AN ENTERPRISE INFORMATION SECURITY MODEL FOR A MICRO FINANCE COMPANY: A CASE STUDY

by

MORNÉ OWEN
9203958

TREATISE

Submitted in partial fulfilment of the requirements for the degree

M TECH: Business Information Systems
in the School of ICT
at the Nelson Mandela Metropolitan University

Supervisor: Prof. S.V. Flowerday

November 2009
Author’s Declaration

I, Morné Owen, hereby declare that:

- The work in this treatise is my own work.

- All sources used or referred to have been documented and recognised.

- This treatise has not previously been submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institution.

____________________________
Morné Owen
November 2009
Abstract

The world has entered the information age. How the information is used within an organization will determine success or failure of the organization. This study aims to provide a model, that once implemented, will provide the required protection for the information assets. The model is based on ISO 27002, an international security standard. The primary objective is to build a model that will provide a holistic security system specifically for a South African Micro Finance Company (MFC). The secondary objectives focuses on successful implementation of such a model, the uniqueness of the MFC that should be taken into account, and the maintenance of the model once implemented to ensure ongoing relevance. A questionnaire conducted at the MFC provided insight into the perceived understanding of information security. The questionnaire results were used to ensure the model solution addressed current information security shortcomings within the MFC. This study found that the information security controls in ISO 27002 should be applicable to any industry. The uniqueness for the MFC is not in the security controls, but rather in the regulations and laws applicable to it.
Acknowledgements

I would like to thank the following:

- My Lord and Saviour, Jesus Christ, for it is He who gives us life, talents and opportunities;
- My wife and kids, who I dearly love, for providing balance in my work-life relationship;
- And a special thanks to my supervisor, Prof. Flowerday, for his inputs, knowledge and encouragement to complete this treatise.
# Table of Contents

Author’s Declaration .................................................................................................................. ii  
Abstract ....................................................................................................................................... iii  
Acknowledgements ....................................................................................................................... iv  
Table of Contents ........................................................................................................................... v  
List of Figures and Tables .............................................................................................................. viii  

CHAPTER 1 INTRODUCTION ...................................................................................................... 1  
1.1 Background ............................................................................................................................. 2  
1.2 Problem Statement .................................................................................................................. 5  
1.2.1 Primary Objective ................................................................................................................ 6  
1.2.2 Secondary Objectives ........................................................................................................... 6  
1.3 Significance of the Study ......................................................................................................... 6  
1.4 Research Methodology ............................................................................................................ 6  
1.5 Outline of the Treatise ............................................................................................................. 7  

CHAPTER 2 CURRENT SECURITY MODELS AND STANDARDS ............................................. 8  
2.1 Introduction ............................................................................................................................. 9  
2.2 Introduction to ISO/IEC 27002:2005 Information Technology .................................................. 9  
2.3 Comparison of Security Standards and Methodologies .......................................................... 10  
2.4 The Importance of Risk Management ..................................................................................... 12  
2.5 General Controls and IT Controls .......................................................................................... 15  
2.6 Structure of ISO 27002 ......................................................................................................... 18  
2.7 ISO 27002 Control Clauses ..................................................................................................... 20  
   2.7.1 Security Policy .................................................................................................................... 21  
   2.7.1.1 Information Security Policy Document ........................................................................ 21  
   2.7.1.2 Review of the Information Security Policy ................................................................. 22  
   2.7.2 Organisation of Information Security ............................................................................... 23  
   2.7.2.1 Internal Organisation .................................................................................................... 23  
   2.7.2.2 External Parties .............................................................................................................. 26  
   2.7.3 Asset Management .......................................................................................................... 27  
   2.7.4 Human Resources Security ............................................................................................. 28  
   2.7.5 Physical and Environmental Security ............................................................................. 30  
   2.7.6 Communications and Operations Management ............................................................. 32
2.7.7 Access Control ........................................................................................................ 35
2.7.8 Information Systems Acquisition, Development and Maintenance ......................... 36
2.7.9 Information Security Incident Management ................................................................. 37
2.7.10 Business Continuity Management ............................................................................. 38
2.7.11 Compliance ................................................................................................................ 39
2.8 Conclusion ....................................................................................................................... 40
CHAPTER 3  CASE STUDY .................................................................................................... 41
3.1 Introduction ...................................................................................................................... 42
3.2 The Micro Finance Industry in South Africa ................................................................. 42
3.3 Overview of the Company used in this Study ................................................................. 44
3.4 Research Methodology ................................................................................................... 46
3.5 Primary Data Collection ................................................................................................. 47
3.5.1 Population ...................................................................................................................... 47
3.6 Primary Data Analysis ..................................................................................................... 48
3.6.1 Questionnaire Design ................................................................................................... 48
3.6.2 Questionnaire Highlights ............................................................................................. 50
3.7 Detail Primary Data Analysis ............................................................................................ 55
3.7.1 Policy (Questions: 1 & 2) ......................................................................................... 55
3.7.2 Organisation of Information (Questions: 3 & 4) ......................................................... 55
3.7.3 Asset Management (Questions: 5 – 7) ........................................................................ 56
3.7.4 Human Resources Security (Questions: 8 – 11) ......................................................... 56
3.7.5 Physical and Environment (Questions: 12 & 13) ....................................................... 57
3.7.6 Communications and operations management (Questions: 14 – 20) ......................... 57
3.7.7 Access Control (Questions: 21 – 29) ........................................................................ 59
3.7.8 Information Systems Acquisition, Development & Maintenance ......................... 60
(Quesions: 30 – 36) .............................................................................................................. 60
3.7.9 Business Continuity (Questions: 37 & 38) ................................................................. 61
3.7.10 Compliance (Questions: 39 & 40) ............................................................................ 61
3.7.11 Questionnaire Conclusion ......................................................................................... 62
3.8 Conclusion ....................................................................................................................... 64
CHAPTER 4  FINDINGS AND RECOMMENDATIONS: BUILDING A FOCUSED
SECURITY MODEL FOR A SOUTH AFRICAN MFC ........................................................... 65
4.1 Introduction ...................................................................................................................... 66
4.2 Baseline Solution for a MFC ......................................................................................... 66
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.1</td>
<td>Policy</td>
<td></td>
</tr>
<tr>
<td>4.2.1.1</td>
<td>Introduction</td>
<td>71</td>
</tr>
<tr>
<td>4.2.1.2</td>
<td>Information Assets should be Documented and Assigned to an Owner</td>
<td>71</td>
</tr>
<tr>
<td>4.2.1.3</td>
<td>Define Regular Review Intervals for the Policy</td>
<td>72</td>
</tr>
<tr>
<td>4.2.1.4</td>
<td>Provide for Staff Awareness and Training Regarding the Content of the Policy</td>
<td>72</td>
</tr>
<tr>
<td>4.2.1.5</td>
<td>Clearly Define Roles and Responsibilities</td>
<td>73</td>
</tr>
<tr>
<td>4.2.1.6</td>
<td>Define How Information Security Risks are Managed</td>
<td>74</td>
</tr>
<tr>
<td>4.2.1.7</td>
<td>Legal and Regulatory Requirements</td>
<td>74</td>
</tr>
<tr>
<td>4.2.1.8</td>
<td>How to Handle Incidents</td>
<td>74</td>
</tr>
<tr>
<td>4.2.1.9</td>
<td>Compliance to the Policy</td>
<td>75</td>
</tr>
<tr>
<td>4.2.1.10</td>
<td>Penalties and consequences</td>
<td>75</td>
</tr>
<tr>
<td>4.2.3</td>
<td>Organisation</td>
<td>75</td>
</tr>
<tr>
<td>4.2.4</td>
<td>Asset Management</td>
<td>75</td>
</tr>
<tr>
<td>4.2.5</td>
<td>Proposed Solution Implementation Check List</td>
<td>76</td>
</tr>
<tr>
<td>4.3</td>
<td>Vetting the Solution</td>
<td>76</td>
</tr>
<tr>
<td>4.4</td>
<td>Conclusion</td>
<td>76</td>
</tr>
<tr>
<td>5.1</td>
<td>Background</td>
<td>79</td>
</tr>
<tr>
<td>5.2</td>
<td>Evaluation of the Research Outcomes</td>
<td>79</td>
</tr>
<tr>
<td>5.3</td>
<td>Directions for Future Research</td>
<td>81</td>
</tr>
<tr>
<td>5.4</td>
<td>Conclusion</td>
<td>82</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>83</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Instrument used for Data Collection</td>
<td>88</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Example of an Information Asset Register</td>
<td>108</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Practical Implementation Check List for ISO 27002</td>
<td>111</td>
</tr>
</tbody>
</table>
List of Figures and Tables

Figures:

Figure 1.1 - CIA Triangle................................................................. 4
Figure 1.2 - Structure of ISO 27002................................................... 5
Figure 2.1 - Using ISO 27002 to achieve CIP compliance....................... 10
Figure 2.2 - Prince2 Risk Management............................................... 13
Figure 2.3 - Security Concepts and Relationships.................................. 14
Figure 2.4 - IT Controls...................................................................... 16
Figure 2.5 - Control Classifications...................................................... 17
Figure 2.6 - ISO 27002 mind map....................................................... 20
Figure 2.7 - Relationship between ISO 27002 control clauses.................. 21
Figure 3.1 - Software Release Management Process.................................. 46
Figure 3.2 - Survey Process.................................................................. 47
Figure 3.3 - Job Role........................................................................... 48
Figure 3.4 - Relationship between ISO 27002 control clauses.................. 49
Figure 3.5 - Response Summary............................................................ 62
Figure 3.6 - Questionnaire Results........................................................ 63
Figure 4.1 - Proposed Information Security Roles for the MFC...................... 73

Tables:

Table 4.1 - Solution Model.................................................................... 67
Chapter 1
Introduction

Chapter 2
Current Security Models and Standards

Chapter 3
Case Study

Chapter 4
Findings and Recommendations: Building a Focused Security Model for a South African MFC

Chapter 5
Conclusion

Chapter 1
1.1 Background
1.2 Problem Statement
1.3 Significance of Study
1.4 Research Methodology
1.5 Outline of the Treatise
1.1 Background

“Many small business owners believe that they do not need to worry much about computer and online security. ‘After all,’ they reason, ‘who would want to target my business when there are so many bigger targets out there?’” (Microsoft, 2005). However, Information Security Management is applicable to any size of organization.

When an organization is small, it is easy to control the security issues as there are only a few people responsible and accountable for the information systems. It is fairly easy to audit any process as the volumes of transactions are normally small. Therefore, security and controls are not as strict as in a formalized business environment.

As the organization grows, compliance and corporate governance become more important especially if the company is no longer privately owned. Shareholders and financiers require an assurance from the board of directors that the necessary policies and procedures are in place to protect their investment. The International Federation of Accountants (IFAC) and the Information Systems Audit and Control Association (ISACA) confirm that enterprise governance should be implemented and maintained by executive management to ensure that goals are achieved by creating long-term plans while mitigating risks and using company resources efficiently (International Federation of Accountants, 2004).

Governance extends to the use of IT within an organization. IT governance is not necessarily the responsibility of technical staff, but needs to be enforced and driven from the executive team. It is important that all IT policies and procedures create an environment for the business to achieve their goals (IT Governance Institute, 2003). The South African Fraud Prevention Services reports that South African business lost R276 million to identity theft-related fraud in the first three months of 2008 alone, a substantial increase on the 2007 figures (Dombo, 2008). Information Security is in the first place a business concern and not a technical issue. Governing for enterprise security is defined by Allen (2005) as ensuring that an organization understands that security is not a by-product, but an essential part of the very fabric of the organisation influencing everything that is said and done. Security should be part of and embedded in every business process.

Bowen, Hash and Wilson (2006), who are in agreement with Allen (2005), define information security governance as being at the core of business strategy through the
implementation of policies and procedures, which create accountability and responsibility in order to effectively manage risk.

Additionally, in order to manage risks, they first must be identified and defined. Threats are the cause of risk. Trèek (2003) defines the identification process as follows:

- Identify what is important to the company’s survival;
- Using your existing knowledge of your company, create a list of possible threats that could exploit vulnerabilities;
- Evaluate the list in step 2 and determine the probability of occurrence;
- Calculate the loss of revenue for each threat;
- The risks with the highest expected loss of revenue (probability x loss of revenue), should be prioritized first and mitigated accordingly.

The most difficult step in the process is to define a threat’s probability of occurrence. The process mentioned above illustrates that information security is in the first place a business issue. The implementation of technical solutions is effected at an operational level and does not necessarily guarantee that threats are adequately mitigated. Sherwood (1996) echoes this principle by warning that a security system should improve the efficiency of business processes, otherwise business users will not accept its importance and will find ways to jeopardize it.

To ensure that the security model enhances business processes, it should be applied holistically to IS / IT within the organization. It is important that an organization identifies how much security is required per process to ensure adequate protection based on the specific needs of the process (Gerber & Von Solms, 2005). One can therefore deduce that what works as a best practice in one organization does not necessarily work for another. Anderson and Choobineh (2008) confirm that best practice should include policies, procedures, people and technology all efficiently combined to ensure business goals are achieved. They are of the opinion that the implementation of this best practice should be adjusted as required per process to ensure the level of security is sufficient.

Enterprise Security Management (ESM) is a holistic approach to system security that encompasses all aspects of an organization’s network and allows for security policies to integrate all of these components (Kim, Kim & Lee, 2006). This research project will attempt
to define what is needed for an enterprise security management system specifically tailored for a micro finance company (MFC) by using Information Technology – Security techniques – Code of Practice for information security management (ISO/IEC 27002:2005). This international standard provides guidelines on how to manage information security by focusing on information as an asset (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). A balance must be maintained to provide a secure environment and to ensure: information security Confidentiality, Integrity and Availability, while allowing the flexibility needed for an organization to profitably operate (Figure 1.1, CIA Triangle). Too much security will result in unusable systems and too little will expose risk and hamper integrity. If employees encounter problems when performing their responsibilities due to locked down systems, they will not be productive and will be determined to undermine security in order to complete their work (Post & Kagan, 2007).

Figure 1.1 CIA Triangle

The necessity for collaboration and inter-communication between organizations has led to the development of new technology, for example Web 2.0 (social networking sites, wiki’s, blogs, etc.) that intends to use the Internet as a platform to share information (Webopedia Computer Dictionary, n.d.). The result of this information sharing tends to blur the ownership of a physical network and therefore one only needs to protect the information and not the network or the IT infrastructure (Jericho Forum, n.d.).

Therefore, the solution is not merely a technical one, but more importantly a business issue. The technical solution must enhance business operability while providing the necessary protection (balanced approach). This is summarized in Figure 2. ISO 27002 which is a holistic security model that covers administrative, technical and physical measures throughout an organization from the lowest level (operational) to the board (strategic) (Bisson & Saint-Germain, n.d.).
1.2 Problem Statement

Creating a holistic information security model is an overwhelming task since it needs to protect an intangible asset which is difficult to value (Gerber & Von Solms, 2005). Too much security will result in inflexible systems and too little will lead to exposure to risk. The balance between confidentiality, integrity and availability (CIA Triangle) must ensure the optimum use of information. Conversely, this is a difficult task.

