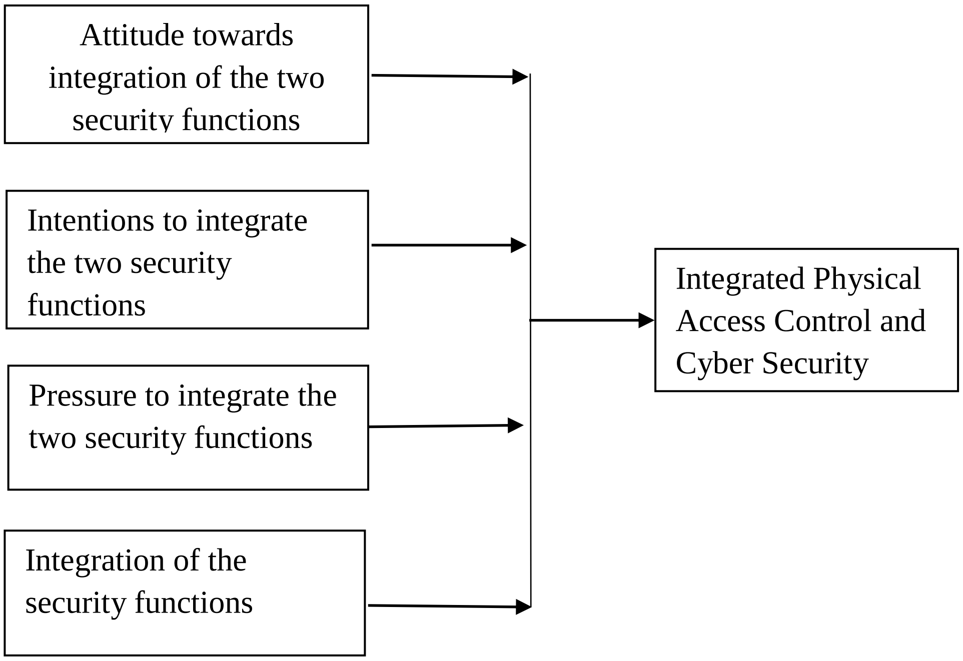

Attitude towards integration of the two security functions
Intentions to integrate the two security functions
Pressure to integrate the two security functions
Integration of the security functions
Integrated Physical Access Control and Cyber Security

Figure 7 Proposed conceptual framework

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 INTRODUCTION

This chapter defines the methodology that was used to indicate the research design, target population, sampling technique, data collection tool, and data analysis that was be utilized to investigate the factors hindering integration of physical access control and cyber security in banks in Kenya.

3.2 RESEARCH DESIGN

In order to investigate the factors hindering integration of physical access control and cyber security in banks in Kenya, a descriptive research design was adopted. A descriptive research design involves a detailed analysis of a group, or an individual or an institution with the aim being to establish relationships that have ensued to the behaviour of a study (Robson, 2002). The research will be centred on commercial banks in Kenya. This design is ideal due to the fact that it guarantees a complete description of the situation, thus reducing biasness in the process of data collection (Kothari, 2008).

Qualitative and quantitative research methods were utilized. Quantitative approach is valuable as it enables the use of structured questionnaire in data collection and makes it possible to measure variables and consequently use of descriptive statistics in presenting the findings (Algozzine & Hancock, 2016). The qualitative approach encompasses studies that make no attempt to quantify the results (Dawson, 2009). The choice of using qualitative data collection approach was influenced by the fact this design is flexible as it enables making changes and refining the research ideas as the study progresses (Dawson, 2009).

The qualitative method mainly involves subjective assessment of opinions, attitudes, and behaviour (Kothari, 2004).

The qualitative tool has the ability to evoke a more truthful touch of the research setting which cannot be gotten by using quantitative analysis. In this study, the qualitative technique to be used will be semi-structured interviews which will be used to assess the factors hindering integration of IT security and physical access control in Kenya's banking institutions as well as the practitioners' attitude towards integrating the two security functions.

3.3 TARGET POPULATION

The target population for this study comprises of the all the 43 banks in Kenya. The respondents covered by the study include employees in the IT security department and the physical access control department. This is because the study mainly revolves around the two security functions. According to the Kenya Bankers Association (KBA), there are about 5,400 employees working in Kenyan banks security units, which comprise of both cyber security and physical access control units (KBA, 2016).

3.4 SAMPLING PROCEDURE

The study utilized statistical calculation in determining the sample size. In any research, selected sample enables the researcher to make an overview about a given population. A sample is defined as subset of a population (Blumberg, Cooper & Shindler, 2014). This is however useful only if it accurately represents the larger population. Barbie and Mouton (2006) argues that a sample size refers to the actual respondents the researcher aims to interview. To ascertain that the selected sample is representative of a given population, a researcher needs to clearly describe the traits of the population, establish the required sample size and select the appropriate methodology for picking members from the population.

This study adopted Taro Yamane statistical formula for sample size determination that was introduced in 1967. The target population for this study was 5,400 bank employees working in the security units, both physical access control and cyber security (KBA, 2016).

Thus, the sample size calculation

$$n = \frac{N}{1+Ne^2}$$

Where, n = sample size, N = target Population, and e^2 = probability error (derived from the confidence interval).

The target population (N) was 5400, whereas the study settled for 90% confidence interval which means the probability error allowed was, 10% (0.1).

Therefore the calculation for the sample size;

$n = \frac{5400}{1+\ 5400(\ 0.1^2)}$

$n = \frac{5400}{1+5400(0.01)}$

$n = \frac{5400}{1+54} = \frac{5400}{55}$ = 98.18, round off to the nearest person, = 99 individuals

Thus, **n = 99 respondents**

3.5 DATA COLLECTION

Both primary and secondary data relating to factors hindering integration of the security functions in banks was collected. Questionnaires and semi-structured interviews were used to collect primary data. The questionnaire was preferred as the main data collection tool due to its ease of use and administration, cost effectiveness and scalability,

The semi-structured interviews were used in the case where the respondents are not in a position to fill the questionnaires. This were administered face to face and through phone calls.

The questions used in the semi-structured interviews were the same ones as those on the questionnaire. The questionnaires comprised of both open and close ended questions which shall be grouped in two sections, A and B.

Section A focussed on the profile of the respondents while section B contained questions relating to the research objectives. The questionnaires were administered through drop and pick from the respondents who were given ample time to fill them. Secondary data was gathered from, publications, organization reports and other research work related to the factors hindering the integration of the security functions in Kenya’s banking institutions.

3.6 RELIABILITY AND VALIDITY OF THE INSTRUMENT

3.6.1 Pilot Test Report

A pilot study was carried out with 4 employees from two different banks, who were not included in the actual survey. The four employees consisted of two respondents from the physical access control department and two from the cyber security department.

The pilot enabled me to get acquainted to the research and its organization as well as find areas that required amending. This also assisted me rectify inconsistencies arising from the data collection tool thus ensuring that only what was intended was measured thus enhanced its reliability.

Reliability is the measure of consistency of data collected which is determined using the test–retest reliability method. It can be increased by including multiple items that are similar on the measure, through testing a diverse sample of respondents and by using uniform testing procedures. Reliability of the research tool was improved with the help of the pilot study which involved 4 respondents. Data collected from the pilot study was be included in the actual study.

3.7 DATA ANALYSIS AND REPORT WRITING

The filled questionnaires was edited to enhance completeness and consistency. This was done prior to processing the acquired responses.

The analysis was done using both qualitative and quantitative analysis. Content analysis and descriptive analysis were the qualitative methods that were used. Content analysis was used to analyse the respondents' feedback on the factors hindering integration of physical and cyber security functions in banking institutions. The data was coded to facilitate grouping of the responses into various sets. Means, median, mode and standard deviation which fall under descriptive statistics was used in analysing the data collected.

Data collected was presented in tables and other graphical presentations as found appropriate. This made it easy to understand and analyse the data.

The tool used for the analysis process was SPSS Version 20. This was preferred due to the below reasons:

1. Simplifies the analysis process, as what could take weeks to be analysed manually is done with a few clicks of a button.
2. Makes it possible to compare multiple sets of data in a very short time.
3. It makes it possible to collate open question responses.
4. It has the ability to explore relationships between responses to different questions.

3.8. PROJECT PLANNING AND MANAGEMENT

Table 3 project planning and management

Activity	**Aug 17**	**Sept 17**	**Oct 17**	**Nov 17**	**Dec 17, Jan 18-May 18.**	**July, 18**
Research Title Submission	🟥					
Proposal preparation	🟦	🟦				
Literature review	🟧	🟧				
Proposal writing		🟩	🟩			
Proposal Submission & presentation		▨	▨			
Data collection			🟦	🟦		
Data analysis				🟫	🟫	
Test Research outcome					🟦	
Presentation of results					🟨	🟨
Writing report						🟪
Final presentation						🟪

3.9. PROJECT SCHEDULE

Table 4 Project Schedule

Activity	Start date	End date
Consultations and picking of project titles	1st Aug, 2017	15th Sept, 2017
Preparing the proposal	1st Aug, 2017	17th Oct, 2017
Milestone one presentation	18th Oct, 2017	18th Oct, 2017
Working towards Milestone Two	19th Oct, 2017	March, 2018
Working towards milestone three	April, 2018	June, 2018
Milestone Three Presentations	July, 2018	July, 2018

CHAPTER FOUR

RESULTS AND DISCUSSION

This section of the study presents the data gathered from the field survey, supported by precise analysis and subsequent interpretation of the implication of the results. The study sought to examine the factors hindering the integration of the physical security access and the cyber security amongst commercial banks in Kenya. The field survey sought respondent's opinions on various issues that relate to the adoption of integration of physical and cyber security aspects of the bank security. The participants in this study included firsthand commercial banks employees working in different levels of the banks security framework.

4.1 RESPONSE RATE

The data in table 5 below highlights the distribution of respondents by the response rate computed in frequency and percentages.

Table 5: The Study Response Rate

Response	**Frequency**	**Percentage**
Responded	85	85.9%
Not-responded	14	14.1%
TOTALS	**99**	**100%**

The response rate computed in table 5 highlights that 99 questionnaires were issued out to the respondents who agreed to take part in the study. 85 questionnaires were successfully returned in time for data analysis, which represents about 85.9% response rate. According to Mugenda and Mugenda (2008), a response rate of 50% and above offer a moderate valid picture on ground, a response rate of above 60 % offered a good dataset that will present valid representation of the ground and finally a response rate of above 70% will offer a very good representation of the actual picture of ground. As presented, the study generated a response rate of about 86% which implies that the obtained data is sufficient for conducting efficient and valid data analysis process.

4.2 DEMOGRAPHIC INFORMATION

The demographic section highlights respondent's background information which include; age distribution, education level, department attached and job experience.

Distribution of respondents by Age

The data in table 6 below highlights the distribution of respondents by age computed in percentages which were derived from the frequency distribution.

Table 6 Age distribution

Age Category	**Frequency**	**Percent**
18 - 30 years	22	25.9 %
31 - 35 years	26	30.6 %
41 - 45 years	22	25.9 %
Over 46 years	15	17.6 %
Total	**85**	**100.0 %**

The findings presented in the above table indicate that majority of the respondents i.e. 22 (30.6%) are in the age category of 31 – 35 years while 26 respondents (25.9%) are in the age groups 18 – 30 years and 41 – 45 years. The finding also indicates that 15 of the respondents (17.6%) are over 46 years of age. The findings in this test reveal a moderate distribution in age among the teams responsible for management of security in commercial banks. This implies that age is an important factor for security personnel working in the different departments within the bank.

Distribution of respondents by education level

The data in table 7 below presents the distribution of respondents by education level calculated in percentages derived from frequency aggregations.

Table 7 Respondents distribution by education level

Academic Attainment	**Frequency**	**Percent**
Diploma	30	35.3 %
Degree	35	41.2 %
Masters/Post-graduate Diploma	20	23.5 %
Total	**85**	**100.0 %**

The findings presented in above table indicate that majority of the respondents i.e. 41.2% indicated to have a bachelor’s degree while 35.3% indicated to have attained a Diploma. 23.5% of the respondents indicated to have attained a postgraduate qualification (Masters or Post-graduate Diploma). This implies that academic attainment is an important element in the implementation of security initiatives within commercial banks.

