Establishment of an Information Technology Risk Management Framework within Food Manufacturing Enterprises in South Africa

S. Sandi

2020

Establishment of an Information Technology Risk Management Framework within Food Manufacturing Enterprises in South Africa

by

Siyabulela Sandi

s203021371

Treatise

submitted in partial fulfillment of the requirements for the degree

MPhil in IT Governance

in the

Faculty of Business and Economic Sciences

of the

Nelson Mandela University

Supervisor: Dr. Hettie Booysen

Date: April 2020

Declaration of originality

I, **Siyabulela Sandi**, student number *s203021371* hereby declare that the treatise for MPhil in IT Governance is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another university or for another qualification.

SIGNATURE:

DATE: 29 November 2019

Acknowledgements

I would like to thank my entire family for the encouragement, motivation, and inspiration that they gave me throughout this journey of pursuing a Masters of Philosophy in IT Governance. Without mentioning all the names, this includes my life partner Amanda Mangaliso, my sisters Monica Ntanta and Zingiswa Sandi. Without their support this would have been impossible to achieve and I believe I would have taken longer to finish the journey than I did.

I also would like to thank my colleagues at work for their support, Lunga Tukani and JP Nortje for their wise words and encouragements. Thank you Prof Von Solms from the Centre for Research in Information and Cyber Security: School of ICT of Nelson Mandela University for being such an amazing coordinator and professing your knowledge of the subject matter.

Last but not least my gratitude goes to my supervisor Dr. Hettie Booysen for thoroughly going through this treatise, for her academic guidance and her constructive criticism. Thank you very much Dr. Booysen.

Abstract

Enterprises of all kinds, regardless of the sector, are directly or indirectly dependent on Information Technology (IT) to carry out their daily activities. With this in mind, and correlated with the problem statement that it is “the lack of IT governance principles that lead to exposing enterprises to IT-related threats, vulnerabilities, and risks”, the objective of this study was to establish an Information Technology Risk Management Framework for enterprises within the Food manufacturing industry in South Africa that will ensure that IT-related threats, vulnerabilities, and risks are properly managed.

In order to accomplish this, the research followed a process called design science research. The design science research paradigm was used to create a design artificial artefact in the form of a framework. The Nelson Mandela University – Design Science Framework Methodology (NMU-DSFM) was adopted since the objective of the study was to develop a framework.

The study has revealed that enterprises within the sector are indeed lagging behind in terms of IT governance principles, hence an artefact called the IT Risk Management Framework for Enterprises within Food Manufacturing Industries in South Africa was developed.

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

TERM	DESCRIPTION
AI	Artificial Intelligence
BIA	Business Impact Analyses
CG	Corporate Governance
CIA	Confidentiality, Integrity and Availability
CTF	Cyber Task Force
ERP	Enterprise Resource Planning
ERM	Enterprise Risk Management
IOSCO	International Organisation of Securities Commissions
IS	Information Systems
ISMS	Information Security Management System
ISO	International Standards Organisation
IT Governance	Information Technology Governance
IT Management	Information Technology Management
ITGI	Information Technology Governance Institute
KRI	Key Risk Indicators
NACD	National Association of Corporate Directors
NMU-DSFM	Nelson Mandela University – Design Science Framework Methodology
OECD	The Organisation for Economic Co-operation and Development
ROI	Return on Investment
SLA	Service Level Agreement

Chapter 1
Introduction

1.1 Background

Enterprises of all shapes and sizes face some uncertainty about not achieving their business objectives owing to unforeseen circumstances. Chapman and Cooper (2003, p238), define risk as "exposure to the possibility of economic or financial loss or gains, physical damage or injury or delay as a consequence of the uncertainty associated with pursuing a course of action". Risk management involves coordinated activities to direct and control an enterprise with regard to risk and includes methodologies and mechanism, undertaken to ensure that the chances of negative incidents that may prevent the enterprise from achieving its objectives are minimized.

Information Technology Governance (IT Governance) is becoming essential in all enterprise structures as it creates effective value of IT investments and enables excellent achievement in the management of IT processes in general. Information technology governance allows effective communication with all stakeholders internally and externally, reduces redundancy across the IT environment and drives cost savings. As per Von Solms (2009), IT Governance has components, just like any Governance structures, for example, the components of Corporate Governance include Financial Governance, HR Governance and IT Governance. IT risk management is a component of IT Governance, and to achieve good IT Governance, IT risk management should be effective. It is not enough for enterprises to have state of the art IT systems. They also need structures to govern those.

Information Technology Governance should be used to deal with issues affecting IT-related risks such as data management, information availability, and denial of IT services. "Information Technology Governance involves managing IT operations and IT projects to ensure alignment between these activities and the needs of an organisation defined in its strategic plan" (Global Technology Audit Guide (GTAG), 2012, p2).

1.2 Information Technology Risk Management Context

Information technology risk management has become a topical issue over the last few years. This is because of the increasing number of cyber-attack incidents that occur globally that are among the top risks and concerns at company board level. Although there have been many incidents in South Africa throughout the years, Liberty Life is the latest in a series of companies to fall victim to cyber-attacks. In June 2018, hackers accessed Liberty Life email servers. The company maintained that no one lost any money as a result of the breach because the hackers had obtained mostly emails. In another incident in 2017, Old Mutual experienced unauthorized entry of one of its system which led to access of some customer information such as names, telephone numbers, and investment values.

With regard to enterprises within the food manufacturing industry in South Africa, systems to track and trace products for recall purposes have been identified as improper and lacking adequate governance (Department of Health: Republic of South Africa, 2018). This has contributed to difficulties, for example, in understanding the root cause of the listeria outbreak that occurred during 2017 and 2018 in South Africa within the food manufacturing sector. Moreover, poor IT Governance can create a loophole for cyber-criminals to illegally infiltrate a system, encrypt data, and hold information hostage for ransom. Therefore, proper and adequate governance is needed to safeguard food quality and people’s lives.

Furthermore, as per the article by MyBroadband (2019, August 13), “South Africa is amongst one of 17 countries hit by North Korean attackers to raise money for its weapons of mass destruction programmes”. The article further states that “the UN Security Council is investigating at least 35 cases where North Koreans launched cyber-attacks in 17 countries with the aim of raising funds, however, the report is not yet published”.

As organisations become increasingly dependent on IT and intellectual assets, the key areas of IT risk are usually seen as IT infrastructure and network security, data integrity, confidentiality, privacy and compliance, business continuity and disaster recovery, and general IT management issues (Calder, 2009). As enterprises within the food manufacturing sector increasingly depend on IT, an effective IT risk management framework needs to be developed to safeguard IT environments. The dependence on IT in food manufacturing enterprises is due to integration of technology into manufacturing processes, for example:

Robotics - robots are used in manufacturing processes instead of humans.

Enterprise Resource Planning - integrated applications are used to manage businesses.

Electronic Commerce – customers buy products online.

Electronic Data Analysis – analysis of data for manufacturing purposes.

3D Food Printers - prepare a meal in an automated additive manner.

Information technology risk management is a component of IT Governance and a mechanism to ensure that proper action is taken into account regarding IT risks at the time that the enterprise becomes aware of the risk. “Information technology risk is a component of the overall risk universe of the enterprise” (ISACA, 2009, p11). Owing to vast technological advances and high competition amongst enterprises, IT dependency has been increasing in general, hence IT risk management is essential. Information Technology risks should be managed properly to enhance effective communication inside the enterprise and externally.

Wilkin and Chenhall (2010, p119) classify four focus areas in the IT risk management literature: (a) “Understanding the types of IT risks in different contexts”, (b) “identifying strategies to manage risk”, (c) “establishing the role of the board”, and (d) “establishing the role of senior management”. The approach will be discussed and developed during the actual research phase to address shortcomings such as failure to use appropriate risk metrics, taking known risk into account, and failure in monitoring and managing existing risk.

Ineffective IT risk management principles can lead to financial losses, business disruptions, poor performance of IT assets, and surprises in general because an enterprise may not be aware of its current risk exposure which can negatively affect the performance of its IT assets, and prevent it from achieving its objectives. The goal of IT risk management is to safeguard IT assets such as data, “hardware, software, personnel and facilities from all threats, both external (e.g. natural disasters) and internal (e.g. technical failures and unauthorized access), so that the costs of losses resulting from the realization of such threats are minimized" (Gottfried, 1989 cited by Bandyopadhyay, Mykytyn, & Mykytyn, 1999, p437). Effective IT risk management safeguards data centres, such as server rooms, to ensure that they are properly secured in case of natural disasters like earthquakes, floods, and thunderstorms as well as for protection of information from unauthorized access by cybercriminals.

The IT risk management lifecycle consists of four phases:

IT risk identification;

IT risk assessment;

IT risk response and mitigation;

IT risk control monitoring and reporting.

Information Technology risk is centred on the comprehensive cycle of risk management processes. A failure to execute any one of the four phases in a broad and thorough method will result in an unsuccessful risk management process (CRISC, 2015). A failure to perform one phase may lead to a deficiency that may affect the other phases. Therefore, IT risk management requires a holistic approach that is continuous and does not end at the first cycle.

1.3 Research Rationale and Significance

IT risk management, especially organisation-wide risk management, is a valuable part of the governance and effective management of an organisation (CRISC, 2015). There are certainly some benefits of having effective IT risk management which are:

Better oversight of enterprise assets;

Minimized losses;

Identification of threats, vulnerabilities, and risk;

Prioritization of risk response efforts;

Legal and regulatory compliance;

Increased likelihood of project success;

Improved performance and the ability to attain enterprise goals.

Information Technology risk management is crucial for good performance of enterprise IT assets. Von Solms (2009), has alluded to the fact that it is essential that enterprises perform their own IT risk analysis to ensure that, if there are any serious IT risks, measures can be taken accordingly.

Given the problem of a lack of IT risk management principles within enterprises in the food manufacturing industry, and given that IT risk management is a component of IT Governance, in order to achieve effective IT risk management philosophies, good IT Governance measures need to be fully implemented within an enterprise. Effective IT risk management is impossible without good IT Governance.

1.4 Problem Statement

Through researching IT risk management and IT Governance in the food industry, focussing on discussions with role players, and examining internal data, audit reports and global trends, it has been noted that enterprises within the sector are lagging behind in IT Governance principles. By doing so, they are exposing themselves to IT-related threats, vulnerabilities and risks.

A sound IT risk management framework within food manufacturing enterprises in South Africa will, therefore, enable pro-active identification of IT-related threats, vulnerabilities and risks that could impact on food manufacturing processes owing to the integration of technology and technology based activities, such as, robotics, Enterprise Resource Planning (ERP), E-Commerce and 3D food printing.

1.5 Thesis Statement

A sound IT risk management framework can assist enterprises within the food manufacturing sector in South Africa in ensuring that IT-related threats, vulnerabilities, and risks are managed effectively.

1.6 Research Objectives

Primary objective

The primary objective of this research study was to establish a framework that would ensure that IT-related threats, vulnerabilities, and risks are properly managed. Application of such a framework would enable enterprises within the food manufacturing sector to make appropriate risk-aware decisions, therefore improving performance and enabling achievement of the objectives of the enterprises.

Secondary objectives

To determine that enterprises are well informed about the extent of risk, risk appetite, and risk tolerance.

To provide guidelines on how to conduct IT risk identification, assessment, response and mitigation, and control monitoring and reporting.

To create a risk-aware culture within food manufacturing enterprises for better decision making.

To ensure the integrity, confidentiality, and availability of information.

1.7 Delineation

This research study focused on the establishment of an IT risk management framework within food manufacturing enterprises, particularly in the poultry industry in South Africa and on the benefits of having such a framework. However, the study did not consider implementation of the framework. The framework was developed to provide guidelines for effective IT risk management.

1.8 Research Process

This research study followed the design science research paradigm. “A paradigm is a shared world view that represents the beliefs and values in a discipline and that guides how problems are solved” (Schwandt, 2001). The design science research paradigm was used to create a design artificial artefact in the form of a framework.

As per Österle, Becker, Frank, Hess, Karagiannis, Krcmar, and Sinz (2011, p3), there are four principles that need to be considered when performing design science research namely: “abstraction – the artefact must be applicable to a class of problems”, “originality – the artefact must substantially contribute to the advancement of the body of knowledge”, “justification – the artefact must be justified in a comprehensible manner and must allow for its validation”, and “benefit – the artefact must yield benefit either immediately or in the future for the respective stakeholder groups”. These principles were incorporated in the research approach.

Nelson Mandela University – Design Science Framework Methodology (NMU-DSFM) was implemented in this study since the objective of the research was to develop an IT risk management framework. A framework is defined as a basic structure underlying a system, concept, or text. For this research study, a basic structure was developed following internationally accepted concepts and best practices and this structure was aligned with NMU-DSFM. An extensive review of literature related to the research problem was conducted and interviews, questionnaires, and surveys were used to collect the data.

A meeting with the Chief Executive Officer and Chief Financial Officer of the enterprise chosen for this study was held to attain authorization to conduct relevant interviews and issue questionnaires to appropriate individuals. Furthermore, a series of meetings was arranged with relevant individuals within the IT department, more particularly with the IT Manager who was in charge of the department at the time of this study.

Following NMU-DSFM, a framework was drafted, distributed to stakeholders for critical analysis and tested for acceptance. After the stakeholders were satisfied with the framework, a final draft was made available and submitted for evaluation.

Chapter 2
IT GOVERNANCE

2.1 IT Governance overview

Enterprises of all shapes, types and sizes encounter some IT-related threats, vulnerabilities, and risks. According to Kbar (2008, p669), a threat is “anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset”. Kbar (2008, p669) further states that a “threat is a possible danger that might exploit a vulnerability to breach security”. Alzadjali, Al-Badi and Ali (2015, p425) define vulnerability as “the probability of an asset not being able to resist the actions of a threat agent”.

Vulnerability relates to a weakness or gap in a security program that can be exploited by threats to gain unauthorized access to an information system. In summarizing the statements of Kbar (2008) and Alzadjali et al. (2015), accurately assessing threats and identifying vulnerabilities is critical to understanding the risk to an enterprise and ensuring that the identified risk is within the risk appetite. Alzadjali et al. (2015, p427) also mention that “risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is little or no risk”. There is, therefore, always a direct correlation between threats and vulnerabilities.

For effective risk management, enterprises need to develop, adopt and implement mechanisms to combat the identified risks. One of the best mechanisms is to establish sound IT Governance structures within the enterprise. Information gathered through a variety of investigative approaches (as described in Section 1.4), indicates that sound IT Governance structures are lacking in enterprises within the food manufacturing industry in South Africa.

Information Technology Governance is the process, mechanism, and methodology used to prevent risks from occurring. “IT governance is the component of Corporate Governance (CG), so does IT governance also consists of a number of subcomponents such as Information Security Governance, Performance and Capacity Governance, Information Risk Management Governance, etc.” (von Solms, 2009, p17). As per Wilkin and Chenhall (2010) and Zarvić, Stolze, Boehm and Thomas

(2012), the term “IT governance” appeared for the first time in research conducted during the 1990’s. According to Aasi, Rusu and Vieru, (2017, p44), “Loh and Venkatraman’s (1992) work is one of the first studies to use the concept IT governance, pointing out that IT governance is starting to be acknowledged as a significant part of IT strategy”.

“IT governance is defined as the responsibility of the Board of Directors and Executive Management” (IT Governance Institute (ITGI), 2003, p11). The Institute of Directors Southern Africa (2016, p62) affirms this ITGI (2003) statement by citing KING IV Principle 12 that, “the governing body should govern technology and information in a way that supports the organisation setting and achieving its strategic objectives”. The ITGI (2003, p16) further state that, “IT governance is an integral part of the enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives”.

According to Calder and Watkins (2012, p44), “IT governance is the framework for the leadership, organisational structures and business processes, standards and compliance to these standards, which ensures that the organisation’s information systems support and enable the achievement of its strategies and objectives”. The definitions provided above indicate that there is agreement amongst authors that IT governance is fundamental to enabling an organisation to achieve strategies and objectives that are IT-related.

According to Aasi et al. (2017, p45), “IT governance is a continuous life cycle that can be entered at any point”. Ko and Fink (2010) further state that governance of information technology is an ongoing concern; According to Aasi et al. (2017) as well as Ko and Fink (2010), IT governance is not a once-off IT management mechanism but evolves as technology changes rapidly.

2.2 Importance of Information Technology Governance

Regardless of the size and nature of a business, IT governance is critical in ensuring that the mandate of the organisation is carried out effectively in order to achieve IT-related objectives. Hosseinbeig, Moghadam, Vahdat and Moghadam (2011, IT Governance section) describe IT as an essential part of all organisations, where there is, for example, considerable dependence on "IT for presenting key information to the organisation and supporting business deals". Consequently, sound levels of IT governance are needed. An increasing number of virtual threats has increased organisational vulnerability, and, as a result of larger investments, IT has become a very important resource which is in need of proper governance.

As per the Center for National Computing (2005, p5), "IT governance has become very topical for a number of reasons" including that:

> Governance, in general, has taken on greater significance as a consequence of a number of corporate scandals.
>
> Management's awareness of IT-related risks has increased.
>
> There is a focus on IT costs in all organisations.
>
> There is a growing realization that more management commitment is needed to improve the management and control of IT activities.

Although the Center for National Computing's statement is dated 2005, it is still relevant today owing to a number of information security incidents that have recently taken place in the South African financial industry. These include the Liberty Life email server attack in June 2018, the Old Mutual unauthorized system access by hackers in 2017 and the Standard Bank cyber-attack from Japan in May 2016. These incidents have led to robust discussions about the state of IT governance amongst enterprises within the South African financial industry, and other industries in general.

Although these incidents happened between 2016 and 2018, initiatives and discussions to combat IT-related threats in the form of cyber-attacks have already begun in South Africa. In this regard, Cybercrimes and Cybersecurity Bill B6-2017 was first published in 2015, updated in 2017 and introduced in Parliament on 22 February 2017 (Van Niekerk, 2017). The International Organisation of Securities Commissions (IOSCO) has also started with some work to raise awareness of existing international cyber guidance and encourage the adoption of good practices among the IOSCO regulatory community of which South Africa is part. To carry out this work, the IOSCO Board established a Cyber Task Force (CTF) in October 2017.

The Center for National Computing (2005, p5) further states that IT governance is needed because there is "non-existence of accountability and not enough shared ownership and clarity of responsibilities for IT services and projects within enterprises in general". They state that "organizations need to obtain a better understanding of the value delivered by IT, both internally and from external suppliers", and that "management needs to understand whether the infrastructure underpinning today's and tomorrow's IT (technology, people, processes) is capable of supporting expected business needs".

With reference to the Problem statement of this study (Section 1.4), the Center for National Computing (2005) statement above is in fact accurate regarding IT governance problems encountered by enterprises within the food manufacturing industry. Through IT audits of food manufacturing enterprises, the following issues related to IT governance were found:

Absence of documented IT policies and strategies;

Redundant IT infrastructure;

Disaster Recovery Plan not tested (no evidence);

IT Risk Assessment not conducted;

No IT training and awareness programs.

These issues contributed to a recent incident where the IT system of a food manufacturing enterprise was unlawfully accessed by hackers and customer information obtained. It can be concluded that enterprises within the food manufacturing industry are lagging behind in terms of IT governance principles.