In achieving this balance, the information security model must support easy integration across multiple platforms including the organizational, technical and physical aspects as set out in ISO 27002. Broderick (n.d.) confirms that the challenge is to ensure that your information security model is so integrated with business that it will enable better business decision making. Furthermore, it should protect business processes allowing them to run efficiently and optimally. The solution should ensure that the core of the business is protected and that the cost of security is covered by the implementation of a successful secure business process (Theodosios & Stephanides, 2005).
Additionally, obtaining certification for ISO 27002 is a mammoth task as a company must conform to all 11 sections (about 150 controls). Von Solms and Von Solms (2001) are of the opinion that due to the nature of this exercise many large organizations will decide against certification. This could lead to an implemented security solution that does not meet the basic requirements of a best practice security system, leaving the company open to risk.

1.2.1 Primary Objective

The primary objective of this research project is to develop an enterprise security model for a Micro Finance Company (MFC) by creating a secure next generation system in order to secure its information assets by means of adhering to an international security standard i.e. ISO 27002.

1.2.2 Secondary Objectives

- How does a company successfully implement ISO 27002 ensuring that its information assets are adequately protected?
- What unique measures can be used to ensure that ISO 27002 is implemented correctly for a MFC?
- What is needed to maintain your Information Security Management System once implemented?

1.3 Significance of the Study

The significance of this study is to create an enterprise security model specifically for a MFC based on ISO 27002. The case study will focus on a company established in 2001, with a staff compliment of 1400, geographically disbursed throughout its 90 branches nationwide. It will take into account the regulatory requirements for the finance industry in South Africa.

1.4 Research Methodology

Firstly, an extensive literature survey will be conducted in order to gain an in-depth knowledge of the subject matter and to make inferences from the work of experts in the field
of Information Security Management. The sources of data will stem from journals, academic papers, books, case studies, international standards and best practices.

Secondly, the empirical part of this research project will involve the following:

- A case study which can be defined as a research strategy, an empirical inquiry that investigates a phenomenon within its real-life context (Yin, 1984). As the objective of this study is to build a model for Information Security Management, a case study is suitable in analyzing the current day-to-day operations of a micro finance company and to create a relationship reflecting the theories applied.
- The data generation methods used will include questionnaires and semi-structured follow-up interviews to determine how Information Security Management is currently practised within the micro finance company in protecting information as an asset. This will provide more information about the ‘as is’ model which will be used to transform the Information Security Management model to the proposed one based on this study’s findings. Furthermore, the interviews will be used to gather opinions about the proposed model thereby providing a ‘check’ on the model’s feasibility and these recommendations will be used to refine the proposed solution findings.

1.5 Outline of the Treatise

The treatise starts by indicating how important Information Security Management is to an organization. Information Security Management is more of a business (governance and compliance) than a technical issue. Information risks should be identified and a strategy adopted to mitigate them. Chapter 1 introduces the problem, objectives of the study and research methodology. Chapter 2 focuses on current standards that can be used for implementing an Information Security Management System based on ISO 27002. Thus, an in-depth study will be made of this standard to determine how the controls can be implemented for a micro finance company. This will lead to Chapter 3, a case study of how the proposed information security model can be implemented. The relationship between the literature study and case study will be examined in determining the research findings. Chapter 4 will provide the solution: a focused security model for a micro finance company. It will move from theory to implementation stating how technology can help in solving information security problems. Chapter 5 will conclude with a summary of the research problem and research findings.
Chapter 2

Current Security Models and Standards

Chapter 1
Introduction

Chapter 2
Current Security Models and Standards

Literature Study

Chapter 3
Case Study

Empirical Research

Chapter 4
Findings and Recommendations:
Building a Focused Security Model
for a South African MFC

Chapter 5
Conclusion

Chapter 2
2.1 Background
2.2 Introduction to ISO/IEC 27002:2005
Information Technology – Security
Techniques – Code of Practice for
Information Security Management
2.3 Comparison of Security Standards and
Methodologies
2.4 The Importance of Risk Management
2.5 General Controls and IT Controls
2.6 Structure of ISO 27002
2.7 ISO 27002 Control Clauses
2.8 Conclusion
2.1 Introduction
There are a vast number of models and standards available for Information Security. Most of them have at the heart, an Information Security Policy. The policy focuses mainly on the process of implementation and must be created to provide adequate coverage of the security risks while meeting the organisations goals and culture (Höne & Eloff, 2002). This could prove to be a difficult task if one is not clear on the contents of the policy.

In choosing a standard or framework it must be adapted to fit the culture of the organisation and provide a balance between Confidentiality, Integrity and Availability. The board and directors are ultimately accountable and must ensure that risks are satisfactorily managed. It is their duty to promote information security and ensure that all staff are educated and trained in it.

2.2 Introduction to ISO/IEC 27002:2005 Information Technology
ISO (International Organisation for Standardisation) is a non-governmental organisation that has a membership that spans 157 countries which includes both the governmental and private sectors. They ensure that acceptable standards are built into products. Publication as an International Standard requires that at least 75% of its members must approve it (ISO/IEC 27002:2005).

ISO 27002 is an Information Technology security technique consisting of 11 security control clauses containing 39 main security categories. It includes a section on risk assessment and management which is used to identify security vulnerabilities, allowing the organisation to determine its appetite for risk and ultimately how to manage (mitigate) the risk.

ISO 27002 formally known as ISO 17799, is based on the British Standard BS7799-1. The rename from ISO 17799 to ISO 27002 was made by ISO to create the 27000 series for information security. In this study, reference to ISO 17799, BS7799-1 and ISO 27002 are used interchangeably.

ISO 27002 is defined as a best practice. “Best Practice” can be defined as a technique or methodology that has proven to lead to superior results which can be used as a benchmark to
strive for. Implementation of a best practice supports the idea that no practice is best for everyone in every situation (Business Dictionary.com, n.d.).

2.3 Comparison of Security Standards and Methodologies

As mentioned before, there are a number of standards and methodologies available. Some of the more popular ones will be discussed and a comparison to ISO 27002 will be made for each of them.

The Information Security Forum has published *The standard of good practice for information security*. This standard addresses information security from a business perspective and is used as a practical guideline to implement security (Information Security Forum, 2007). This standard responds to the needs of international organisations by implementing the latest ‘hot topics’ of security and is aligned with ISO 27002. It is updated every two years to ensure that it remains relevant and recently it was aligned with CobiT 4.1.

The North American Electric Reliability Council uses the Critical Infrastructure Protection standard to ensure that all critical cyber assets are protected. Compliance to this standard can be achieved by using ISO 27002 as depicted in Figure 2.1 (Continuity Central, 2007).

![Figure 2.1 Using ISO 27002 to achieve CIP compliance (Continuity Central, 2007)](image)

The National Institute of Standards and Technology (NIST) of the United States released three computer security standards: Special publication 800-12 which provides a broad overview of computer security and controls, 800-14 describes common security principals used and 800-26 provides advice on how to manage IT Security (NIST, 2007). In 800-12 Computer Security is defined as the protection required for an information system to ensure
Confidentiality, Integrity and Availability of information system resources (NIST, n.d.). It is
divided into 3 sections:

- Management Controls - ensure that risk is adequately identified and managed;
- Operational Controls - focus on what people (as opposed to systems) need to
  implement;
- Technical Controls - focus on what the computer systems need to execute.

Implementing ISO 27002 will satisfy NIST’s information system security requirements.

The Generally Accepted System Security Principles (GASSP) is a set of guidelines created
by the International Information Security Foundation (I²SF) that defines information security
as a set of the following measures:

- Preventative – a control that avoids an undesirable event, for example the use of
  passwords, firewalls and encryption;
- Detective – a control that identifies the occurrence of an undesirable event, for
  example visitor logs, motion sensors and closed circuit TV;
- Recovery – a control that restores information assets to their expected state by
  adhering to Confidentiality, Integrity and Availability (I²SF, 1999).

Focus is placed on making users aware of the ‘acceptable use’ of information as an asset
through awareness and training. GASSP states that management is responsible for creating
the policies required to govern information security and to define how much risk each
individual or business unit is authorised to assume. This fits the ISO 27002 model where the
importance of information security starts with the board and directors formulating a policy
for implementation.

Since the implementation is driven by policy, it is vital that senior management approves it
and are involved in ensuring that their information risks are adequately managed. Other
frameworks for example CobiT (Control Objectives for Information Technology), assists in
the auditing function to ensure that the information security policy is implemented correctly.
Information Security forms part of IT Governance which is the responsibility of executives
and the directors of the board (IT Governance Institute, 2007).
This research project proposes that ISO 27002 is used as a security standard to implement a casual security model for a MFC. It is clear that other security standards are similar in nature and covers more or less the same scope. The advantage of using an International Standard is that it is more widely accepted (157 countries including both government and private sectors).

2.4 The Importance of Risk Management

Risks are defined in Prince2 (Projects in controlled environments) as “the uncertainty of outcome (whether positive opportunity or negative threat)” (Office of Government Commerce, 2005). Another definition states that “Risk is the exposure to the chance of injury or loss; a hazard or dangerous chance” (Dictionary.com, 2006)

Risks should be managed to ensure that the value of information assets are not compromised. The management of Risk is an ongoing activity, as illustrated in Figure 2.2, which covers both Risk Analysis and Risk Management. Risk Analysis consists of:

- Identifying risks – anything that could compromise Confidentiality, Integrity and Availability of information;
- Evaluating the risk impact – assessing the probability of the risk occurring and its impact on the system;
- Identifying options of managing the risk which could include: prevention (remove the risk), reduction (treat the risk), transference (passed to 3rd party for example insurance), acceptance (tolerate the risk) or contingency (plans implemented when the risk occurs);
- Finally, implementing the most feasible solution.

Risk Management therefore ensures that the solution implemented provides the necessary risk mitigation by monitoring and reporting its success or failure.
The ISO 27002 process starts by identifying the security requirements by assessing an organisation’s risks. Risks are identified by examining:

- the business strategy and objectives;
- legal, statutory and contractual requirements;
- and the vision or strategy an organisation has developed to support its operations.

According to ISO 27002, a risk assessment is used to identify, quantify and prioritise risks against criteria for risk acceptance relevant to the organisation. The risk assessment enables management to understand the risks (risk analysis). The process is an iterative one to be performed periodically especially when changes occur in security requirements and the risk situation. Once the risks are identified they must be evaluated by creating a risk profile (probability vs. impact). Figure 2.3 illustrates the Common Criteria (2004), which is a risk assessment model created by the IT Security community. It protects the assets (information) by implementing counter measures which reduce or remove the risk.
The owners are responsible for the safeguarding of the assets as they are valued. Threat agents will see a value in the assets if they are able to abuse them to achieve the opposite of the owner. Threat agents include: hackers, crackers, computer process, etc. The threats could cause loss of asset Confidentiality, Integrity and Availability. Threats therefore increase risks to the asset, based on the likelihood of the threat materialising and the impact (damage) caused. Owners need to prove that they have safeguarded the assets by demonstrating that the countermeasures they put in place are (1) sufficient and (2) correct (Common Criteria, 2004).

Every organisation has an appetite for risk (risk tolerance) to be defined before determining the treatment for risks. Risk appetite is the level at which the organisation is willing to accept risk without implementing a costly control to reduce the risk. It is the total impact of risk an organisation is prepared to accept in meeting its strategic objectives (KPMG, 2008).
Risk treatment options include the following:

- reduce the risk by applying controls for example: Disaster recovery plans and Business continuity plans;
- accept the risk – do nothing; depends on the risk appetite of the organisation;
- risk avoidance for example: implement policies, training and education and applying technology;
- risk transference for example insurance (Office of Government Commerce, 2005).

2.5 General Controls and IT Controls
The purpose of a control is to reduce the risk to an acceptable standard whilst considering legislation and regulation, organisational objectives, operational requirements and constraints, costs required to implement the control and the need to balance the cost to mitigate the risk vs. the damage a risk could create. Controls that are used to mitigate risk should meet the requirements identified by the risk assessment.

IT Controls ensure that information is reliable and mitigates the risk in the use of technology. They cover a large spectrum from policies to implementation, technical systems to physical access protection (GTAG, 2005). IT Controls are interdependent and function together to support the automation of business and managing IT (Figure 2.4). It follows a top-down approach starting with governance and management through to implementation.
Controls are classified to explain where they fit in the overall system (Figure 2.5). The classification of controls ensures that risks are controlled in a holistic fashion. IT controls include the following:

- General controls or infrastructure controls apply to the entire system from information security policies to disaster recovery plans. It supports the notion of a holistic information security system.
- Application controls are specific to an application, for example data edits, transaction logging, reporting. They are classified as preventive, detective or corrective.
- Governance controls enable the board to ensure that effective information security policies and IT Governance policies and procedures are in place. The board must review the compliance metrics to monitor the efficiency of the controls put in place.
- Management controls safeguard critical assets, sensitive information and operational procedures. They need to ensure process continuity via the implemented IT controls.
- Technical controls form the basis for all other controls and for example, ensure the reliability of information by implementing access control based on authorisation.
Controls are classified into three groups based on their design and effectiveness:

- Preventative Controls are put in place to prevent the unwanted from happening. For example, the use of a firewall to prevent malicious code being executed and unauthorised access gained to sensitive data.

- Detective Controls monitor preventative controls for breach or failure. The log of the firewall could be checked for any exceptions or attempt to execute malicious code.

- Corrective Controls are used to restore the system to a state of good health. Back-ups are normally used to achieve this.

It can therefore be concluded that these controls assist and guide management, both business and IT, to ensure that their most valuable asset, their information, is adequately protected from internal and external threats.

ISO 27002 suggests that only those controls applicable to an organisation should be implemented. The controls should be chosen when project and system design specifications are created and not as an afterthought. Controls alone will not ensure a holistic security solution. Management must ensure that processes are in place to monitor, evaluate and improve the security controls on an on-going basis.
2.6 Structure of ISO 27002

ISO 27002 starts by defining information security. Information is stored in many forms, for example electronically, the spoken word, on paper, etc. It is important that it is adequately protected regardless of the form of storage.

What is information security? It is the protection of information from all sorts of threats in order to ensure business continuity, to minimize business risk and to support business opportunities (ISO 27002:2005).

Why is information security needed? Information, as previously stated, is a very valuable business asset and should therefore be protected. Information is the lifeblood of any organisation and without it, the organisation will die (Doherty & Fulford, 2006).

As discussed previously, controls are put in place to manage risk. ISO 27002 suggests the following controls should be implemented from a legislative point of view:

- data protection and privacy of personal information. In South Africa the Protection of Information Bill will result in stiff penalties if breached (ITWeb, 2008);
- protection of organisational records. This is applicable as there is a requirement to keep certain records for a period of time;
- intellectual property rights.

In the micro finance industry, it is vital that customer confidential information is adequately secured. Any banking related transaction should be tamper proof and protected. Organisational records are not limited to paper or image format, but could also include telephone recordings in which a contract was created. Protecting intellectual property is vital in our industry as we believe that IT is the enabler providing a competitive edge.

ISO 27002 provides the following as common practice controls:

- information security policy document;
- allocation of information security responsibilities;
- information security awareness, education and training;
- correct processing in applications;
- technical vulnerability management;
- business continuity management;
- management of information security incidents and improvements.