4.2.3 Respondents Department attached

The data in table 8 below highlights the tabular distribution of respondents in terms of the security department in which they work in with aggregations based on frequency distribution.

Table 8 Security departments at the Commercial Bank

Department attached	**Frequency**	**Percent**
ICT Cyber Security	39	45.9%

CCTV Control Room	18	21.2%
Physical Checkpoint at Entrance/Exit	19	22.4%
Bank Floor Surveillance	9	10.6%
Total	**85**	**100.0%**

The findings in the above table present the respondents distribution in terms of their roles within the security architecture of the commercial bank. The findings indicate that majority of the respondents i.e. 45.9 %, indicated that they are attached to the ICT cyber security division while 22.4 % indicated that they are attached to the physical barrier check points at the bank entrance. The findings also indicate that 21.2% of the respondents were attached to the CCTV control room department and finally, about 10.6% of the respondents indicated to be attached to the bank hall physical surveillance. The findings indicate the importance of cyber security to the commercial banks. In addition, only few members of the bank security team work under the physical security surveillance unit, with preferences being the entrance check point and the CCTV control units.

This implies that the cyber surveillance, physical check points and CCTV monitoring are critical in enforcing bank security thus an indication of their importance in the integration process.

4.2.4 Distribution of Respondents by Work Experience

The data in table 9 below highlights the tabular representation of the respondent’s distribution in terms of work experience.

Table 9 Respondents work experience

Work Experience	**Frequency**	**Percent**
Below 5 years	32	37.6 %
6 - 10 years	23	27.1 %
11 - 15 years	13	15.3 %
16 - 20 years	11	12.9 %
Over 20 years	6	7.1 %
Total	**85**	**100.0 %**

The findings in the above highlight the distribution of respondents by work experience. The findings indicate that majority of the respondents i.e. 32 (37.6 %) have working experience of below 5 years while 23 (27.1%) of the respondents have a working experience of about 6 – 10 years. 13 (15.3%) of the respondents indicated to have a working experience of between 11 – 15 years. 11 (12.9%) of the respondents indicated that they have a working experience of 16 – 20 years.

Finally, 7.1 % of the respondents indicated that they have a working experience of over 20 years. The findings indicate that a significant portion of the respondents have a short stint of experience in their current role in the security unit in which they work. This implies that security roles within the banking sector are continuously altered to avoid redundancy of respondents staying at one position for a long period of time.

4.2.5. Respondents comments for the open questions

The data presented in table 4.6 highlights the respondents views on the preference for approach to security integration.

Table 10 Preference for security model

Option	**Frequency**	**Percentage**
Separated	78	91.8%
Integrated	7	8.2%
TOTAL	**85**	**100%**

The tabulated findings in table 6 above shows that majority of the respondents, 78 (91.8%) stated that their security functions are managed as two separate units. The findings also indicate that 7 (8.2%) of the respondents indicated that the security functions are integrated. They further described the security functions as being integrated at the management level but not in terms of infrastructure used by the two security units. Findings deduced show strong preference for the independent approach of managing the two security functions. The findings indicate that preference for integrated security model is significantly influenced by the need for centralized security approach.

4.2.6. Incidents for both physical access and cyber security

The data presented in table 4.8 highlights, respondent’s views on whether they have ever experienced or witnessed incidents that affected the present security structure for both the physical security access and the cyber security.

Table 11 Security incidents

Option	**Frequency**	**Percentage**
Yes	81	95.3%
No	4	4.7%
TOTAL	**85**	**100%**

The findings in table 7 above show that an overwhelming number of respondents, 81 (95.3%) conceded to have encountered security breaches that affected both physical access control and cyber security. The attackers gained unauthorized physical access to the premises with the aim of attempting to get access to the bank’s network. Most of the respondents confirmed that the attempts to gain unauthorized access to the network resources were captured by the SEIM tool which in turn raised a red flag to the cyber security team who stopped the attacker before they could gain unauthorized access to the network resources.

A small percentage of the respondents confirmed that review of successful security breaches showed that the attackers were able to gain access to network resources as a result of taking advantage of weaknesses in the physical access control system of the organization.

On the flip side however, 4 (4.7%) of the respondents indicated that they haven’t experienced security incidents that affected both security functions.

4.2.7. Access to network resources for new employees

The study sought to examine the strategy used in granting access to network resources for new employees.

Table 12 Access to network resources

No.	**Respondents comments on access to network resources for employees new to a commercial bank**	**Frequency & Percentage**

1.	*New employees fill a network access request form which is then approved by their departmental heads and the head of the networks department. Once approved, employees are granted access to the network.*	**55(65%)**
2.	*New employees are granted access to network resources after HR sends formal requests to the network department to grant the new employees' access.*	**16(19%)**
3.	*New employees have automatic access to basic network access, however formal application is needed for higher level access.*	**14(16%)**
TOTAL		**85 (100%)**

4.2.8. Revocation of network resources upon termination of employee services

The table below outlines the findings in regards to procedures followed when revoking access to the network resources when an employee is leaving the organization.

Table 13 Revocation of network resources

No.	**Respondents comments on the termination of network resources for the employees who have ceased to work for the organization**	**Frequency & Percentage**
1.	*The employee must obtain the formal clearance from the network department. Network access is first disabled which is followed by the head of the network department signing off the official clearance form.*	**76(89.4%)**
2.	*The human resources department sends a list of users who have left the organization to the networks department then disable the users' access to the network.*	**9 (10.6%)**
TOTAL		**85 (100%)**

4.2.9. Delay in revocation of network access rights

The study sought to determine whether instances of delay have ever been registered in the process of revoking the network access.

Table 14 Delay in access rights revocation

Option	**Frequency**	**Percentage**
Yes	69	81.2 %
No	16	18.8%
TOTAL	**85**	**100%**

The findings in table 10 above indicate that a substantial number of respondents, 69 (81.2%) have experienced a situation where the revocation of access to network resources is not done in a timely manner. The respondents indicated that the delay is as a result of the employees' not getting formal clearance from the network department during their exit thus their access is revoked during monitoring of network access by the network department.

The findings also indicate that 16 (18.8%) respondents haven't experienced delay in revocation of access to network resources for employees who have left the organization.

4.2.10. Attitudes of Financial Institutions and Adoption of Integrated Security Framework

The first objective of the study was to assess the influence of banks' attitude towards the implementation of integrated security framework that links the cyber security and the physical access control units. The study examined different aspects that influence commercial banks' attitude towards the adoption of an integrated security framework.

The data in table 10 below highlights the respondents' opinion on the effects of commercial banks attitude on the integration of cyber security and physical access control.

Table 15 Attitudes for security integration mean and standard deviation

Attitudes to security integration	**N**	**Mean**	**Std. Deviation**
Commitment to security reforms	85	4.55	.546
Vulnerabilities influence decisions	85	4.48	.503
Internal security arrangements	85	4.56	.606
Unpopular security reorganization	85	4.01	.715
Security integration on risk exposure	85	4.25	.554
Security integration on operational costs	85	4.31	.578
Uncertainty due to retraining costs	85	4.52	.503
High initial costs for integration	85	3.93	.704
Increased costs for maintaining specialized team	85	3.91	.684

Constant audit increase operational costs	85	4.72	.503

The findings presented in the above table highlight the respondents' opinion on the influence of organizational attitude towards the integration cyber security and physical access control within commercial banks. A scale of 1 – 5 was used where; 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5 = strongly agree. The findings indicate that respondents strongly agree that all commercial banks are committed to security reforms in the banking sector (mean of 4.55, SD =0.546). The respondents also agree that the commercial banks utilize the prevailing vulnerabilities to make decisions on the need for integration of cyber security and physical access control (Mean = 4.48, SD = 0.503).

The findings also indicate that respondents strongly agree that existing internal security arrangements are more preferred to integrated security platforms (Mean = 4.56, SD = 0.606).

Also derived from the findings is the fact that respondents agree that the need for security reorganization is viewed as a time consuming initiative thus unpopular amongst the executives as it's perceived to consume valuable time (mean of 4.01, SD = 0.715). The respondents also agree that the requirements for security integration are perceived to increase the level of risk exposure as compared to the disintegrated security models (Mean = 4.25, SD = 0.554). Additionally, the findings show that respondents agree that the integration of security systems will lead to cutting on security team numbers thus reducing operational costs (Mean = 4.31, SD = 0.578). The respondents strongly agree that commercial banks management is reluctant to integrate the security functions as there will be need to retrain its staff on the new security technology which could be costly (Mean of 4.52, SD = 0.503).

Further, the findings show that respondents agree that the initial investments on the security integration process is costly and has little returns in reduction/ cutting of operational costs (Mean of 3.93, SD = 0.704). Findings also show that, respondents agree that, the integration of security systems in commercial banks will require the hiring of a specialized team capable of handling the security challenges, which will increase remuneration costs of running the new integrated system (Mean = 3.91, SD = 0.684). The findings agree that the need to integrate security apparatus will require constant evaluation and audit to continuously address new threats which could eventually be costly (Mean of 4.72, SD = 0.503). The findings in this study show that, commercial banks as corporate organizations, perceive the need for security integration as a need that is informed by existing gaps. This implies that organizational initiatives on security costs, levels of skills training and the perceived impacts on overall organizational efficiency form the primary determinants for the integration of cyber and physical access control within commercial banks.

4.2.11. Regression Test between Organization Attitudes and Security Integration

The regression test was used to examine the correlation between organizations' attitude and the adoption of integrated security framework within commercial banks.

Table 16 Model Summary for Organizational Attitudes

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.515	.265	.412	.25761
a. Predictors: (Constant), Organizational Attitude				

The computed results in table 11 above present the model summary for the regression test between organizations' attitude and security integration within commercial banks. The test deduces the R-value as 0.515 which implies that there is a strong positive correlation between organizations' attitude and the implementation of an integrated security framework within commercial banks. The test also deduces an r-square value of 0.265 which implies that the organizations' attitude accounts for 26.5% in variability on the implementation of integrated security framework within commercial banks. This also indicates that 73.5% in variability on the integration of security framework within commercial banks is subject to the factors external to organizations' attitude.

Table 17 ANOVA table for Organization Attitudes

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	.136	1	.136	9.056	.005
	Residual	5.508	83	.066		

	Total	**5.645**	**84**			
a. Dependent Variable: Security Integration						
b. Predictors: (Constant), Organizational Attitude						

The findings in table 12 above presents the Analysis of Variance (ANOVA) that shows the relationship between organizations' attitude and integration of security functions. The study deduces a Fischer statistical value (F = 9.056), computed at 0.01 significance level. The data indicates that there exists significance internal variance between the independent and the dependent variable. The p-value deduced is 0.005 ($p < 0.01$). This implies that there exists a significant statistical association between organizations' attitude and the organizations' preparedness to embrace an integrated security framework.

Table 18 Coefficients table for Organization Attitudes

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	Std. Error	Beta		
1	(Constant)	3.047	.806		3.781	.000
	Organizational Attitude	.027	.019	.155	1.434	.005
a. Dependent Variable: Security Integration						

The findings in table 13 above presents the coefficients table for the regression test between organizations' attitude and integration of the security framework. The test was evaluated at 0.01 significance level. The Beta coefficients value for organizational attitude is 0.027, whereas for the Constant value was 3.047. The regression equation for the study is; Y = A + BX, where Y = security integration, A = constant and X = organizations' attitude. The equation generated is: Y (security integration) = 3.047 + 0.027X. This implies that, for every unit change in organizations' attitude, a 0.027 unit's change is recorded for the security integration component.

4.2.12. Intentions of Commercial Banks and Adoption of Integrated Security Framework

The data in table 14 below highlights the computation for the intentions by the commercial banks in the uptake of an integrated security framework.