2.3 Drivers of Information Technology Governance

Bhattacharjya and Chang (2007) cited by Rubino & Vitolla (2014) state that, based on research performed by Bhattacharjya and Chang (2006), Lazic and Heinzl (2011), Peterson (2004), Schlosser et al. (2010), Simonsson and Johnson (2006), Tiwana and Konsynski (2010), IT governance is becoming more popular and some enterprises seem to understand the importance of having IT governance in their governance structure, however, many enterprises have not yet recognised this. Calder (2009) indicates that there are drivers for IT governance adoption and describes these drivers as:

The search for competitive advantage, in the dynamically changing information economy, through intellectual assets, information and IT.

Rapidly evolving governance requirements across the Organisation for Economic Co-operation and Development (OECD), underpinned by the capital market and regulatory convergence.

Increasing information and privacy-related legislation (compliance).

The proliferation of threats to intellectual assets, information and IT.

The need to align technology projects with strategic organisational goals, ensuring that they deliver planned value (‘project governance’).

Calder (2009) further states that the above mentioned points are drivers for IT governance because enterprises want to comply with relevant regulations and with governance requirements. Furthermore, enterprises want to protect their information assets and be competitive because dependence on technology amongst enterprises has increased.

For the adoption of IT governance principles, enterprises need to understand their strategic objectives and align them with their IT plans. A decision needs to be made whether the enterprise wants to be competitive or not with regard to rapidly evolving IT usage and information security within the information assets of the enterprise. Regulations related to IT management are changing as technology advances rapidly, consequently the need for compliance has become essential and without effective IT governance, this can be impossible to achieve.

2.4 Benefits of Information Technology Governance

Adopting and implementing effective IT governance principles remains the responsibility of the board of directors of an enterprise. Musson and Jordan (2006, Introduction section) highlight that, “IT systems have a long-term effect on a company’s operations, and the IT infrastructure which develops over time, if not managed, can impede future strategic intentions” hence effective IT governance principles are essential. Ko and Fink (2010, p663) also mention that “effective IT governance ensures IT systems sustain and extend an organisation’s strategies and objectives and if not managed appropriately could hinder the success of enterprise strategies”. Both the statements by Musson and Jordan (2006) as well as Ko and Fink (2010) allude to the fact that IT governance is essential, yet if not managed effectively could impede future strategic intentions of the enterprise.

In order to reap benefits, investments need to be made and investing in IT governance certainly is beneficial. Musson and Jordan (2006, Introduction section), suggest that, “IT has great potential for creating a competitive advantage”. Generally, the benefits of having effective IT governance include that confidentiality, integrity, and availability (CIA) of information is assured (CRISC, 2015). CRISC (2015, p23) define the CIA as a model that is designed to guide IT-related policies within an enterprise. If the CIA model is adopted effectively, IT governance improves. Furthermore, through effective IT governance, “enterprises become aware of the extent of risk, risk appetite, and risk tolerance”. Consequently, a risk-aware culture is created, and guidelines for IT risk management process are provided.

A literature review, based on the study by the Center for National Computing (2005), identified the following benefits that arise from IT governance:

Transparency and Accountability: Improved transparency of IT costs, IT processes and IT portfolios (projects and services). Clarified decision-making accountabilities and definition of user and provider relationships.

Return on Investment/Stakeholder Value: Improved understanding of overall IT costs and their input to return on investment (ROI). Focused cost-cutting combined with an ability to reason for investment. Stakeholders are allowed to see IT risk/returns. Improved contribution to stakeholder returns. Enhancement and protection of reputation and image.

Opportunities and Partnerships: Providing a route to realise opportunities that might not receive attention or sponsorship. Positioning of IT as a business partner (and clarifying what sort of business partner IT is). Facilitating more business-like relationships with key IT partners (vendors and suppliers). Achieving a consistent approach to taking risks. Enabling IT participation in business strategy (which is then reflected in IT strategy) and vice versa. Improving responsiveness to market challenges and opportunities.

Performance Improvement: Achieve clear identification of whether an IT service or project supports “business as usual” or is intended to provide future added value. Increased transparency will raise the bar for performance, and advertise that the bar should be continuously raised. A focus on performance improvement will lead to the attainment of best practices. Avoid unnecessary expenditures since expenditures are demonstrably matched to business goals. Increase ability to benchmark.

External Compliance: Enabling an integrated approach to meeting external legal and regulatory requirements.

2.5 Focus areas of Information Technology Governance

As identified by the IT Governance Institute (2003), there are five key focus areas for IT governance, as illustrated in Figure 2.1.

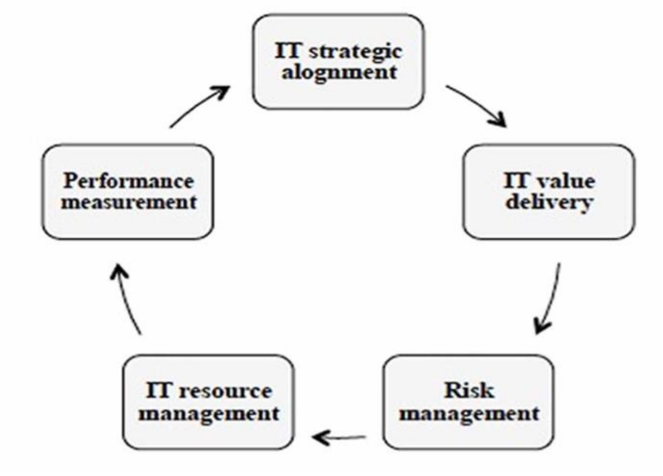


Figure 2.1: Five Focus Areas of Information Technology Governance (Source: ITGI, 2003)

2.5.1 Information Technology Strategic Alignment

“This is to ensure a linkage between business strategic plans and IT plans, and defines, maintains and validates IT value propositions and aligns IT and enterprise operations” (Aasi et al., 2017, p45) . To make appropriate and sound business decisions, IT strategies need to be aligned with business strategies.

2.5.2 Information Technology Value Delivery

Aasi et al. (2017, p45) specify that IT value delivery is the “execution of the value propositions through the delivery cycle, makes certain that IT delivers the promised benefits vs. the strategy. The main concern is optimizing costs and proving the intrinsic value of IT throughout the delivery cycle”.

2.5.3 Risk Management

Like any component of IT governance, risk management is crucial. According to Aasi et al., (2017, p45) “risk management ensures risk awareness by senior officers in the organisation, clear transparency and understanding of the organisation’s desire for significant risk and compliance requirements, and embedding of risk management responsibilities in the organisation”. The main concern is to do with embedding accountability to mitigate significant risks.

2.5.4 Information Technology Resource Management

Information Technology resource management is a method to “ensure optimal investment and proper management of critical IT resources: applications, information, infrastructure and people” (Aasi et al., 2017, p45) . Aasi et al., (2017, p45) further alludes to the fact that IT resource management remains “the main concern regarding optimizing knowledge and infrastructure. The IT resource management area overlaps all the other four areas”.

2.5.5 Performance Management

This is the process of overseeing, observing, tracking, and monitoring the execution of IT strategies and IT projects. Aasi et al., (2017, p45) states that, “performance management applies to the use of resources, performance of processes and delivery of services”. For instance, performance management includes the use of a Balanced Score Card (BSC), “which transforms and translates strategies into action for achieving goals that are quantifiable beyond conventional accounting” (Aasi et al., 2017, p45)

2.6 Conclusion

Effective IT governance is very important in the governance structures of any enterprise. Ali (2006), as cited by Parry and Lind (2016, p23), “found important positive relationships between the overall level of effective IT governance and the existence of the following: ethics/culture of compliance in IT, corporate communication systems, IT strategy committee, and the involvement of senior management in IT”. For IT governance to be effective, good ethical leadership, effective strategic management, efficient communication channels within the enterprise, and senior management buy-in is needed. As noted by many authors, IT governance is the responsibility of the Board of directors who need to ensure that good IT governance principles are achieved through setting up effective IT governance frameworks to ensure that IT-related threats, vulnerabilities, and risks are easily identified. Creation of an effective IT governance framework is the primary objective of this research study.

Sharma et al. (2009) cited by Parry and Lind (2016, p23) specify that, “there are several factors that may lead to effective IT governance in organisations”. They state that “some of these factors are good project management ability and senior management support or involvement”. They further elaborate on the fact that “effective IT governance is predicated on three broad categories of factors”. These factors are:

Leadership, organization, and decision rights;

Importance of flexible and scalable processes improvement and

The use of enabling technology.

Chapter 3 of this treatise reviews literature about IT risk management. Chapter 2 (this chapter) reviewed literature about IT governance because without good IT governance, there can be no effective IT risk management. The main objective of this research study is to establish an IT risk management framework, and, as stated in Section 2.1, IT risk management is a subcomponent of IT governance. For IT risk management to be effective, effective IT governance principles need to exist.

Chapter 3
IT RISK MANAGEMENT

3.1 Governance and Risk Management Background

“Governance is the accountability for the protection of assets of the organization” (CRISC, 2015, p2). The Board is accountable for governance, and they delegate to senior management the responsibilities of managing daily operations of the enterprise in alignment with the strategic plans approved by them. Risk management is an important part of governance; for management to make sound and effective decisions, risk management processes should be effective and efficient.

In accordance with other authors, CRISC (2015, p2) mention that, “corporate governance is the system by which an organization is evaluated, directed and controlled”. As with corporate governance, IT governance is the system by which IT-related processes, methods, policies, and structures are evaluated, directed and controlled. The main objective of any form of governance is to ensure value creation for the stakeholders. CRISC (2015, p2), state that “value creation is comprised of benefits realization, risk optimization, and resource optimization”. They further state that “risk optimization is an essential part of any governance system”, therefore IT risk management is very important in enterprise structures to ensure that IT-related threats, vulnerabilities, and risks are mitigated as soon as the enterprise becomes aware of them.

3.2 Information Technology Risk Management Overview

Information Technology risk management is an integral part of the governance structure of an enterprise, and a mechanism to ensure that proper action is taken into account regarding IT risks at the time the enterprise becomes aware of a risk. It is, therefore, pivotal to have effective IT governance principles within an enterprise, more especially effective IT risk management processes. As stated by different authors, IT risk management consists of four major components, namely: *risk identification, risk assessment, risk response and mitigation, and risk control monitoring and reporting*. Literature about these components will be reviewed in Section 3.6 of Chapter 3.

Almost every year, enterprises make hundreds of thousands, even millions of investments in information technology. “As spending on IT rises steeply, organizations become increasingly technology-dependent and consequently, they become highly vulnerable to the risks of IT failure. Therefore, IT risk management is one of the important issues facing information systems (IS) executives today” (Bandyopadhyay et al., 1999, p437)**.**

As per Gottfried (1989) cited by Bandyopadhyay et al. (1991, p437), the aim of IT risk management is to protect IT assets such as data, “hardware, software, personnel and facilities from all threats, both external (e.g. natural disasters) and internal (e.g. technical failures, sabotage and unauthorized access) so that the costs of losses resulting from the realization of such threats are minimized”. Rainer, Snyder and Carr (1991) cited by Bandyopadhyay et al. (1999, p437), state that, “the purpose is to avoid or lessen losses by selecting and implementing the best combination of security measures”**.**

Stoneburner, Goguen and Feringa (2002) cited by Carcary (2012, p5), define risk management as “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions”. According to Sumner (2009) cited by Carcary (2012, p5), “a risk preparedness strategy should be developed for high impact, high probability risks”. IT risk management is a process that allows the enterprise to be well aware of the extent of risk, risk appetite, and risk tolerance.

3.3 Principles of Risk Management

All governance structures are established on principles and risk management is no exception as it is principle-based. Enterprises ought, at all levels, conform with standards of risk management to ensure that rewards offered by these principles are obtained. ISO (2009, Enteprise Risk Management section) explains these principles, as listed below:

Risk management creates and protects value – Risk management contributes to the achievement of objectives, improves performance and creates and protects the value of the organisation.

Risk management is an integral part of all organizational processes – The process of risk management is not a stand-alone activity that is separated from the main activity. It is part of the responsibilities of management and an integral part of all organisational processes.

Risk management is part of decision making – Risk management helps decision-makers make informed decisions.

Risk management explicitly addresses uncertainty – Risk management explicitly takes account of uncertainty, the nature of uncertainty and how it can be addressed.

Risk management is systematic, structured and timely – A systematic, timely and structured approach contributes to efficiency and consistent, comparable and reliable results.

Risk management is based on the best available information – Inputs to the process are based on information sources such as historical data, experience, stakeholder's feedback, forecasts, and experts' judgments.

Risk management is tailored – Risk management is aligned with the organisation's external and internal context and risk profile.

Risk management takes human and cultural factors into account – The capabilities, perceptions, and intentions of external and internal people are recognised through risk management.

Risk management is transparent and inclusive – Appropriate and timely involvement of stakeholders, especially on decision making at all levels in the organisation, ensures the effectiveness and efficiency of the risk management process.

Risk management is dynamic, iterative and responsive to change – Risk management continually senses and responds to changes.

Risk management contributes to continual improvement of the organization – The organisation should develop and implement strategies to improve risk management on a continual basis.

Enterprises with effective risk management activities benefit from the rewards associated with the principles of risk management (outlined above). For full benefit, these principles should be adhered to at all times. As mentioned in Section 2.1 and in the Problem statement (Section 1.4), application of risk management principles has been found lacking in enterprises within the food manufacturing industry in South Africa.

3.4 Importance of Information Technology Risk Management

Information Technology risk management within the structures of an enterprise is pivotal to ensuring that the benefits, as listed in Section 3.5 are experienced. Laurentiu & Adrian (2008, p144) state that “the problem of control of IT risk is very important for a company”. They further illustrate the point that effective controls will treat threats, vulnerabilities, and the impact that enterprises may encounter. Various authors have alluded to the fact that having an effective IT risk management approach is important to ensure that IT risks are controlled proactively. Laurentiu & Adrian (2008, p144), further note that IT controls achieved through effective IT risk management are important in the sense that they are:

Controls that will detect threats and issues in good time and will anticipate or prevent them where necessary and appropriate.

Controls that will enable vulnerabilities to be fixed and system weaknesses resolved.

Controls to manage the impact of any issues or threats that have succeeded in exploiting vulnerabilities or unresolved weaknesses.

Scarlat, Chirita, and Bredea (2011) are adamant that IT risk management is important, owing to the fact that key risk areas are identified easily during the process through key risk indicators (KRI). Scarlat et al. (2011, p6) define KRI as a tool that, “provides a forward direction, and information about risk, which may or may not exist and is used as a warning system for future actions”. They further state that with KRI, a specific risk can be monitored so that mitigation actions can be undertaken as soon as the risk arises. Coleman (2009) cited by Scarlat et al. (2011, p6) define a risk indicator as a “statistic or measurement that can provide perspective into a company's risk position”. A risk indicator can be reviewed occasionally to alert the enterprise of the variations that may point out risks. KRI are metrics that are used by the enterprise to indication in what way uncertain an activity is. There is, therefore, a common view that KRI is an important tool to effective IT risk management to ensure that threats, vulnerabilities, and risks are mitigated accordingly as the enterprise becomes aware of them.

Information Technology risk management is important for enabling an enterprise to set boundaries regarding the amount of risk that is acceptable. CRISC (2015, p54) defines risk appetite as “an amount of risk that an enterprise is willing to accept”. CIRSC (2015, p54) further states that, “risk appetite should be defined and approved by senior management and clearly communicated to all stakeholders, and a process should be in place to review and approve any exceptions”.

The National Association of Corporate Directors (NACD), are of the view that a robust risk appetite or per se risk appetite statement can be used to:

Establish performance targets - Risk appetite statements help organisations set more balanced performance targets that avoid incentivising excessive risk-taking. Executive management and the Board determine trade-offs between promoting superior performance and limiting exposure. Pushing these determinations down into the organisation drives strategic alignment.

Shape corporate culture - An organisation's overall risk awareness improves significantly when the risk appetite statement is translated into actionable guidance with well-defined thresholds and tolerance levels, as well as when it is used across the organisation to measure and monitor acceptable variation in performance.

Improve communication, including reporting to the Board - An effective risk appetite statement is an important communication tool for driving alignment with awareness of the strategy. A robust statement clarifies acceptable (or on-strategy) risks that management intends to take and forces dialogue on whether the strategy's potential rewards outweigh the inherent risks.

Make decisions about compensation - A formal risk appetite statement can inform a company's overall compensation philosophy with the goal of preventing employees from taking unacceptable risks to achieve performance targets.

CRISC (2015, p54) defines risk tolerance "as an acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives". Nicholson, Soane, Fenton-O'Creevy and Willman (2005) cited by Lucarelli, Uberti, and Brighetti (2015, p467) state that, "risk propensity affects judgment and decision making in many different domains which renders it complex to define and to measure". These authors further allude that risk tolerance is the other important part of risk management, more particularly in decision making with regard to risk, hence, it is pivotal to have such tools (key risk indicators, risk appetite and risk tolerance) in the governance of IT.

Radeschütz, Schwarz and Niedermann (2015, p69), are of a view that Business Impact Analyses (BIA) is a very important part of risk management in order for enterprises to achieve their IT-related objectives, and, in general. These authors assert that "increasing competition and significantly shortened product lifecycles lead to a situation where fast adaption and continuous optimization of business processes are critical factors in determining the success of a company". They also state that "business process optimization aims to improve processes of an organization, for example by discovering and removing unnecessary activities and by replacing activities by more efficient ones" (Radeschütz et al., 2015, p69). Hence BIA plays an important role in governance structures of any enterprise.

3.5 Benefits of Information Technology Risk Management

As mentioned in Chapter 1, "IT risk management, especially organization-wide risk management, is an important part of the governance and effective management of the organization" (CRISC, 2015, p2). CRISC (2015) also note that having effective IT risk management certainly has some benefits, such as:

Better oversight of enterprise assets;

Minimized losses;

Identification of threats, vulnerabilities, and risk;

Prioritization of risk response efforts;

Legal and regulatory compliance;

Increased likelihood of project success;

Improved information security;

Improved performance and the ability to attain enterprise goals;

Better monitoring and reporting.

IT risk management is vital to enterprise IT asset performance. Von Solms (2009) has alluded to the fact that it is important for enterprises to perform IT risk analysis to determine any serious IT risks, if so, measures to be taken accordingly.

With regard to the above statement by Von Solms (2009), and referencing the problem statement (Section 1.4) and the last paragraph in Section 2.2, it has been found that enterprises within the food manufacturing industry are not performing IT risk analysis hence it can be concluded that they are lagging behind in terms of IT governance issues.

3.6 Components of Information Technology Risk Management

As mentioned in Section 3.2 of this chapter, IT risk management consists of four components. As such, it is a comprehensive process that requires organisations to (i) Frame risk (i.e., establish the context for risk-based decisions), (ii) assess risk, (iii) respond to risk once determined, and (iv) monitor risk on an ongoing basis using effective organisational communications and a feedback loop for continuous improvement in the risk-related activities of organisations (NIST, 2011).