The importance of the information security policy has already been discussed in the comparison between some of the security standards and frameworks and provides the executive mandate to ensure its successful implementation. The board could shift this responsibility and therefore need to ensure that they allocate the responsibilities accordingly while keeping senior management accountable (FFIEC, 2006). The board needs to ensure that all staff in the organisation is familiar with the information security policy and how it affects their day-to-day operations. Any application should be tested thoroughly to guarantee the integrity of the data. Technical and business continuity plans must be created and tested. The management theorem: “you cannot manage what you cannot measure” is very true of information security and therefore all incidents must be recorded and enhancements made to negate a re-occurrence.

In summary, the successful implementation of ISO 27002 should start with an information security policy endorsed by management. A security framework must be used to implement, monitor and improve information security. The requirements for information security, risk assessment and risk management must be well defined. Awareness and communication of information security to the organisation is vital to ensure its success. A budget must be allocated to information security to implement and enhance it as needed. All security incidents must be logged and resolved via a formalised process. Information security management should be measured on an on-going basis.

This research project will take the recommended controls into consideration as well as evaluate which other controls are required for a micro finance company. A model will be built for implementation that will adequately protect the information assets.
2.7 ISO 27002 Control Clauses

Each clause in the standard will be evaluated to determine if it is applicable to a micro finance company, taking into consideration any regulatory and other laws. These clauses will be used to create security standards and build an effective information security management system that will adhere to the **Confidentiality, Integrity and Availability** of information (Figure 1.1). The mind map below (Figure 2.6) illustrates the main sections of the standard which will be covered in this chapter.

![ISO 27002 mind map](image)

*Figure 2.6 ISO 27002 mind map (IsecT Ltd, 2009)*

The relationships between the control clauses of ISO 27002 are illustrated in Figure 2.7.
2.7.1 Security Policy

The implementation of a holistic information security system starts with a directive from management. Consideration must be given to the business requirements and applicable laws and regulations. Policies are created at senior management level and guide the organisation through the implementation and maintenance phase.

Designing and implementing networks and systems that are secure should be done in the planning phase and not as an afterthought. All levels of management should be aware of the relevant security risks and measures to prevent them (OECD, 2002).

2.7.1.1 Information Security Policy Document

Management must approve the information security policy document and ensure that it is communicated to all employees and other relevant parties. It is vital that policies are published in a central place for ease of reference. Versioning should be implemented to keep track of changes and to ensure that the correct version is used.
The information security policy document is the ‘voice’ of management to the rest of the organisation in which they express their commitment to security and how it will be managed.

The policy document should clearly define information security, what are the objectives and how will information security enable the organisation to share information. Information security should align with the business strategy enabling it to achieve its goals (Ericsson, 2007). Any organisation should have a plan to assess and manage risks as discussed in the Importance of Risk Management section. A high-level definition of the security policies, principles, standards and compliance requirements that relate to a MFC could include:

- compliance with legislative, regulatory and contractual requirements e.g. National Credit Act (NCA), Privacy Bill, Electronic Communications and Transactions Act (ECT);
- education of users on information security and a continual awareness of what it entails;
- ensuring that business continuity management is in place;
- consequences of policy violations.

Any policy should be treated as company confidential by implementing the necessary controls to safeguard it. If there is a requirement to distribute it to external parties, be careful that confidential information is not disclosed to them. A Non-Disclosure Agreement (NDA) should be signed to protect the vested interests of both parties. An NDA is a legally binding contract where the two parties pledge to protect each other’s trade secrets and not to disclose them without one another’s consent (Nolo, 2008)

2.7.1.2 Review of the Information Security Policy
Business requirements are dynamic and change often. The information security policy must be reviewed on a regular basis to ensure that it is still relevant and that it protects the information assets appropriately, especially when major changes in the mode of operation are made by IS. In order to ensure that the information policy provides efficient and effective protection that remains relevant, an owner needs to be appointed by management to keep the policy up to date (Karyda, Kiountouzis & Kokolakis, 2005). Regular reviews should lead to assessing opportunities for improvement of the information security policy. Management reviews should be defined and scheduled.
The input to the management review should include feedback from all involved in the use of information to determine the balance between too much security and too little. External reviews are a good source of information to see how well the organisation benchmarks against current standards and frameworks. The organisation must be able to measure how compliant they are in the implementation of information security and address the areas where it is not sufficient. As mentioned before, business is dynamic and any changes in strategy or regulatory requirements that affect the policy must be implemented. The review should look at existing security incidents and how to avoid them. “A policy is not a one time, fire and forget event” (Luzwick, 2001).

The output from the management review should include:

- an enhanced approach in securing information assets;
- better controls implemented;
- optimum use of resources.

All reviews must be documented. Any changes to the policy must be approved by management and communicated to the organisation (continuous education).

An information security policy is relevant to any business. It proclaims management’s commitment to the protection of the information assets and guides staff on how to use it in a secure fashion. The policy acts as the foundation on which the security model is built.

### 2.7.2 Organisation of Information Security

ISO 27002 considers both the internal and external aspects of an organisation. The focus internally is to create a framework for the successful implementation of information security within the organisation. The external focus ensures that the information and processing facilities used by third parties are properly secured and well managed.

#### 2.7.2.1 Internal Organisation

A management framework must be created to ensure the successful implementation of information security within the organisation. It starts with an approved information security
policy by management and a commitment of resources to implement the policy. External security experts or groups should be used to ensure that the policy is in line with standards, best practices and industrial trends. The process of handling a security incident should be well documented.

Kritzinger and Smith (2008) define six IT authority levels starting at the top representing the board and directors who take ultimate responsibility for information security. They define the second level as Executive Management, who includes the CEO and could closely work with the board and overlap in responsibilities such as Information Security Governance. Middle management is the third level and constitutes department heads who must ensure that policies and procedures are implemented correctly. The Technical Management level includes those who are responsible for designing and operating the computer systems. The Information Security Management level is the fifth and they are responsible for the day-to-day monitoring of all information in the organisation. The sixth level includes the users of the system who have the responsibility to secure the information with which they work (Kritzinger & Smith, 2008).

Without the support of management directing the organisation and making the objectives of the information security policy clear, successful implementation will not be achieved. Management should clearly define the security goals while meeting the organisation requirements and aligned to business strategy. As discussed previously, they must create and review the information security policy, implement it and rate its effectiveness, commit resources for implementation and educate the users.

Additionally, information security should be co-ordinated across the organisation preferably by a cross-functional group including managers, users, administrators, application designers and auditors (Kritzinger & Smith, 2008). This group should ensure that security activities are performed according to the information security policy and they need to establish how to handle non-compliance. They are responsible for the information security methodologies and processes including risk assessments, identifying significant threats, ensuring user awareness and training, reviewing incidents and recommending appropriate action.

Furthermore information security responsibilities should be clearly defined in line with the policy especially where individual assets must be protected or specific security processes
must be followed. Certain responsibilities will be delegated to individual managers who can delegate these tasks, but the responsibility to ensure that the task is performed correctly will remain with them. Some of the areas that these individuals are responsible for include the identification of the assets and security processes in their area, identifying the entity responsible for these assets and security processes, and documentation of authorisation levels. In larger organisations a security manager will look after security and identify the controls required to protect each asset. At the implementation level each manager must ensure that a resource is assigned to implement the controls in order to protect the asset on an on-going basis.

Any new information processing facility should be authorised by management to validate its purpose and use. Calder and Watkins (2005) describe this as any new component added to the system such as a new software system, a new Data Centre or a new server. It virtually touches anything in the networked office. Authorisation should be obtained from the manager currently looking after security in that facility to ensure that the new system adheres to security policies and requirements. New hardware and software introduced should be checked for compatibility with existing systems, taking into account any new threats or vulnerabilities identified and how to mitigate them. This could be a mammoth task and therefore it is desirable to divide the facilities into manageable sizes. The size of the organisation will determine how many managers are needed per facility.

Managers and staff have access to confidential information and therefore a mechanism must be in place to protect it. Confidentiality agreements or non-disclosure agreements should be used to protect the company’s confidential information using legally binding terms. The NDA should define the information to be protected, how long it will be in effect, discuss termination of the agreement and responsibilities of the signatories, amongst other things. Ownership of information with regards to trade secrets and intellectual property should be defined clearly. In addition, since NDA’s are legally binding they therefore should adhere to local applicable laws and regulations. It is standard practice to include a NDA in the employee’s contract.

In the event of a security breach, staff should follow procedures to determine when and which authorities to contact. Authorities include: law enforcement, fire brigade, emergency services. When under attack from the internet, telco providers and internet service providers should be
informed to determine where they can assist. These contacts must be maintained and documented in the disaster recovery and business continuity plans.

Regular change in IT necessitates that the information security practices are kept current. One recommended way to do this is to join a specialist information security group such as the Information Security Specialist Group (BCS-ISSG) which is a subgroup of the British Computer Society. This will allow for information sharing and could result in a more proactive approach to the latest threats and vulnerabilities.

Because systems change on a regular basis, Management should initiate a regular independent review of information security or when major changes have been made to business strategy or regulatory requirements. The results of this review must be recorded and if it is found not to be satisfactory, the onus is on management to take corrective action.

In summary, a successful implementation of information security starts with management demonstrating their commitment to the process by implementing the necessary internal controls and measuring their effectiveness.

2.7.2.2 External Parties
Any organisation needs to interact with external parties as defined in their value chain. In the micro finance industry these include financiers, customers, retailers and service providers. The risks in dealing with external parties must be defined (a risk assessment) and the correct controls put in place before engaging with such parties. Flowerday and Von Solms (2005) warn that information could leave the boundaries of an organisation and via the internet be made available to literally any computer connected to it.

Therefore the value of the information and how it will accessed (remotely, on-site, off-site) should carefully be considered. It is advisable to create a contract so that both parties fully understand their obligations and responsibilities. If deemed necessary, the information security of third parties should be checked to ensure that the asset is protected adequately.

In the value chain, customers are the heart of any organisation and interaction should be encouraged. The risks in giving customers access to the organisation’s information or assets
should be determined before giving them any access. The controls required for disclosure depend on how much information and how sensitive the information is. An access control policy is required to ensure proper authorisation before granting access, revoking access and what is considered forbidden access. It should clearly define the customer’s obligations and use of the information.

2.7.3 Asset Management

In Chapter 1 it was mentioned that information should be treated as an asset. An asset is something of value. Every asset should have a dedicated owner and recorded on an asset register. The owner can delegate the responsibility of the asset, but remains accountable for the proper protection thereof.

The asset register must record the information required to recover from a disaster including the type of asset, its location, backup information and value to the organisation. Ownership should be documented and the information classified. The level of protection is determined based on the importance of the asset and its business value. According to Sholes (2007), more than 50% of assets on an asset register cannot be located. This stresses the importance of keeping the register up to date.

Assets can be classified into various groups:

- Information assets include databases, contracts, system documentation, user manuals, training material, procedures and business continuity plans.
- Software assets include application, operating system, development tools and utilities.
- Physical assets are computers, communication equipment, etc. Services include power, cooling, lighting, etc.
- People, their qualifications and skills are an important asset.
- Reputation and image of the organisation is classified as an intangible asset.

Once the assets are grouped, an inventory of assets must be created to facilitate successful risk management. This inventory documents ownership of an asset. Ownership of assets results in properly classified assets and the regular review of the access control granted to an asset. Ownership can be allocated to a business process, a defined set of activities, an
application or a defined set of data. Groups of assets can be combined as a service. The service owner is then responsible for its delivery and maintenance. Acceptable use of assets should be governed by defined rules. These rules should be documented and implemented. They will cover both the internal organisation and external parties.

Information should be treated as any other asset and therefore be classified to ensure that it is adequately protected. An information classification scheme should be used to define the required level of protection needed taking into account any special handling measures. ISO 27002 states that information should be classified in terms of its value, legal requirements, sensitivity and criticality to the organisation. The asset owner should define the asset’s classification. Stevens (2005) states that defining ownership and custodianship of information is often a difficult task as information flows through an organisation to external parties. The classification scheme ought not to be complicated and should be practical to implement. The level of protection is determined by the requirement for Confidentiality, Integrity and Availability of information. Assets, in either physical or electronic formats, should be labelled in order to facilitate information sharing arrangements. It is easy to label a document, but electronic media must also be labelled for example, on the screen when displayed. Electronic information can also be labelled via meta-data.

2.7.4 Human Resources Security

Any candidate for employment, whether on contract, permanent or third party, should be screened before employment is offered. This is to ensure that they are suitable for the position under consideration, in order to attempt to reduce the risk of fraud, theft and abuse of systems. The prospective candidates should be briefed on the security roles and responsibilities which should be documented in the job description in line with the information security policy.

Screening checks include character references, a completeness and accuracy check on the candidate’s curriculum vitae, confirmation on academic qualifications, identity check, check for criminal records and credit checks. Depending on the level of the position and the sensitivity and confidentiality that the role requires, more detailed checks might be required (ISIQ, 2007).
Furthermore, a screening process should be defined for third parties and contractors especially if an agency is involved. The agency needs to understand its obligations in providing the necessary reference and other checks.

The information gathered regarding all prospective candidates should be collected and handled according to the applicable laws in South Africa. This information can also be classified as sensitive and therefore should be protected.

The terms and conditions to be signed by any employee, contractor or third party should clearly state their obligation with regard to information security. The terms and conditions should be aligned with the information security policy and should clarify the use of sensitive information, the respect of the common law (e.g. copyright laws), the handling of classified information, off-site use of information and how non-compliance will be treated. Terms and conditions should be agreed upon and could even have a limited time period after termination of employment.

A code of conduct can be used to govern the behaviour during the time of employment. Management is responsible for ensuring that the employee or contractor of third party is made aware of any security threats and concerns on a day-to-day basis and their responsibility to ensure that the risks are reduced in their normal work. On-going awareness and training is necessary to ensure that all are informed. A disciplinary process should be in place for any breach.

Therefore, security awareness should start with the induction programme and the policies and procedures should be explained to the employee and where required, the contractor or third party. The acceptable use of information processing facilities e.g. log on procedures and use of software, should be explained. The level of training should be suitable and relevant to the person’s role within the organisation.

When a security breach occurs, and the necessary evidence collected, a formal disciplinary meeting should be held. Depending on the severity of the security breach the process should allow for instant dismissal in which all access rights are removed and the person escorted off the site. The disciplinary process should be a warning to other employees, contractors and third parties not to cause a security breach.
An important step in the employment process is to ensure that a formal exit procedure exists on termination of employment. The employee, contractor or third party must be reminded of what was agreed in their contract and the clauses regarding post-employment. All assets in the possession of the employee, contractor or third party of the organisation must be returned via a formal procedure and so documented. Any knowledge important to ongoing operations that will part with the employee must be documented if not done so already. Access rights should be removed or re-evaluated. Access rights include physical and logical access, keys, identification cards, access to systems e.g. domain accounts. Any passwords known to the exiting party should be changed upon termination. Where a person was part of a group, access to that group must be revoked and the rest of the group informed of this action.

2.7.5 Physical and Environmental Security

Secure areas should prevent unauthorised physical access, damage and interference to the organisation’s premises. Data Centres should be housed in such environments where information processing facilities are appropriate. Depending on the requirement, security perimeters should be clearly defined and the strength and siting used based on this requirement. The building housing the Data Centre should be physically sound to the extent that it would resist burglary, not be conducive to flooding, the external walls of a solid construction and all external doors are appropriately protected against intruders.