Table 19 Commercial banks intentions Factors Mean and Standard Deviation

Intentions of commercial banks	**N**	**Mean**	**Std. Deviation**
Security integration create deterrence	85	4.05	.738
Integrated model enhances coordination	85	3.84	.614
Security integration enhances accountability	85	3.26	.657
Security integration improves security and competitiveness	85	3.44	.566
Integration enhances internal monitoring	85	3.31	.708
Integration helps to prevent insider fraud	85	3.45	.608
Integration helps to seal – off fraud loopholes	85	3.51	.629

The findings present the respondents opinion on the influence of organizations' intention in implementing an integrated security framework within commercial banks. A scale of 1 – 5 was used where; 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5 = strongly agree. The findings indicate that the respondents agree that commercial banks need for integrated security approach is informed by the need to create deterrence to possible crimes in the future (mean of 4.05, SD = 0.738). The findings also indicate that commercial banks prefer integrated security model as it enhances coordination and control of security processes (Mean = 3.84, SD = 0.614). Additionally, the findings indicate that the respondents agree that commercial banks intention to integrate security functions is informed by the need to enhance the levels of security accountability (Mean = 3.26, SD = 0.657).

The respondents were neutral on the issue of security integration as an initiative to improve on the general bank security and as a strategy to enhance their competitive edge (mean of 3.44, SD = 0.566).

The findings also indicate that the respondents considered that commercial banks would prefer security integration with intentions to enhance the levels of monitoring employee activities and evaluate their productivity (Mean of 3.31, SD = 0.708).

The findings demonstrate that respondents consider security integration as a banks' initiative meant to enhance the ability to detect and deter insider threats (Mean of 3.45, SD = 0.608). Finally, the respondents are in agreement that commercial banks prefer the integrated security as it enables them to seal-off any fraud loopholes common with disintegrated security systems (Mean = 3.51, SD = 0.629). These findings imply that commercial banks interested in changing the security framework would only be motivated by their interest to boost specific security factors within the institution such as, elimination of fraud and continuous staff monitoring.

4.2.13. Regression Test for Banks Intentions and Adoption of Integrated Security

The regression test seeks to examine the levels of association between the independent variable (bank intentions to integrate their security functions) and the dependent variable (integration of security functions). This would help in demonstrating the level of dependence and the statistical effect of the two variables.

Table 20 Model Summary for bank intentions

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.647	.419	.389	.59948
a. Predictors: (Constant), Bank Intentions				

The Model summary presented in table 15 above indicates that the regression test records the r-square values as 0.647 and the r-square value as 0.419.

This implies that there exists a strong correlation between commercial bank intentions to integrate the two security functions and the likelihood of integrating the two security functions.

In addition, the computed results imply that, bank intentions account for 41.9% in variability for the integration of security framework in commercial banks, therefore 58.1% of variability in the integration of cyber and physical access control security framework is subject to factors external to commercial banks intentions.

Table 21 The ANOVA for bank intentions and security integration

Model	**Sum of**	**df**	**Mean**	**F**	**Sig.**

		Squares		Square		
1	Regression	.234	1	.012	12.534	.007
	Residual	.134	83	.029		
	Total	.368	84			
a. Dependent Variable: Security Integration						
b. Predictors: (Constant), Bank Intentions						

The computed results in table 16 above present the Analysis of Variance (ANOVA) output on the influence of bank intentions to integrate the security functions and integration of the two security functions. The results indicate that the Fischer statistical value is F = 12.534 at significant level 0.01. The p-value deduced is 0.007, which implies that there exists significant statistical association between commercial banks' intentions to integrate the two security functions and the implementation of integrated security infrastructure within commercial banks.

Table 22 Coefficients for bank intentions

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.139	.004		10.291	.000
	Bank Intentions	.215	.000	.080	.731	.007
a. Dependent Variable: Security Integration						

The findings in table 17 above present the coefficients results for the regression test between bank intentions to integrate the two security functions and the integration of security infrastructure. The test was implemented at 0.01 significant level recording p-values of 0.000 for constant and 0.007 for bank intentions, which indicates that p values are less that 0.01 ($p< 0.01$), which implies that the results are significant at this level. The beta coefficients are, Constant = 0.139 and bank intentions 0.215.

The regression equation deduced is: Y (security integration) = 0.139 + 0.215X. This implies that for every unit change noted in commercial banks intentions to integrate the two security functions, 0.215 unit's change is recorded for the likelihood in the integration between, cyber and physical access control within commercial banks.

4.2.14. Pressure on Financial Institutions and Adoption of Integrated Security Framework

The findings in table 18 below present the descriptive results for the pressure that triggers the need for organizations' to integrate the security functions computed in Means and Standard deviation.

Table 23 Bank pressure's Mean and Standard Deviation

Pressures of financial integration	**N**	**Mean**	**Std. Deviation**
Persistent security threats	85	3.98	.654
Need for optimal efficiency in procedures	85	4.01	.500
Security hitches and incorrect response	85	4.32	.539
Industry regulations on security standardization	85	3.89	.802
Integration motivated by competitors operations	85	3.88	.714
Integration informed by continued global changes	85	4.22	.697
Integration is a legal requirement	85	3.46	.765

The findings presented in the above table presents the respondents opinion on the influence of organizations' pressure to adopt integrated security framework within the commercial banks. A scale of 1 – 5 was used where; 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree and 5 = strongly agree. The findings indicate that respondents agree that existence of persistent security threats form the basis for the consideration to integrate the security units in commercial banks with a mean of 3.98 (SD = 0.654).

The findings also indicate that the respondents agree that the pressure to ensure optimal efficiency in bank procedures also forms the basis for the need to integrate security systems (Mean = 4.01, SD = 0.500).

The findings further indicate that respondents agree that cases of security hitches and lack of correct responses to coordinate the hitches also form the basis for the need to integrate the security apparatus within commercial banks (Mean = 4.32, SD = 0.539).

Additionally, the findings show that respondents agree that the industry standards for commercial banks as set by regulatory agencies require standardized security systems integration for all commercial banks (Mean = 3.89, SD = 0.802). The findings indicate that the need for integrated security functions is informed by the need to replicate operational strategies from other competitors within the financial sector (mean = 3.88, SD=0.714). In addition, the findings indicate that respondents agree that continuous modifications in security systems by commercial banks across the world is informed by the changing approaches to security risks. This majorly influences local banks to follow suite in integration of their security models, with a mean of 4.22 (SD=0.697). Finally, the findings indicate that respondents are skeptical as to whether integrated security framework in commercial banks is a requirement by the law in Kenya (mean = 3.46, SD = 0.765). The findings imply that commercial banks are driven by the present situations in adopting strategic changes such as the adoption of integrated security framework. This indicates that if the present security model used by the commercial banks is exposed to different threats which create a loopholes in the coordination between the two security levels, it may trigger the banks to adopt an integrated security framework.

4.2.15. Regression test for banks' pressure factor on security integration

The regression test was used to assess the association between the study variables which include the dependent variable (integration of security functions) and the independent variable which is the pressure that inspires the banks to embrace an integrated security model.

Table 24 The model summary for bank pressures

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.581	.338	.234	3.80261
a. **Predictors: (Constant), Organization Pressures**				

The findings in table 19 above presents the model summary for the banks' pressure in the adoption of an integrated security framework. The R-value for the study is 0.581 and the R-square value is 0.338. This implies that there exists a strong positive correlation between banks' pressure to integrate the security units and the adoption of integrated security infrastructure. In addition, the results imply that banks' pressure accounts for 33.8% in variability in the implementation of an integrated security framework, which indicates that 66.2% in variability for the implementation of an integrated security framework is influenced by factors external to the banks' pressure.

Table 25 The ANOVA for bank pressures

Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	6.887	1	6.887	12.119	.009
	Residual	269.701	83	3.249		
	Total	276.588	84			
a. Dependent Variable: Security Integration						
b. Predictors: (Constant), Organization Pressures						

The findings presented in table 20 above highlight the ANOVA results for the regression test between banks pressure to integrate the security units and integration of the security units. The Fischer value aggregated is, F = 12.119, with a p-value of 0.009 ($p < 0.01$). This demonstrates a significant difference in mean variance between the variables being tested. The Findings imply that there exists a significant statistical association between the prevailing banks' pressure and the adoption of integrated security framework within commercial banks.

Table 26 The coefficients table for commercial bank pressures

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	Std. Error	Beta		
1	(Constant)	34.102	3.228		10.565	.000
	Organization Pressures	.169	.116	.158	1.456	.003
a. Dependent Variable: Security Integration						

The findings in table 21 above present the coefficients for the test between commercial banks' pressure to integrate the security functions and integration of the security functions. The test was executed at 0.01, significance level. The Beta coefficients for the constant value is 34.102, and that of the organizations' pressure to integrate is at 0.169.

The regression equation obtained in the test is: Y (security integration) = 34.102 + 0.169X. This implies that for every unit change in the banks' pressure to integrate a 0.169 unit's change is deduced for integration of security functions within commercial banks.

4.2.16. Multivariate Regression Test of the Factors Hindering Security Integration

The study performed a multivariate regression test for the combined independent variables, notably; organizations' attitude towards integration of security functions, organizations' intentions to integrate the two security functions and the banks' pressure to integrate the security apparatus against the dependent variable, integration of security functions within commercial banks.

Table 27 Model summary for multivariate regression

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.824	.679	.615	.25726
a. Predictors: (Constant), Organization Pressures, Organizational Attitude , Bank Intentions				

The Model summary presented in table 21 above indicates that the R-value for the combined research variables is 0.824. This implies that combined research variables, namely; organizations' attitude towards integration of security functions, organizations' intentions to integrate the two security functions and the banks' pressure to integrate the security apparatus have a strong positive correlation with the adoption of integrated security framework within commercial banks. The R-square value is 0.679, which implies that the combined research variables account for 67.9% variability in the adoption of an integrated security framework within commercial banks. This also indicates that about 32.1% variability in integration of security functions within commercial banks is subject to factors external to the three factors covered in this study.

Table 28 ANOVA for multivariate regression

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.284	3	.095	11.429	.004
	Residual	5.361	81	.066		
	Total	5.645	84			

a. Dependent Variable: Security Integration
b. Predictors: (Constant), Organization Pressures, Organizational Attitude , Bank Intentions

The ANOVA table 23 above indicates that the Fischer value for the combined test is 11.429, at 0.01 significance level. The p-value deduced in this test is 0.004 ($p < 0.01$). This indicates that there exists significant statistical association between organizational factors notably; organizations' attitude towards integration of security functions, organizations' intentions to integrate the two security functions and the banks' pressure to integrate the security apparatus on the implementation of an integrated security framework within commercial banks.

Table 29 Coefficients for the multivariate regression

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
		B	Std. Error	Beta		
1	(Constant)	3.600	.980		3.675	.000
	Organizational Attitude	.124	.019	.142	1.299	.008
	Bank Intentions	.118	.017	.054	.488	.006
	Organization Pressures	.213	.017	-.151	-1.394	.000
a. Dependent Variable: Security Integration						

The coefficient table 24 above presents the regression beta coefficients for the regression test between the combined independent variables and the dependent variable.

The test was executed at significance level, 0.01. The p-values deduced indicate that there exists significant association between the variables.

The regression equation for the study is:

Y (integration of the security functions) = 3.60 + 0.124X_1 + 0.118 X_2 + 0.213 X_3.

This implies that, for every unit change in organizations' attitude towards integration of the security units results in 0.124 units change in integration of the security functions, for every unit change in organizations' intention to integrate the two security units results in a 0.118 unit's change in integration of the security functions and finally for every unit change in banks' pressure to integrate the security functions results in 0.213 units change in integration of the security functions.

4.3 DISCUSSION.

4.3.1. Discussion of the Findings

The main purpose of this study was to determine the factors hindering the integration of physical access control and cyber security in commercial banks in Kenya. The study identified three main areas, which include; commercial banks' attitude toward integration, commercial banks' intention to integrate and pressure that commercial banks' face from both internal and external forces. The study narrowed son these factors and sought to examine the extent to which they influenced the process of integrating physical access control and cyber security.

4.3.2. What factors determine commercial banks attitude towards integration of the security functions?

The findings show that commercial banks attitude account for 26.5% in variability on the commercial banks' decision on whether to integrate physical access control and cyber security. In addition, the findings deduce that, any unit change made on the aspect of commercial bank attitudes will trigger a 0.027 unit's change in the prospect of security integration.