CRISC (2015) refers to the four components as IT risk identification, IT risk assessment, risk response and mitigation, and risk and control monitoring and reporting (Figure 3.1). The IT Risk Management Life Cycle (Figure 3.1) illustrates fairly that one cycle depends on the other and the IT risk management process is not complete if one cycle is ineffective.

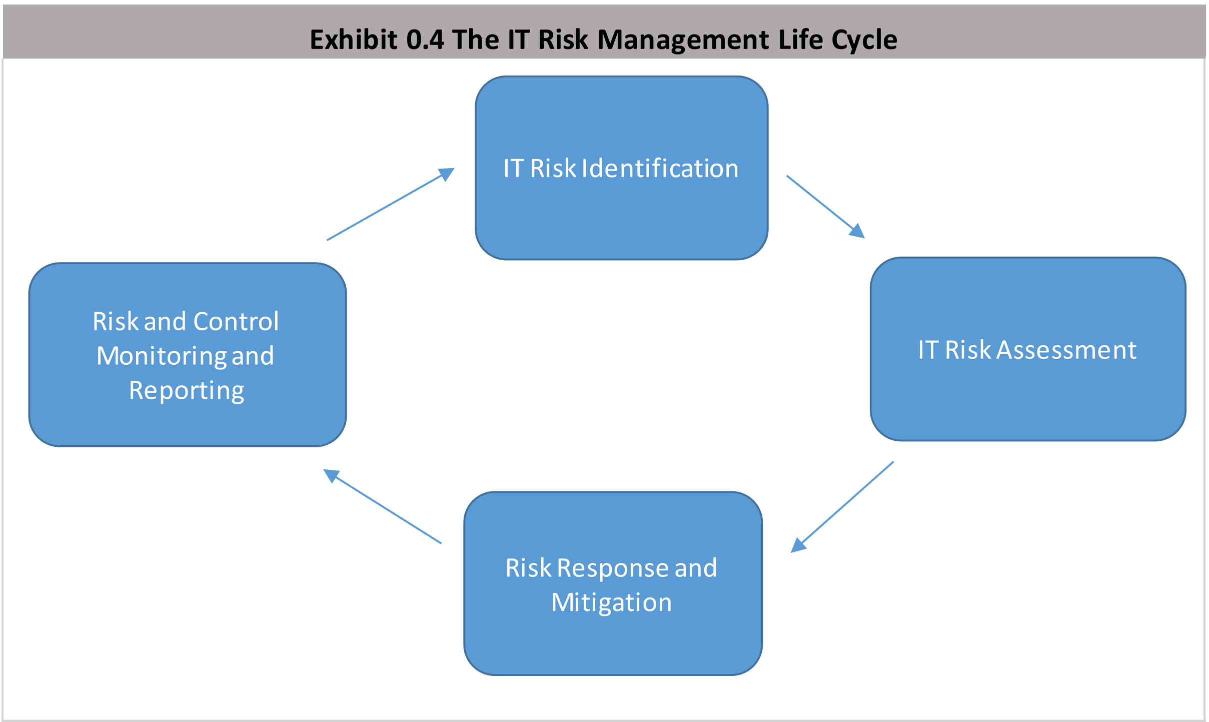


Exhibit 0.4 The IT Risk Management Life Cycle
IT Risk Identification
IT Risk Assessment
Risk Response and Mitigation
Risk and Control Monitoring and Reporting

Figure 3.1: The Information Technology Risk Management Life Cycle (Source: CRISC, 2015)

3.6.1 Risk Identification

“Risk management for IT begins with the risk identification process, which allows organizations to determine early the potential impact of the realization of internal and external threats on the entire IT environment” (Bandyopadhyay et al., 1999, p438). The NIST (2011) publication further discusses that the objective of risk identification is to produce a risk management approach that discourses how enterprises propose to assess, respond to, and monitor risk, making explicit and transparent the risk perceptions that enterprises regularly use in making both investment and operational decisions.

Many authors have noted that risk management starts with risk framing, which specifically means establishing the risk context which includes establishing the business context. NIST (2011, July 13) agrees with this view, stating that “the first component of risk management addresses how organizations frame risk or establish a risk context that is, describing the environment in which risk-based decisions are made”. CRISC (2015) has mentioned that there are numerous good sources for risk identification and classification that are available, including ISO 31000:2009 – Risk Management Principles and Guidelines, COBIT 5 for Risk, IEC 31010:2009 Risk

Management – Risk Assessment Techniques and ISO/IEC 27001:2013 – Information Technology – Security Techniques – Information Security Management System – Requirements.

As mentioned by other authors, there are several methods to identify risks. CRISC (2015) has identified three methods, namely:

The historical or evidence-based method, such as a review of historical events, for example, the use of a checklist and the review of past issues or compromise.

Systematic approaches (expert opinions), where a risk team examines and questions a business process in a systematic manner to determine the potential point of failure.

An inductive method (theoretical analysis), where a team examines a process to determine the possible point of attack or compromise.

CRISC (2015) also mentions that there are numerous types of risks that enterprises should consider during the risk identification phase. These are described in (Table 3.1)

Table 3.1 Business-related IT Risk Types (Source: CRISC 2015)

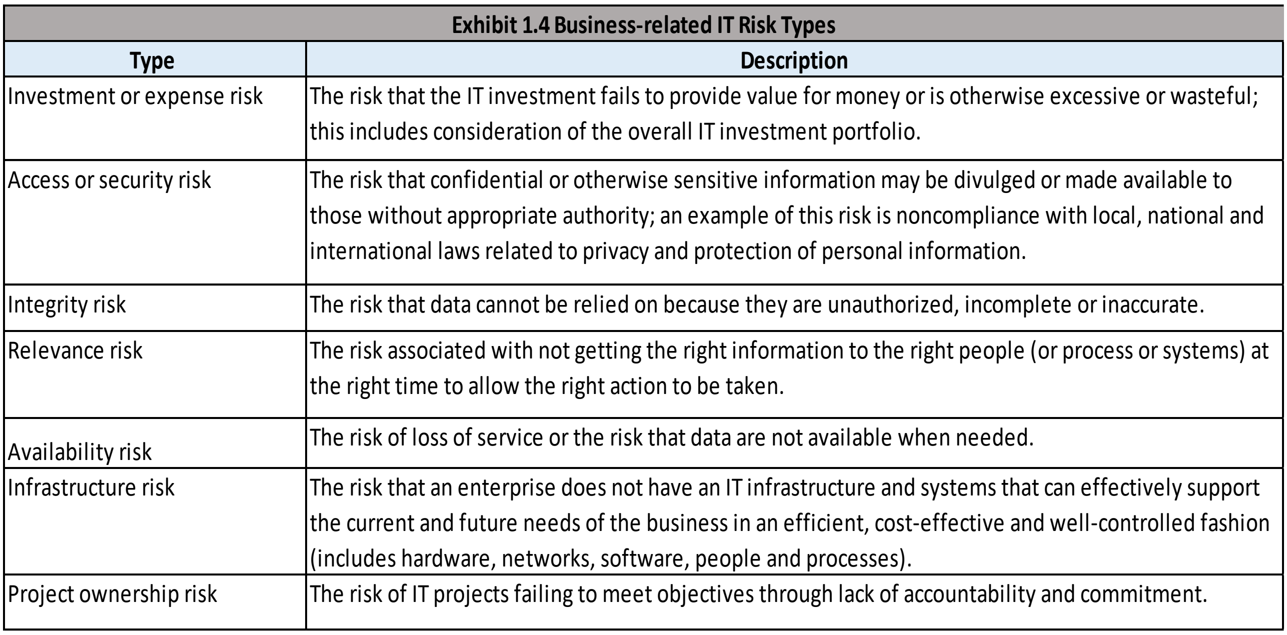


Exhibit 1.4 Business-related IT Risk Types

Type	Description
Investment or expense risk	The risk that the IT investment fails to provide value for money or is otherwise excessive or wasteful; this includes consideration of the overall IT investment portfolio.
Access or security risk	The risk that confidential or otherwise sensitive information may be divulged or made available to those without appropriate authority; an example of this risk is noncompliance with local, national and international laws related to privacy and protection of personal information.
Integrity risk	The risk that data cannot be relied on because they are unauthorized, incomplete or inaccurate.
Relevance risk	The risk associated with not getting the right information to the right people (or process or systems) at the right time to allow the right action to be taken.
Availability risk	The risk of loss of service or the risk that data are not available when needed.
Infrastructure risk	The risk that an enterprise does not have an IT infrastructure and systems that can effectively support the current and future needs of the business in an efficient, cost-effective and well-controlled fashion (includes hardware, networks, software, people and processes).
Project ownership risk	The risk of IT projects failing to meet objectives through lack of accountability and commitment.

3.6.2 Risk Assessment

Risk assessment is defined as a process to evaluate the risk that has been identified during the risk identification phase. CRISC (2015, p67) further states that "risk assessment includes assessing the critical functions necessary for an enterprise to continue business operations". Calder (2009a, p14), articulates that "risk assessment is a complex and data-rich process". Calder (2009a), further state that, for an enterprise of any size, the only practical way to perform risk assessment is to create a database that contains details of all assets within the scope of the Information Security Management System (ISMS), and then link to each asset the details of its threats, vulnerabilities, impacts and their likelihood, together with the details of the asset ownership and its confidentiality classification.

As per the NIST (2011) publication, assenting to Calder (2009a), the purpose of the risk assessment component is to identify:

Threats to the enterprise (i.e. operations, assets, or individuals) or threats directed through the enterprise against other enterprises.

Vulnerabilities internal and external to the enterprise.

The harm (i.e. consequences/impact) to the enterprise that may occur given the potential for threats exploiting vulnerabilities.

The likelihood that harm will occur.

3.6.2.1 Risk Assessment Tools

After the risks have been identified and the purpose of the risk assessment has been understood, effective tools should be used to assess the risks. Calder (2009a) is of the view that risk assessment tools must be in line with the requirements of the Standards *A.7.1.1 (ISO 27001 – Control and Objective)* which states that "all assets shall be clearly identified and an inventory of all important assets drawn up and maintained", otherwise there is no point in deploying them. As mentioned by different authors and prescribed by the Standard, risk assessment tools should be able to:

Identify the assets within the scope of the ISMS;

Identify the threats to those assets;

Identify the vulnerabilities that might be exploited by the threats;

Identify the impact that losses of confidentiality, integrity, and availability may have on the assets.

As allude to by Calder (2009a), these risk assessment tools are gap analysis, vulnerability assessment, and penetration testing. However, going forward, it is suggested that these tools could be supplemented by modern technology such as Artificial Intelligence (AI) to proactively identify potential risks based on historical information.

3.6.2.2 Risk Criteria and Risk Levels

Risk criteria are used as part of a process to evaluate the significance of the enterprise’s risk and are used to determine whether or not the risk is acceptable as per risk tolerance of the enterprise. According to ISO (2009, p41), “the enterprise should define its criteria to be used to evaluate the significance of risk”. The publication further states that the criteria should reflect the enterprise's values, objectives, and resources. ISO (2009) also mentions that when defining risk criteria factors to be considered, the following should also be included:

The nature and types of causes and consequences that can occur and how they will be measured;

How likelihood will be defined;

The timeframe(s) of the likelihood and/or consequence(s);

How the level of risk is to be determined;

The views of stakeholders;

The level at which risk becomes acceptable or tolerable;

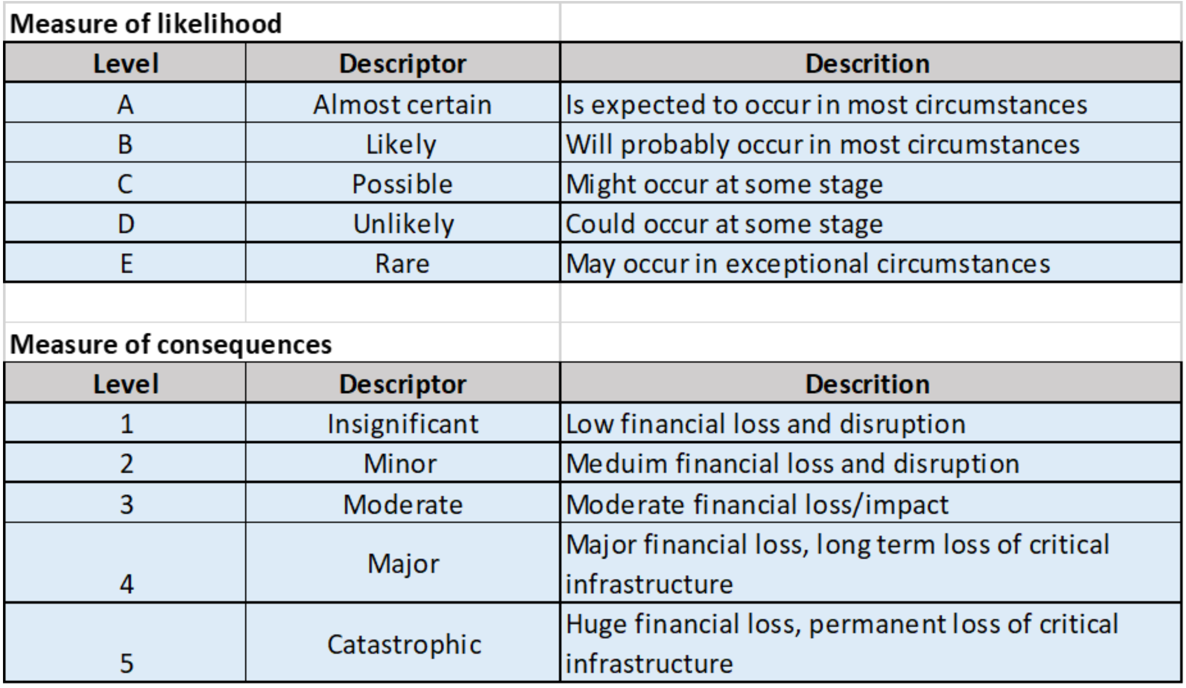
Whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

To balance out the process, risk levels are to be developed. According to ISO (2009),

> Levels of risk should be expressed in the most suitable terms for that type of risk and in a form that aids risk evaluation. In some instances, the magnitude of risk can be expressed as a probability distribution over a range of consequences.

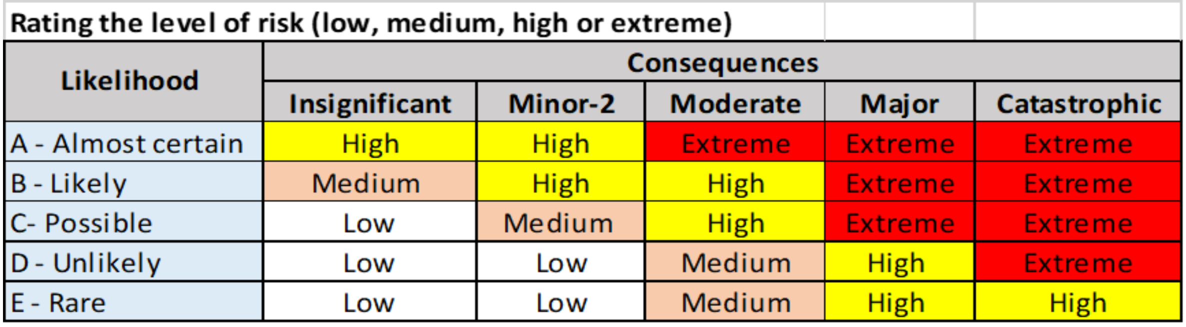
Depending on the definition of the risk criteria and risk levels, the enterprise should measure the likelihood and the consequences and rate the risks accordingly (Goy, 2010), as shown in Table 3.2 and Table 3.3.

Table 3.2 Measure of likelihood and consequences (Source: Goy, 2010)



Measure of likelihood		
Level	Descriptor	Descrition
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some stage
D	Unlikely	Could occur at some stage
E	Rare	May occur in exceptional circumstances
Measure of consequences		
Level	Descriptor	Descrition
1	Insignificant	Low financial loss and disruption
2	Minor	Meduim financial loss and disruption
3	Moderate	Moderate financial loss/impact
4	Major	Major financial loss, long term loss of critical infrastructure
5	Catastrophic	Huge financial loss, permanent loss of critical infrastructure

Table 3.3 Rating the level of risk (Source: Goy, 2010)



Rating the level of risk (low, medium, high or extreme)					
Likelihood	Consequences				
	Insignificant	Minor-2	Moderate	Major	Catastrophic
A - Almost certain	High	High	Extreme	Extreme	Extreme
B - Likely	Medium	High	High	Extreme	Extreme
C- Possible	Low	Medium	High	Extreme	Extreme
D - Unlikely	Low	Low	Medium	High	Extreme
E - Rare	Low	Low	Medium	High	High

3.6.3 Risk Response and Mitigation

According to CRISC (2015, p115), “the risk response phase of risk management requires the organisation to make the decisions regarding the correct way to respond to and address risk”. CRISC (2015) further alludes to the fact that the response decision is based on the information and work carried out during the risk identification and risk assessment phases. Furthermore, the CRISC (2015) publication states that the risk response decision must ensure that business processes are protected but not unduly impaired or impacted by controls that are put in place to address the risk.

As per Magro and Kellow (2004, p3), “once the assessment of the risks for likelihood and consequences is concluded, it is essential to examine and measure whether the risk is worthy of developing a management strategy”. According to Zhi (1994), cited by Baccarini, Salm and Love (2004), there are four main strategies for responding to project risks, namely:

Risk acceptance;

Risk mitigation;

Risk avoidance;

Risk transfer.

3.6.3.1 Risk Acceptance

According to Prasetyo and Sucahyo (2014, p100), “risk acceptance is the decision to accept the risk and the responsibility for the decisions taken in managing these risks”. Furthermore, CRISC (2015) state that the choice to accept the risk is a mindful judgment made by senior management to recognize the existence of risk and expressively decide to allow the risk to remain without being treated. CRISC (2015) further highlight that the responsibility for the impact rests with management, should a risk event occur. For example, any potential losses from a risk not covered by insurance or over the insured amount is an example of accepting the risk or when the benefits accompanying the risk are very attractive therefore accepting the risk.

3.6.3.2 Risk Mitigation

Risk mitigation means that action is taken to reduce the frequency and/or impact of a risk to be within risk appetite. According to Gonen (2011, p969), risk mitigation “refers to action taken to reduce either the probability of occurrence of an unfavourable event or the impact of this event”. Gonen (2011, p969) also states that “risk mitigation is usually executed in the form of a plan designed to handle possible high-threat events”. CRISC (2015, p116) also mention that, “risk may require mitigation through several controls until it reaches the level of risk acceptance or, in an exceptional case, risk tolerance”, for example, establishing standards to guide business practices and decision making (Policies, Performance Management, and Contingency Plans). CRISC (2015) also mention different types of control that can be used as in the control matrix in Table 3.4.