A manned reception area should be used to control access to the building and access should be granted to authorised personnel only. Physical entry controls should be used to ensure only authorised personnel have access to these areas. To achieve this, visitors should be signed into a visitor’s book and given access only to the areas they need to visit. Access to areas where sensitive information is processed should be monitored and reviewed and access only granted based on successful authorisation. Every person should wear some sort of visible identification and personnel should immediately contact security if they encounter unescorted visitors. Access rights to secure areas should be regularly reviewed and updated and revoked when necessary.

Furthermore, areas where information processing facilities are found should not be accessible to the public. Buildings should not give away their importance in information processing
facilities. The building should enhance the protection of Data Centres by not making their location obvious. Scalet (2005) suggests that signs indicating the location of the Data Centre should not be used.

External and environmental threats should be taken into account when designing the secure access areas. These include disasters such as: fire, flood, earthquake and explosion. Neighbouring buildings should be inspected for possible threats including fire and water damage and corrective action taken if needed. Scalet (2005) suggests neighbours should not include airports, chemical facilities and power plants. Hazardous or combustible materials should be stored at safe distances from the secure area. The disaster recovery equipment should be housed at a safe distance from the main site. Fire fighting equipment should be installed in the secure areas.

When working in secure areas, it should be monitored and controlled. Unsupervised working in secure areas should not be tolerated. Vacant secure areas should be physically locked and checked on a regular basis.

In addition, delivery and loading areas should be separated from information processing areas to avoid unauthorised access. Incoming material should be checked for threats before moving it into the operational area and it should be registered in accordance with the asset management procedures. Equipment must be protected against physical and environmental threats. Equipment used in sensitive information processing facilities should be sited so that access to it is minimal. Equipment should be maintained according to the requirements of the manufacturer. Only authorised personnel should carry out repairs and service equipment. An incident register for all failure faults should be kept. Eating, drinking and smoking should be prohibited in secure areas. Environmental conditions such as temperature and humidity should be checked and controlled.

The risk in regard to supporting utilities i.e. electricity, water supply, sewage, heating/ventilation and air-conditioning should be adequately controlled. Regular inspections and tests are required to ensure their proper functioning. An Uninterruptable Power Supply (UPS) is of utmost importance to ensure proper shutdown or continuous run of equipment. A backup generator will be required once the UPS runs out of power. Both the UPS and generator should be inspected and tested at regular intervals. Emergency power off switches
should be installed near emergency exits in equipment rooms to facilitate rapid power down in case of emergency. Telecommunications equipment should be connected to the service provider by at least two different routes to provide failover. Multiple power grids will also provide for power failover. Data cables should be protected from interference or interception. These cables should be underground where possible and segregated from power cables. Cables should be clearly labelled to minimise problems during maintenance.

The use of off-site equipment should be authorised by management. Equipment and media taken off-site should not be left unattended in public places. It is vital to adhere to the manufacturer’s instructions to safeguard the media for example, from exposure to direct sunlight. Insurance cover should be in place to protect the off-site equipment.

Before disposing of equipment it should be cleared of any licensed software and any sensitive data. Techniques should be used to ensure the data is non-retrievable. Information can be compromised through the inadequate disposal or re-use of equipment. Any equipment to be taken off-site must be undertaken with prior authorisation. Equipment should only be taken off-site for a limited period and returns should be checked for compliance.

### 2.7.6 Communications and Operations Management

Operational procedures and responsibilities are required to ensure the correct and secure operation of information processing facilities. Operating procedures should be documented, maintained and made available to users who need them. These procedures should specify how to process and handle information, how backups should be performed, scheduling of jobs, instructions for handling errors and exceptions, system restart and recovery procedures for use in the event of system failure and the management of log information.

Change management supports the operational procedures by ensuring that changes happen in a controlled fashion to information processing facilities and systems. Change management consists of identification and recording of significant changes, planning and testing of changes, assessment of the impact, formal approval procedure, communication of change details to all relevant persons and fallback procedures to recover from unsuccessful changes. Inadequate change control can result in system or security failures. Changes should only be made if there is a valid business case to do so. Applying the latest versions of an operating
system might not be the best thing for an organisation, if for some reason it causes system downtime.

Operational duties should be segregated to reduce the risk of system misuse. No single person should be able to access, modify or use assets without authorisation or detection. The person who initiates the change should not be the same one who authorises it. The development, test and operational facilities should be separated from the production environment to ensure that unauthorised changes are not made. It is important to define rules for the deployment of development software to the operational environment. Development and operational software should run on different systems as well as hardware and networks where possible. Development tools should generally not be needed in the operational environment and must be guarded against. The test environment should be setup in the same way as the operational environment. Users should use different user profiles for operational and test systems and the applications should portray whether you are using the test or production application. Sensitive data should not be copied into the test environment. The UAT (User Acceptance Testing) environment should be stable within which to conduct meaningful testing. Development staff should not have access to the live system to ensure that malicious code is not deployed or sensitive information compromised.

Third parties should adhere to operational procedures and change management. Third party service delivery management should periodically be checked to ensure that they adhere to security controls, service definitions and delivery levels included in their agreement. The third party should provide regular reports, reviews and audits. The responsibility to manage a third party must be designated to a specific individual. Changes made to services by a third party should be managed carefully to ensure business continuity.

Operational procedures and change management guide day-to-day activities, whilst system planning and acceptance should be performed to minimise the risk of system failures. Capacity planning monitors resources to determine the requirements of the future. Capacity planning should take future business growth into consideration and be aligned with the business strategy. Ample lead time should be given for acquiring equipment of high importance and cost. Systems acceptance ensures that new information systems, upgrades and new versions of software are well tested before deployment to the production environment. Systems acceptance is a formal acceptance procedure which may include
certification or accreditation. Controls are required against malicious code to ensure the integrity of information and software. Various software products are available to protect systems.

In the unlikely event of a compromised system, backups ensure that data can be restored to a reliable state. All essential information should be backed up and these backups should be tested on a regular basis. Network security management ensures the protection of information in networks and the protection of the supporting infrastructure. Networks could span multiple organisations and it is important to ensure that sensitive information is adequately protected across all networks. All media should be controlled and physically protected to prevent unauthorised disclosure, modification or destruction of assets. Removable media should be governed by procedures to protect its use. Media should be disposed of according to procedure when no longer needed ensuring that sensitive information will not be compromised. Information handling procedures guide the use of information regarding handling, processing, storing and communicating information consistent with its classification. This process applies to all formats of media and is not limited to documents or computer systems such as mobile communications, mail and voice. System documentation should be protected against unauthorised access to protect systems, applications and data structures.

As stated before, information is the life blood of any organisation and therefore it needs to be exchanged within an organisation and with external entities. It is vital to protect it adequately. Formal policies and procedures should be implemented to ensure integrity of data. Exchange agreements should be used between the organisation and external parties. Physical media in transit must be protected against unauthorised access, misuse or corruption during transport. Electronic messaging (e.g. email, Electronic Data Interchange (EDI), etc.) forms a significant part of communication between organisations and must be protected. Business to business processing is on the increase and sharing of information poses a risk which should be mitigated. Electronic commerce includes on-line transactions and public available information. Electronic commerce between parties results in data being transported over public and private networks; this data will require protection. On-line transactions must be protected from incomplete transmission, mis-routing, duplication or replay. The more vulnerable the transaction, the more security controls required. Information on a publicly available system should be protected against unauthorised modification.
To ensure the successful protection of information, monitoring is required. It involves looking after systems and logging all information security events. Audit logs are used to record all user activities, exceptions and information security events and should be kept for a defined time period to assist in investigations as required. System use should be monitored based on a risk assessment to ensure users are using the system for which they are authorised. Logs should be protected as they provide a full audit trail of what happened on a system and may be required in an investigation. Administrator and system operator logs should be reviewed on a regular basis. Faults should be logged, analysed and appropriately fixed.

2.7.7 Access Control

The access control policy defines rules and rights for each user or group of users. Access control covers both physical and logical aspects. According to ISO 27002, access rules should be based on the premise “that all is forbidden until expressly permitted”. User access management ensures authorised user access to information systems by registering users for system access, allocating them privileges in a controlled fashion and managing passwords through a formal process. User access rights should be reviewed on a regular basis.

Users must understand that they have a responsibility with regards to information security. Without user participation it will be difficult to have a secure system. Users should ensure that their password use is according to the information security policy which could include keeping passwords confidential and selecting a password of a particular strength. Users must understand that unattended equipment must be made secure before leaving the equipment. Active sessions should be logged off and screensavers with password options should be used. A clear desk and clear screen policy reduces the risk of unauthorised access, loss or damage of information.

Users are primarily responsible for their own workstations. The IS/IT departments are responsible for network-, operating system- and application access control. Network access control prevents unauthorised access to network devices. A policy governs which services a user has access to and includes how these services should be used once authorisation has been granted. External connections, for example via Virtual Private Network (VPN) should be governed by authentication methods. Segregation of networks is important as mentioned
previously where the development, testing and production environments are separated on different networks. Operating system access controls are vital in preventing unauthorised access to systems. Secure log-on procedures should be used to authenticate the user and minimise the opportunity for unauthorised access. Each user should uniquely be identified on the network to trace their activities and ensure that they adhere to the acceptable use of the systems. A password management system ensures the quality of passwords used by restricting the re-use of passwords and enforcing strong passwords to be used. System utilities capable of overriding systems and application controls should be carefully regulated. Inactive sessions should automatically shutdown after a defined period of time to prevent unauthorised access. Connection time to certain resources can be limited thereby reducing the chance of unauthorised access obtained. Application and information access control allows only authorised personnel to access applications and their own information based on the access control policy. Only menus within an application are accessed so that there is control over the read, write, execute and delete rights per application. Sensitive systems should have an isolated computing environment. The sensitivity of an application should be identified and documented by the application owner who then decides how isolation should be achieved.

Furthermore, with the advances made in mobile computing, new threats are created that could lead to a compromise of information. Care should be taken when using mobile devices in public areas so as to avoid physical access control and unauthorised disclosure of information. Teleworking allows users to work at a fixed site outside of their organisation. The necessary controls should be in place to secure the teleworking site.

### 2.7.8 Information Systems Acquisition, Development and Maintenance

ISO 27002 defines information systems as operating systems, infrastructure, business applications, off-the-shelf products, services and user developed applications. Information security should be included in the design to ensure that the business processes are adequately protected. Correct processing in applications will prevent errors, loss, unauthorised modification or misuse in applications. Data input validations should be used to ensure correctness of data. Automatic examination and validation can be used where appropriate. Control of internal processing ensures that the data captured is not corrupted through hardware or processing errors. Balancing controls and check totals should be used to validate information. Message integrity between applications can be ensured with the use of
cryptography. Data output should be validated to ensure that processing and storage are correct.

In addition, cryptographic controls protect the confidentiality, authenticity or integrity of information. A policy should be used to determine whether a specific cryptographic control should be used or not. All cryptographic keys should be managed and protected against modification, loss and destruction.

In the use of any system, changes to operational software are unavoidable and should be controlled to minimise the risk of corruption. When performing updates to the software ensure that a rollback plan is in place. Any upgrade should support the business requirements. Test data should be carefully selected and protected. It is not advisable to use databases for test data that contains sensitive information. Only authorised personnel should have access to program source code.

When new systems are developed, security should be part of the development and support process and not an afterthought. Proper change control is required to minimise the corruption of information services. New software should be tested in a segregated environment before deploying to the production environment. When operating systems are changed, business critical applications should be tested to ensure that they work correctly and are secure. Software package changes should be restricted to only critical updates. Information leakage is normally caused by Trojan code and measures can be taken to protect systems from it. Outsourced software development should be supervised and monitored to ensure that it meets organisation standards and that the code does not contain vulnerabilities. Technical vulnerabilities must be evaluated as soon as possible and appropriate action taken to address the associated risk. It is important to keep an accurate inventory of software deployed to estimate the possible damage that could be caused by a vulnerability. It is recommended that patches are tested before deploying them to the production environment.

2.7.9 Information Security Incident Management

Reporting of information security events and weaknesses should be reported through appropriate management channels as quickly as possible. A formal reporting procedure should be used together with an incident response and escalation procedure. All employees,
contractors or third parties must report any security weaknesses and should not attempt to test
them as it could result in damage to information systems or result in system loss.

Once an information security weakness or event has been reported, procedures and
responsible people should manage it quickly and effectively. The monitoring of systems,
alerts, and vulnerabilities should also be used to detect information security incidents. Based
on the type and occurrence of incidents logged, learning should take place to try and prevent
a re-occurrence. This could include enhancing the security system and introducing new
controls. Evidence must be collected if there is legal action indicated after an information
security incident. It is vital that evidence will stand up in court and that it meets the required
quality and completeness.

2.7.10 Business Continuity Management
Business continuity management is used to counteract interruptions to the business and to
ensure the continuity of critical business processes during a disaster. A process should be in
place to ensure that the business can recover to an acceptable level of operation through the
use of preventive and recovery controls. The consequences of disasters should be subject to a
business impact analysis. Information security should be incorporated in the business
continuity plan to ensure that the critical information assets are protected.

In order to create a successful business continuity plan, business continuity risk assessments
should be conducted to identify the probability and impact of interruptions and their
consequences for information security. The business continuity plan should not only look at
the critical business processes, but at the organisation as a whole and how information
security will be affected. A business continuity plan must be created to determine how the
system will be restored to an acceptable level and in which time frame with adequate
information security to protect the assets. A business continuity framework will ensure that
all business continuity plans adhere to the same information security standards and
requirements and that priorities are identified for testing and maintenance. Business
continuity plans should be tested on a regular basis to ensure they are up to date and effective.
2.7.11 Compliance

Compliance with legal requirements is needed to avoid breaches of any law, regulatory or contractual obligations. Information management systems may be subject to these laws and should be designed to be compliant. All applicable legislation should be identified and the organisation must meet these requirements in the use of their information systems. Intellectual property rights must be protected, both those that belong to the organisation and those of externals. Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licenses. Careful attention must be given to software with license agreements to ensure that the organisation does not operate in breach. Important records should be protected and classified accordingly e.g. transaction logs, audit logs, accounting records, etc. Retention periods and type of storage should be recorded. The media should be inspected at regular intervals to ensure that it does not deteriorate beyond use. In the long term, paper and microfiche are recommended. All media should be handled according to the manufacturer’s instructions. Personal information must be protected as per the relevant legislation, regulations and contractual agreements. Consider appointing a data protection officer to ensure that the organisation is compliant.

Users should be deterred from misusing the information processing facilities. If any system is used for non-business purposes without the consent of management, it should be deemed inappropriate and unauthorised. Users should be aware of the scope of their permitted access. If any monitoring software is to be loaded on an individual’s computer, they should be informed of such in writing.

Managers must ensure on a regular basis that staff is compliant with the information security policy of the organisation. They should review the compliance of information processing in their area and correct any non-compliance immediately.