The findings indicate that commercial banks' attitude is determined by numerous factors that influence the strategic decision of whether the integrated security approach will eventually be adopted by the organizations. Commercial banks' attitude contributed significantly to the conclusive decision of adopting the independent approach of managing the security units. It was also evident that the financial institutions find the independent approach convenient despite the loopholes that exist as a result of the approach.

Commercial banks attitude incorporates an array of factors that wield significant influence on the commercial banks decision on whether to integrate physical access control security and the cyber security. The factors noted include:

a. **Banks' commitment to security reforms**.

   This will entail adopting the integrated approach when managing physical access control and cyber security.

b. **Managements' willingness to reorganize the current security model.** Any reforms done in any institution must be approved by management. Successful and smooth integration of the two security functions will only take place if management approval and sponsorship is obtained.

c. **The ability of the integrated approach to resolve existing vulnerabilities which exist as a result of the independent management of the two security functions.**

   Vulnerabilities are weaknesses that can be exploited by threats which would then lead to a security breach. The integrated model should be in a position to resolve all weaknesses identified in the independent security model.

d. **The ability of the integrated approach to reduce the risk exposure in regards to the two security functions.**

   Commercial banks should be convinced that the integrated model will reduce risk exposure.

e. **Reduction of the banks operational costs**.

   Integration of the security functions should result in reduction of operational costs for financial institutions.

f. **Integration and maintenance costs.**

   The sum of the initial integration costs and the maintenance costs should not exceed the current budget that's allocated to the two security functions. In case they do, the benefits arising from the integrated approach should exceed the costs.

These factors determine overall decision on integrating physical access control and cyber security.

4.3.3. What factors determine intentions of commercial banks to integrate physical access control and cyber security?

The findings show that commercial bank intentions accounts for 41.9% in the variability in consideration for the embracing integrated security architecture between commercial banks. Furthermore, the findings show that commercial banks intention wields quantitative statistical association with security integration, with unit change in bank intentions deducing a 0.215 unit's change in the decision for merger of physical access control and cyber security.

The findings highlight that commercial banks intention incorporate significant and diverse factors that wield considerable influence on commercial bank determination of approach to be adopted in managing security functions. The factors include:

a. **The need for detective controls that will reduce the likelihood of security breaches.**

Detective controls are meant to prevent an attack from taking place. Commercial banks insist on getting assurance that the integrated model will reduce the likelihood of security breaches occurring.

b. **The need to enhance coordination in management of the security functions.** Financial institutions will only have intentions to integrate the security functions if there is assurance that the integrated model will enhance ordination of the security processes. This is important to financial institutions as it will enable easier investigation after a security breach has occurred.
c. **Improve accountability in case of security breaches.** Banks will only implement the integrated security model if accountability during and after security breaches will be improved. This is essential as it will help in identifying the source of the security breach and which loophole was exploited for the security breach to be successful.
d. **Improve internal monitoring and detect security breaches before they occur.** Financial institutions need to be convinced that the integrated model will improve internal monitoring and detect security breaches before they occur. This will be the main determinant of whether they will implement the integrated model or retain the independent security model.
e. **Prevention of insider fraud and gagging any fraud loopholes.** The banks are sometimes victims of fraud that is initiated by its own staff. From the research done, financial institutions would need to be convinced that the integrated security model will enhance detection of insider fraud and also assist in sealing all known loopholes that can be exploited by disgruntled employees.

The study establishes that the above factors determine if the commercial banks' will adopt the integrated strategy on security framework on integrated or separated security architecture.

4.3.4. What sources of pressure would influence integration of security functions by commercial banks?

The study found that commercial banks face internal and external pressure that influences their adoption of the integrated approach or retention of the independent approach of managing the security functions.

The study found that pressure faced by commercial banks accounts for 33.8% variability on the determination of the security architecture preference. In addition, the findings note that bank pressure wields statistical influence on the outcome of security architecture decisions. A unit change in commercial banks' pressure deduces a 0.169 unit's change in the determination of the security model to be adopted.

The study established that commercial banks pressure may originate from both internal and external factors as shown below:

Internal sources of pressure.

a. **Persistent security threats.** Financial banks are prone to security threats due to the sensitivity and nature of operations they handle. Any security threat that exploits existing vulnerabilities leads to a security breach which could easily destroy a banks reputation to its customers. Persistent security threats are thus a major source of pressure to financial institutions which could easily influence them to integrate physical access control and cyber security.
b. **The need for efficiency in security procedures.** Independent management of security functions creates many loopholes which could be exploited by attackers. Financial institutions are thus at a verge to improve efficiency of security procedures so as to seal all loop holes. This can be achieved by implementing the integrated security model which has the ability to improve efficiency of security procedures.
c. **Security breaches and incorrect responses.** Security breaches in financial institutions could lead to negative impacts which include: fines and penalties by the regulator, litigation, negative impact on reputation on customers. The integrated security model could come in handy as it has the ability to detect security breaches before they occur and also improve response to security breaches due to its ability to automatically correlate events in both physical access control and cyber security.

External sources of pressure.

a. Industrial standards.

Banks operate in the banking industry which has certain standards that they should all adhere to. The purpose of the industrial regulations is to ensure standardization in the banking sector. From the research done, financial institutions pointed out that their integration of the security functions would be highly determined by whether the industrial standards recommend the same, which in this case is not the case. The banks pointed out that they are reluctant to implement the integrated security model as it is not recommended by the industrial standards thus their preference for the independent security model.

b. **Legal requirements by the regulator.**

   Banks are regulated by the Central Bank of Kenya which has published guidance notes for cyber security which are to be adhered to by all banks in Kenya. From the research done, banks pointed out that they are reluctant to implement new security models as they do not know what impact it would have to their compliance to the cyber security guidelines. This would mean that a compliance review by an external party would be necessary which comes at extra cost thus their reluctance to implement the integrated security model.

c. **Need for integration motivated by competitors.**

   Financial institutions are reluctant to implement new technical solutions that have not been tested by their competitors in the region.

   This is due to the fact that they will not have any institutions from which benchmarking can be done thus their fear of blindly implementing any untested technical solutions. Banks pointed out this as one of the reasons why they have not implemented the integrated security model as none of the banks in Kenya have implemented the integrated security model thus there are no institutions to benchmark against.

d. **Need for integration informed by continued global changes.**

   Globally, 21 % of the organizations have implemented the integrated security model and have reaped benefits its benefit. From the research done, financial institutions in Kenya are aware of the benefits that they could possibly reap from implementing the integrated security model. This is a great source of pressure for financial institutions which in turn makes them think about implementing the integrated security model.

The study found that these factors wield significant pressure on commercial banks which inform their decision of the security architecture.

4.3.5. What factors hindering integration of physical access control and cyber security in banking institutions in Kenya?

From the research done, the following factors were identified as the hindrance for integration of physical access control and cyber security in Kenya:

a. Compliance to legal requirements:

Banks are regulated by the Central Bank of Kenya which has published guidance notes for cyber security which are to be adhered to by all banks in Kenya. From the research done, banks pointed out that they are reluctant to implement new security models as they do not know what impact it would have on their compliance to the cyber security guidelines. This would mean that a compliance review by an external party would be necessary which comes at extra cost thus their reluctance to implement the integrated security model.

b. Absence of organizations to benchmark with:

Financial institutions stated that they are reluctant to implement new technical solutions that have not been tested by their competitors in the region. This is due to the fact that they will not have any institutions from which benchmarking can be done thus their fear of blindly implementing untested technical solutions. Banks pointed out this as one of the reasons why they have not implemented the integrated security model as none of the banks in Kenya have implemented the integrated security model thus there are no institutions to benchmark against.

c. Absence of industrial regulations:

Banks operate in the banking industry which has certain standards that they should all adhere to. The purpose of the industrial regulations is to ensure standardization in the banking sector. From the research done, financial institutions pointed out that their integration of the security functions would be highly determined by whether the industrial standards recommend the same, which is not the case. The banks pointed out that they are reluctant to implement the integrated security model as it is not recommended by the industrial standards thus their preference for the independent security model.

d. Unknown cost implications:

Implementation of the integrated security model would definitely come with cost implications. From the research done, banks are reluctant to adopt the integrated model given that the cost implications are unknown and that no cost benefit analysis has been done for the integrated security model.

e. Organizational culture:

From the research done, the financial institutions pointed out that there is a great division between the physical access control unit and the cyber security unit.

The division is caused by the different work cultures and reporting structures that exist. The division is evident even in their recognition by the two units. Physical security personnel are merely referred to as the security staff while the cyber security staff are commonly referred to as geeks. The culture is thus one of the factors that hinder integration of the two security units.

f. Lack of a road map:

From the research done, implementation of the integrated security model would mean coming up with a strategy on how the new model will replace the independent security model. The strategy could best be established by coming up with a road map on how to transition from the independent security model to the integrated model. Financial institutions pointed out that the process of developing a road map is quite a complex and costly exercise which they wish to avoid. This is thus a major reason why they prefer retaining the independent security model.

4.3.6. Conceptual framework that will guide the implementation of existing security integration solutions.

The finding from the study done indicate that integration of physical access control and cyber security is mainly informed by willingness of the commercial banks to reform the existing security model so as to implement the integrated model. The security reforms will entail:

i. **Establishing a road map that will act as a guide in the implementation of the integrated model.**

   This is done by doing a current state analysis of the security environment and comparing it to the future state which the banks wish to achieve. This will result to identification of existing gaps which the financial institutions can then come up with objectives of how to close the gaps.

ii. **Structural changes so as to integrate the two security units into one.**

   This will involve structurally integrating the physical access control unit and the cyber security unit to form one unit.

iii. **Making strategic decisions on how best the two security functions can be integrated.**

   This will involve defining the unit’s objectives which should be in support of the banks business objectives.

iv. **Redefine operation policies so as to guide the new integrated security model.** The policies will be guided by the strategic decisions, which include objectives of the integrated security unit.

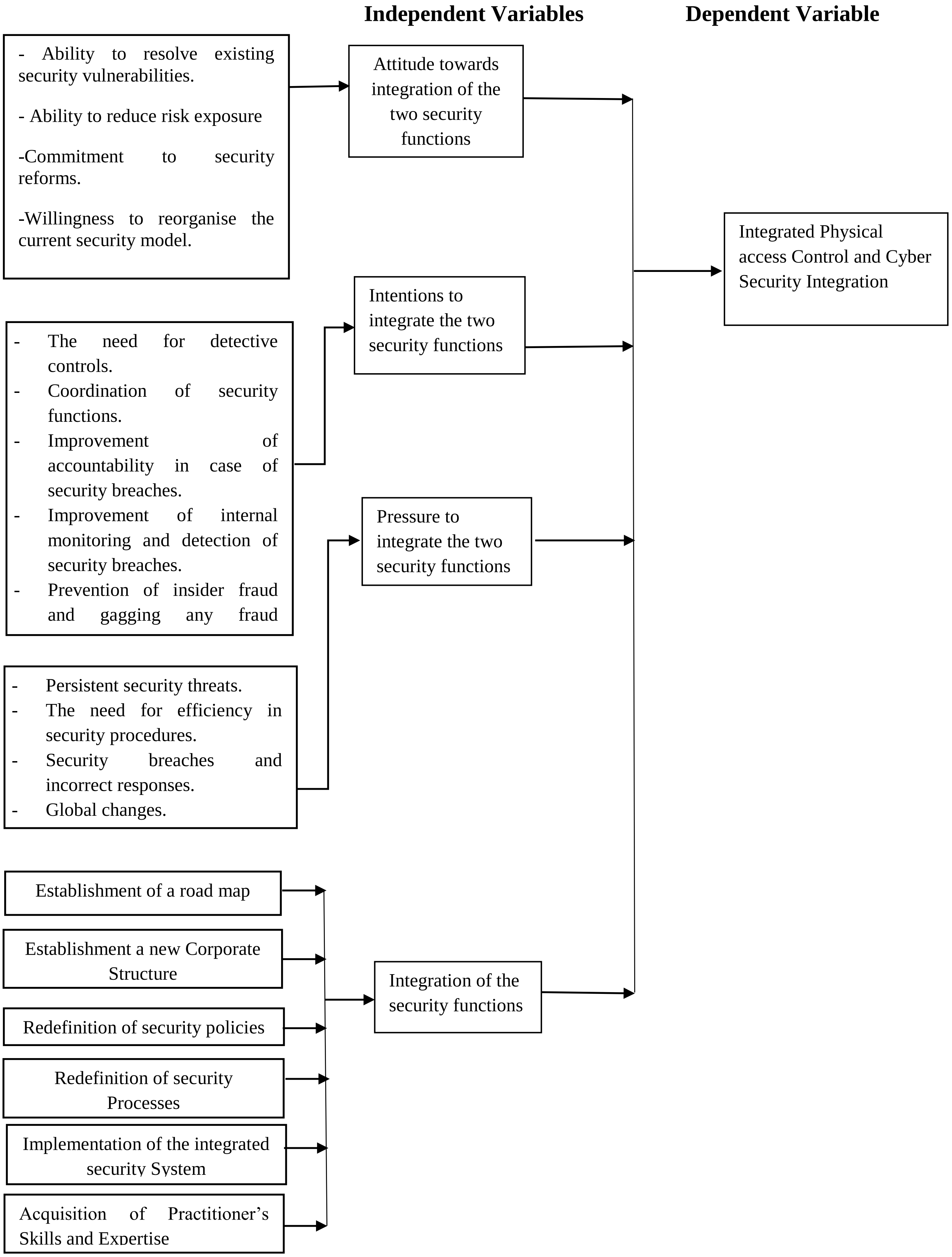
v. **Establishing the best way to integrate the security processes.** This will be guided by the policies that will be defined for the integrated model as business processes are mainly guided by policies.