Table 3.4 Control Matrix (Source: CRISC, 2015)

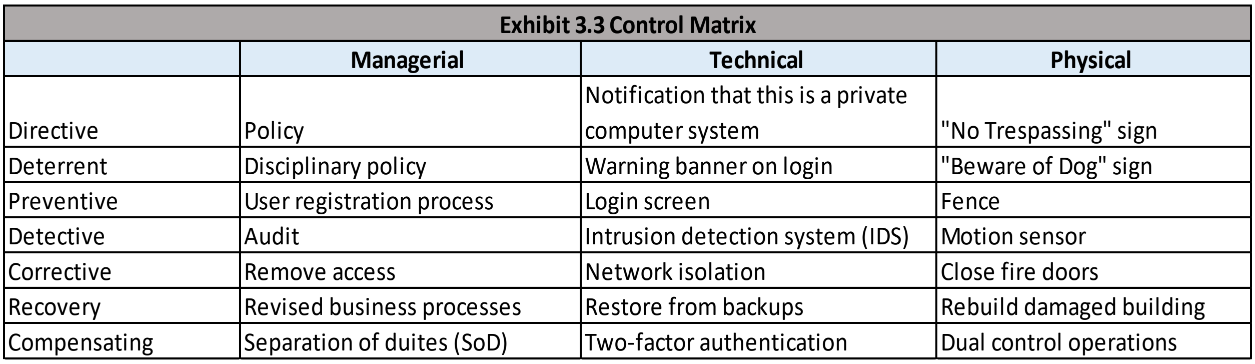


Exhibit 3.3 Control Matrix

	Managerial	Technical	Physical
Directive	Policy	Notification that this is a private computer system	"No Trespassing" sign
Deterrent	Disciplinary policy	Warning banner on login	"Beware of Dog" sign
Preventive	User registration process	Login screen	Fence
Detective	Audit	Intrusion detection system (IDS)	Motion sensor
Corrective	Remove access	Network isolation	Close fire doors
Recovery	Revised business processes	Restore from backups	Rebuild damaged building
Compensating	Separation of duites (SoD)	Two-factor authentication	Dual control operations

3.6.3.3 Risk Avoidance

Risk avoidance means withdrawing the events that give rise to risk. Risk avoidance applies when no other remedial action is suitable. As per Wijanarka (2014, Risk avoidance section), “risk avoidance can be applied when there is no appropriate response, for example, the other cost-effective response is not available to reduce the risk likelihood and impact, or the risk cannot be shared or transferred to other parties”. For example, stop processing customer information on a particular system due to a number of security breaches without mitigation, and opt-out for a new innovative system.

3.6.3.4 Risk Transfer

Risk transfer is a management decision to reduce the cost of loss through sharing the risk of loss with other organisations (CRISC, 2015). According to Wijanarka (2014, Risk Response section), “the risk transfer option occurs when organisations reduce the risk likelihood or impact by transferring the risk to, or sharing it with other parties”. This is normally done through the use of contracts, insurance, disclaimers, and/or releases of claims to transfer the liability for the expected loss to other parties involved.

3.6.4 Risk Control Monitoring and Reporting

According to the *COBIT 5 for Risk Management Practice* MEA01.01-*Establish a monitoring approach* cited by CRISC (2015, p159), setting up an “Information Systems (IS) control monitoring process requires the enterprise to engage with stakeholders to establish and maintain a monitoring approach to define the objective, scope, and method for measuring business solutions, service delivery and contributions to the enterprise objectives”.

CRISC (2015) further state that the controls required through risk management must align with the IT security and related policies of the enterprise. Furthermore, the IS control monitoring function must ensure that IT security requirements are being met, standards are being followed, and staff are complying with the policies, practices, and procedures of the enterprise.

Risk management is a recurring methodical process. According to Wijanarka (2014, Monitoring and review section), “monitoring and review process should be carried out during the IT risk management process”. Wijanarka (2014) further mentions that the intention of monitoring and review in risk management is to:

Obtain more information to improve skills in the management of risk;

Learn from the success or failure of risk management that has occurred;

Detect changes in risk criteria;

Identify new risks, which have not been defined in the earlier process.

As per CRISC (2015, p160), the objective of risk monitoring and evaluation is to “collect, validate, evaluate the business, IT and process goals and metrics, to monitor that processes are performing against agreed-on performance and conformance goals and metrics, and provide reporting that is systemic and timely”. Park, Keil and Kim (2009) state that the reason why many IT projects fail is that reporting is not effective, hence to have a successful project it is pivotal to have proper reporting procedures.

3.7 Conclusion

Sound, proper and effective IT risk management is essential to protect and attain the goals of the enterprise. Through Chapter 2 and Chapter 3 of this treatise, the principles of risk management have been deliberated and practical steps have been used to establish the benefits, objectives, and models associated with risk identification, risk assessment, risk response and mitigation, and risk control monitoring and reporting. All authors cited in Chapter 2 and Chapter 3 of this treatise have alluded to the statement made by CRISC (2015) that the objective of risk management is to discover and address all risk in an appropriate manner and to ensure that the enterprise has reduced risk to acceptable levels and does not become a victim of a risk that should have been identified and mitigated.

According to ISACA (2009), ineffective IT risk management principles do not only encompass the negative impact of operations and service delivery, which bring destruction or reduction of the value of the enterprise, but also the lost opportunities and benefits of using technology to enable or enhance an enterprise’s competitive advantage in order to achieve IT-related goals. Frequent monitoring and reporting on risk is pivotal as mentioned in Section 3.4 of this treatise, the use of Key Risk Indicators (KRI) helps the enterprise in the monitoring of trends, compliance and general issues that are related to risk.

Information Technology risk management is not a once-off event, rather it is a never-ending process. CRISC (2015) alludes to the fact that, as the external and internal environments change with technology changes, and as the nature of attacks and attackers evolves, so also does the need to revisit the risk management effort, and reassess risk, revise risk responses, and improve the risk culture and awareness of risk throughout the enterprise.

Chapter 4
METHODOLOGY

4.1 Introduction

In resolving the problem at hand, the structured approach that was followed will be discussed. As highlighted in the Problem Statement (Section 1.4) and considered in the literature review (Chapter 2 and Chapter 3), it is evident that enterprises within the food manufacturing industry in South Africa are lagging behind in terms of IT governance principles. As mentioned by various authors cited in Chapter 2 and Chapter 3, sound, proper and effective IT risk management is essential to protect and attain the goals of an enterprise. Therefore, it can be noted that enterprises within the food manufacturing industry in South Africa lack sound IT risk management principles. This is due to a gap, in that the value IT brings to the enterprise is not fully realized and IT infrastructure is not seen as an intellectual asset within enterprises in the industry.

The above-mentioned gap will be addressed by reflecting on the research paradigm that was followed. Furthermore, the research methodology used in this study will be discussed, the main aim being to develop a road map to guide the researcher to establish a sound IT risk management framework for the food manufacturing industry in South Africa. The chapter will conclude by discussing numerous research methods that could be followed, providing direction on how research contribution is established.

4.2 Research Paradigm

A design science research approach was used in this study to address the problem at hand. According to Meyers, Jacobsenand Henderson (2018, p158), design science research “is an innovative, change-oriented research methodology developed by educational researchers to bridge the theory-to-practice gap and balance scientific rigor with relevance”. Meyers et al. (2018) further state that design science methodology assists scholars to find interrelating variables and allows a systems-based understanding of the events being studied, making it a beneficial approach for exploring and facilitating change in complex research. A paradigm is a shared world view that represents the beliefs and values in a discipline and that guides how problems are solved (Schwandt, 2001).

According to Schorr and Hvam (2018, p26), design science research on IT services must include:

Designing an IT artefact (constructs, methods, models or instantiations);

Solving a relevant organizational problem;

Evaluation of an IT artefact;

Research contributions;

Application of rigorous methods;

Communication of research.

The statement by Schorr and Hvam (2018) is supported by Osterle, Becker, Frank, Karagiannis, Krcmar,…and Sinz (2011, Design Science Research section) who state that, “design-oriented IS research objectives is to develop and provide an artefact as a research contribution”. As mentioned by Schorr and Hvam (2018), Osterle et al. (2011) further articulate that this artefact should aim to address a real-world problem. Osterle et al. (2011) furthermore note that the real-world problem that is identified can consist of several stakeholders. These stakeholders will form a vital part in developing the artefact. An artefact can take one of a number of forms including a strategy, framework or model. For the purposes of this research study, the design science research paradigm was used to create a design artificial artefact in the form of a framework.

According to Liehr and Smith (1999, p13) cited by Imenda (2015), a framework is a structure that provides “guidance for the researcher as study questions are fine-tuned, methods for measuring variables are selected and analyses are planned”. With this Liehr and Smith’s (1999, p13) statement in mind, an artefact in the form of a framework was created to provide guidance, methods, and analyses to address the problem at hand.

As per Osterle et al. (2011), there are four principles that need to be considered when performing design science research, namely:

Abstraction – The artefact must be applicable to a class of problems;

Originality – The artefact must substantially contribute to the advancement of the body of knowledge;

Justification – The artefact must be justified in a comprehensible manner and must allow for its validation;

Benefit – The artefact must yield benefit either immediately or in the future for the respective stakeholder groups.

These principles were incorporated accordingly into the research process in order to create the best possible framework for addressing the problem at hand.

4.3 Research Methodology

Abiding by the principles mentioned in Section 4.2, the Nelson Mandela University – Design Science Framework Methodology (NMU-DSFM) was adopted since the objective of the study was to develop a framework. According to Osterle et al. (2011, p4), “a framework is a basic structure underlying a system, concept, or text”. An artefact in the form of a framework was the result of this study.

The NMU-DSFM consists of four consecutive phases as shown in Figure 4.1. Each phase consists of various objects that must be completed before moving to the next phase.

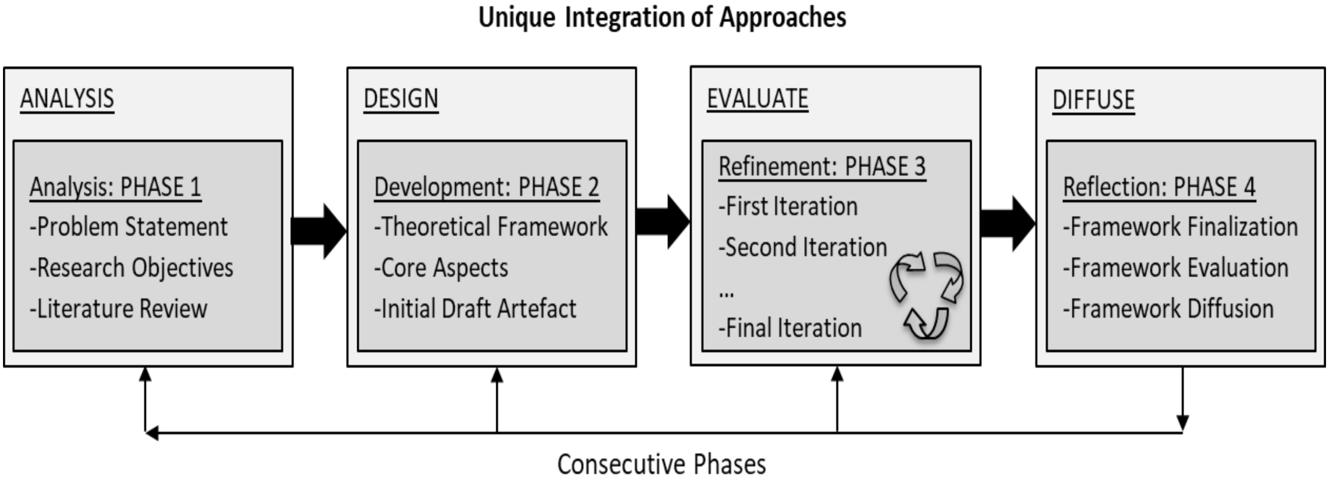


Figure 4.1 Unique Integration of Approaches (Source: NMU-DSFM)

For the purposes of this study, a basic structure was developed following concepts from design science research and aligned into the NMU-DSFM.

Each phase in the NMU-DSFM includes comprehensive guidelines on how to complete that particular phase. Herrington, McKenney, Reeves, and Oliver (2007) cited by Delport (n.d.), provide a table that contains elements within each phase (Table 4.1).

Table 4.1 Design Science Research (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**
Phase of design-based research	*The elements that need to be completed*
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem
	Consultation with researches and staeholders
	Research Review
	Literature Review
PHASE 2: Development of solutions informed by existing core aspects and technological innovations	Theoretical framework
	Development of draft core aspect to guide the design of the intervention
	Description of proposed intervention
PHASE 3: Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteraction)
	Particaipants
	Data collection
	Data analysis
	Implementation of intervention
	Second and further iterations
	Particaipants
	Data collection
	Data analysis
PHASE 4: Reflection ion core aspects of produced artefact and enhanced solution implementation	Design principles
	Designed artefact(s)
	Professional development

As shown in Figure 4.1 and Table 4.1, the phases are analysis, design, evaluate and diffuse. All these phases are based on the principles that focus on the output of an artefact in the form of a framework.

4.4 Research Approach Contextualisation

For contextualization of this research, Table 4.1 was modified and a third column added to produce Table 4.2. The third column provides further particulars on the position of the study within each of the four phases in the NMU-DSFM. Each phase will be discussed individually starting from Phase 1.

4.4.1 Phase 1

As per Herrington et al. (2017) cited by (Delport, n.d., p49), the goal of Phase 1 is the "analysis of the practical problems by researchers and stakeholders in collaboration". As part of completing Phase 1 for this study, a statement of the problem was defined through collaboration with stakeholders. After a Problem statement had been written, the research objectives were formulated and literature based on the problem at hand was reviewed (Table 4.2).

Table 4.2 Phase 1 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**	**Position**
Phase of design-based research	*The elements that need to be completed*	Position in study
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem Consultation with researches and staeholders	Initial problem were identified during research proposal phase. Consultation with stakeholders within food manufacturing enterprises in South Africa will be facilitated.
	Research Review	Initial research objectives were identified, based on the problem statement.
	Literature Review	Literature review was conducted on Chapter 2 & 3 to further understand the identified problem.

4.4.2 Phase 2

According to Herrington et al. (2017) cited by Delport (n.d., p50), the goal of Phase 2 is the "development of solutions informed by existing core aspects and technological innovations". Table 4.3 shows elements that are underlying in Phase 2. Phase 2 required the researcher to address the theoretical framework elements, through identifying criteria from the literature that was reviewed in Chapters 2 & 3. The main aim of this phase was to identify core aspects that are typical in a sound IT Risk Management Framework which are relevancy, usability, scalability, and simplicity. The output of Phase 2 was a first draft IT Risk Management Framework.

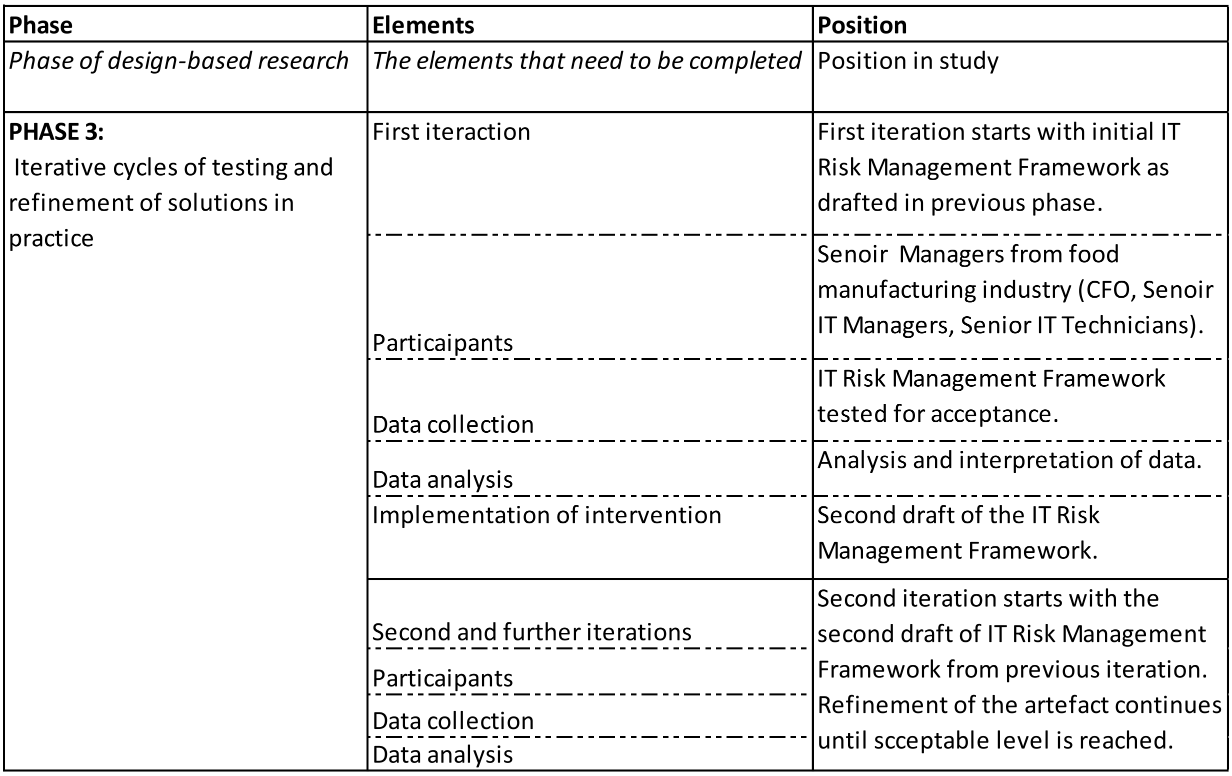
Table 4. 3 Phase 2 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.)

Phase	**Elements**	**Position**
Phase of design-based research	*The elements that need to be completed*	Position in study
PHASE 2: Development of solutions informed by existing core aspects and technological innovations	Theoretical framework Development of draft core aspect to guide the design of the intervention	Study relevant policy documents, best practices, and standards to extract core aspects.
	Description of proposed intervention	Develop the initial draft of IT Risk Management Framework for enterprises within food manaufacturing industries in South Africa from the core aspects extracted.

4.4.3 Phase 3

According to Herrington et al. (2017) cited by Delport (n.d., p51), the goal of Phase 3 is "iterative cycles of testing and refinement of solutions in practice". As shown in Table 4.4, the researcher was required to refine the artefact (IT Risk Management Framework) through a series of iterative cycles. The process of refinement was continued until stakeholders reached an acceptable level with regard to the framework acceptability. The initial draft framework from Phase 2was presented to the stakeholders and feedback was gathered and then incorporated into a second draft of the IT Risk Management Framework. The second draft of the framework was again presented to the stakeholders. Phase 3 was repeated until the framework reached an acceptable level as determined by the stakeholders.

Table 4.4 Phase 3 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))



Phase	Elements	Position
Phase of design-based research	*The elements that need to be completed*	Position in study
PHASE 3: Iterative cycles of testing and refinement of solutions in practice	First iteraction	First iteration starts with initial IT Risk Management Framework as drafted in previous phase.
	Particaipants	Senoir Managers from food manufacturing industry (CFO, Senoir IT Managers, Senior IT Technicians).
	Data collection	IT Risk Management Framework tested for acceptance.
	Data analysis	Analysis and interpretation of data.
	Implementation of intervention	Second draft of the IT Risk Management Framework.
	Second and further iterations Particaipants Data collection Data analysis	Second iteration starts with the second draft of IT Risk Management Framework from previous iteration. Refinement of the artefact continues until scceptable level is reached.