Technical compliance checking should happen on a regular basis to ensure that information systems are compliant with security implementation standards. This could be a manual and/or automatic process (if tools are available) in creating a report for a technical expert to analyse. Penetration tests or vulnerability tests should be planned and executed with caution as it could lead to a compromise of information security. Such tests should be documented and repeatable. Audits on information systems involving checking operational data, should be planned carefully to minimise the risk of business process disruptions. Audit requirements,
including the scope of the audit, should be discussed before the audit takes place. Information system audit tools should be protected to prevent any misuse or compromise. Software and data files used must be kept separate from the production environment. Third parties who could compromise the data may be involved. Therefore, controls such as physical access and changing of passwords should be considered once users are finished with the information and no longer require access.

2.8 Conclusion
Implementing ISO 27002’s 11 controls will result in a holistic security system. Figure 2.7 illustrates the relationships between the various controls. ISO 27002 covers the security requirements as directed from the board (the policy) all the way down the chain of command to operational implementation.

In the financial services industry, compliance, business continuity, access control and development and maintenance of information systems are vital for success. IT is seen as the business enabler providing a competitive edge. Implementing information security successfully will enhance the information asset’s Confidentiality, Integrity and Availability, therefore enhancing the overall productivity of the organisation.

Chapter 3 will focus on building a case study of how one would go about implementing ISO 27002. A survey will be used to determine the current state of information security within a MFC and will be rated based on awareness and successful implementation. A roadmap will be created to ensure that all risks are successfully mitigated.
Chapter 3

Case Study

Chapter 1
Introduction

Chapter 2
Current Security Models and Standards
Literature Study

Chapter 3
Case Study
Empirical Research

Chapter 4
Findings and Recommendations: Building a Focused Security Model for a South African MFC

Chapter 5
Conclusion

Chapter 3

3.1 Background
3.2 The Micro Finance Industry in South Africa
3.3 Overview of the Company used in this Study
3.4 Research Methodology
3.5 Primary Data Collection
3.6 Primary Data Analysis
3.7 Detail Primary Data Analysis
3.8 Conclusion
3.1 Introduction

As referred to in Chapter 1, a case study is defined as a research strategy, an empirical inquiry that investigates a phenomenon within its real-life context (Yin, 1984). The objective of this study is to build a model for Information Security Management and therefore a case study is suitable in analyzing the current day-to-day operations of a MFC and to create a relationship reflecting the theories applied.

The primary data generation method used consisted of a questionnaire to determine how Information Security Management is currently practised within the micro finance company in protecting information as an asset. This provides more information about the ‘as is’ model which will be used to transform the Information Security Management model to the proposed one based on this study’s findings.

In this section, an in-depth study will be made of the current MFI in South Africa to determine the information security requirements both from a regulatory perspective and an organisation perspective.

3.2 The Micro Finance Industry in South Africa

South Africa experienced a major boom in the provision of unsecured loans in the mid 1990’s. An “unsecured loan” is when the lender does not hold any security against the borrower who may default on said loans (Cameron, 2000). These credit providers were not governed by the Usury Act of 1968 which was “To provide for the limitation and disclosure of finance charges levied in respect of money lending transactions, credit transactions and leasing transactions and for matters incidental thereto” (Guarantee Trust Hypertext Systems (Pty) Ltd, 2003).

The market segment was the emerging market catering for people in the lower income groups. This was a large market and was estimated at 80% of South Africa’s adult population (South Africa, 2006). High interest rates (up to 1000% p.a.) and illegal methods of collecting money were the norm. Due to these practices the industry developed a bad reputation and lenders were referred to as ‘loan sharks’.
The South African Government intervened in the early 2000’s and through the Department of Trade and Industry formed the Micro Financing Regulatory Council (MFRC). The MFRC’s main purpose was to empower borrowers to make informed financial decisions and to support them in managing complaints (South Africa, 2006b). The Usury Act Exemption Notice was used to protect borrowers in making use of unsecured loans by stipulating the following:

- The lending institution is registered with the MFRC and complies with the Exemption Notice and the conditions therein;
- The loan amount does not exceed R10 000;
- The repayment period does not exceed 36 months, and
- The loan amount is not paid in terms of a credit card scheme or withdrawn from a cheque account so as to leave the account with a debit balance.

The above rules were implemented to protect especially the consumers of the emerging market who had to obtain financial assistance from micro lenders because they did not qualify for finance at the more established institutions i.e. major banks. The MFRC plays the role of policeman to ensure that the rules are implemented.

The MFRC is responsible for ensuring that the industry adheres to the abovementioned criteria. Their core responsibilities are defined as follow:

- **Accreditation and Compliance**: all lenders register with the MFRC and abide by the Exemption Notice;
- **Complaints and Enforcement**: deals with all complaints from borrowers and advise them of their rights;
- **Debt Relief Programme**: a project to enhance the financial well-being of debt ridden and vulnerable consumers;
- **Education and Communication**: both the lenders and the consumers should be educated about the MFRC’s role;
- **Investigation and Prosecutions Division**: to investigate those not abiding by the laws both registered and unregistered credit providers and to assist the South African Police in any court cases.
In 2005, the MFRC was replaced by the National Credit Regulator (NCR). It was established as the regulator under the National Credit Act No. 34 of 2005 (The Act) and is responsible for the regulation of the South African credit industry (National Credit Regulator, 2008).

3.3 Overview of the Company used in this Study

This study was performed at a South African based micro finance company with a staff compliment of ~1400 members and 90 branches nationwide. The company’s success has been based on its good collection capability and has, since its inception, diversified its product range to unsecured loans, insurance, cellular and educational products. All these products function on the same premise that there is a monthly instalment to collect.

The products are sold through its various channels: branches, telesale call centres and agents. Pre-contract data is stored in a staging database where rules for scoring and affordability are applied. Based on the client’s score, which consists of a number of behavioural rules, a credit risk rating is applied. This risk rating and the client’s affordability is used to determine the product set for which the client qualifies.

The NCA stipulates that the client must be given a quote for any credit products before the contract is finalised (South Africa, 2006b). Once the client has accepted the quote, a contract is created on the Debtor’s Management System where the contract lifecycle is managed from disbursement (financial products), collection of instalments to credit control through either the call centre or legal action.

The Debtors Management System is shared by all the business units allowing for one view of the customer. The information is not classified for ownership or confidentiality and will have to be addressed to ensure that the correct level of protection is used. The staging data is stored in separate databases which make it easier to define ownership. The challenge starts once the contract is created and must be managed through its life cycle as ownership does shift during various processes.

As previously stated, the company has 80 branches which are connected to head office via a VPN solution that provides a secure mechanism for data communication. All domain security is controlled by Microsoft’s Active Directory. A DMZ (demilitarized zone) is created to
protect the company’s information assets, most importantly structured data (databases). A DMZ can be defined as a computer host or small network that creates a neutral area between the public (external) network and a company’s internal network thus protecting critical data from external users (Ewens & Hoppe, 2008).

All applications are custom written and maintained. Access is restricted to the production environment through a software release management team ensuring that change control is implemented in a controlled environment. Business sign-off is obtained through User Acceptance Testing (UAT) before any system is placed into production.

Figure 3.1 (personal communication, Rudy Kriel, March 2009) outlines the process flow of the software release management function. It embeds the Systems Development Life Cycle (SDLC) processes from requirements analysis through to the coding and testing phases. All of these phases must be completed before a deployment can be scheduled. The developer team does not have access to the live environment and all deployments are facilitated through the Software Release Management (SRM) team providing segregation of duties. The deployment plan caters for a full rollback should there be unexpected problems with the newly deployed version of a system.

Database access is controlled by the Database Administration (DBA) team. They play a similar role to the SRM team for any backend related changes. They need to ensure that any backend process or script they are asked to run was tested and signed-off by business.
3.4 Research Methodology

The theory of this study was explained in Chapter 2 based on ISO 27002 and chosen as the information security standard of choice. The 11 controls were discussed in detail to ensure that the requirements of a **holistic security system** are taken into account. According to Olivier (2006), a questionnaire starts with a theory from which a hypothesis is formulated based on a phenomenon that is observable. Once the data is collected, it is analysed and the hypothesis tested to confirm or modify the theory.

The goal of the questionnaire was to confirm whether information security perceived and used by the MFC was correctly understood. The results of the questionnaire will be analysed and used to inform a model based on a sound security standard, eliminating errors and omissions.
3.5 Primary Data Collection

A questionnaire was created to determine the ‘as is’ or current state of how information is currently perceived and protected. Questions broadly covered the understanding of the information security policy through to implementation. The questionnaire was hosted on the company’s intranet and was based on ISO 27002. Figure 3.2 depicts the survey process.

![Diagram](image)

*Figure 3.2 Survey Process*

3.5.1 Population

The population consisted of the senior management team and the ICT team. A total of 51 responses were received out of a possible 105. Due to such a high response rate, the results are viewed as representative of the population. The job roles of the participants are indicated in Figure 3.3. The results obtained represent a mixture of business and ICT users across all business units at various levels. It is important to gauge the understanding of the employees in relation to Information Security applied and how well users are protecting information as an asset. Furthermore, the management team should drive the CIA concept down to the lower levels of staff to ensure information is adequately protected. The directive starts with the board and then ensuring communication throughout the organisation.
Part of the research problem of this study is to highlight that users in general do not understand the importance of a holistic information security system and therefore the inclusion of the senior management team in the population. Users tend to display the urge to get things done without realising the risks involved. The findings of this study will incorporate the risks elements as well.

### 3.6 Primary Data Analysis

#### 3.6.1 Questionnaire Design

Figure 3.4 is adapted from Figure 2.7 to indicate how the questionnaire questions relate to the controls in ISO 27002. Questions were selected on controls more applicable to the micro finance industry, specifically for a company that maintains and develops a large number of
custom written systems. In this type of environment, the communications and operations management, access control and information systems acquisition, development and maintenance controls are very important. Therefore, the number of questions which focused on these controls were increased.

The aim of this study was to ensure that a holistic security model was built and therefore a balanced approach was taken to ask questions from 10 of the 11 controls. Incident management will be part of the final solution although no questions were asked on this control in the questionnaire. The logging, reviewing and resolution of incidents, forms part of the job role of the current ICT team.

Figure 3.4 Relationship between ISO 27002 control clauses (Calder, 2006)
3.6.2 Questionnaire Highlights

The following questions were deemed very important and thus must be adequately addressed in the final solution. The analysis of the data will be discussed in the next section (3.5 Analysis of Responses). The full questionnaire is attached in Appendix A.

The security model starts with the ‘buy-in’ from senior management. Therefore, it is important to ensure that an information security policy is in place and implemented by the workforce. The first questions were based on the information security policy to check if it existed and whether the staff were aware of it. 71% agreed that the policy was approved by management and therefore knew that the company had one in place. However, 72% of respondents do not actively review the policy to ensure that their information assets are protected. Senior management should ensure that processes are put into place to support this policy.

The results concur with the researcher’s perception of the status quo. All policies are published and available to all staff members. The staff members are all aware of what is available. It seems, however, that the implementation of these policies is weak. This needs to be addressed to ensure ownership of information assets. This is seen in Question 5 where active support is given for information security, but there seems to be a lack of ownership by the lower management business teams of the information itself. This should be addressed by the implementation of suitable procedures that support these policies.

1. (Section: Information security policy document.) The MFC has a management approved Information security policy that is published and communicated to all employees.
2. (Section: Review of Informational Security Policy.) Management review the information policy at regular intervals to ensure that it protects your information assets.

3. (Section: Management Commitment to Information Security.) Management demonstrates active support for security measures within the organisation. This is achieved via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security policies.
Since the majority of the systems are custom written, a major focus was placed on the Software Development Life Cycle. The company comes from an era where segregation of systems (developer sand pit, user acceptance testing and production) did not exist. Developers had full access to the production systems and change control was not enforced. This strategy served the company well in its formative years as speed to market was imperative. When growth is experienced, stabilisation requirements and system up-time becomes paramount. To protect the system, formal segregation of systems were introduced with proper user acceptance testing and sign-off. All deployments are documented. This was introduced at the beginning of 2009 and hence some users (22%) are neutral on segregation which could be because they are not aware of it or not part of the SDLC.

15. (Section: Separation of development, test and operational facilities.) The development and testing facilities are isolated from operational facilities. For example, development and production software are run on different computers. Where necessary, development and production networks are kept separate from each other.

The Software Release Management team has a checklist that must be completed before any new system or enhancement/bug fix is deployed to the production system. The neutral response to question 16 indicates that some respondents have no involvement in the SDLC.
16. (Section: System acceptance.) System acceptance criteria is established for new information systems, upgrades and new versions. Suitable tests are carried out prior to acceptance.

Physical security plays an important role in protecting information processing facilities. The Data Centre is currently securely protected with security doors, biometrics and CCTV cameras. The question could be somewhat misleading due to what defines an ‘information processing service’, but the general, understanding would have focused on the Data Centres.

12. (Section: Securing offices, rooms and facilities.) The rooms housing the information processing services, are locked or have lockable cabinets or safes.
Although there is a formal process for registering and de-registering staff, it seems that not all respondents agree on its implementation. IT can only de-register staff if HR informs them to do so. This procedure has been a problem in the past, but has now been addressed.

21. (Section: User Registration.) Formal user registration and de-registration procedures exist for granting access to all information systems and services.

![Survey Results]

- Fully Agree: 6 (12%)
- Agree: 33 (69%)
- Neutral: 7 (14%)
- Disagree: 3 (6%)
- Fully Disagree: 0 (0%)
3.7 Detail Primary Data Analysis

The results are analysed based on the controls of ISO 27002 as set out in Figure 3.2. In this section the researcher will analyse the primary data, in detail, to determine the current state or perception of information security within the MFC.

3.7.1 Policy (Questions: 1 & 2)

ISO 27002 starts with a policy for information security. Subsequently, two questions in the questionnaire were aimed at the awareness of the current policy and if it was still relevant. The majority agreed that the policy is published and communicated to all staff. This is indeed the case as all company policies published on the intranet are accessible to all staff. However, the response to the second question indicates that there is a perception that management does not review the policy to ensure its relevance. However, the MFC has a formal risk committee to ensure that all policies are kept up to date and all risks satisfactorily mitigated.

As referred to in Chapter 1, the board directs and controls the company. If there is a lack of commitment from top management, it will be difficult to implement policies. The questionnaire responses indicate that there is ‘buy in’ from the board.

The Information Security Policy is a vital document in ensuring that the correct procedures are in place to adequately protect information assets (ISO/IEC 27002:2005). For this reason the first few questions focussed on policies and procedures. Procedures implement policies and must be monitored at operational level.

3.7.2 Organisation of Information (Questions: 3 & 4)

65% of respondents agree that management supports the security measures of the organisation. Without management support, it would be impossible to implement the required security controls.

Question 4 addresses security in third party agreements. The neutral majority indicates that they are not responsible for creating these agreements. It is company policy to have NDAs (Non-Disclosure Agreements) signed by all external consultants and suppliers before allowing them to contract work or supply services.
3.7.3 Asset Management (Questions: 5 – 7)

Although there is a perception at the MFC that information has been classified and owners allocated to it, there is no formal classification implemented. Business Unit owners and application owners tend to believe that they own certain data, based on the applications they use. Information assets must be identified and classified to ensure that the correct access restrictions are enforced and to protect the integrity of the data (Peltier, 2005).

The classification of data ensures that it is correctly managed as far as compliance and sensitivity is concerned. It is interesting to note that 48% of respondents are under the impression that we have done this. As this is not the case, there is a false sense of protection regarding the information assets and this should be addressed urgently.