vi. **Finding a suitable system that will be used to manage the two security units.**
This can be done by eitheir integrating the two existing security systems using a middleware or acquiring a new system that can handle manage operation of both physical access control and cyber security. A middle ware is a software that acts as a bridge between two systems with the intention of enabling communication between the two systems. This decision may be influenced by the banks financial ability to acquire a new system. For banks which do not wish to incur high costs in the integration process, the option of integrating the two existing systems with the help of the middleware would be most suitable.

vii. **Find a suitable way to get skills needed to manage and operate the new system.** This can be achieved by either training existing personnel or getting a new team of specialists who have experience in managing a system that handles integrated security functions.

The below diagram shows the conceptual framework that outlines how integration of the security functions can be achieved, the determinants of banks' attitude and intentions towards integration and sources of pressure for commercial banks in regards to integration of physical access control and cyber security. The factors indicated below were identified during the research.

Figure 8 Conceptual Framework


Independent Variables
Dependent Variable
- Ability to resolve existing security vulnerabilities.
- Ability to reduce risk exposure
-Commitment to security reforms.
-Willingness to reorganise the current security model.
Attitude towards integration of the two security functions
- The need for detective controls.
- Coordination of security functions.
- Improvement of accountability in case of security breaches.
- Improvement of internal monitoring and detection of security breaches.
- Prevention of insider fraud and gagging any fraud
Intentions to integrate the two security functions
- Persistent security threats.
- The need for efficiency in security procedures.
- Security breaches and incorrect responses.
- Global changes.
Pressure to integrate the two security functions
Establishment of a road map
Establishment a new Corporate Structure
Redefinition of security policies
Redefinition of security Processes
Implementation of the integrated security System
Acquisition of Practitioner's Skills and Expertise
Integration of the security functions
Integrated Physical access Control and Cyber Security Integration

4.3.7. Relation of findings to previous studies.

The findings show that commercial banks attitude wield significant influence on the determination of choice for security integration between physical access control and cyber security. These findings are consistent with Murari and Tater (2014) who submitted that organizational attitude towards strategic programs such as the adoption of integrated security framework is significantly influenced by the perceptions harbored by the internal stakeholders who include the employees, executives and the shareholders. The findings agree with Staal (2015) who stated that integrating two security components adds up to a factor of virtualization, where electronic network links all the security apparatus under a digital shell framework which enhances operational coordination.

The findings in this study demonstrate that commercial banks intentions wield surmountable influence on the decision to retain or change the security architecture. These findings are consistent with Bhasin (2007) who noted that the intentions underpinning the urgency of a commercial bank to formulate its general security protocol is informed by the changing levels of risk exposure and the need for better and effective coordination. The findings also support views by Hunton (2009) who explained that the intention to have a leaner operational framework could best be achieved through the integration of all the security components.

The findings highlight that intentions to integrate the security architecture within the commercial banks is influenced by the underlying pressures that pose a threat to effective security coordination. The findings are consistent with Bohme and Moore (2012), who submitted that security vulnerabilities that impact both physical access control and the cyber security wield significant influence on the need for enhanced security coordination. The findings also indicate that the perceived shortcomings in effective operational coordination between the physical access control and the cyber security wield significant pressure on the need for consideration of security framework changes.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This chapter outlines the summary of findings, limitations of the study and recommendations for further research work.

5.1.1. Factors that determine the attitude of banking institutions towards integration of physical access control and cyber security.

The study established that banks' attitude towards integration of the two security functions is determined by the banks' commitment to security reforms, the ability of the integrated approach to resolve existing vulnerabilities and also reduce the firms' risk exposure.

In addition, the managements' willingness to reorganize the current security model and the reduction of operational costs also determine the banks' attitude towards the integrated security model.

5.1.2. Factors that determine the intention of banking institutions to integrate the two security functions.

The study established that the banks' intention to integrate their security functions is determined by the need for detective controls, the need to enhance coordination of security functions and the urge to improve accountability during security breaches. In addition the study established that the need to improve internal monitoring by detecting security breaches before they occur and the need to prevent insider fraud by gagging any fraud loopholes determines the banks' intentions to adopt the integrated security model.

5.1.3. Sources of pressure that would influence integration of the two security functions in banking institutions.

The study identified internal and external sources of pressure that would push the financial institutions to integrate physical access control and cyber security. The internal sources identified include: persistent security threats, the need for efficiency in security procedures and incorrect response during security breaches. The external sources of pressure identified include: legal requirements, industry regulations, the need for integration motivated by competitors and the need for integration informed by continued global changes.

5.1.4. Factors hindering integration of physical access control and cyber security in banking institutions in Kenya

The study established factors that hinder financial institutions from integrating the physical access control and cyber security units. These include: absence of organizations which financial institutions can benchmark with, absence of industrial regulations that support integration of the security units, unknown cost implications, organizational culture and lack of road map that would guide the integration process.

5.1.5. Conceptual framework that will guide the implementation of existing security integration solutions

The findings of the study were then used to develop a conceptual framework that is recommended as a guide for all financial institutions that wish to integrate their security functions.

5.2. ASSUMPTIONS AND LIMITATIONS OF THE STUDY

This study was limited to the 43 commercial banks in Kenya. This study assumed that all commercial banks have the cyber security and physical access control units.

5.3.RECOMMENDATIONS FOR FURTHER WORK

Due to time constraints, the researcher could not undertake extensive research in regards to integration of physical access control and cyber security. The researcher therefore recommends further research to get insightful information regarding integration of the security units. Some of the topics that can be researched include:

1. Effects of integration of physical access control and cyber security on compliance of financial institutions to the CBK cyber security guideline.
2. Effects of integration of physical access control and cyber security in Kenya.
3. Cost implications on organizations that have integrated physical access control and cyber security.

REFERENCES

Aberdeen Group (2017). *In Cyber Security, It's About Time: A Case In Data Protection* http://www.aberdeen.com/research/16168/16168-KB-CyberSecurity-Value-Time.aspx/content.aspx (Accessed on August 26th 2017)

Algozzine, B., & Hancock, D. (2016). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.

Algozzine, B., & Hancock, D. (2016). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.

Baffour, B. A. (2015). Examining the Impact of Information Technology on the Financial Performance of Asutifi Rural Bank. (*Doctoral Dissertation, Kwame Nkrumah University of Science and Technology*)

Barbie, E., & Mouton, J. (2006). Research methodology by numbers-a teaching tool. *Durban University of Technology*.

Bart, I.Y., Shankar, V., Sultan, F. and Urban, G.L. (2005), "Are the drivers and role of online trust the same for all web sites and consumers? A large scale exploratory empirical study", *Journal of Marketing*, Vol. 69, October, pp. 133- 152.

Bhasin, M. (2007). Mitigating cyber threats to banking industry. *The Chartered Accountant*, *50*(10), 1618-1624.

Blumberg, B. F., Cooper, D. R., & Schindler, P. S. (2014). *Business research methods*. McGraw-hill education.

Böhme, R. & Moore, T. (2012). How do consumers react to cybercrime? *eCrime researchers summit (eCrime),* IEEE, 1 – 12

Chak, S. K. (2015). *Managing Cybersecurity as a Business Risk for Small and Medium Enterprises* (Doctoral dissertation).

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

Coombs, W. T. (2006). The protective powers of crisis response strategies: Managing reputational assets during a crisis. *Journal of Promotion Management*, 12(3-4), 241-260.

Damenu, T. K., & Beaumont, C. (2017). Analysing Information Security in a Bank using Soft Systems Methodology. *Information & Computer Security*, *25*(3).

Dawson, C. (2009). Introduction to research methods: A practical guide for anyone undertaking a research project. Hachette UK.

Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), 528 - 535.

Gustafsson, M., Andersson, D., & Waldén, A. (2008). *How a bank organization handles robberies-A question of crisis management.*

Kai-ming Au, A., & Enderwick, P. (2000). A cognitive model on attitude towards technology adoption. *Journal of Managerial Psychology, 15*(4), 266-282.

Kenya Bankers Association (2016). The List of Organization members: http://www.kba.co.ke/members.php (Accessed on August, 26th 2017)

Koranteng, N. D. (2011). Internal control and its contributions to organizational efficiency and effectiveness: A case study of Ecobank Ghana Limited. *Unpublished MBA thesis, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana*.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

Kothari, C. R. (2008). Research Methodology: Methods and Techniques. Delhi: *New Age International Publishers.*

Kurt, A. (2015). *Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study* (Doctoral dissertation, Carnegie Mellon University).

Miller, K. (2009). Organizational Communication; Approaches and Processes. Wadsworth Cengage Learning; Boston.

Murari, K., & Tater, B. (2014). Employee's attitude towards adoption of IT-based banking services: A case of Indian private sector banks. *Competitiveness Review*, *24*(2), 107-118.

Mwesigwa, R. (2010). *Consumers' attitudes, perceived risk, trust and internet banking adoption in Uganda* (Doctoral dissertation, Makerere University).

National Cyber Security Center [NCSC] (2014). Cyber security beeld Nederland. National Cyber Security Centrum: Den Haag.

Raytheon/ Websence, (2015). 2015 Industry Drill-down Report: Financial Services https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf (accessed; 25th August 2017)

Robson, C. (2002). Real world research: A resource for social scientists and practitioners-researchers. *Massachusetts: Blackwell Pushers*.

Staal, F. J. (2015). *Cybercrime and the impact on banks' frontline service employees: a qualitative study towards the impact of cybercrime on the experiences, concerns and* *actions taken by Frontline Service Employees within the banking sector* (Master's thesis, University of Twente).

Symantec, (2012). Internet security threat report trends for 2011. Volume 17 https://www.symantec.com/about/newsroom/press-kits/istr-17 (accessed on 25th August 2017).

Tarimo, C.N., (2006). ICT security readiness checklist for developing countries: A social technical approach (Doctoral dissertation, Stockholm University).

Van Niekerk, J.F., Von Solms, R., (2010).Information Security Culture: A Management perspective. Computers & Security. 29 pp. 476-486

Ula, M., Ismail, Z., & Sidek, Z. M., 2011. A Framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, pp. 1-12.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

Yamane, T. (1967). Elementary sampling theory.

APPENDICES

APPENDIX 1: LETTER OF INTRODUCTION

ISABELLA NJUMBI GITAU,

P.O BOX 303-10303,

MWEA, KENYA

20TH NOVEMBER 2017

Dear Sir/Madam,

REF: AUTHORITY TO CONDUCT ACADEMIC RESEARCH IN YOUR ORGANIZATION.

Am Isabella Njumbi Gitau, a student pursuing MSc. Information Technology Management at the University of Nairobi. I am undertaking a research entitled “Factors hindering integration of physical access control and cyber security in the banking sector in Kenya". My focus will be on the physical security and the cyber security units of the organization. The information availed will be aggregated with total confidentiality.