4.4.4 Phase 4

According to Herrington et al. (2017) cited by Delport (n.d., p53), the goal of Phase 4 was to “reflect on core aspects of produced artefact and enhance solution implementation”. Phase 4, as shown in Table 4.5, emphasises three elements. Firstly, the refined framework from Phase 3 was compared with the identified core aspects of Phase 2 (relevancy, usability, scalability, and simplicity). Secondly, it was determined if the framework complied with these core aspects. Lastly, after finalization, the framework was published, with the aim of assisting enterprises within the food manufacturing industry in South Africa with the implementation of an effective IT Risk Management Framework.

Table 4.5 Phase 4 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**	**Position**
Phase of design-based research	*The elements that need to be completed*	Position in study
PHASE 4: Reflection ion core aspects of produced artefact and enhanced solution implementation	Core Aspects	To ensure that IT Risk Management Framework complies with identified core aspects from Phase 2 (relevancy, usability, scalability, and simplicity)
	Designed artefact(s)	Finalisation of the framework.
	Professional development	Make available (Diffuse) to enterprises within food manufacturing industry as far as possible and publish solution.

The above 4 phases were considered when developing the artefact. Each phase was completed in full before moving to the next phase until the final artefact was established.

4.5 Research Methods

As per Osterle et al. (2010) cited by Delport (n.d., p53), researchers are, “free to decide on research objectives and research methods to use”. A mixed-method approach was followed in this study. According to Johnson (2019) mixed-method researchfocuses on research questions that call for real-life contextual understandings, employs rigorous quantitative and qualitative research, involves multiple sources and types of data, systematically integrates and triangulates different types of data to maximize the strengths and counterbalance the weaknesses of each data type and, develops and integrates conceptual and theoretical frameworks into the development of research questions. Table 4.6 defines and describes several methods that were used in each phase in this study.

Table 4.6 Research methods definitions and descriptions (Source: Delport (NMU))

Research Methods	Phase of Process	Definition
Literature Review	Phase 1 & 2	An iterative process of obtaining information sources relevant to one's study (Olivier, 2009)
Semi-structured interview	Phase 1	A verbal interchange where the interviewer attemps to elicit information from another person by asking questions. Although there is a set of predetermined questions, this interview is conversational in nature and allows participants to explore issues they feel are important (Longhurst, 2003).
Modelling	Phase 2 & 3	A model captures the essential aspects of a system or process, while it ignores the non-essential aspects and can serve as a blueprint for a new systems or processes (Oliver, 2009).
Focus group	Phase 3	Involves a group of people who meet in an informal setting to talk about a topic set by the researcher and allows the group to explore the subject from as many angles as they please (Longhurst, 2003).
Questionnaire	Phase 4	An instrument consisting of a series of questions and/or attitude / opinion statement designed to elicit responses which can be converted into measeres of the variable under investigation (Franklin & Osborne, 1971).

Phase 1 was based on a literature review in order to formulate the initial problem statement as well as the objectives of the research. After the initial problem statement had been developed, semi-structured interviews were conducted with relevant stakeholders within the food manufacturing industry, to better understand the problem at hand.

Phase 2 was based on what was learned from the previous phase and core aspects were identified which formed the basis of an effective IT Risk Management Framework for enterprises within the food manufacturing industry in South Africa. Furthermore, the IT Risk Management Framework was developed from the initially identified core aspects in Phase 2 using a process called modelling techniques. After that, the IT Risk Management Framework was presented to stakeholders within the food manufacturing industry.

In Phase 3, a focus group approach was used to determine if the draft IT Risk Management Framework was acceptable. The results from the focus groups were examined, taking the feedback into consideration, and changes were made to the draft framework. The process was continued until the framework was accepted and this was considered to be the final IT Risk Management Framework. In Phase 4, the final IT Risk Management Framework was evaluated using the core aspects discussed in Phase 2. The overall research method that was used, formed part of the mixed-method approach for this study.

4.6 Conclusion

Throughout the study, with the real-world problem at hand, the NMU-DSFM was followed in order to provide a research contribution. As already mentioned, the NMU-DSFM was incorporated with the four phases to address the real-world problem at hand in order to create a designed artificial artefact in the form of a framework. As mentioned in Section 4.5, as per the statement of Osterle et al. (2010) cited by Delport (n.d., p53), researchers are “free to decide on research objectives and research methods to use”. Indeed, a mixed-method research approach was followed in addressing the problem at hand. Furthermore, as already mentioned, the main objective of the study was to guide enterprises within the food manufacturing industry in South Africa with the implementation of a sound IT Risk Management Framework. The NMU-DSFM was followed in order to achieve the study objectives.

Chapter 5
Results and discussion

5.1 Introduction

As discussed in Chapter 4, the NMU-DSFM was followed in order to develop an IT Risk Management Framework for enterprises within the food manufacturing industry in South Africa. The NMU-DSFM consists of four consecutive phases (Figure 5.1), each with various objects that must be completed before moving to the next phase. Chapter 5 provides a detailed consideration of the first three phases (Phase 1 – Analysis, Phase 2 – Development and Phase 3 – Refinement) in relation to the development of the framework. Phase 4 (Reflection)is discussed in Chapter 6.

Discussion of Phase 1 will focus on how the Problem Statement was formulated. Phase 2 discussion will cover identification of the core aspects that were necessary for establishing the framework. Refinement of the framework through successive iterations will form the substance of the Phase 3 discussion, which will be followed by consideration of the final refined IT Risk Management Framework.

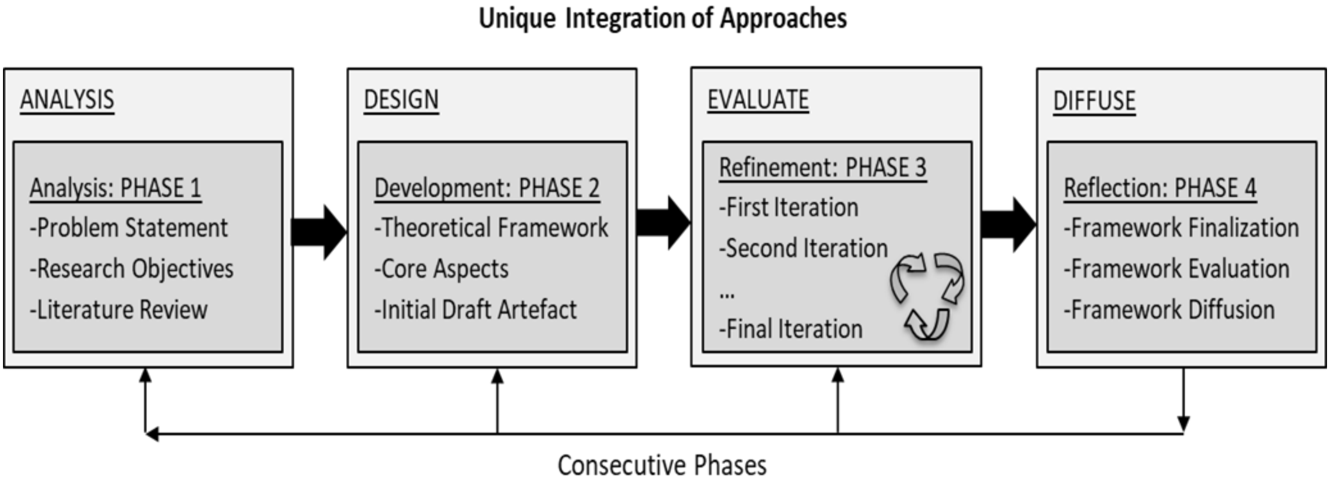


Figure 5.1 Unique Integration Approaches (Source: NMU-DSFM)

5.2 Phase 1 – Analysis

As shown in Table 5.1, the creation of the artificial artefact started with Phase 1 of the NMU-DSFM. Phase 1 focused on the analysis of the problem at hand.

Table 5. 1 Phase 1 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**
Phase of design-based research	*The elements that need to be completed*
PHASE 1: Analysis of practical problems by researchers and stakeholders in collaboration	Statement of problem
	Consultation with researches and stakeholders
	Research Review
	Literature Review

Enterprises within the food manufacturing industry in South Africa are facing IT-related challenges. Preliminary investigations of these enterprises revealed some negative issues related to IT governance, including:

Absence of documented IT policies and strategies;

Redundant IT infrastructure;

Disaster Recovery Plan not tested (no evidence);

IT Risk Assessment not conducted;

No IT training and awareness programs.

A recent incident involving a food manufacturing enterprise where customer information was obtained by hackers who gained unauthorised access to the system illustrates how these negative issues related to IT governance are impacting the food manufacturing industry. Enterprises within the food manufacturing industry appear to be lagging behind in relation to the implementation of effective IT governance.

Lack of IT governance (as per the report) is reflected in key areas such as poor user access management controls, poor physical access controls and poor security controls. It was found that employees are using one password to access the ERP system and access levels are not defined, backup tapes are not taken regularly, and firewall SLA is not renewed in time with the service provider resulting in outdated system protection measures. Furthermore, it was noted that most networked computers did not have active antivirus software. Based on these preliminary observations, an initial study problem statement was constructed, fulfilling a requirement of Phase 1 of the framework development process (Figure 5.1). Subsequently, a stakeholder was identified and engaged as the primary collaborator for this research study, thus enabling consultation about how the initial problem statement could be addressed.

The stakeholder and primary collaborator for this study was Sovereign Foods (Pty) Ltd (Sovfoods), an enterprise in the food manufacturing industry that produces and processes chicken products. The Sovfoods senior management was visited on the 15th of February 2019. During this visit, semi-structured interviews (Appendix A.1) were conducted with various members of the enterprise, including IT Management, Risk, Business Intelligence, and Internal Auditing. During the interview sessions and from reviews of internal audit reports, it was noticed that IT governance policies and frameworks did not exist.

Based on these observations, and taking all the preliminary information into consideration, a final problem statement was formulated. To address the formulated problem, research objectives for the study were set (as discussed in Chapter 1). One of these objectives was to conduct a comprehensive literature review (as documented in Chapters 2 and 3 respectively). After a review of the literature, it was easy to understand the challenges facing enterprises within the food manufacturing industry and their needs. Phase 1 ended once each element had been addressed in relation to resolving the problem at hand.

5.3 Phase 2 – Development

Phase 2 focused on the development of the draft core aspects to guide the design of the intervention (Table 5.2).

Table 5.2 Phase 2 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**
Phase of design-based research	*The elements that need to be completed*
PHASE 2: Development of solutions informed by existing core aspects and technological innovations	Theoretical framework
	Development of draft core aspect to guide the design of the intervention
	Description of proposed intervention

The Phase 1 literature review process was continued with the objective of identifying the core aspects required for Phase 2. Four core aspects needed to guide the design of the IT Risk Management Framework were identified as relevancy, usability, scalability, and simplicity. In addition, as per the requirements of Phase 2, criteria on which to base the IT Risk Management Framework were identified. In this regard, three criteria were identified from the literature, namely Risk governance, Risk evaluation and Risk response (Figure 5.2).

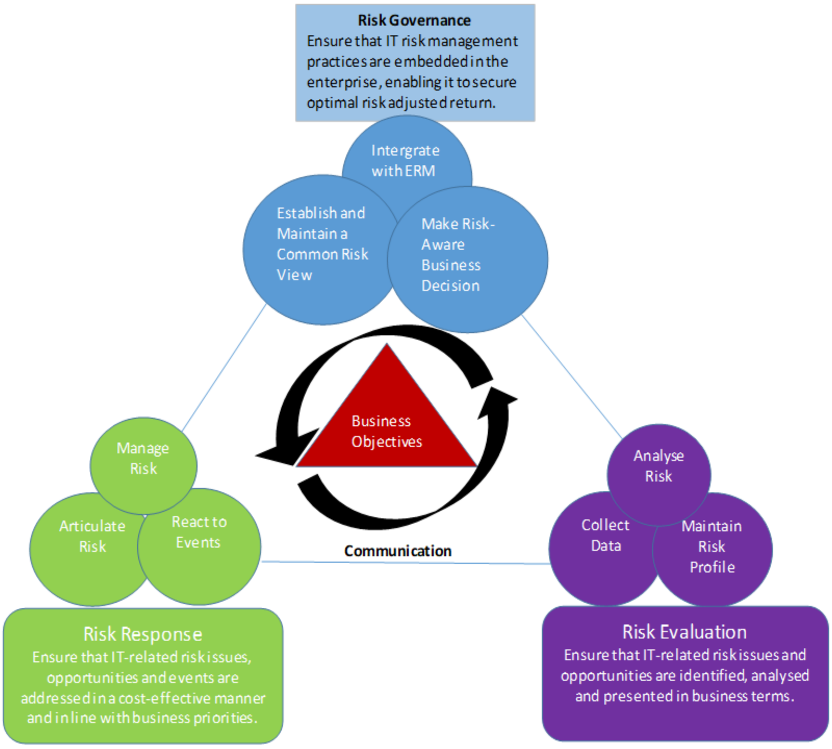

Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk adjusted return.
Intergrate with ERM
Establish and Maintain a Common Risk View
Make Risk-Aware Business Decision
Business Objectives
Manage Risk
Articulate Risk
React to Events
Analyse Risk
Collect Data
Maintain Risk Profile
Communication
Risk Response
Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Risk Evaluation
Ensure that IT-related risk issues and opportunities are identified, analysed and presented in business terms.

Figure 5.2 Criteria (Risk IT Framework: ISACA 2009)

5.3.1 Risk Governance (Criterion 1)

Risk governance (Figure 5.2) should ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. As discussed in the literature review, governance is the process through which an enterprise is directed and controlled. An IT Risk Management Framework has an important role to play in guiding, directing and controlling an enterprise to ensure that risk-aware decisions are made. For this to be possible, IT risk strategies should be integrated with the enterprise's risk management (ERM). Also, it is important for an enterprise to establish and maintain a common risk view.

Furthermore, as referenced in the literature and cited by ITGI (2003, p13), "governance of IT is an important part of the enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives". Therefore, Criterion 1 (risk governance) should play a significant role in the design of the IT Risk Management Framework.

5.3.2 Risk Evaluation (Criterion 2)

ISACA (2009) cited by Mozsár & Michelberger (2019, p115) define risk evaluation (Figure 5.2) as the process that “ensures IT-related risks and opportunities are identified, analysed and presented in business terms”. Implementing risk evaluation would, therefore, ensure that an enterprise collects relevant data, and maintains a risk profile. As per the NIST (2011) publication, in agreement with Calder, the purpose of the risk evaluation is to identify:

Threats to the enterprise (i.e. operations, assets, or individuals) or threats directed through the enterprise against other enterprises;

Vulnerabilities internal and external to the enterprise;

The harm (i.e. consequences/impact) to the enterprise that may occur given the potential for threats exploiting vulnerabilities, and

The likelihood that harm will occur.

The process of risk evaluation is important to ensure that enterprises within the food manufacturing industry focus on what matters so as to prioritise risk responses and eliminate waste in the process. Therefore, the second criterion (as shown in Figure 5.2) which is risk evaluation was incorporated into the design of the IT Risk Management Framework.

5.3.3 Risk Response (Criterion 3)

Risk response (Figure 5.2) is the third criterion that should be incorporated into an IT Risk Management Framework. Effective risk response would ensure that IT-related risk issues, opportunities, and events were addressed in a cost-effective manner and in line with business priorities. When considering risk response, there are strategic options that should be taken into account, namely: risk acceptance, risk mitigation, risk avoidance, and risk transfer (as discussed Sections 3.6.3.1, 3.6.3.2, 3.6.3.3, and 3.6.3.4 of the literature review). Therefore, risk response criteria were taken into account when designing the IT Risk Management Framework. This will be discussed in detail as part of the contextualisation phase.

5.4 Phase 3 – Refinement

Once Phase 1 and Phase 2 had been completed, it was necessary to refine the artefact as required in Phase 3 (Table 5.3). Applying the Phase 3refinement iterations process, yielded a final version of the IT Risk Management Framework. The refinement iterations process involved participation from the stakeholders, data collection, data analysis, and implementation of the intervention.

Table 5.3 Phase 3 (Source: Adapted from Herrington, McKenney, Reeves and Oliver (2007) by Delport (n.d.))

Phase	**Elements**
Phase of design-based research	*The elements that need to be completed*
PHASE 3: Iterative cycles of testing and refinement of solutions in practice	Implementation of intervention (First iteraction)
	Participants
	Data collection
	Data analysis
	Implementation of intervention
	Second and further iterations
	Participants
	Data collection
	Data analysis

5.4.1 Refinement Iteration 1

The draft artefact, created during Phase 2, was used as the input for the first refinement iteration. The draft IT Risk Management Framework was presented to stakeholders on 01 July 2019 in a focus group session. The stakeholders in the focus group were, amongst others, IT managers, IT technicians, Risk managers, Business Intelligence personnel, and Information managers. The draft artificial artefact, the IT Risk Management Framework, was deliberated broadly.

Although the structure and design of the framework were accepted, stakeholders pointed out that the four phases of risk management needed to be further defined to give clarity on how to perform each of them. The outcome of the stakeholder focus group gathering was the refinement of the initial artificial artefact from Phase 2.

5.4.2 Refinement Iteration 2

The result of the first iteration was used as the input to the second refinement iteration. The process for the second refinement was undertaken on 24 July 2019, in the form of another contact group session, attended by the same members who attended the first iteration session. The refined artefact as per the suggestions of the first iteration was presented to stakeholders for further discussion and comments.

After thorough discussion, the second refinement of the artefact was accepted. However, the IT Manager suggested that the CEO and CFO should be part of the engagement since the IT Manager was not a representative of the Board. The verdict was that the refined iteration be sent to the CEO and CFO for comment, along with the first draft of the artefact. These artefacts were sent to the CEO and CFO on the same day (24 July 2019).

Comments from the CEO and CFO were received on 01 August 2019. The CEO and CFO were happy with the second refined iteration and did not make any changes nor add any comments. They acknowledged and were happy that all the relevant stakeholders had taken part in the refinement of the iteration. The second refined iteration was accepted without any further changes.

5.5 Finalised IT Risk Management Framework

As per the first three phases of the NMU-DSFM that have been discussed in Sections 5.2, 5.3 and 5.4, respectively, a final IT Risk Management Framework for enterprises within the food manufacturing industry in South Africa was established. This final artefact in the form of the IT Risk Management Framework will be discussed in a general sense, and then it will be contextualized within the food manufacturing enterprises in South Africa.

5.5.1 General Framework Discussion

As referred to in Section 5.3 (Phase 2), the establishment of this framework for enterprises within the food manufacturing industry in South Africa is based on three criteria. These criteria are as follows:

Risk governance;

Risk evaluation;

Risk response.

These criteria are clearly defined in the literature review in Chapter 3 and are represented in Figure 5.2. As seen in Figure 5.2, these criteria form the three points of a triangle. Risk governance is shown at the top, due to the fact that governance is the top management responsibility. Risk evaluation and risk response are fundamental components on which IT risk should be based. The three criteria combined together form the general components of the IT Risk Management Framework.