The MFC currently does not have any procedures for labelling and handling of data. Vague retention policies exist to ensure that all data is backed up forever. This results in difficulty in determining the importance of data and therefore all data is treated in an equal fashion.

3.7.4 Human Resources Security (Questions: 8 – 11)

All user access to systems is governed and users, contractors and third parties are given access as required. A formal process currently exists to obtain access to systems based on job role. However, without a proper information classification scheme, it is very difficult to ensure that the correct role gains access and only to the applicable information for that role.

Background checks are done for new candidates through the Kroll System which validates qualifications, checks for criminal records and any judgements. In addition, PPA (Personal Profile Analysis) and psychometric tests can be performed. It is important to screen prospective employees to limit the risk of employing undesirable individuals. Corporate espionage is a real threat and should be taken into account with each new candidate (Naef, 2007).

At the MFC a recent security awareness program was conducted; however it focused on password security. It was discovered that there was no formal security training process in place for staff members. This poses a serious threat as staff could through negligence, breach information security. It came to the light that certain staff members have shared their logon
credentials with others. This clearly indicates a lack of understanding amongst staff members of the damage that can be done via impersonation and identity theft.

Access rights to systems are revoked as part of the exit procedure of any employee, contractor or third party. A formal process for this policy and procedure is in place. Some staff members are immediately dismissed due to disciplinary issues and care should be taken that the procedure is followed to ensure that their access to the various systems is removed. Technology allows one to connect from a remote location to a work network via a Virtual Private Network (VPN). It is therefore important to ensure that once employment has been terminated, all access to systems and buildings is removed.

3.7.5 Physical and Environment (Questions: 12 & 13)
It was found that the Data Centre is housed in a separate part of the building and only authorised personnel have access to it. It is secured with a security gate / door that require the correct pin code to be entered on the pin pad to gain access. The second security door requires a fingerprint (biometric) scan to gain access to the center. CCTV cameras are fitted recording any movement within the room. Limiting physical access to data centres and information processing rooms reduces the risk of accidental and malicious damage. Food, drink and smoking is prohibited in these facilities to protect the equipment.

The data centre is housed on the first floor to protect it from low level water flooding and drainage problems. Fire suppression equipment is installed and the temperature is constantly monitored to ensure the optimal performance of the equipment. It is important to look after the data centre as this is where all of the information assets are stored.

3.7.6 Communications and operations management (Questions: 14 – 20)
Uncontrolled changes to information processing facilities could lead to errors, failures and breach of confidentiality, integrity and availability of information. It is therefore important that any changes, enhancements or new systems are implemented in a controlled fashion.

The majority of respondents agreed that change management is in place. The researcher found this to be an accurate assumption as a patch management procedure (operating system service packs, security updates) is in place. Any changes to the Data Centre must be approved
by the change control board. New information systems or enhancements to existing systems are channelled through the Software Release Management team and only implemented once all required sign-off has been granted.

Separate environments exist namely: developer sandpit (development environment), User Acceptance Testing and production environment. Developers do not have access to the production environment. This ensures that new enhancements or changes are not deployed to the production environment by accident.

It was noted that User Acceptance Tests are performed on all new systems and upgrades. Formal business sign-off is obtained and tests checked for correctness before deployment is allowed to the production environment.

Additionally, the installed anti-virus software ensures protection against malicious code. This is installed on all user machines and servers. The respondents may have understood malicious code to be part of the custom written software in which the logic of a function is purposefully flawed to cause damage.

Again the company’s backup policy states that backups of all data will be made daily. Two IBM tape libraries are used for the backups. The LTO2 tapes are stored off-site at MetroFile, a third party specialising in storage of documents and electronic media. The backups are randomly selected for testing every quarter. It was revealed that twice a year, the tapes are taken to the company’s Business Continuity Planning partner, Continuity SA in Midrand, to have the data restored and the systems tested.

It was found that electronic messaging as far as Electronic Data Interchange (EDI) is concerned, is well protected. The question in the questionnaire specifically refers to email, EDI and Instant Messaging (IM). Not all the respondents make use of all these communication mediums. Thus email and IM is not well protected in the sense that it is not encrypted when transmitted.

However, systems are monitored by review of log files and the respondents agreed that controls for monitoring of systems are in place; hence, access is restricted to the functions required.
3.7.7 Access Control (Questions: 21 – 29)

If access to systems is given to un-authorised users, data could become compromised due to neglect or misuse. Thus access should only be given to authorised staff as dictated by their job function. The staff member’s department head is responsible for requesting access to the required systems. A list should indicate who is allowed to request access per application and this should be formally documented.

It was noted that user registration processes are in place to grant and revoke access to information systems as needed. These processes are controlled by the Software Help Desk and they have a list of users allowed to ask for access to be assigned to staff. This list consists of departmental heads and supervisors who are assigned to certain applications. The HR exit form makes provision for de-registration of applications and systems which includes removal of domain credentials, email, access to databases and applications.

An acceptable use policy of all information processing facilities is included in the employee contract and although there is no separate statement to keep passwords confidential, it is implied in the contract. In addition, the Information Security policy contains a section regarding ‘good passwords’ highlighting the importance of educating the users, in order to protect their passwords and subsequently the data.

Remote users are granted access via VPN. All these accounts are given an expiry date when VPN access is removed. Then the user has to re-apply for renewal. Access is normally granted for a period of 6 months or on termination of employment the VPN access is removed.

The MFC uses Microsoft Active Directory to authenticate all its users. Every user has a unique logon name and password. A strong password level is currently set which forces the use of at least one capital letter, special characters (@, #, $), numbers and a minimum length of 6 characters. Once again, access to systems is based on job functions.

The respondents were not sure if measures were in place to protect against the use of mobile devices, yet access to information systems was only granted on successful logon through the
Active Directory system. Therefore data should not be stored on the local drives of laptops and this could possibly raise security concerns.

3.7.8 Information Systems Acquisition, Development & Maintenance
(Questions: 30 – 36)

Security flaws in applications could allow hackers to breach systems allowing them unauthorised access to your information. It does not help to have the best physical security, while your data can be stolen through flaws in published applications (Jackson, 2009).

The majority of the respondents are of the opinion that security is part of any system design and the MFC had catered for security in the technical design of any new system. But it was found that information had not been classified and therefore difficult to gauge if the security requirements and controls reflected the business value of information assets. The majority of the respondents tend to agree that requirements do not reflect the business value.

If an application allows for data to be captured without any validation, users will find ways to shortcut the capturing process and capture incorrect data which will lead to GIGO (Garbage In, Garbage Out). Part of our functional specifications is to ensure that the correct validations are built into our systems. The respondents agree with this statement and there are controls built to check the integrity of data processed through the system. Finally, cubes, used for Business Intelligence, allow users to slice and dice data and are often used for reporting purposes which also validates the integrity of the data.

It was found that the Software Release Management team controls all changes to the live environment and ensures that all quality checks on new systems and enhancement have been performed before deployment to production happens. These checks are done in the UAT environment and include quality assurance of the code, user acceptance testing and a full impact analysis. Code coverage reports are provided to ensure that the code is properly tested. Code is peered review to ensure that standards are adhered to. It is important to apply these checks and controls to ensure that the system deployed is in actual fact performing functions as advertised. Systems, and ultimately information, can be breached by deploying faulty and incorrect applications. A door can be opened for malicious code.
3.7.9 Business Continuity (Questions: 37 & 38)
The ‘A’ in the CIA triangle is for availability. A disaster would cause data not to be available and therefore Business Continuity Plans (BCPs) must ensure recovery from backups. The MFC makes use of the syndicated services of Continuity SA for BCP. It is tested bi-annually to ensure successful recovery. The respondents agree that the MFC has a BCP in place. The current BCP strategy is to collect the existing debtors’ book, while origination of new business will have to wait until full recovery from the disaster. The BCP requirements are updated annually.

3.7.10 Compliance (Questions: 39 & 40)
The respondents indicated that they are not sure if all systems comply with regulatory and contractual requirements as they are probably not aware of all the requirements. The MFC’s Risk committee is responsible for ensuring that compliance is adhered to. Non-compliance could lead to confidentiality and integrity issues.

The use of applications and/or infrastructure for any non-business purpose could lead to a breach of applications or systems. The acceptable use policy of the MFC’s information processing facilities clearly states that it is for the use of business purposes only. The respondents are in agreement with this statement.
3.7.11 Questionnaire Conclusion

The MFC’s respondents agreed overall with most of the questions. Figure 3.5 indicates that there are a large number of respondents who are neutral on many questions and this indicates a lack of training/awareness or understanding.

![Response Summary](image)

*Figure 3.5 Response Summary*

Figure 3.6 summarises the responses per security control and this highlights that the policy needs to be communicated to all staff again as only 50% seem aware of its existence. Without the staff understanding the importance of the information security policy, it will be difficult to enforce the security procedures and hold the staff accountable for their actions.

What is a concern is that more than a third of respondents are not aware of the Business Continuity Plan which indicates that when a disaster strikes, the possibility exists that chaos could occur as key personnel has not been identified to perform key functions. This will be catered for in the study’s findings and recommendations.
Figure 3.6 Questionnaire Results
3.8 Conclusion

The Micro Finance Industry in South Africa has been regulated by the MFRC who introduced statutory and regulatory requirements. If a micro financier is found to be in breach of these requirements, they could lose their license to operate. Therefore, information risks should be identified and correctly mitigated and this has implications on how information is processed and stored.

Information security is crucial to any organisation, since it is the life blood of the organisation. Therefore it is vital that information security is implemented holistically to ensure that information assets are adequately protected. The use of a standard, such as ISO 27002, ensures that a holistic solution is created. The questionnaire conducted at the MFC was based on this standard and provides insight into what is required to build a holistic information security system for this MFC. The CIA triangle (Figure 1.1) is re-affirmed in ISO 27002 and enforces the holistic characteristics of the information security system.

The results obtained in the questionnaire will be used as a guide to build a holistic information security model in the next chapter. In building this model, attention will focus on ensuring that the research problem is addressed by the solution provided.
Chapter 4

Findings and Recommendations: Building a focused security model for a South African MFC

4.1 Background
4.2 Baseline Solution for a MFC
4.3 Vetting the Solution
4.4 Conclusion
4.1 Introduction
Chapter 1 referred to the implementation of a holistic security model, a mammoth task, as it is difficult to secure something that is intangible. However, information is the most valuable asset for a financial organisation and therefore necessitates that it is adequately protected.

In the previous chapters security best practises and standards were discussed. The survey conducted in Chapter 3 gained an insight into the understanding and current use of information security, and its shortcomings, for a MFC.

The survey results and the knowledge gained from the literature study will be used to build a security model that will address the specific needs of a MFC. This chapter will focus on what is required in the baseline solution and how technology can help in the implementation thereof.

4.2 Baseline Solution for a MFC
The solution is based on ISO 27002 incorporating the findings of the empirical work. All control clauses are included to ensure a holistic solution. Policies, procedures and technology will be used to propose the solution. Table 4.1 summarises the solution requirements based on the 11 controls of ISO 27002. The roles are defined in section 4.2.1.5 which forms part of the Information Security Policy.
<table>
<thead>
<tr>
<th>ISO 27002 Control</th>
<th>Policy Section</th>
<th>Procedures Required</th>
<th>Responsible</th>
<th>Survey Finding</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Policy</td>
<td>Information Security Objectives</td>
<td>Board to approve; CIO to vet; Information Security Officer to create and maintain</td>
<td>Security objectives must be made clear to all staff at all levels</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information asset register</td>
<td>Information Security Officer</td>
<td>Not defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy review intervals</td>
<td>Information Security Officer</td>
<td>Staff not aware that the policy is reviewed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff awareness and training</td>
<td>Information Security Officer</td>
<td>Policy published on intranet, but more awareness required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Define roles and responsibilities</td>
<td>Information Security Officer</td>
<td>Roles not clearly defined in current policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td></td>
<td>Risk committee addresses risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Legal and regulatory requirements</td>
<td></td>
<td>Handled by legal and compliance dept</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incident management</td>
<td>Information Security Officer</td>
<td>Central help desk should log these issues and resolve them accordingly</td>
<td></td>
</tr>
<tr>
<td>2. Organisation of Information Security</td>
<td>Information Security</td>
<td>Internal to the MFC</td>
<td>Senior Management</td>
<td>Internal staff bound by contract. NDAs used as primary legal agreement for externals.</td>
</tr>
<tr>
<td>3. Asset Management</td>
<td>Information Security</td>
<td>Information Asset Register</td>
<td>Information Asset Classification Scheme</td>
<td>Management Asset Owners</td>
</tr>
<tr>
<td>4. Human Resources Security</td>
<td>Personnel Security</td>
<td>Screening process Employment contract Code of conduct Induction program Disciplinary Termination</td>
<td>Screening</td>
<td>Human Resources</td>
</tr>
<tr>
<td>5. Physical Environmental</td>
<td>Physical &amp; Environment</td>
<td>Secure areas External &amp;</td>
<td>Monitoring</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Security &amp; Environmental Threats</td>
<td>Maintenance</td>
<td>Power/Cooling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>al Security</td>
<td>Environmental Threats</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equipment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supporting utilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Off-site equipment usage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Asset disposal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It is protected from water flooding and drainage problems. Only authorised personnel have access to it. Monitoring via CCTV and alarm linked temperature control is installed.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Change management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third party service delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Capacity planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DR</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information processing facilities are controlled. A change management procedure is in place to ensure only authorised changes are pushed to the production environment. SLAs exist for 3rd parties. Capacity planning needs to be more formal. DR plan is tested bi-annually off-site.

<table>
<thead>
<tr>
<th>7. Access Control</th>
<th>System Access Control</th>
<th>User access</th>
<th>Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Passwords</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clear desk</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sessions</td>
<td></td>
</tr>
</tbody>
</table>

User access granted based on job function. Password policy dictates strong passwords changed every 45 days.

<table>
<thead>
<tr>
<th>8. Information Systems Acquisition, Development and Systems</th>
<th>Information Security Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security part of the technical design of the system. Information not classified and therefore difficult to ensure proper security on the data. Application validation has been implemented to ensure
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10. Business Continuity Management</td>
<td>Business Continuity Plan</td>
<td>Preventative and recovery controls; Testing</td>
<td>Board; Business Unit Managers; Information Security Officer</td>
<td>Limited BCP exists. The MFC will only be able to collect on the outstanding debtors book and not originate any new business. Testing is bi-annually.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11. Compliance</td>
<td>Compliance</td>
<td>Regulatory</td>
<td>FAIS; NCA; RICA; Consumer Protection Act; ECT; WASPA Code (direct marketing)</td>
<td>Board; Compliance and Risk Committee; Information Security Officer</td>
<td>The MFC Risk Committee must ensure that systems are compliant. Respondents were not sure that this was the case.</td>
<td></td>
</tr>
</tbody>
</table>
4.2.1 Policy
It was noted in Chapter 2 that the policy document should clearly define what information security is, what the objectives are and how it will enable the organisation to share information. The policy should protect the company’s information assets from internal and external threats. The CIA triangle (Fig 1.1) plays an important role in reminding users of the objectives of information security.

The sections that the policy should contain are explained in 4.2.1.1 to 4.2.1.10.