Participation in the study involves completion of a questionnaire which consists of 2 parts which may require approximately 15 to 25 minutes to complete. I would be grateful if you would volunteer to assist in this study by completing the attached questionnaire. I will appreciate if the questionnaire is completed by January 10, 2018.

Any enquiries you may have concerning this study should be directed to me by email (bella.gitau@gmail.com)

Your kind support and authority hereby sought is essential to assist me carry out the research work

Yours sincerely,

Isabella Njumbi Gitau

APPENDIX 2: QUESTIONNAIRE

SECTION A: BACKGROUND INFORMATION

1. Age Distribution

i. 18 – 30 years □

ii. 31 – 35 years □

iii. 36 – 40 years □

iv. 41 – 45 years □

v. Over 46 years □

2. Education Level

i. Secondary School Certificate □

ii. Diploma □

iii. Degree □

iv. Masters/Post-Graduate Diploma □

3. Security Functionalities at the Commercial Bank

i. ICT Cyber Security □

ii. CCTV control Room □

iii. Security Barrier at Entrance/Exits □

iv. Security Surveillance at Bank Floor □

4. Job Experience

i. Below 5 years □

ii. 6 – 10 years □

iii. 11 – 15 years □

iv. 16 – 20 years □

v. Over 20 years □

5. **What best describes the two security functions? (Please tick as appropriate)**

Integrated ( )

Separated ( )

If the two security functions are integrated, briefly describe how the two are integrated.

……………………………………………………………………………………………
……………………………………………………………………………………………
…………

6. **Have you had incidents that affected both the physical access control and cyber security functions?**

Yes ( )

No ( )

If yes, briefly describe the security breach.

……………………………………………………………………………………………
……………………………………………………………………………………………
…………

7. **Briefly describe how access to the network resources is granted to new employees.**

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……

8. **Briefly describe how access to the network resources is revoked once an employee resigns or is dismissed.**

……………………………………………………………………………………………
……………………………………………………………………………………………
…………

9. **Are there times when revoking of user rights to network resources is delayed once a user has resigned or has been dismissed? Tick the appropriate answer.**

Yes ( )

No ( )

If no, what measures are taken to ensure that the user rights are terminated in a timely manner?

……………………………………………………………………………………………
……………………………………………………………………………………………
…………

In the subsequent sections, kindly indicate how much you agree/disagree with the following statements on a scale of 1 to 5 as per the table below:

Level of Agreement				
(1)	(2)	(3)	(4)	(5)
Strongly Disagree	Disagree	Neutral	Agree	Strongly agree

SECTION B: **ATTITUDE OF FINANCIAL INSTITUTIONS TOWARDS SECURITY INTEGRATION**						
Please indicate the extent to which you agree with the following statement on the financial institutions attitude towards hindrances to security integration						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	Commercial banks are committed to security reforms in the banking sector.					
2.	The commercial banks use prevailing vulnerabilities to make decisions on security integration					
3.	The existing internal security arrangements are preferred to integrated security platforms					
4.	The need for security reorganization is viewed as a time intensive initiative thus is unpopular with executives as it's viewed to consume valuable time and financial resources.					
5.	The requirements for security integration are viewed as more likely to increase the level of risk exposure than the disintegrated security models.					
6.	The integration of security systems will lead to reduction in numbers of the security team thus reducing operational costs					
7.	Banks management is reluctant to integrate the security as it will need to re-train its staff into new security models which could be costly.					
8.	The initial investments on the security integration process is costly and has little returns in relation to cutting of operational					

	costs					
9.	The integration of security systems in commercial banks will require the hiring of a specialized team capable of handling the security challenges, which will increase remuneration costs of running the new integrated system					
10.	Integrating the two security functions will require constant evaluation and audit to continuously address new threats which could eventually be costly					

SECTION C:

INTENTION OF COMMERCIAL BANKS ON SECURITY SYSTEMS INTEGRATION

Please indicate the extent to which you agree with the following statement on the commercial banks intention on systems integration for commercial banks

No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	Banks need for integrated security approach is informed by need to create deterrence to possible crimes in future					
2.	Banks prefer the integrated security model as it enhances coordination and control of security processes					
3.	The intention to integrate security is informed by the need to enhance the levels of security accountability					
4.	The need to integrate the security functions is brought about by the desire to improve on the bank’s security as a strategy to enhance competitive edge					
5.	The banks opt to integrate the security systems with intentions to enhance the levels of monitoring employee activities and evaluate their productivity.					
6.	Commercial Banks opt to integrate the security functions so					

	as to enhance the ability to detect and deter insider fraud and schemes.					
7.	Commercial banks prefer having integrated security as it enhances their ability to seal-off any fraud loopholes common with disintegrated security system.					

SECTION D: PRESSURE TO INTEGRATE

Please indicate the extent to which you agree with the following statement on the pressure Financial Institutions are subjected to in relation to integrating security Systems

No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	Persistent security threats are the basis for the need to integrate the security systems in commercial banks					
2.	The pressure to ensure optimal efficiency in bank procedures is the basis for the need to integrate security systems					
3.	Cases of security hitches and lack of correct responses to coordination form the basis for the need to integrate the security functions					
4.	The industry standards for commercial banks as set by regulatory agencies encourage integration of the security systems for all commercial banks					
5.	The need for an integrated security system is informed by the need to replicate operational strategies from other competitors					
6.	Continuous modifications in security systems by commercial banks across the world is informed by the changing approaches used to respond to new security risks.					

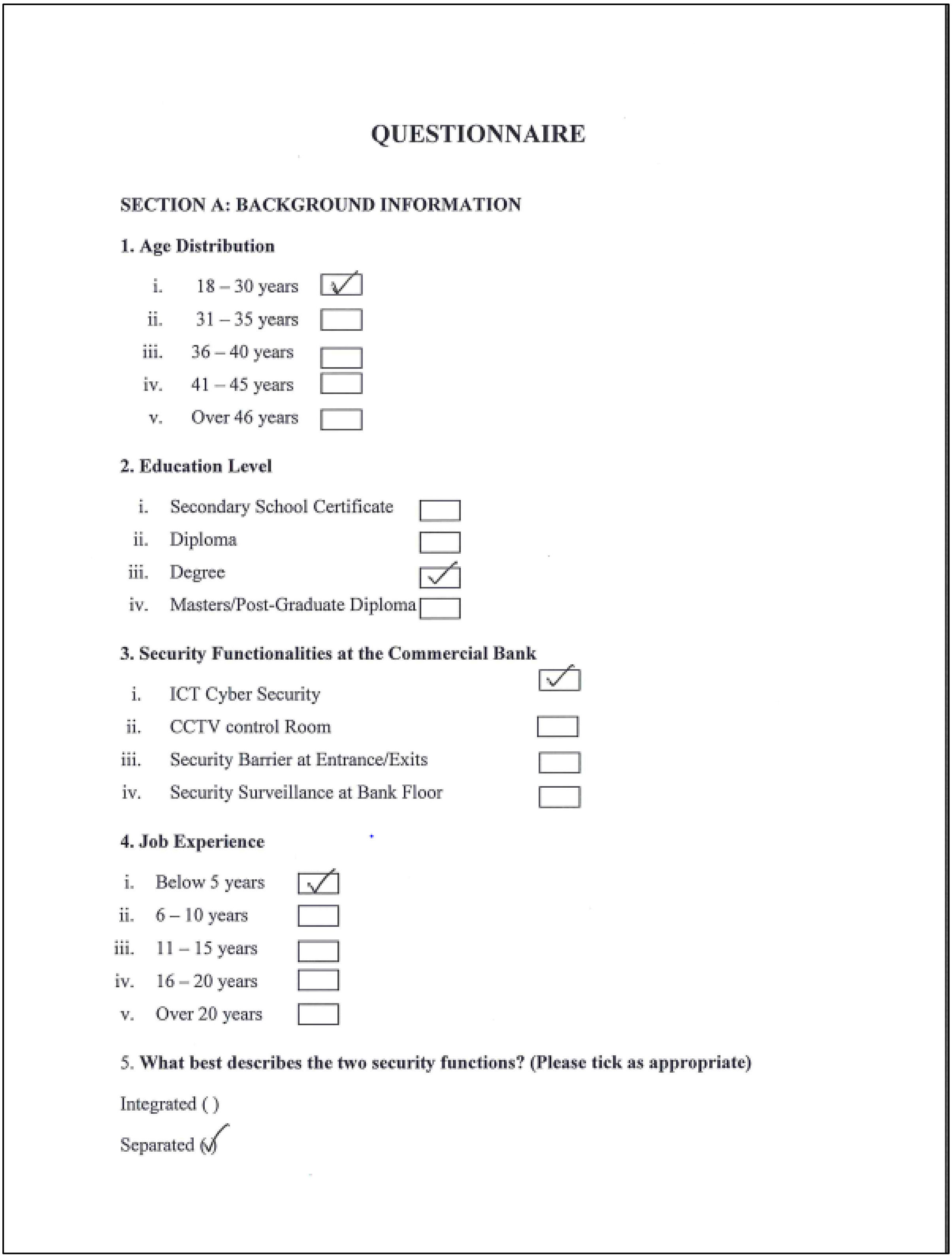
7.	The requirements for integration of security systems in commercial banks is a requirement by law					

SECTION E: INTEGRATION OF THE SECURITY FUNCTIONS						
Please indicate the extent to which you agree with the following statement on the strategy to implement security integration in commercial banks						
No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	There is need to carry out parallel change in implementation of security structure within commercial banks					
2.	The best way to implement security systems integration is through formulation of policy framework to guide the transition process					
3.	The implementation of security integration should be done through a structured process that identifies high risk areas which are given higher priority in the integration process whereas the least risk areas are implemented in last phases of the process.					
4.	The integration of the security systems should be undertaken by professionals contracted externally as the internal team supervises the whole process.					
5.	The implementation of the integrated security system should coincide with the training levels required for the new system and integrated security framework					
6.	There should be continuous changes made in the security teams under the new integration models to prevent likelihood of internal disgruntled employee attacks and racketeering					

7.	The commercial bank should set up a security committee that will be tasked in supervising the whole implementation process and offer guidance to the executive committee on the operational strategy to be formulated.					

Thank you very much for your Answers, may God bless you

APPENDIX 3: SAMPLE OF FILLED QUESTIONAIRE



QUESTIONNAIRE

SECTION A: BACKGROUND INFORMATION

1. Age Distribution

- i. 18 – 30 years ☑
- ii. 31 – 35 years □
- iii. 36 – 40 years □
- iv. 41 – 45 years □
- v. Over 46 years □

2. Education Level

- i. Secondary School Certificate □
- ii. Diploma □
- iii. Degree ☑
- iv. Masters/Post-Graduate Diploma □

3. Security Functionalities at the Commercial Bank

- i. ICT Cyber Security ☑
- ii. CCTV control Room □
- iii. Security Barrier at Entrance/Exits □
- iv. Security Surveillance at Bank Floor □

4. Job Experience

- i. Below 5 years ☑
- ii. 6 – 10 years □
- iii. 11 – 15 years □
- iv. 16 – 20 years □
- v. Over 20 years □

5. **What best describes the two security functions? (Please tick as appropriate)**

Integrated ( )

Separated (✓)

If the two security functions are integrated, briefly describe how the two are integrated.

……N/A as the two security functions are separated.

…………………………………………………………………………………………………

…………

6. **Have you had incidents that affected both the physical access control and cyber security functions?**

Yes (✓)

No ( )

If yes, briefly describe the security breach.

…unauthorised users tried to gain access to the physical………

…building and succeeded. They then went ahead to keystroke…

…loggers on the machines but they did not suceed in stealing information as the SIEM tool captured the attempt and sent an alert to the cyber sec team

7. **Briefly describe how access to the network resources is granted to new employees.**

…new employees fill an network access request form which is…

…then approved by the head of department and head of

…networks department. once approved, the new employee is then

…granted access to the system.

8. **Briefly describe how access to the network resources is revoked once an employee resigns or is dismissed.**

…the employee leaving the company has to obtain clearance from the

…networks department. they networks department first disables the employee

…access to the ~~system~~ network and then signs off on the employees clearance form.