These three criteria form the basis for ensuring that the problem at hand, as per the Problem Statement, is resolved and that enterprises within the food manufacturing industry achieve their objectives. As stated in Chapter 1, the key objective of this study was to establish a framework that will ensure that IT-related threats, vulnerabilities, and risks are properly managed and to ensure that enterprises within the sector are able to make appropriate risk aware-decisions, improving performance and ability to allow achievement of the enterprise's objectives. Therefore, having effective *risk governance*, effective *risk evaluation* processes, and effective *risk response* activities (as discussed in Sections 5.3.1, 5.3.2, and 5.3.3 respectively) will ensure that objectives of the enterprise are achieved.

5.5.2 Contextualisation of the Framework

As mentioned in Section 5.5.1, the three criteria combined together form the general components of the IT Risk Management Framework. However, in this study, the three criteria were developed further into four categories as per the phases of the risk management process. These phases were discussed in the literature review in Chapter 3 and are as follows:

IT risk identification;

IT risk assessment;

IT risk response and mitigation;

IT risk control monitoring and reporting.

In order to achieve effective IT risk management, enterprises within the food manufacturing industry in South Africa should address the above four phases accordingly when conducting IT risk management activities. These phases are contextualised further in more detail in the subsections below. Risk appetite, risk tolerance, key risk indicators, key performance indicators, and business impact analyses were also incorporated to resolve the problem at hand.

5.5.2.1 Information Technology Risk Identification

This is the first phase of the IT risk management process, “risk identification is the process for discovering, recognizing and documenting risks that an enterprise might be facing” (CRISC, 2015, p21). Risk identification allows enterprises within the food manufacturing industry to determine early the potential impact of internal and external threats on the entire IT environment, identifying major trends and their variation over time. The enterprises within the sector should start by identifying key risks that can negatively affect the achievement of objectives as defined in the IT strategic plan. Of course, when conducting risk identification activities, there are some factors that need to be taken into account. These factors are external and in some cases internal. These factors are grouped as follows:

External Factors

Political factors: Government intervention in economic issues;

Social factors: Socio-cultural factors involve the shared belief and attitudes of the population;

Economic factors: Including economic growth, interest rates, exchange rates and inflation;

Technological factors: Technological landscape changes;

Legal factors: A set of rules and regulations.

Internal Factors

Strategic objectives;

IT-related governance frameworks;

Policies and procedures;

Leadership style (ethics, values, and transparency);

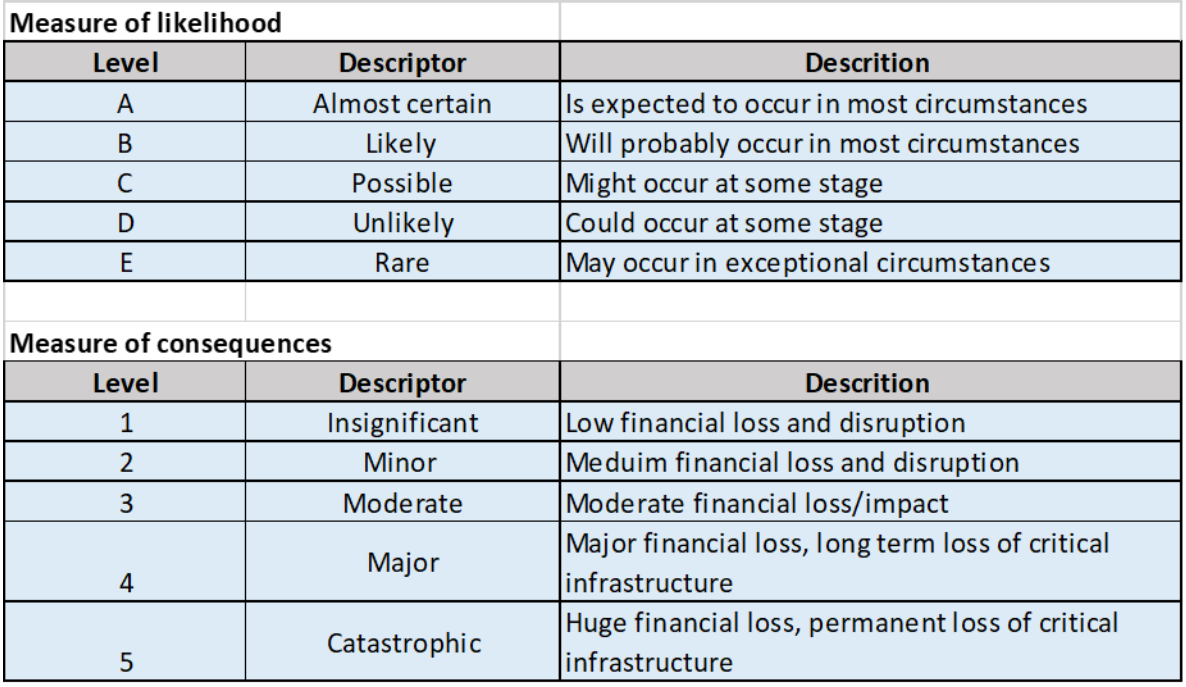
IT architecture and infrastructure.

As discussed above and stated in the literature review (Section 3.2), IT risk management consists of four components. For the process of risk management to be effective, risk identification should be completed first. Enterprises within the food manufacturing industry should conduct risk identification activities with due care to ensure accuracy of identified risks. Effective risk identification will ensure that further risk management components are as effective as possible, furthermore ensuring that the primary and secondary objectives of this study are achieved as they are stated in Chapter 1.

5.5.2.2 *Information Technology Risk Assessment*

After risks have been identified, the severity, thereof, to the enterprise should be assessed. The objective is to evaluate the risk that has been identified during the identification phase to determine its potential impact on the enterprise. Through this process, likelihood and consequences should be determined and risk should be rated depending on the severity. Criteria, as presented in Table 5.4, should be used in assessing the identified risks and should be developed and adopted in assigning the level of severity.

Table 5.4: Measure of likelihood and consequences



Measure of likelihood

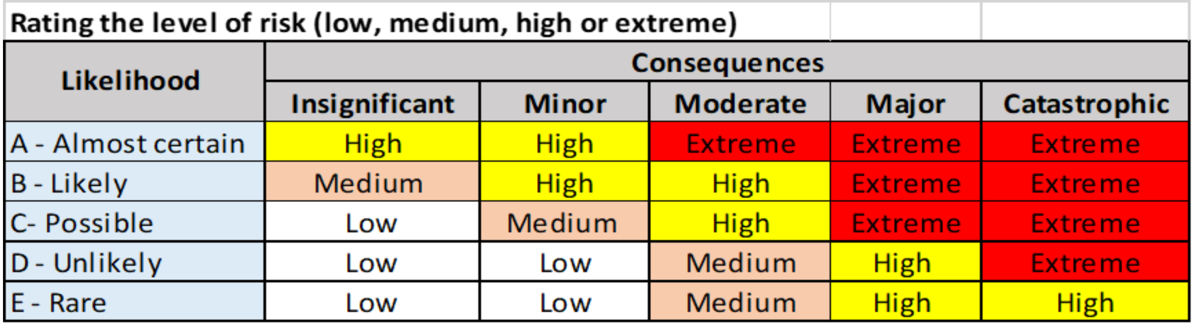
Level	Descriptor	Descrition
A	Almost certain	Is expected to occur in most circumstances
B	Likely	Will probably occur in most circumstances
C	Possible	Might occur at some stage
D	Unlikely	Could occur at some stage
E	Rare	May occur in exceptional circumstances

Measure of consequences

Level	Descriptor	Descrition
1	Insignificant	Low financial loss and disruption
2	Minor	Meduim financial loss and disruption
3	Moderate	Moderate financial loss/impact
4	Major	Major financial loss, long term loss of critical infrastructure
5	Catastrophic	Huge financial loss, permanent loss of critical infrastructure

After the likelihood and consequences have been developed when assessing the identified risk, a risk rating model aligned with the strategic objectives of the enterprise should be developed. The model presented in Table 5.5 should be used.

Table 5.5: Rating model



Rating the level of risk (low, medium, high or extreme)					
Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
A - Almost certain	High	High	Extreme	Extreme	Extreme
B - Likely	Medium	High	High	Extreme	Extreme
C- Possible	Low	Medium	High	Extreme	Extreme
D - Unlikely	Low	Low	Medium	High	Extreme
E - Rare	Low	Low	Medium	High	High

Therefore, as alluded to by ISO (2009, p17), “the enterprise should define its criteria to be used to evaluate the significance of risk”. ISO (2009) further states that the criteria should reflect the enterprise's values, objectives, and resources.

With reference to the rating model in Table 5.5, for enterprises within the food manufacturing industry where likelihood is ‘likely’ and consequence is ‘major coming to a rating of ‘**extreme**’, this would mean that drastic action must be taken to respond to the risk. Where likelihood is ‘rare’ and consequence is ‘minor’ coming to a rating of ‘low’, the enterprise could accept the risk and carry on with its operations.

5.5.2.3 Information Technology Risk Response and Mitigation

At this stage, after risks have been identified and evaluated, the enterprise will have an understanding of their current risk exposure. This is where management will be required to make decisions regarding the correct way to respond and to address the risk. This should be based on the information provided during IT risk identification and IT risk assessment, however, response activities should depend on the enterprise’s resources, budget, and strategic plans. The purpose is to ensure that risks identified are treated accordingly, in line with the risk appetite and risk tolerance of the enterprise. When performing response activities, there are four options to choose from namely: risk acceptance, risk mitigation, risk avoidance, and risk transfer

As per Prasetyo and Sucahyo (2014, p100), “risk acceptance is the decision to accept the risk and the responsibility for the decisions taken in managing these risks”. With this statement in mind, enterprises within the food manufacturing industry need to make appropriate risk aware decisions about how to respond to identified risks.

As alluded to earlier, the effectiveness of response options depends exclusively on the effectiveness of the first two phases (risk identification and risk assessment). CRISC (2015), furthermore state that the choice to accept the risk is a mindful judgment made by senior management to recognize the existence of the risk and expressly decide to allow the risk to remain without being treated.

Risk Acceptance: “Risk acceptance is a senior management decision, where risk acknowledgment is made and knowingly decide to allow the risk to remain without mitigation” (CRISC, 2015, p116). Risk acceptance takes place when the risk meets the risk acceptance criteria, and there is no need for implementing additional controls, therefore the risk can be retained. For example, any potential losses from a risk not covered by insurance or over the insured amount would be an example of risk acceptance, or when the benefits accompanying the risk are very attractive therefore accepting the risk.

As mentioned, is Chapter 3, the responsibility rests with management should a risk event occur. This means that enterprises within the food manufacturing industry should be vigilant and management should understand business processes very well before accepting the risk. This will ensure that consequences do not negatively affect the enterprise. Furthermore, enterprises within the sector will ensure that IT-related threats, vulnerabilities, and risks are easily managed.

Risk Mitigation: Risk mitigation means that action should be taken to reduce the frequency and impact of risk. This should be performed through several controls until the level of risk is within the acceptable level and tolerable level. When implementing risk mitigation activities, the enterprise should consider the return on investment associated with the reduction of risk and furthermore the potential to exploit new business opportunities afforded by the control for example, establishing standards to guide business practices and decision making (Policies, Performance Management, and Contingency Plans).

As per Gonen (2011, p969), risk mitigation “refers to action taken to reduce either the probability of occurrence of an unfavourable event or the impact of this event”. This means that enterprises within the food manufacturing industry need to take effective action in risk mitigation to ensure that the frequency of happenings, and impact thereof, is reduced. Gonen (2011, p969), also states that “risk mitigation is usually executed in the form of a plan designed to handle high-threat possible events”. Therefore, enterprises within the food manufacturing industry should develop strategies on how to eliminate the identified risk, as noted above.

Risk Avoidance: Risk avoidance should apply when no other risk response is adequate. This occurs when management decides to exit activities that give rise to the risk for example, stopping the processing of customer information on a particular system due to a number of security breaches without mitigation, and opting out for a new innovative system. As per Wijanarka (2014), risk avoidance can be applied when there is no appropriate response action. This will only happen where management within the food manufacturing industry exhausts their options in mitigating the identified risk. The option would be to opt out and stop engaging with processes that relate to the identified risk.

Risk Transfer: This occurs when senior management decides to share the risk of loss with another organization. This is normally done through the use of contracts, insurance, disclaimers, and/or releases of claims to transfer the liability for the expected loss to other parties involved. According to Wijanarka (2014), the risk transfer option occurs when organisations reduce the risk likelihood or impact by transferring the risk to, or sharing the risk with, other parties. For enterprises within the food manufacturing industry to minimise losses, some interventions need to take place. Should a loss occur and the enterprise is of a view that they cannot cover all the costs, risk of loss should be shared with other institutions.

IT Risk Control Monitoring and Reporting: As far as the lifecycle of risk management is concerned, once a risk has been identified, evaluated, and responded to, enterprises should develop risk control monitoring and reporting activities. Therefore, owing to the changing nature of risk and associated controls, ongoing risk monitoring controls should be taken into account during this phase. This is because controls implemented during the response and mitigation phase can become less effective, the operational environment may change, and new threats, technologies, and vulnerabilities may emerge, putting the enterprise at risk.

As mentioned by CRISC (2015, p160), the objective of risk monitoring and evaluation is to "collect, validate, evaluate the business, IT and process goals and metrics; to monitor that processes are performing against agreed-on performance and conformance goals and metrics, and provide reporting that is systemic and timely". After all the three phases have been completed, enterprises within the food manufacturing industry need to establish monitoring and reporting activities. This can be achieved by implementing regular review activities and ongoing reporting e.g. through the use of Key Risk Indicators (KRI) and Key Performance Indicators (KPI). Risk management is a repeated systematic process.

As mentioned by Wijanarka (2014, Monitoring and Review section), "monitoring and review process should be carried out regularly during IT Risk Management". Enterprises within the sector of food manufacturing need to perform risk management on an ongoing basis. Wijanarka (2014) further states that the main objective of monitoring and review in risk management is to:

Obtain more information to improve skills in the management of risk;

Learn from the success or failure of risk management that has occurred;

Detect changes in risk criteria;

Identify new risks, which have not been defined in the earlier process.

5.6 Key Risk Indicators

To achieve effective risk management, as considered in Chapter 3 and further discussed in this chapter, it is important to incorporate relevant metrics to ensure effective control, monitoring and reporting. By doing so, enterprises within the food manufacturing industry should use KRI to achieve this. As mentioned in the literature, Scarlat, et al. (2011) are adamant that KRI is an important tool for effective IT risk management to ensure that threats, vulnerabilities, and risks are mitigated accordingly, as the enterprise becomes aware of them.

Key risk indicators are important in the sense that specific risks can be monitored so that mitigation actions can be undertaken as soon as the risk arises. To achieve the best results from the risk management process, resolve the problem at hand, and achieve the benefits of having effective IT risk management, KRI needs to be incorporated in the process of IT risk management.

5.7 Key Performance Indicators

To ensure continual improvements, that objectives are achieved as intended, and that the problem at hand is resolved, KPI play a crucial role in monitoring activities. Key performance indicators can be used to evaluate the success of an organization or of a particular activity in which it engages.

As per CRISC (2015, p153), KPI "is a measurable value that demonstrates how effectively a company is achieving key business objectives". Through the use of KPI, enterprises within the food manufacturing industry can measure their success in relation to having effective IT risk management. This will allow enterprises within the sector to make risk aware decisions regarding IT-related threats, vulnerabilities, and risk as encapsulated in the secondary objectives of this study. Therefore, KPI should be incorporated for the purpose of resolving the problem at hand.

5.8 Risk Appetite

Furthermore, risk appetite is as important as KRI and KPI. As mentioned in Chapter 3, CRISC (2015, p54) defines risk appetite as, “an amount of risk that an enterprise is willing to accept”. CIRSC (2015, p54) further states that, “risk appetite should be defined and approved by senior management and clearly communicated to all stakeholders, and a process should be in place to review and approve any exceptions”. An enterprise within the food manufacturing industry should define its own risk appetite as this will allow it to achieve benefits as stated in Section 3.5 of the literature review. CRISC (2015) alludes to the fact that having effective IT risk management will yield some benefits to enterprises. These benefits are stated as:

Better oversight of enterprise assets;

Minimized losses;

Identification of threats, vulnerabilities, and risks;

Prioritization of risk response efforts;

Legal and regulatory compliance;

Increased likelihood of project success;

Improved information security;

Improved performance and the ability to attain enterprise goals;

Better monitoring and reporting.

Therefore, defining risk appetite will enable enterprises in the sector to obtain these benefits, achieving the primary and secondary objectives of this study and moreover resolving the problem at hand as per the problem statement.

5.9 Risk Tolerance

As far as defining risk appetite, enterprises within the sector need to understand what their risk tolerance is. As per CRISC (2015, p54), risk tolerance “is an acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives”. Nicholson et al. (2005, p467) cited by Lucarelli, Uberti and Brighetti (2015) state that, “risk propensity affects judgment and decision making in many different domains which renders it complex to define and to measure”.

These authors further allude that risk tolerance is the other important part of risk management, more particularly in decision making with regard to risk, hence it is pivotal to have such tools (key risk indicators, key performance indicators, risk appetite and risk tolerance) in the governance of IT. Therefore, from the statements above, it is clear that risk tolerance, in relation to key risk indicators, key performance indicators and risk appetite, is fundamental to ensuring that the problem at hand is resolved.

5.10 Business Impact Analyses

As alluded to in this study and noted by Radeschütz et al. (2015, p69), Business Impact Analysis (BIA) “foresees the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies”. Business impact analysis is critical in the sense that IT-related threats, vulnerabilities, and risks within enterprises in the sector will be closely monitored through evaluating the potential effects of an interruption to IT infrastructure.

Furthermore, Radeschütz et al. (2015, p69) are of the view that BIA is a vital part of risk management in order for enterprises to achieve their IT-related objectives, and in general. These authors also state that “increasing competition and significantly shortened product lifecycles led to a situation where fast adaption and continuous optimization of business processes are critical factors in determining the success of a company”. Therefore, to ensure that the problem at hand is resolved, BIA, along with the other tools mentioned above should be implemented within IT governance activities of enterprises in the sector.

5.11 Conclusion

As stated in Chapter 4, a unique integrated research approach was formulated for this study by following the NMU-DSFM. By following an integrated research approach, the objective was to discuss the creation of the research contribution. As an outcome, an artificial artefact in the form of a framework was established. The framework was named the IT Risk Management Framework for Enterprises within the Food Manufacturing Industry. As stated, and illustrated in Figure 5.1, only the first three phases were discussed in Chapter 5. The fourth phase will be discussed in Chapter 6.

Chapter 6 will consider Phase 4, which relates to the validation of the framework against the initially identified core aspects (relevancy, usability, scalability, and simplicity). Chapter 6 will, therefore, present the validation of the final IT Risk Management Framework.

CHAPTER 6
FRAMEWORK validation

6.1 Introduction

At this stage, it is clear that the final IT Risk Management Framework for enterprises within the food manufacturing industry has been developed. As mentioned in Chapter 5, the final framework consists of four categories as per the phases of risk management. The framework was constructed using the first three phases (Phase 1, 2, and 3) of the unique integrated research approach as per the NMU-DSFM (Figure 6.1). However, this research approach requires that a fourth and final phase be completed, consequently, Phase 4 (Figure 6.1) will be considered in this chapter.