4.2.1.1 Introduction
The objective of Information Security is to ensure that:

- Information is protected from unauthorised disclosure (Confidentiality);
- Information is protected from unauthorised modification and that information can be treated as correct and complete (Integrity);
- Information is available as and when needed (Availability)

The implementation of CIA will ensure that the MFC is seen as a reliable and esteemed business partner whose information should be treated as being correct (not compromised) and available when needed. This provides a level of comfort that information is protected and guarded against violations or misuse, in so far as being able to track where a violation or misuse occurred. The ability to recover from such a violation or misuse is paramount.

The MFC is responsible for debit order collections and disbursements to clients’ accounts. Thus, transactions between the MFC and other parties must be secured to ensure the confidentiality and reliability of the information.

4.2.1.2 Information Assets should be Documented and Assigned to an Owner
All information assets should be documented using a Data Classification scheme. In order to accurately protect information assets their confidentiality, integrity and availability requirements should be documented. The information owner takes responsibility for the use of the information asset and must ensure that it is used appropriately.
The MFC has to treat banking and client identity information as confidential. This information should be defined as such on the information asset register and documented as to how it should be used within the company.

4.2.1.3 Define Regular Review Intervals for the Policy
Creating the policy is not a one-time effort but a continual process to ensure that it is relevant to the business strategy and applicable laws (Layton, 2007). Since the MFC does a substantial amount of in-house systems development, it is suggested that the Information Security policy is reviewed once a quarter or when there has been a substantial change in regulatory or law requirements.

The MFC’s risk committee meets on a regular basis to review policies and to see that risks are adequately treated. The information security policy should be reviewed at these intervals and/or when significant changes have occurred influencing the policy.

4.2.1.4 Provide for Staff Awareness and Training Regarding the Content of the Policy
The MFC publishes all policies on its intranet to which all staff has access. It is expected that staff familiarise themselves with these policies and understand the contents. The findings of the research questionnaire indicated that staff are aware of the policies but do not fully understand the content. Tipton & Krause (2007) suggest that a link of the policy is emailed to all staff members and that agreements are in place to state that they have read and understand the contents thereof, in order to ensure that they will comply.

In addition, the MFC’s employment contract provides for a general use clause of all company networks, email usage and systems. Information security should be part of the induction training to ensure that all staff is made aware of the importance of using information assets securely. Awareness campaigns should be launched from time to time to bolster the concept with staff and especially after the information security policy has been updated.

The MFC can create screensavers and desktop backgrounds to remind staff of the information security responsibility.
4.2.1.5 Clearly Define Roles and Responsibilities

Figure 4.1 summarises the proposed roles involved in information security for the MFC. It starts with buy-in from the board who directs and controls the MFC. They ensure that the information security policy is drafted and show their support so as to implement successfully.

The second level is the executive management level. They report directly to the board. An Information Security Officer is required at this level to develop, implement and maintain the information security policy, and the procedures and controls that compliment it.

Middle management forms the third level. They ensure that policies and procedures are adhered to. The technical management is responsible for designing and implementing the information systems and needs to monitor the systems on a daily basis. The information owners are defined at this level as well as the end user level to ensure a holistic approach to ownership. The information security forum consist of the members of the executive and middle management and are responsible for keeping the information security policy up to date to review and monitor security incidents and to act as ambassadors for information security.

![Figure 4.1 Proposed Information Security Roles for the MFC](image-url)
4.2.1.6 Define How Information Security Risks are Managed
In Chapter 2 it was mentioned that ISO 27002 uses a risk assessment to identify, quantify and prioritise risks against criteria for risk acceptance relevant to the organisation. The risk assessment enables management to perform a risk analysis. This is an iterative process to be repeated periodically. The Common Criteria (Fig 2.3) should be used as a risk assessment model to implement counter measures to reduce or remove the risk.

4.2.1.7 Legal and Regulatory Requirements
The MFC is a member of the Financial Services Board and governed by the National Credit Act. The regulatory requirements should be documented and defined for each information system as required. Regular reviews are required to ensure that the MFC is compliant with all legal and regulatory requirements. The information security forum will conduct these reviews and escalate any concerns to the executive management.

Additionally, procedures are required to implement legal compliance in respect of intellectual property rights, retention of company records, the use of cryptographic controls and penalties for misuse of information systems.

4.2.1.8 How to Handle Incidents
A procedure is required to prescribe the actions required in case of a security breach or incident. All incidents should be documented for review and corrective action taken when necessary. The MFC’s central help desk will log all security incidents and notify the information security officer who needs to take appropriate action. Periodically when the information security forum meets, all logged incidents should be reviewed against the risk analysis to ensure that these risks are effectively controlled.

All security incidents should be logged with the MFC’s central help desk. Once logged, a ticket will be generated and the incident investigated. Depending on the incident severity, 1 being the entire company is affected to a 4 where only a sub-system is affected, corrective action will be taken within SLA limits.
4.2.1.9 Compliance to the Policy
The information security forum should have regular reviews to ensure that the information security policy is followed. The standards, procedures and controls accompanying the policy should be audited on a regular basis to ensure on-going compliance.

4.2.1.10 Penalties and consequences
Penalties for the violation of any part of the information security policy should be clearly stipulated in the MFC’s disciplinary procedures. The MFC uses the following disciplinary process:

<table>
<thead>
<tr>
<th>Description</th>
<th>1st Offense</th>
<th>2nd Offense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refusing / failure to comply with security instructions, standards and procedures.</td>
<td>Final written warning</td>
<td>Dismissal</td>
</tr>
</tbody>
</table>

4.2.3 Organisation
The focus internally is to create a framework for the successful implementation of information security within the organisation. The roles and responsibilities clearly define what is required and by whom. The internal requirements affect all staff at all levels.

The external focus ensures that the information and processing facilities used by third parties are properly secured and well managed. This includes accessing data outside of the boundaries of the MFC and therefore ensuring adequate protection. Virtual Private Networks (VPN) provide for a secure tunnel for the transmission of data.

4.2.4 Asset Management
Information assets must be recorded on an asset register. Appendix B is based on The State of Queensland (2009) information asset register. It contains the minimum items that should be included in the MFC’s information asset register. Ownership should be documented and assets grouped to facilitate successful risk management.
Access control granted to assets should periodically be reviewed. The MFC uses Microsoft Active Directory to grant/deny domain access to objects, for example files and folders. Applications share a common access mechanism that defines the functionality that users have available to them based on their job role.

4.2.5 Proposed Solution Implementation Check List
Appendix C summarises how the remaining ISO 27002 controls could be implemented. It looks at the important areas within each control and what is required to successfully implement it. This table could be used as a checklist to ensure adherence to a holistic approach.

4.3 Vetting the Solution
ISO 27001 is the standard used to audit the security framework and thus ensures a holistic solution is created. The mind map used in Figure 2.6 summarises the 11 controls of ISO 27002 and can be used to ensure that all the important aspects of each control have been addressed.

The purpose of this study is to provide a holistic information security framework for a MFC. To gain an understanding of the specific needs of the MFC, empirical research through the use of a questionnaire was done and those needs were taken into account in the proposed solution. The suggested solution model is based on the ISO27002 security standard which addresses the Confidentiality, Integrity and Availability of information assets.

4.4 Conclusion
The solution needs to be a holistic security system catering for the specific needs of the MFC. In Chapter 2, ISO 27002 was discussed in detail as a standard for implementing information security. By implementing the 11 controls, such a holistic solution should be achievable. It was stated that implementing ISO 27002 was a mammoth task and a balance was sought between the protection of the information assets and allowing business processes to run efficiently and optimally.
Therefore, the specific needs of the MFC were addressed in Chapter 3 through the use of a questionnaire to determine the current shortcomings and where more focus could be placed in respect of information security. The responses were taken into account in the building of the solution model to ensure a focused solution based on the specific requirements of the MFC.

The questionnaire highlighted that the MFC understood the importance of protecting information assets and that without information they could not function. This was evidenced by an information security policy already in place and approved by the board. However, information is not classified and roles and responsibilities not clearly defined. A new information security policy should be put in place to cover these shortcomings.

In this study it was found that the uniqueness of information security for a MFC did not rest only in the 11 controls of ISO 27002, which is a guideline and best practice applicable to any industry. Hence, the uniqueness for the MFC is rather found in the compliance of the specific regulation and legislation by which the MFC is bound in its operation.

This chapter, focused on what was necessary to build a baseline solution that if implemented could ensure that the MFC’s information assets are adequately protected based on their specific requirements. The solution begins with understanding the risks that need to be managed and the creation of an information security policy motivating its importance from the board, down to the practical implementation of the other 10 controls of the ISO 27002 standard, resulting in a holistic information security system.
Chapter 5

Conclusion

Chapter 5
5.1 Background
5.2 Evaluation of the Research Outcomes
   Vetting the Solution
5.3 Directions for Future Research
5.4 Conclusion

Chapter 2
Current Security Models and Standards
-------------------------------------
Literature Study

Chapter 3
Case Study
--------------------
Empirical Research

Chapter 4
Findings and Recommendations:
Building a Focused Security Model for a South African MFC

Chapter 5
Conclusion
5.1 Background

Information is the most important asset of this organization. This study focused on building a holistic information security model to protect, specifically, the information assets of a particular MFC which other similar companies could use. ISO 27002 was used as a guideline to ensure the proposed model covers all critical areas.

The literature study combined with the empirical research was used to formulate the items required in a security model. Appendix B and C provide checklists that should be completed to ensure that the model is correctly implemented.

Using checklists ensures that all the necessary steps for good security are implemented. However, cognizance should be taken that information security is everyone’s responsibility. All staff members need to understand the importance of the information that they use on a daily basis and be aware of any risks in the use thereof. These risks should be controlled by implementing an appropriate risk management strategy.

5.2 Evaluation of the Research Outcomes

In Chapter 1 the primary objective of this study is to develop an enterprise security model for a micro finance company by creating a secure next generation system.

A holistic information security framework should cover Confidentiality, Integrity and Availability of all the information assets of the MFC. As information is not only limited to computer systems, it is important to ensure that even paper based information is treated accordingly. However, the focus of this study was primarily on computer based systems and networks. The model solution in chapter 4 was entirely based on ISO 27002. Therefore, this study can be used to implement a secure next generation system that should protect the information assets of a MFC.

Secondary objective one: How does a company successfully implement ISO 27002 ensuring that its information assets are adequately protected? Implementing ISO 27002 is a mammoth task and all 11 controls should be implemented to ensure all information assets are adequately protected. Information must be classified and assigned to owners to ensure the protection required is implemented. This study found that once risks are identified, as well as
information classified and assigned to an owner, it should be possible for them to adequately protect their information. A checklist helps to ensure that controls are not forgotten and therefore provides the support for implementing a holistic information security model which adequately protects the information assets. Thus, this study recommends that a checklist is used to implement ISO 27002 ensuring that all 11 controls are implemented and that the directive comes from the board.

**Secondary objective two:** *What unique measures can be used to ensure that ISO 27002 is implemented correctly for a micro finance company?* The main requirement for a MFC is to ensure that its customer confidential information with regards to banking detail is adequately protected. Banking and personal information should be encrypted and classified as highly sensitive to ensure it is protected. However, the MFC must adhere to all the ISO 27002 controls to ensure that its information assets are protected. None of the controls should be neglected thus ensuring that a holistic information security system is implemented.

The findings of the empirical research stressed how important it is to ensure that staff at all levels are aware of the importance of information security and that these assets are clearly classified and assigned to an owner. Although this is not a unique MFC requirement, without this classification no information asset will be protected adequately.

The MFC’s information systems must be vetted against all regulatory and compliance requirements. All the relevant statutory, regulatory and contractual requirements should be defined and documented as they pertain to each information system.

Therefore, this study has addressed the unique measures for the MFC by using the 11 controls of ISO 27002 and taking the specific regulation and legislation for the MFC into account, hence producing a holistic information security framework.

The uniqueness of the MFC’s information security requirements is not found in ISO 27002, because information security applies to all industries and trades. However, the MFC’s uniqueness lies in compliance with regulation and legislation that governs its existence. The information security uniqueness for the MFC was found not to be as daunting as first anticipated, as information security is applicable to all organisations.
Therefore, the major finding of this study is that information security is applicable to all organisations and that the MFC specifically has to adhere to regulation and legislation applicable to them.

Secondary objective three: What is needed to maintain your Information Security Management System once implemented? The information security policy should be reviewed at regular intervals to ensure it remains relevant. Roles and responsibilities should be defined to ensure that information assets at various levels are protected. It is the responsibility of the data owner to ensure the level of protection of the asset assigned to him.

In addition, regular reviews of the information asset register should be conducted to ensure it is kept up to date and all assets correctly defined in terms of use and security. This should ensure that the level of protection for information assets is kept current.

Furthermore, all security incidents should be logged and resolved through a formal process. The information security officer should ensure that when a breach occurs it is addressed quickly and efficiently. Controls should be put in place to manage the risk in the future efficiently and effectively. Thus, this study has addressed what is needed to maintain the Information Security Management System by adhering to the above recommendations.

5.3 Directions for Future Research
Having concluded this study, a few recommendations are made for further research:

- The model built for the MFC can be used for other organisations as the MFC’s requirements are in many instances very similar to that of other organisations. The information asset register might have to be altered slightly to cater for specific needs. However, the ISO 27002 security controls in general should be used by all organisations.

- This study primarily focused on ISO 27002, but other standards and guidelines should be taken into account. In the literature study chapter, various other models were mentioned and it is probably advantageous to combine them with ISO 27002. CobiT
should be used from an audit perspective to ensure that information assets are adequately protected.

- The technology used by the MFC is based purely on Microsoft products. Solutions from other vendors provide a similar function and should be considered. Although this study did not focus purely on a technical implementation, strong focus was placed on Microsoft Active Directory for authentication credentials and protection of data at the Operating System level.

5.4 Conclusion

This study presented a solution for building a holistic information security system for a MFC. In order for successful implementation of such a framework it is imperative that the directive comes from the board to ensure the importance thereof and is enforced on the MFC.

The information security policy is the document that represents the voice of the board’s directive in regard to information security. The roles and responsibilities in respect of information security should be clearly defined to ensure that ownership is taken of the information assets. The information security officer is primarily responsible for implementing the security policies and procedures and should report to the Chief Information Officer.

Implementing an information security model is not a once-off exercise, but an on-going iterative cycle. As data requirements change, due to business dynamics, and therefore risks, the policy must be updated to ensure the underlying procedures implemented remain relevant.

As data is used by everyone in the MFC, training and awareness on protecting the MFC’s most valuable asset cannot be stressed enough. Everyone is responsible for protecting the information assets as they use them on a daily basis.
References


85


Appendix A - Instrument used for Data Collection

1. (Section: Information security policy document.) The MFC has a management approved Information security policy that is published and communicated to all employees.

2. (Section: Review of Informational Security Policy.) Management review the information policy on regular intervals to ensure that it protects your information assets.
3. (Section: Management Commitment to Information Security.) Management demonstrates active support for security measures within the organisation. This is achieved via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security policies.

4. (Section: Addressing security in third party agreements.) The agreements with third parties, involving accessing, processing, communicating or managing the organization’s information or information processing facility, or introducing products or services to information processing facility, complies with all appropriate security requirements.
5. (Section: Ownership of Assets.) Each information asset identified, has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.