9. **Are there times when revoking of user rights to network resources is delayed once a user has resigned or has been dismissed? Tick the appropriate answer.**

Yes (✓)

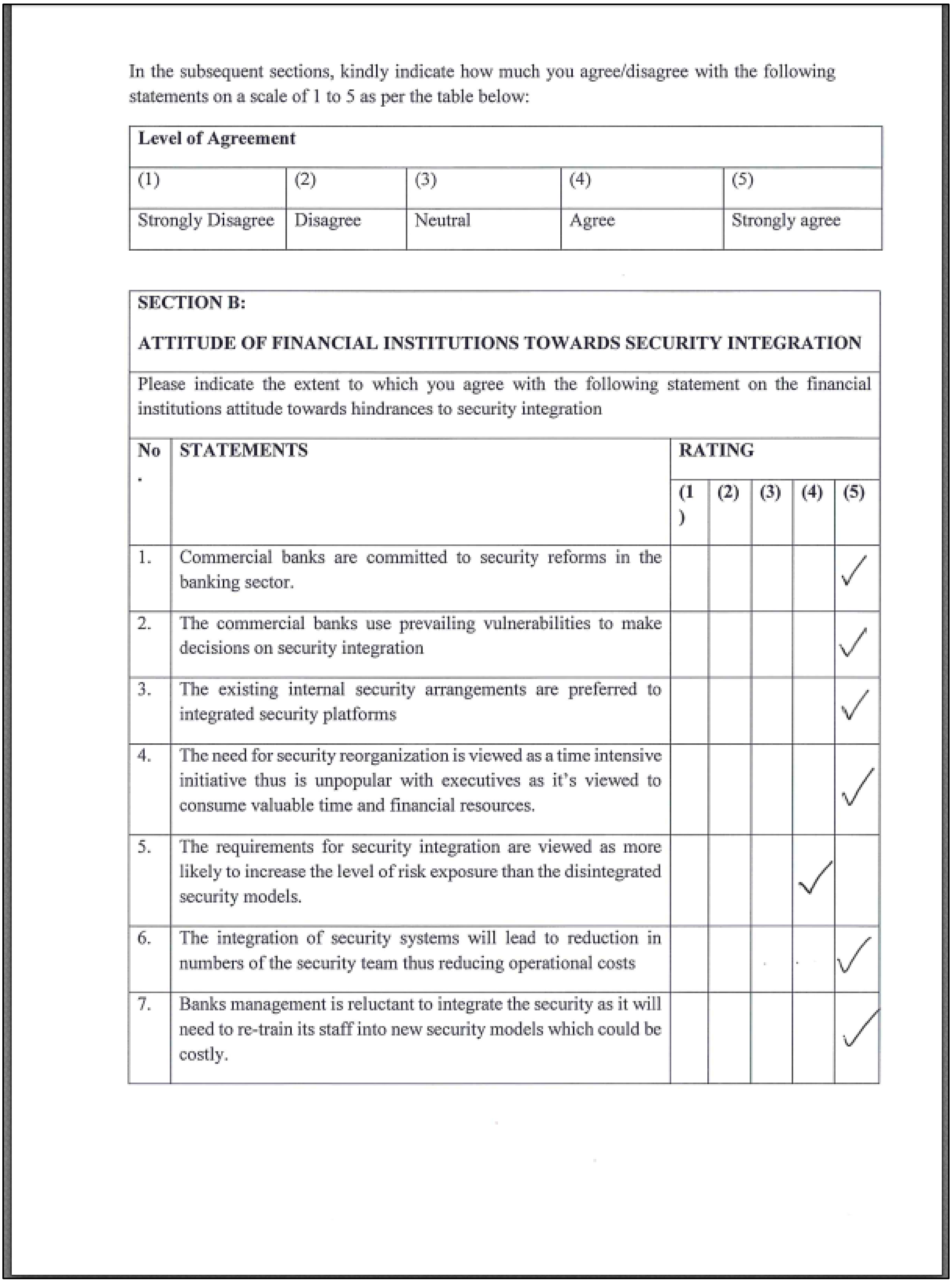
No ( )

If no, what measures are taken to ensure that the user rights are terminated in a timely manner?

………N/A:…………………………………………………………………………………

…………………………………………………………………………………………………

…………



In the subsequent sections, kindly indicate how much you agree/disagree with the following statements on a scale of 1 to 5 as per the table below:

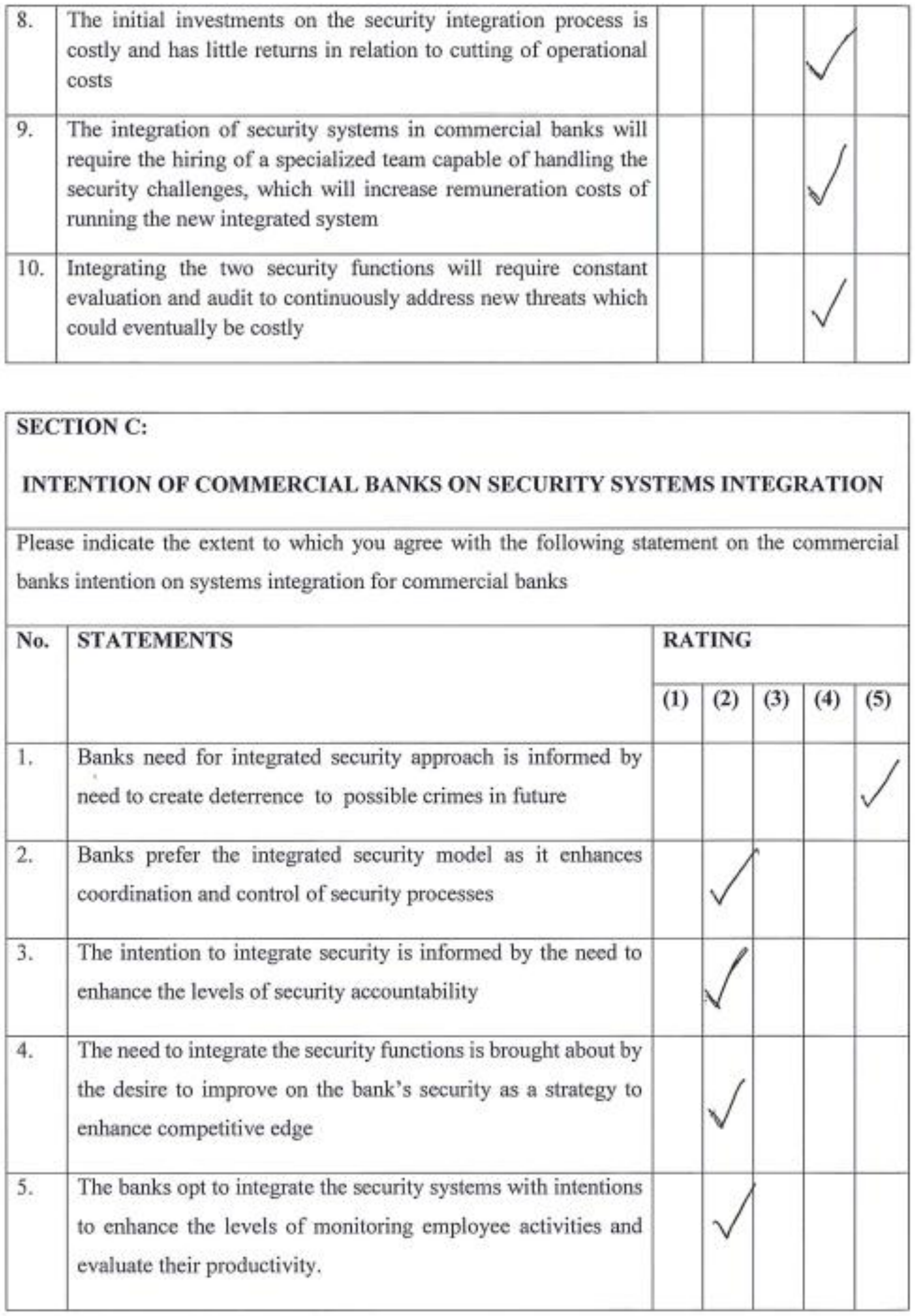
Level of Agreement				
(1)	(2)	(3)	(4)	(5)
Strongly Disagree	Disagree	Neutral	Agree	Strongly agree

SECTION B:

ATTITUDE OF FINANCIAL INSTITUTIONS TOWARDS SECURITY INTEGRATION

Please indicate the extent to which you agree with the following statement on the financial institutions attitude towards hindrances to security integration

No.	**STATEMENTS**	**RATING**				
		(1)	**(2)**	**(3)**	**(4)**	**(5)**
1.	Commercial banks are committed to security reforms in the banking sector.					✓
2.	The commercial banks use prevailing vulnerabilities to make decisions on security integration					✓
3.	The existing internal security arrangements are preferred to integrated security platforms					✓
4.	The need for security reorganization is viewed as a time intensive initiative thus is unpopular with executives as it's viewed to consume valuable time and financial resources.					✓
5.	The requirements for security integration are viewed as more likely to increase the level of risk exposure than the disintegrated security models.				✓	
6.	The integration of security systems will lead to reduction in numbers of the security team thus reducing operational costs					✓
7.	Banks management is reluctant to integrate the security as it will need to re-train its staff into new security models which could be costly.					✓



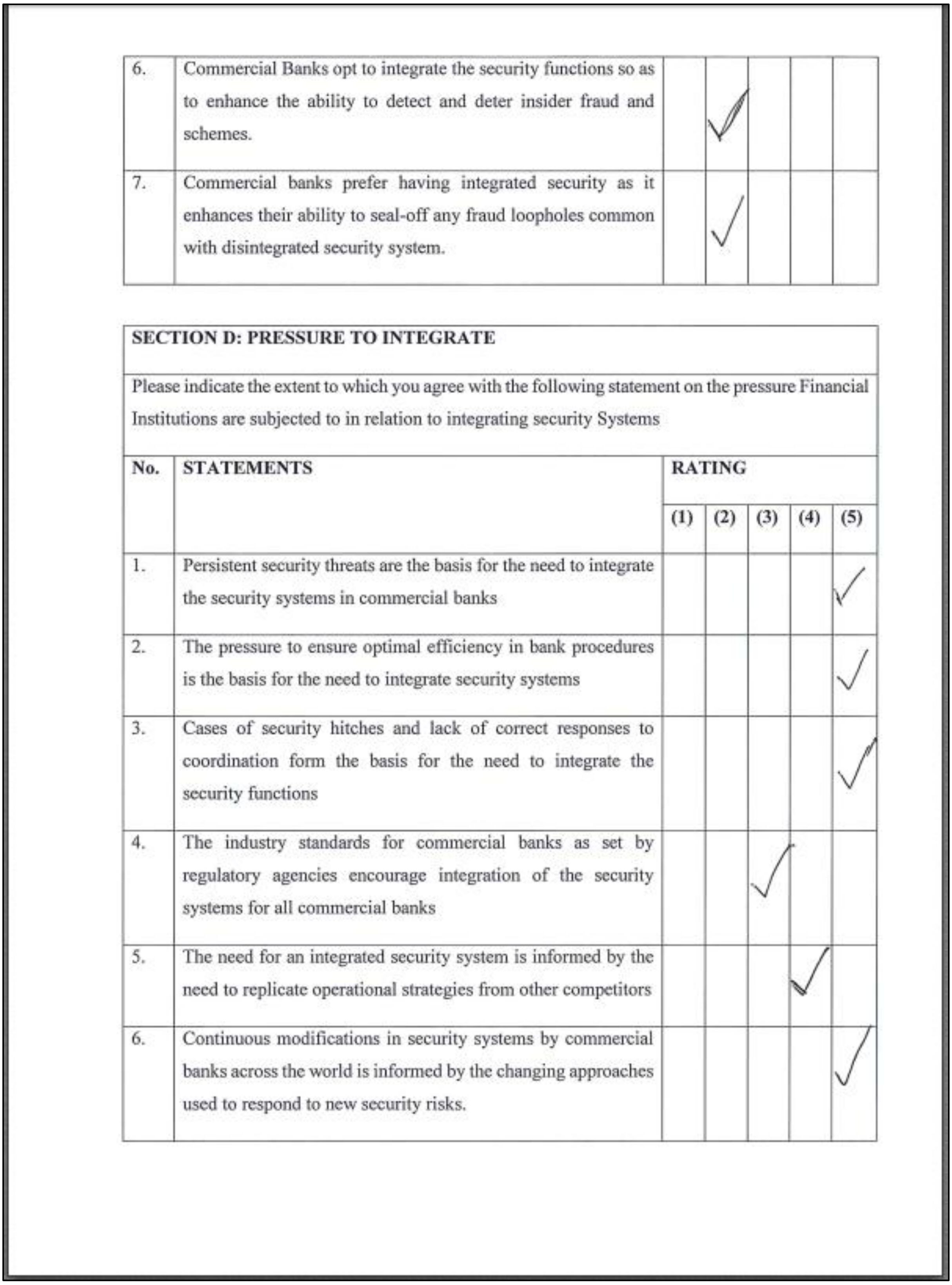
8.	The initial investments on the security integration process is costly and has little returns in relation to cutting of operational costs				✓	
9.	The integration of security systems in commercial banks will require the hiring of a specialized team capable of handling the security challenges, which will increase remuneration costs of running the new integrated system				✓	
10.	Integrating the two security functions will require constant evaluation and audit to continuously address new threats which could eventually be costly				✓	