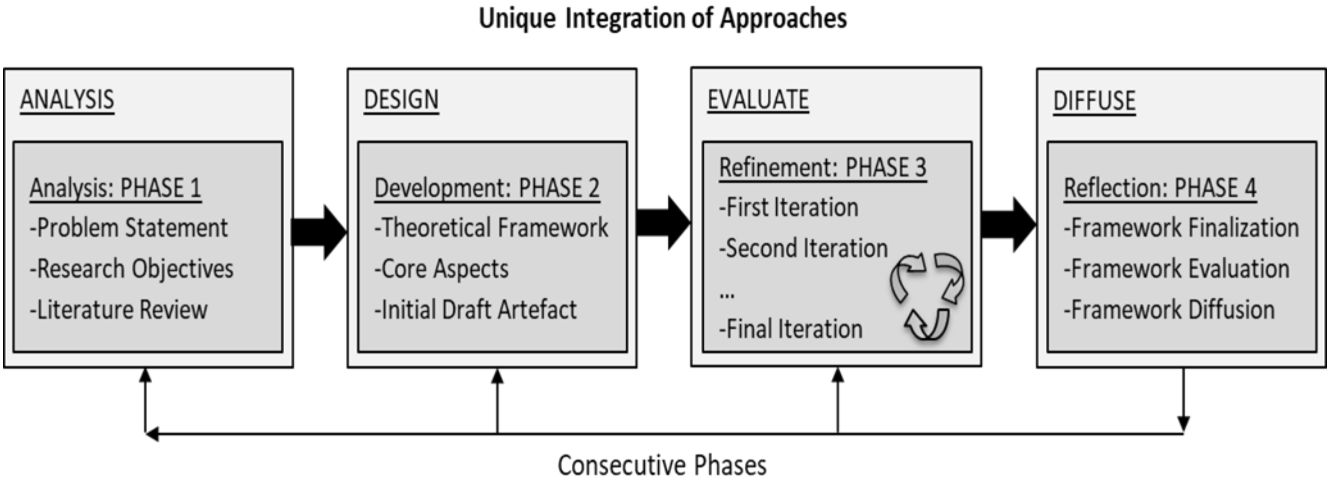


Figure 6.1 Unique Integration Approaches (Source: NMU-DSFM)

Phase 4 is a validation phase required by the integrated research approach. Therefore, Phase 4 will confirm and validate whether or not the IT Risk Management Framework conforms to the core aspects of relevancy, usability, scalability, and simplicity referred to in Chapter 4. Furthermore, the method by which data was analysed will also be discussed.

6.2 Data Collection

A workshop was used to validate the IT Risk Management Framework. This workshop was held on 08 May 2019, with a total of 12 stakeholders represented. These stakeholders primarily came from Sovereign Foods Ltd (an enterprise within the food manufacturing industry). Amongst the stakeholders that attended the workshop were personnel from the IT, Risk Management, Business Intelligence, Internal Audit, and Information Management departments. The workshop was presented in two sessions; the first two hours was for a theoretical background presentation which provided necessary background information regarding the IT Risk Management Framework. The second session was mainly focussed on the phases of the IT Risk Management Framework and other relevant subtopics.

After the two sessions were over, a survey in the form of a questionnaire was completed by the 12 stakeholders that attended the workshop. The survey consisted of five statements that were developed by the researcher. The response to each statement had to be indicated on a Likert scale whether “strongly disagree”, “disagree”, “agree”, or “strongly agree” with the statement. This approach was to test the IT Risk Management Framework’s ability to conform to the identified core aspects of *relevancy, usability*, *scalability, and simplicity*. Table 6.1 illustrates the mapping of the core aspects of the contexts of the five questions in addition, three sets of open-ended questions were presented to the stakeholders. The objective of these questions was to determine if there was anything lacking in the theoretical framework presented and whether there were any improvements needed. The full questionnaire has been included as Appendix A.1.

An analysis of collected responses from the questionnaires was completed. The main reason was to show that the IT Risk Management Framework conforms to the core aspects.

Table 6.1 Questionnaire (Attached to Appendix A.2)

Core aspects	Question	Statement
Relevancy	3	Framework have covered comprehensively the components of IT risk management
	5	Framework can be used to cover the minimum basis as required by risk management phases.
Usability	1	Framework can be used as guideline for implementation of IT risk management in food manufacturing industry.
Scalability	4	Framework can be equally implemented in both large and small enterprises within the industry.
Simplicity	2	A person with limited information technology know how would be able to complete the requirements of the framework successfully.

6.3 Data Analysis

The results for each core aspect are discussed below in relation to the questionnaire responses.

6.3.1 Core Aspect of Relevancy

As discussed in Chapter 4, relevancy is very crucial when developing an artificial artefact. In this study, the core aspect of relevancy was focused upon and anything that did not relate to food manufacturing enterprises was excluded. By doing this, the core aspect of relevancy was incorporated into the IT Risk Management Framework.

Questions 3 and 5, as shown in Table 6.1, were presented to the stakeholders. The responses showed that stakeholders felt that the core aspect of relevancy was incorporated adequately. Figure 6.2 represents the results pertaining to the core aspect of relevancy.

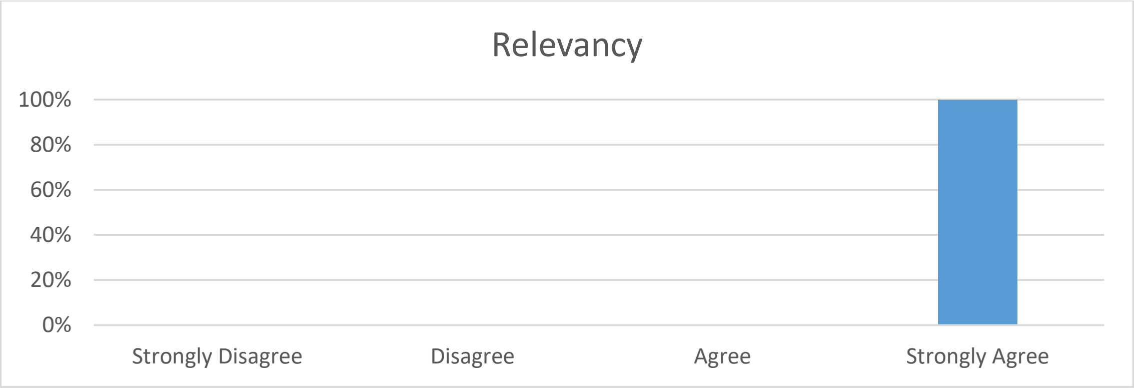


Figure 6.2 Core Aspect of Relevancy

As seen in Figure 6.2, 100% of the stakeholders strongly agreed with the IT Risk Management Framework's ability to conform to the core aspect of relevancy. Therefore, it can be concluded that the core aspect of relevancy has been successfully incorporated in the IT Risk Management Framework.

6.3.2 Core Aspect of Usability

Usability is fundamental to ensuring that the established artificial artefact is effective. In this regard, the core aspect of usability, as discussed in Chapter 4, was validated. The objective was to ensure that the IT Risk Management Framework is able to guide stakeholders on matters related to IT risk management.

Question 1, as shown in Table 6.1, was presented to the stakeholders. Responses to Question 1 indicated that the stakeholders felt that the core aspect of usability was incorporated adequately. Figure 6.3 represents the results pertaining to the core aspect of usability.

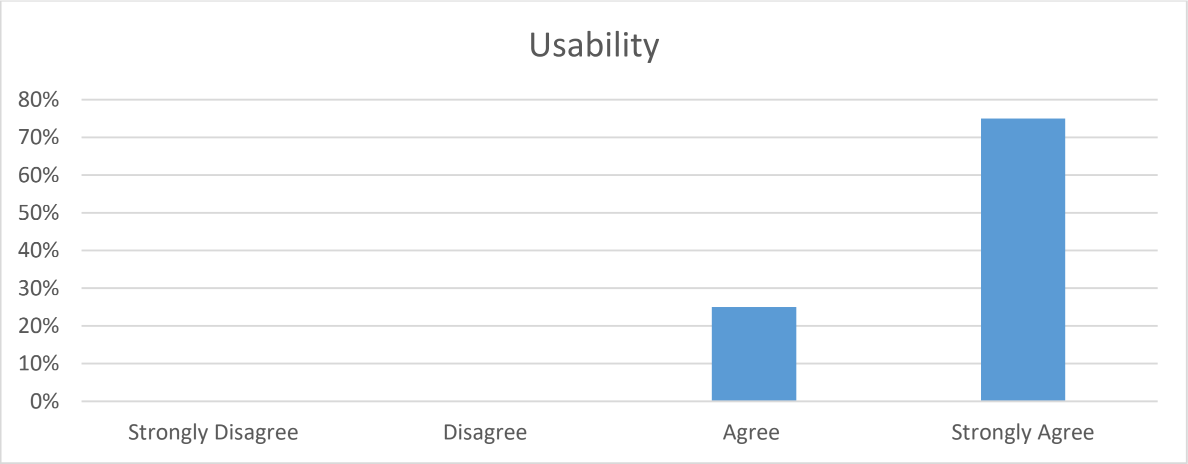


Figure 6.3 Core Aspect of Usability

As seen in Figure 6.3, 25% of the stakeholders agreed and 75% strongly agreed with the IT Risk Management Framework's ability to conform to the core aspect of usability. Therefore, it can be concluded that the core aspect of usability has been successfully incorporated into the IT Risk Management Framework.

6.3.3 Core Aspect of Scalability

Scalability is the third core aspect of the integrated research approach. This needs to be validated when following the integrated research approach to create an artificial artefact. This core aspect is pivotal to the success of the IT Risk Management Framework as it ensures that the IT Risk Management Framework can be scaled to fit the operating environment of enterprises within the food manufacturing industry.

Question 4, as shown in Table 6.1, was presented to the stakeholders. Responses to Question 4 indicate that the stakeholders felt that the core aspect of scalability was incorporated adequately. Figure 6.4 represents the results pertaining to the core aspect of scalability.

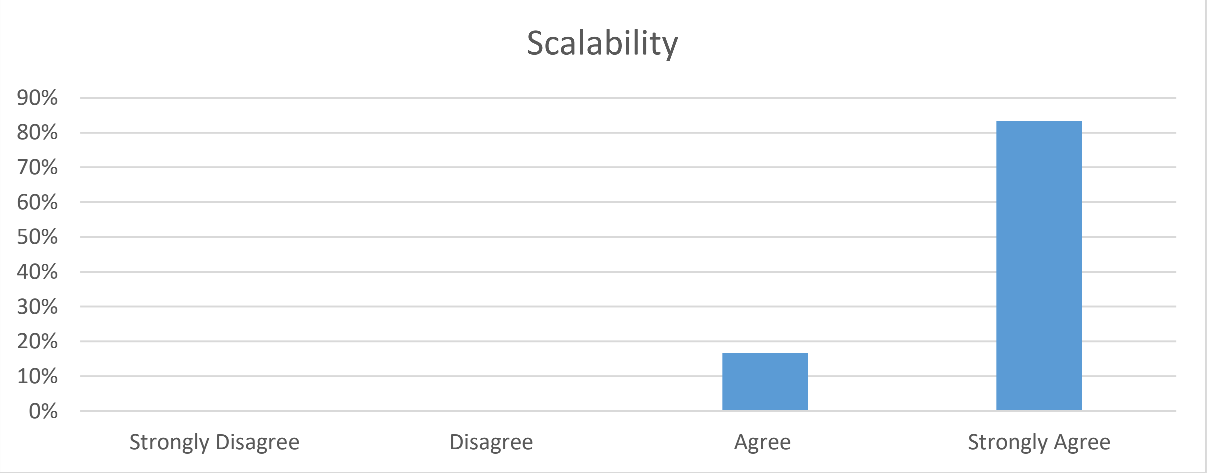


Figure 6.4 Core Aspect of Scalability

As seen in Figure 6.4, 17% of the stakeholders agreed and 83% strongly agreed with the IT Risk Management Framework's ability to conform to the core aspect of scalability. Therefore, it can be concluded that the core aspect of scalability has been successfully incorporated in the IT Risk Management Framework.

6.3.4 Core Aspect of Simplicity

Simplicity is the final core aspect to be validated. This core aspect is needed to ensure that the IT Risk Management Framework is user-friendly, easily understood and can be implemented in a simplistic but organised way.

Question 2, as shown in Table 6.1, was presented to the stakeholders. Responses to Question 2 indicated that the stakeholders felt that the core aspect of simplicity was incorporated adequately. Figure 6.5 represents the results pertaining to the core aspect of simplicity.

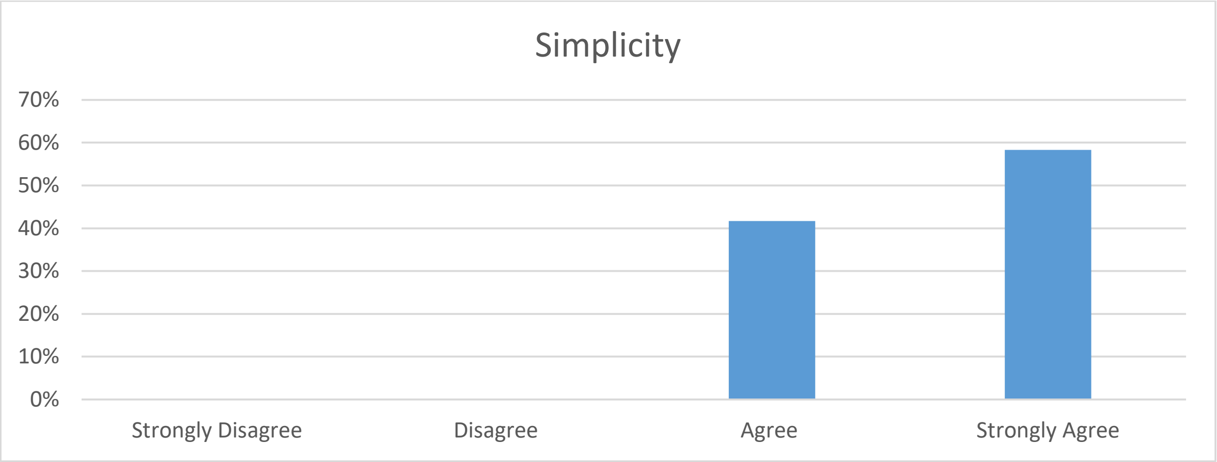


Figure 6.5 Core Aspect of Simplicity

As seen in Figure 6.5, 42% of the stakeholders agreed and 58% strongly agreed with the IT Risk Management Framework's ability to conform to the core aspect of simplicity. Therefore, it can be concluded that the core aspect of simplicity has been successfully incorporated in the IT Risk Management Framework.

6.4 Findings

All four core aspects were validated individually. Figure 6.6 represents a summary of the results of the five Likert scale questions in the questionnaire. All four core aspect, as indicated by the stakeholder's responses (agree and strongly agree) were incorporated successfully indicating that the IT Risk Management Framework conforms to all four core aspects.

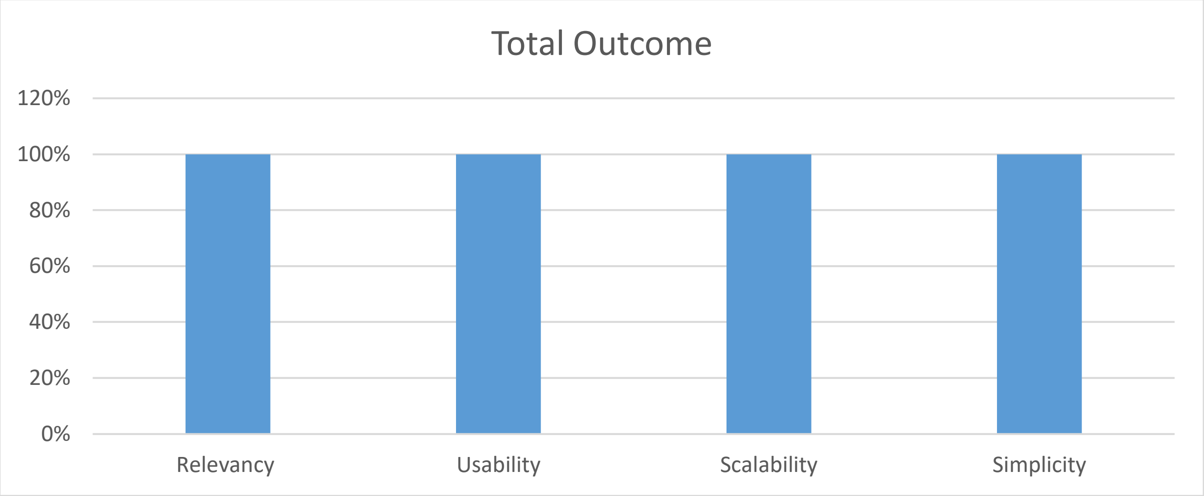


Figure 6.6 Finding on Outcome of Questionnaire

As stated in Section 6.2, three open-ended questions were also part of the questionnaire. The objective of gaining responses to these three questions was to eliminate any gaps that might have existed, and to determine if there was anything lacking with the framework that might need improvements. Regarding the outcomes of the open-ended questions, there was positive feedback from the stakeholders that participated. Some of the feedback or comments were as follows:

“This is the first of its kind, will really help the organization regarding IT risks”.

“In my opinion, I think this is a good starting point, as the organization is lacking behind in terms of IT governance policies”

“I really think, this framework will help us as the company to manage and identify critical issues when it comes to IT-related risks, good one”.

Looking at the comments, it can be affirmed that stakeholders felt that the IT Risk Management Framework would add value to Sovereign Foods and within the food manufacturing industry at large by ensuring that IT-related risks are easily identified, and that proactive decisions are made to achieve strategic objectives of the enterprise.

6.5 Conclusion

As per the integrated research approach, four core aspects (relevancy, usability, scalability, and simplicity) have to be validated to ensure conformity. This chapter discussed the validation of the IT Risk Management Framework. As discussed, data for the validation process was collected on 08 May 2019 via questionnaires completed by 12 stakeholders participated in a validation workshop. During the workshop, a theoretical framework was presented to stakeholders to inform them of the contents of the framework, after this, the questionnaires were handed to the participants. The objective of the questionnaire was to validate that the IT Risk Management Framework conforms to the four core aspects (relevancy, scalability, usability, and simplicity).

It can be confirmed that the IT Risk Management Framework conforms to the four core aspects of relevancy, scalability, usability, and simplicity (Figure 6.6). With this in mind, Chapter 7 i contains reflection on the overall findings of this study. Therefore, the next chapter will discuss the overall conclusions of this research study.

Chapter 7
SUMMARY OF FINDINGS

7.1 Introduction

Chapter 6 covered the validation of the core aspects of relevancy, usability, scalability, and simplicity. This process is the last and final phase as per the phases of the unique integrated research approach. Feedback from stakeholders, who participated in the validation process, indicated that the established IT Risk Management Framework for Enterprises within the Food Manufacturing Industry in South Africa conformed to the four core aspects.

This chapter will focus on a summary of the findings made throughout the study to document that all research objectives, as specified in Chapter 1 have been met and to show that research contributions have been generated.