6. (Section: Classification guidelines.) Information is classified in terms of its value, legal requirements, sensitivity and criticality to the organisation.
7. (Section: Information labelling and handling.) An appropriate set of procedures is defined for information labelling and handling, in accordance with the classification schema adopted by the organisation.

8. (Section: Roles and responsibilities.) Employee security roles and responsibilities, contractors and third party users are defined and documented in accordance with the organisation’s information security policy.
9. (Section: Screening.) Background verification checks for all candidates for employment, contractors, and third party users are carried out in accordance with the relevant regulations.

10. (Section: Information security awareness, education and training.) All employees in the organisation, and where relevant, contractors and third party users, receive appropriate security awareness training and regular updates in organisational policies and procedures when it pertains to their job function.
11. (Section: Removal of access rights.) Access rights of all employees, contractors and third party users, to information and information processing facilities, will be removed upon termination of their employment, contract or agreement, or will be adjusted should their role change.

12. (Section: Securing offices, rooms and facilities.) The rooms housing the information processing services, are locked or have lockable cabinets or safes.
13. (Section: Equipment sitting and protection.) The equipment is protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

14. (Section: Change Management.) All changes to information processing facilities and systems are controlled.
15. (Section: Separation of development, test and operational facilities.) The development and testing facilities are isolated from operational facilities. For example, development and production software is run on different computers. Where necessary, development and production networks are kept separate from each other.

16. (Section: System acceptance.) System acceptance criteria is established for new information systems, upgrades and new versions. Suitable tests are carried out prior to acceptance.
17. (Section: Controls against malicious code.) To protect against malicious code: detection, prevention and recovery controls were developed and implemented. Appropriate user awareness procedures are implemented.

18. (Section: Information backup.) Back-ups of information and software are taken and tested regularly in accordance with the approved backup policy.
19. (Section: Electronic messaging.) The information involved in electronic messaging is well protected. (Electronic messaging includes but is not restricted to Email, Electronic Data Interchange, Instant Messaging)

20. (Section: Monitoring system use.) Procedures are developed and enforced for monitoring system use in the information processing facility.
21. (Section: User Registration.) Formal user registration and de-registration procedures exist for granting access to all information systems and services.

22. (Section: Privilege Management.) The allocation and use of any privileges in the information system environment is restricted and controlled, i.e. Privileges are allocated on a need-to-use basis and allocated only after a formal authorisation process.
23. (Section: Privilege Management.) The users are asked to sign a statement to keep the passwords confidential.

24. (Section: User authentication for external connections.) An appropriate authentication mechanism is used to control access by remote users.
25. (Section: Secure log-on procedures.) Access to the operating system is controlled by a secure log-on procedure.

26. (Section: User Identification and authentication.) Unique identifier's (user ID) is provided to every user.
27. (Section: Password Management system.) Our password management system caters for strong passwords. Users are encouraged to keep them confidential.

28. (Section: Information access restriction.) Information and application system functions are restricted in accordance with an access control policy.
29. (Section: Mobile computing and communications.) Appropriate security measures are in place to protect against the risks of using mobile devices (e.g. laptops, mobile phones)

30. (Section: Security requirements analysis and specification.) When developing or enhancing information systems, security is part of the design.
31. (Section: Security requirements analysis and specification.) The security requirements and controls implemented in our systems reflect the business value of our information assets.

32. (Section: Input data validation.) Applications have the necessary validation controls to ensure the integrity of the data captured.
33. (Section: Control of internal processing.) Validation checks are built into applications to detect any corruption of information either through processing or deliberate acts.

34. (Section: Output data validation.) Processed data (output from application) is tested on a regular basis to ensure information is correctly stored.
35. (Section: Change control procedures.) A Release Management function is in place to minimise the risk of corrupting the information system.

36. (Section: Change control procedures.) The SRM (Software Release Management) function ensures that an impact analysis of the changes is conducted before deployment to the live environment.
37. (Section: Developing and implementing continuity plans including information security.) Plans are in place to restore business operations from a disaster in the required time frame.

38. (Section: Testing maintaining and re-assessing business continuity plans.) Business Continuity Plans are tested and updated on regular intervals.
39. (Section: Identification of applicable legislation.) Each information system complies with the relevant statutory, regulatory and contractual requirements and is defined and documented.

40. (Section: Prevention of misuse of information processing facilities.) The use of any applications or infrastructure for any non-business or unauthorised purpose, without management approval, is regarded as improper use of the facilities.
Appendix B – Example of an Information Asset Register

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset detail information</td>
<td></td>
</tr>
<tr>
<td>Asset identifier</td>
<td>Unique identification code to identify the asset.</td>
</tr>
<tr>
<td>Information asset title</td>
<td>Business use name for the information asset.</td>
</tr>
<tr>
<td>Information asset description</td>
<td>A description regarding the nature of the information contained in the information asset and how the information is used.</td>
</tr>
<tr>
<td>Creator</td>
<td>Organisation or position responsible for creating the content of the information asset.</td>
</tr>
<tr>
<td>Original acquisition/creation date</td>
<td>Date that the information asset was acquired or created.</td>
</tr>
<tr>
<td>Keywords</td>
<td>Theme or keywords that may enable faster searching for the information asset.</td>
</tr>
</tbody>
</table>

**Asset storage information**

| Originating source                  | Internally created or sourced externally.                                   |
| Location                            | The physical storage location of information assets not held electronically. |
| Source systems                      | The business use name of supporting business applications and systems used to capture the information. |
| Storage                             | Details of physical storage systems used to store electronically held information assets. |

**Asset usage information**

<p>| Department                          | Details of the department principally responsible for the capture, storage, usage of the information asset. |
| Mandate                             | The specific warrant which requires the resource to be created or provided.  |
| Scope of use                         | Scope use includes:                                                         |
|                                     | • internally                                                                |
|                                     | • externally                                                                |
|                                     | • the entire MFC                                                            |
|                                     | • certain divisions only                                                    |</p>
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency of updates</td>
<td>The frequency with which information asset content is updated.</td>
</tr>
<tr>
<td>Asset classification information</td>
<td></td>
</tr>
<tr>
<td>Content type</td>
<td>Content types include:</td>
</tr>
<tr>
<td></td>
<td>• Transactional - structured content that supports business processes and workflows and is implemented using structured databases, which tend to be highly normalised and optimised for transactional performance.</td>
</tr>
<tr>
<td></td>
<td>• Analytical - Structured content that supports queries and analysis and is implemented using structured databases, which tend to be purposefully de-normalised and optimised for query ease and performance, and often contain aggregated or derived information.</td>
</tr>
<tr>
<td></td>
<td>• Authored - Unstructured content in a wide variety of formats, such as multimedia, application system programs or text documents with embedded graphics.</td>
</tr>
<tr>
<td></td>
<td>• Published - Unstructured content assembled and/or transformed from its component pieces, into a desired format and disseminated to a target audience and implemented using technologies that optimise discovery, search and retrieval.</td>
</tr>
<tr>
<td>Asset management information</td>
<td></td>
</tr>
<tr>
<td>Information asset owner</td>
<td>Title and name of the information asset owner.</td>
</tr>
<tr>
<td>Information asset custodian</td>
<td>Title and name of custodian.</td>
</tr>
<tr>
<td>Point of contact – key creator/user/manager of the information</td>
<td>Position responsible for ensuring that the quality of the information is maintained and acts as the single point of contact in relation to information quality issues.</td>
</tr>
<tr>
<td>Asset constraints</td>
<td></td>
</tr>
<tr>
<td>Access constraints</td>
<td>Specific constraints relating to access to the information asset.Almost every piece of code needs a...</td>
</tr>
<tr>
<td>Use constraints</td>
<td>Specific constraints relating to the use of the information asset. Almost every piece of code needs a...</td>
</tr>
<tr>
<td>Risk profile</td>
<td>Specific risks to the organisation relating to the misuse or unavailability of the information asset and details of mitigation strategies.</td>
</tr>
</tbody>
</table>
| Access rights                                      | Rules relating to the publication or sharing of the information asset content. Almost every piece of code needs a...
<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset history</td>
<td></td>
</tr>
<tr>
<td>Major maintenance history</td>
<td>Dates and details of changes and enhancements to the information asset.</td>
</tr>
<tr>
<td>Retirement details</td>
<td>Dates and details relating to the retirement or replacement of the information asset.</td>
</tr>
</tbody>
</table>

*Information asset register (The State of Queensland, 2009)*
### Appendix C – Practical Implementation Check List for ISO 27002

Table 4.3 ISO 27002 Implementation Check List

<table>
<thead>
<tr>
<th>ISO 27002 Control</th>
<th>Area</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human Resources</strong></td>
<td>Screening checks</td>
<td>Reference, Qualifications, Criminal- and Credit Checks</td>
</tr>
<tr>
<td></td>
<td>Systems used</td>
<td>Kroll and Credit Bureaus</td>
</tr>
<tr>
<td><strong>Physical &amp; Environment</strong></td>
<td>Data Centres</td>
<td>Prevent unauthorised physical access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Should not be conducive to flooding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>External walls should be of solid construction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All external doors should be protected appropriately against intruders</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manned reception areas should control access to the building</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Visitors should sign a visitor’s book</td>
</tr>
<tr>
<td><strong>Physical &amp; Environment</strong></td>
<td>Data Centres</td>
<td>Monitor areas where sensitive information is processed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Every person should wear some sort of visible identification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unescorted visitors should be reported to security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review access rights to secure areas regularly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Buildings should not ‘advertise’ where the DC is housed</td>
</tr>
<tr>
<td><strong>ISO 27002 Control</strong></td>
<td><strong>Area</strong></td>
<td><strong>Requirement</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Building</strong></td>
<td>Neighbouring buildings should be inspected for possible threats</td>
<td>Fire and water damage</td>
</tr>
<tr>
<td></td>
<td>Hazardous or combustible materials should be stored safe distances away from secure areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delivery and loading areas should be separated from information processing facilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>New equipment should be checked for threats before making it operational</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only authorised personnel should perform maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>Physical &amp; Environment</strong></td>
<td>Supporting utilities</td>
<td>The risk in regard to electricity, water supply, sewage, heating/ventilation and air-conditioning should be controlled</td>
</tr>
<tr>
<td></td>
<td>A UPS should be used for continuous- and clean power</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A backup generator should be available in blackouts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Emergency power off switches should be installed in DC for rapid power down</td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telecommunications</td>
<td>Should be connected to the supplier by at least 2 different routes to provide for failover</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data cables should be protected from interference or interception</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clearly label cables to minimise problems during maintenance</td>
<td></td>
</tr>
<tr>
<td>Off-site usage of equipment</td>
<td>Should be authorised</td>
<td></td>
</tr>
<tr>
<td>Equipment disposal</td>
<td>Licensed software and any sensitive data should be removed so that it is non-retrievable</td>
<td></td>
</tr>
<tr>
<td>Communications &amp; Operational Environment</td>
<td>Operating procedures Documented and maintained  How to process and handle information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup procedures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scheduling of jobs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Instructions for handling errors and exceptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System restart and recovery procedures in the event of system failure</td>
<td></td>
</tr>
<tr>
<td>Change management</td>
<td>Identification and recording of significant changes</td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>Operational duties</td>
<td>Duty segregation to reduce the risk of system misuse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communications &amp; Operational Environment</td>
<td>Development</td>
<td>Rules for deployment should be defined</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Control</td>
<td>Requirement</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Changes made by third parties should be managed carefully to ensure business continuity</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td>Physical</td>
<td>Entrance to buildings via biometrics</td>
</tr>
<tr>
<td>Logical:</td>
<td>Systems / Applications</td>
<td>User access management: users are registered for access to systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User access rights to be reviewed at regular intervals</td>
</tr>
<tr>
<td>Access Control</td>
<td>Logical:</td>
<td>Password usage should be according to the information security policy</td>
</tr>
<tr>
<td></td>
<td>Systems / Applications</td>
<td>Unattended equipment should be made secure before leaving it. Active sessions should be logged off and screensavers with passwords should be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clear desk and clear screen policy reduces the risk of unauthorised access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network access control prevents unauthorised access to network devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy to govern which devices users have access to</td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Secure log-on procedures should be used to authenticate the user</td>
<td>Using Microsoft’s Active Directory</td>
</tr>
<tr>
<td></td>
<td>Each user should have a unique username to trace their activities and to ensure that they adhere to acceptable use of the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password management system ensures the quality of passwords by restricting the re-use and enforcing the use of strong passwords</td>
<td></td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>Logical: Systems / Applications</td>
<td>Applications should limit functionality from the menus down by controlling read, write, delete and execute rights</td>
</tr>
<tr>
<td></td>
<td>Sensitive systems should have an isolated computing environment and should be documented as such</td>
<td></td>
</tr>
<tr>
<td><strong>Software Development</strong></td>
<td>Applications</td>
<td>Correct processing will prevent errors, loss, unauthorised changes or misuse</td>
</tr>
<tr>
<td></td>
<td>Data input validations should be in place</td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control of internal processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balancing controls and check totals</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cryptography</td>
<td>Policy required</td>
<td></td>
</tr>
<tr>
<td>Data output should be validated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software updates</td>
<td>Rollback plan</td>
<td></td>
</tr>
<tr>
<td>Test data should be selected carefully and exclude sensitive data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Only authorised personnel should have access to source code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Security must be included in the SDLC</td>
<td></td>
</tr>
<tr>
<td>Development</td>
<td>Formal Change control</td>
<td></td>
</tr>
<tr>
<td>New software to be tested in separate environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software package changes should be restricted to critical updates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Outsourced software development should be supervised and monitored to ensure quality and no vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patches must be tested before applying to production environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Management</strong></td>
<td>Reporting</td>
<td>To appropriate management channels as soon as possible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Formal reporting procedure required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Once reported, it should be dealt with quickly and effectively</td>
</tr>
<tr>
<td>System monitoring</td>
<td>Alerts and vulnerabilities should be used to detect information security incidents</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Management</strong></td>
<td>System monitoring</td>
<td>Learning should take place based on the type of incidents logged – proactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evidence must be collected if there is legal action after an incident</td>
</tr>
<tr>
<td><strong>Business Continuity</strong></td>
<td>BCP</td>
<td>Process should be in place to recover to acceptable level of operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Consequences of disasters should be subject to business impact analysis</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Applicable legislation must be identified and information systems must be compliant</td>
<td>Intellectual property rights</td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software license agreements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Important records should be protected and classified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Retention policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data protection officer Ensures data is protected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users Deterred from misusing information processing facilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-business use must be with management consent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scope of permitted access should be defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Users should be notified of any monitoring software loaded</td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td>Management Regular reviews to ensure staff is compliant with information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Technical compliance Regular reviews to ensure information systems are compliant with information security implementation standards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Penetration or vulnerability tests should be performed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audits Operational data should be audited</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Scope of audit to be discussed beforehand</td>
<td></td>
</tr>
<tr>
<td>ISO 27002 Area</td>
<td>Requirement</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>Information systems audit tools should be protected against misuse</td>
<td></td>
</tr>
<tr>
<td>Third parties</td>
<td>Change passwords once they are done with audits</td>
<td></td>
</tr>
</tbody>
</table>