SECTION C:

INTENTION OF COMMERCIAL BANKS ON SECURITY SYSTEMS INTEGRATION

Please indicate the extent to which you agree with the following statement on the commercial banks intention on systems integration for commercial banks

No.	STATEMENTS	RATING				
		(1)	(2)	(3)	(4)	(5)
1.	Banks need for integrated security approach is informed by need to create deterrence to possible crimes in future					✓
2.	Banks prefer the integrated security model as it enhances coordination and control of security processes		✓			
3.	The intention to integrate security is informed by the need to enhance the levels of security accountability		✓			
4.	The need to integrate the security functions is brought about by the desire to improve on the bank's security as a strategy to enhance competitive edge		✓			
5.	The banks opt to integrate the security systems with intentions to enhance the levels of monitoring employee activities and evaluate their productivity.		✓			

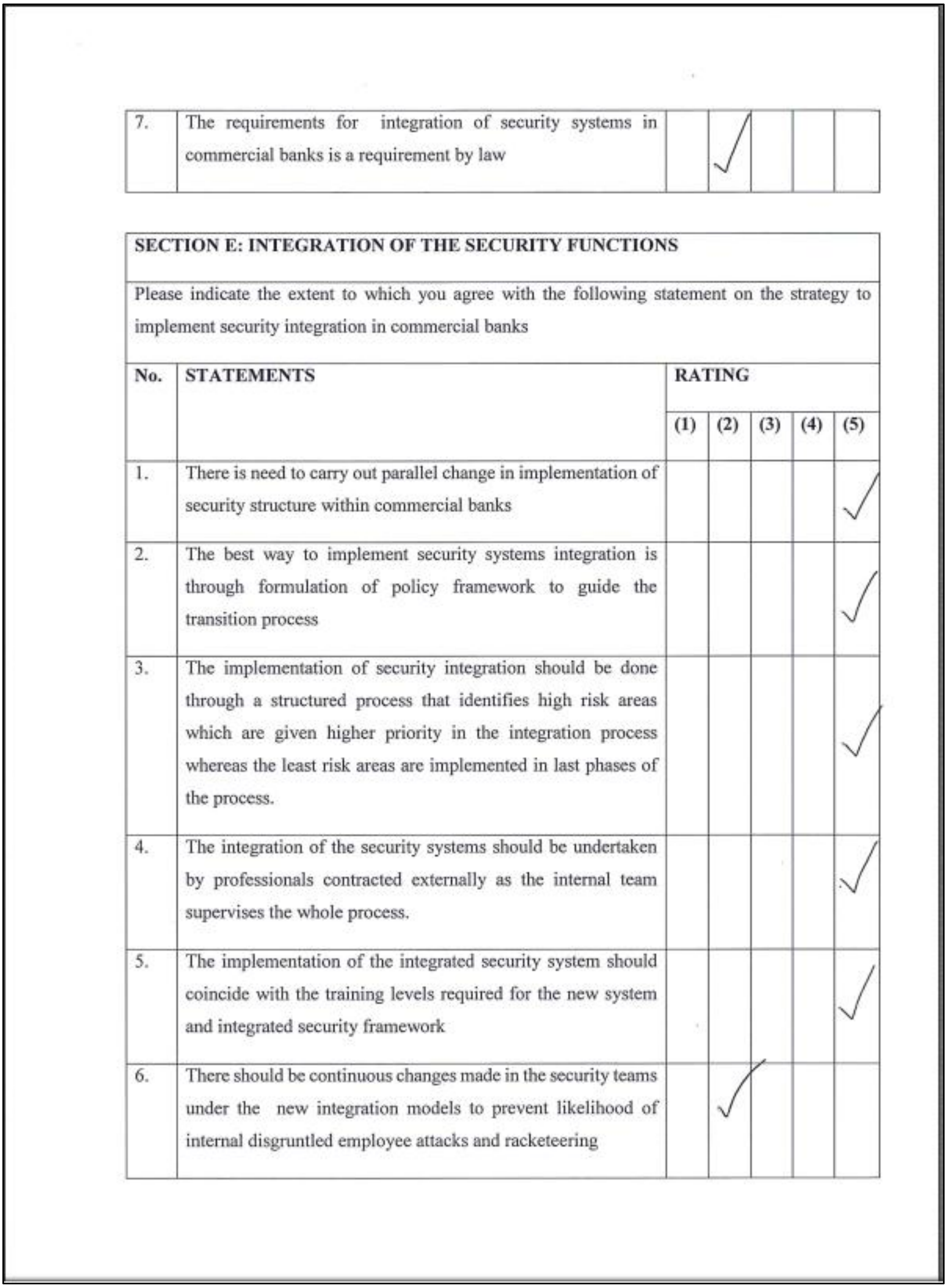


6.	Commercial Banks opt to integrate the security functions so as to enhance the ability to detect and deter insider fraud and schemes.		✓			
7.	Commercial banks prefer having integrated security as it enhances their ability to seal-off any fraud loopholes common with disintegrated security system.		✓			

SECTION D: PRESSURE TO INTEGRATE

Please indicate the extent to which you agree with the following statement on the pressure Financial Institutions are subjected to in relation to integrating security Systems

No.	STATEMENTS	RATING				
		(1)	(2)	(3)	(4)	(5)
1.	Persistent security threats are the basis for the need to integrate the security systems in commercial banks					✓
2.	The pressure to ensure optimal efficiency in bank procedures is the basis for the need to integrate security systems					✓
3.	Cases of security hitches and lack of correct responses to coordination form the basis for the need to integrate the security functions					✓
4.	The industry standards for commercial banks as set by regulatory agencies encourage integration of the security systems for all commercial banks			✓		
5.	The need for an integrated security system is informed by the need to replicate operational strategies from other competitors				✓	
6.	Continuous modifications in security systems by commercial banks across the world is informed by the changing approaches used to respond to new security risks.					✓

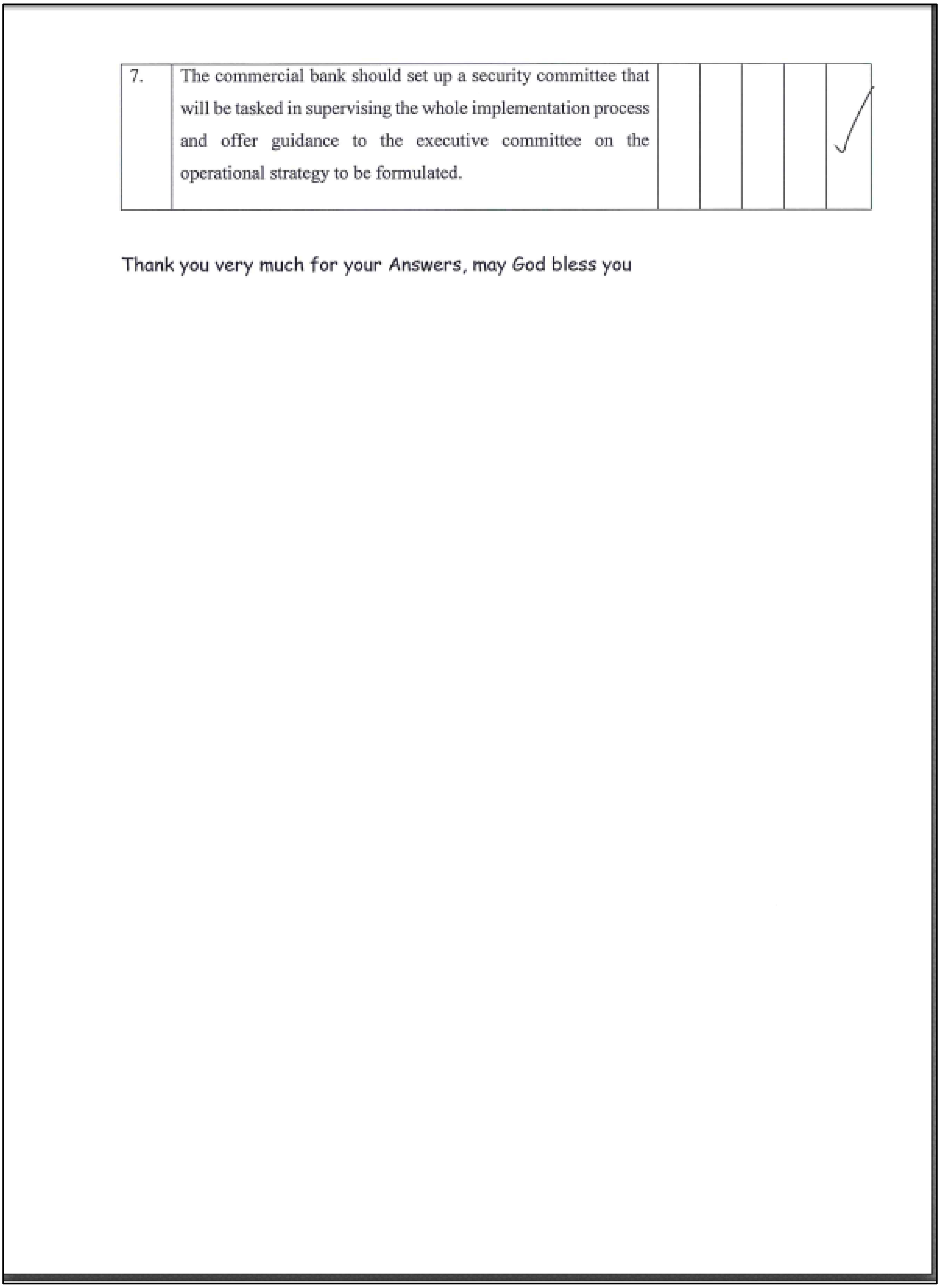


7.	The requirements for integration of security systems in commercial banks is a requirement by law		✓			

SECTION E: INTEGRATION OF THE SECURITY FUNCTIONS

Please indicate the extent to which you agree with the following statement on the strategy to implement security integration in commercial banks

No.	STATEMENTS	RATING				
		(1)	(2)	(3)	(4)	(5)
1.	There is need to carry out parallel change in implementation of security structure within commercial banks					✓
2.	The best way to implement security systems integration is through formulation of policy framework to guide the transition process					✓
3.	The implementation of security integration should be done through a structured process that identifies high risk areas which are given higher priority in the integration process whereas the least risk areas are implemented in last phases of the process.					✓
4.	The integration of the security systems should be undertaken by professionals contracted externally as the internal team supervises the whole process.					✓
5.	The implementation of the integrated security system should coincide with the training levels required for the new system and integrated security framework					✓
6.	There should be continuous changes made in the security teams under the new integration models to prevent likelihood of internal disgruntled employee attacks and racketeering		✓			



7.	The commercial bank should set up a security committee that will be tasked in supervising the whole implementation process and offer guidance to the executive committee on the operational strategy to be formulated.					✓

Thank you very much for your Answers, may God bless you