7.2 Summary of Findings

“In the current competitive business environment, the enterprises are greatly depending on the use of IT to create value for their business” (Debreceny & Gray, 2013; De Haes, Rowlands & van Grembergen 2016 cited by Aasi et al., 2017, p42). Furthermore, Parry and Lind (2016) state that “effective IT governance is essential to good IT project management”. It is clear from the statements made by these authors that IT is critical to the wellbeing of any enterprise, and effective governance is needed to ensure that the strategic objectives of the enterprises are achieved.

As per the discussion in Chapter 3, it is apparent that IT Risk Management is important in enabling the achievement of all IT-related objectives of an enterprise. As illustrated in Chapters 2 and 3, and highlighted in the Problem Statement (Section 1.4), it has been identified, through a series of internal audits, that enterprises within the food manufacturing industry lack IT risk management principles.

To address the problem at hand, a unique integrated research approach was identified with the purpose of developing an artefact in the form of a framework. This was deliberated thoroughly in Chapter 4 and an IT Risk Management Framework was established to address the problem at hand.

The unique integrated research approach discussed in Chapter 4, was given further consideration in Chapter 5. Each phase of the unique integrated research approach as per the NMU-DSFM was discussed in conjunction with stakeholders from the food manufacturing industry.

Chapter 6 presented findings of the validation phase. The IT Risk Management Framework was validated for conformance to the core aspects of *relevancy, usability, scalability, and simplicity*. As discussed in Section 6.5, the validation process took place on 08 May 2019 and 12 stakeholders participated. A theoretical framework was presented to the stakeholders to inform them of the contents of the framework. After the theoretical framework was presented, questionnaires were handed to the participants. Data collected from the questionnaires was used to test the conformance to the four core aspects. The results of the validation process suggested that the IT Risk Management Framework conformed fully to the core aspects.

7.3 Meeting the Objectives

The aim of this study was to address a real-world problem as communicated in Chapter 1 in the Problem Statement. As indicated in the research objectives, the primary aim was to establish a framework that will ensure IT-related threats, vulnerabilities, and risks are properly managed and ensure that enterprises within the sector are able to make appropriate risk-aware decisions, thus improving performance and the ability to allow achievement of the enterprise's objectives. The secondary objectives were:

To determine that enterprises are well informed about the extent of risk, risk appetite, and risk tolerance;

To provide guidelines on how to conduct IT risk identification, assessment, response and mitigation, and control monitoring and reporting;

To create a risk-aware culture within food manufacturing enterprises for better decision making;

To ensure the integrity, confidentiality, and availability of information.

Chapters 2 and 3 provided extensive literature reviews of the topic in relation to the study objectives. As discussed in Chapter 5, the primary objective of this study was achieved through establishing an artificial artefact in the form of the IT Risk Management Framework. The secondary objectives were also achieved, through modelling of the actual framework, as reported in Section 5.5.2 which constituted the contextualisation of the framework. Stakeholder's participation also affirmed that both the primary and secondary objectives were met, particularly in relation to the fact that outcomes of the validation process confirmed that the IT Risk Management Framework for enterprises within the food manufacturing industry conformed to the four core aspects of the unique integrated research approach.

7.4 Contribution Summary

7.4.1 Research Contribution: The Artefact

The intended key research output of this study was an artificial artefact in the form of a framework, specifically an IT Risk Management Framework for use in the food manufacturing industry in South Africa. The core elements of this framework were drawn from components of risk management in combination with best practices (King IV, ISO 31000, ISO 31010, COBIT 5 and NIST 800-39). These components provide guidelines on how to conduct effective IT risk management and are *IT risk identification, IT risk assessment, IT risk response and mitigation, and IT risk control monitoring and reporting.*

7.4.2 Research Paradigm

As mentioned in Chapter 4, a design science research paradigm was followed, taking into consideration the four principles that need to be adhered to when performing design science research, namely;

Abstraction – The artefact must be applicable to a class of problems.

Originality – The artefact must substantially contribute to the advancement of the body of knowledge.

Justification – The artefact must be justified in a comprehensible manner and must allow for its validation.

Benefit – The artefact must yield benefit either immediately or in the future for the respective stakeholder groups.

In this section, an evaluation will be performed to determine adherence to these principles. This is to ensure that the best possible framework was created to address the problem at hand.

Abstraction

It can be concluded that the established IT Risk Management Framework adheres to the principle of abstraction because it was established to suit all enterprises within the food manufacturing industry in South Africa. Owing to the number of world best practices used, it can also be argued that the framework is not only applicable within the South African context but to the rest of the world.

Originality

As communicated by stakeholders that participated throughout this study, the framework is certainly bringing new insights to the food manufacturing industry that were previously lacking. The artefact contributes to the body of knowledge through providing enterprises with guidance on how to conduct effective IT risk management to ensure IT-related threats, vulnerabilities, and risks are properly managed. Therefore, it can be concluded that the framework adheres to the principle of originality.

Justification

As stated by this principle, the artefact must be justified in a comprehensible manner and must allow for its validation. The Problem Statement (Section 1,4), "through a series of internal audits it has been identified that enterprises within the food manufacturing industry lack IT risk management principles" provides justification for the establishment of the IT Risk Management Framework. Thus it can be concluded that the principle of justification has followed.

Benefit

As per the four principles, benefit is the last value that should be considered when performing a design science research. As discussed in Chapter 6, it is evident that the artefact brings value to stakeholders. Positive feedback about the IT Risk Management Framework was received from all stakeholders who participated in the study. Thus it can be concluded that the study fully adheres to the principle of benefit.

7.5 Conclusion

As already mentioned in Chapter 1, the objective of this study was to establish a framework that will ensure IT-related threats, vulnerabilities, and risks are properly managed and to ensure enterprises within the sector are able to make appropriate risk-aware decisions, thus improving performance and the ability to allow achievement of the enterprise's objectives. This objective was based on the problem identified as the basis for this research study.

In trying to resolve the problem at hand, the idea was to establish an artificial artefact in the form of a framework. In this regard, the IT Risk Management Framework for Enterprises within Food Manufacturing Industry in South Africa was developed as a contribution to resolving the problem at hand (visual portray of the developed framework attached in appendix A.3 as per the contextualisation of the framework in section 5.5.2). As seen through the collaboration of stakeholders, the study has achieved its objective. Stakeholders have attested to the fact that the study conforms to all four core aspects of *relevancy, usability, scalability, and simplicity*. Furthermore, the four principles to be considered when performing design science research were also validated.

It can, therefore, be concluded that the framework developed during this study can be used as a guiding principle for effective IT Risk Management within enterprises in the food manufacturing industry is South Africa. Moreover, after the framework have been implemented, further research can be conducted to determine the value it is bringing to enterprises within the sector.

REFERENCES

Aasi, P., Rusu, L., & Vieru, D. (2017). The Role of Culture in IT Governance Five Focus Areas. *International Journal of IT/Business Alignment and Governance*, *8*(2), 42–61. https://doi.org/10.4018/ijitbag.2017070103

Alzadjali, A. M., Al-Badi, A. H., & Ali, S. (2015). An analysis of the security threats and vulnerabilities of cloud computing in Oman. *Proceedings - 2015 International Conference on Intelligent Networking and Collaborative Systems, IEEE INCoS 2015*, 423–428. https://doi.org/10.1109/INCoS.2015.79

Baccarini, D., Salm, G., & Love, P. E. D. (2004). Management of risks in information technology projects. *Industrial Management and Data Systems*, *104*(3), 286–295. https://doi.org/10.1108/02635570410530702

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (1999). Management Decision Emerald Article : A framework for integrated risk management in information technology. *Management Decision*, *Vol.37*(5), 437–445.

Calder, A., & Watkins, S. (2012). *IT Governance: An international guide to data security and ISO27001/ISO27002* (5th ed.). London: Kogan Page Limited.

Calder, A. (2009a). *Implementing Information Security based on ISO 27001/ISO 27002 - A Management Guide*. (J. van Bon, Ed.) (Second edi). London.

Calder, A. (2009b). *IT Governance - Implementing Frameworks and Standards for the Corporate Governance of IT*. United Kingdom: IT Governance Publishing.

Carcary, M. (2012). IT Risk Management: A Capability Maturity Model Perspective, *16*(1), 3–13. Retrieved from www.ejise.com

Center National Computing. (2005). IT Governance Developing a successful governance strategy: A Best Practice guide for decision makers in IT.

Chapman, C., B & Cooper, D., F. (2003). Risk analysis: testing some prejudices. *European Journal of Operational Research*, *47*, 238.

CRISC. (2015). CRISC Review Manual. USA.

Delport, P. (n.d.). Chapter 4_Research Method_GMM, 43–56.

Global Technology Audit Guide (GTAG). (2012). *Information Techonology Risk and Control* (2nd edition). Retrieved from https://na.theiia.org/standards-guidance / recommended-guidance/practice-guides/Pages/GTAG1.aspx

Gonen, A. (2011). Optimal risk response plan of project risk management. *IEEE International Conference on Industrial Engineering and Engineering Management*, 969–973. https://doi.org/10.1109/IEEM.2011.6118060

Goy, J. (2010). DEVELOPING A MORE SOPHISTICATED APPROACH TO RISK ANALYSIS AND EVALUATION. Retrieved April 24, 2019, from https://ebrary. net/9883/management/conclusion

Hosseinbeig, S., Karimzadgan Moghadam, D., Vahdat, D., & Askari Moghadam, R. (2011). Combination of IT strategic alignment and IT governance to evaluate strategic alignment maturity. *2011 5th International Conference on Application of Information and Communication Technologies, AICT 2011*, 1–10. https: //doi.org /10.1109/ICAICT.2011.6110901

Imenda, S. (2015). Is There a Conceptual Difference between Theoretical and Conceptual Frameworks?, *38*(2), 185–195. https: //doi. org/10. 1080/ 097 18923.2014.11893249

Institute of directors Southern Africa. (2016). Report on corporate governance for South Africa 2016. *King IV Report on Corporate Governance for South Africa King IV Report on Corporate Governance for South Africa*, 71 and 87–94.

ISACA. (2009). The Risk IT Framework. *Press Release*, 40. Retrieved from http://www.isaca.org/About-ISACA/Press-room/News Releases /Spanish / Pages/ISACA-Launches-Risk-IT-Framework-to-Help-Organizations-Balance-Risk-with-Profit-Spanish.aspx

ISO. (2009). ISO 31010: Risk assessment techniques, final draft. *Iso 31010*, *2009*.

ISO 2009. (2009). International Standard Iso 31000:2009, *2009*, 36.

IT Governance Institute (ITGI). (2003). *Board Briefing on IT Governance - 2nd Edition*. *IT Governance Institute*.

Johnson, S. L. (2019). Impact, growth, capacity-building of mixed methods research in the health sciences. *American Journal of Pharmaceutical Education*, *83*(2), 136–139.

Kbar, G. (2008). Security risk analysis for asset in relation to vulnerability, probability of threats and attacks. *2008 International Conference on Innovations in Information Technology, IIT 2008*, 668–672. https://doi.org/10. 1109/ INNOVATIONS.2008.4781631

Ko, D., & Fink, D. (2010). Information technology governance: An evaluation of the theory-practice gap. *Corporate Governance*, *10*(5), 662–674. https:// doi. org/10.1108/14720701011085616

Laurentiu, F., & Adrian, T. (2008). Aspects of It Risk Management for a Company. *Annals of the University of Oradea, Economic Science Series*, *17*(2), 141–146. Retrieved from http://w3.bgu.ac.il/lib/ customproxy.php ?url=http://search .ebscohost.com/login.aspx?direct=true&db=bth&AN=48129244&site=eds live&authtype=ip,uid&custid=s4309548&groupid=main&profile=eds

Lucarelli, C., Uberti, P., & Brighetti, G. (2015). Misclassifications in financial risk tolerance, *18*(4), 467–482.

Magro, W. S., & Kellow, W. T. (2004). Risk management in IT implementation: A human factor. *AACE International Transactions*, RISK.02.1-RISK.02.5. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-11944270395&partnerID=40&md5=e135021c0ab53ebc55a42520e61f70df

Meyers, G., Jacobsen, M., & Henderson, E. (2018). Design-Based Research: Introducing an innovative research methodology to infection prevention and control. *Canadian Journal of Infection Control*, *33*(In Press).

Mozsár, A. L. K., & Michelberger, P. (2019). It Risk Management and Application Portfolio Management. *Polish Journal of Management Studies*, *17*(2), 112–122. https://doi.org/10.17512/pjms.2018.17.2.10

Musson, D., & Jordan, E. (2006). The Benefits of IT Governance. *Ecis*, (2006), Paper 48. Retrieved from http://aisel.aisnet.org/ecis2006/48

MyBroadband. (2019). South Africa targeted in North Korean cyber attack. Retrieved August 21, 2019, from https://businesstech.co.za/ news/technology /334429 /south-africa-targeted-in-north-korean-cyber-attack/

National Association of Corporate Directors. (n.d.). Get the Most From the Risk Appetite Dialogue. (pp. 7,10&11).

Osterle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., ... & Sinz, E. J. (2011). Memorandum on Design-Oriented Information Systems Research. *European Journal of Information Systems*, *20*(1), 7–10.

Park, C. W., Keil, M., & Kim, J. W. (2009). The effect of IT failure impact and personal morality on IT project reporting behavior. *IEEE Transactions on Engineering Management*, *56*(1), 45–60. https://doi.org/10. 1109/ TEM. 2008 .2009794

Parry, V. K. A., & Lind, M. L. (2016). Alignment of Business Strategy and Information Technology Considering Information Technology Governance, Project Portfolio Control, and Risk Management. *International Journal of Information Technology Project Management*, *7*(4), 21–37. https://doi.org/10.4018/ijitpm.2016100102

Prasetyo, S., & Sucahyo, Y. G. (2014). Information Security Risk Management Planning: A Case Study at Application Module of State Asset Directorate General of State Asset Ministry of Finance., 96–101. https://doi.org/ 10. 1109 / ICACSIS.2014.7065875

Radeschütz, S., Schwarz, H., & Niedermann, F. (2015). Business impact analysis—a framework for a comprehensive analysis and optimization of business processes. *Computer Science - Research and Development*, *30*(1), 69–86. https://doi.org/10.1007/s00450-013-0247-3

Rot, A. (2009). *Enterprise Information Technology Security: Risk Management Perspective. World Congress on Engineering and Computer Science*. San Francisco, USA.

Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system: How a framework for IT governance supports ERM. *Corporate Governance (Bingley)*, *14*(3), 320–338. https://doi.org/10.1108/CG-06-2013-0067

Scarlat., E. Chirita., N. & I-A., B. (2011). INDICATORS AND METRICS USED IN THE ENTERPRISE RISK MANAGEMENT (ERM. *The Bucharest Academy of Economic Studies*, 5–18.

Schorr, F., & Hvam, L. (2018). Design science research: A suitable approach to scope and research it service catalogs. *Proceedings - 2018 IEEE World Congress on Services, SERVICES 2018*, 27–28. https://doi.org/10. 1109/ SERVICES.2018.00026

Schwandt, T. A. (2001). *Dictionary of Qualitative Inquiry* (2nd Editio). Thousand Oaks:Sag.

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, (20), 113–132. https://doi.org/10. 23962/10539/23573

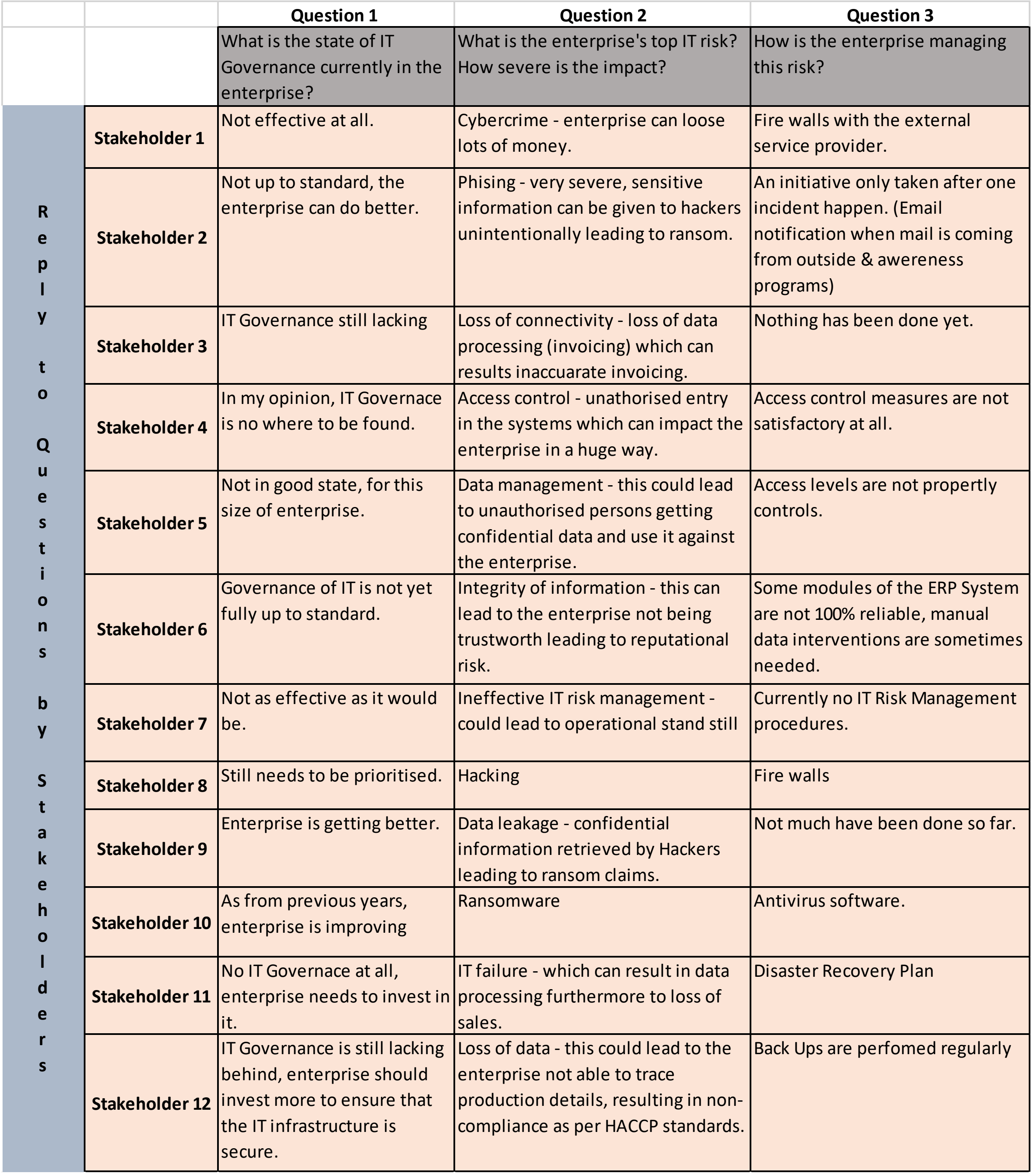
von Solms, S.H., & von Solms, R. (2009). *Information Security Governance*. New York: Springer.

Wijanarka, H. (2014). IT risk management to support the realization of IT value in public organizations. *Proceedings - 2014 International Conference on ICT for Smart Society: "Smart System Platform Development for City and Society, GoeSmart 2014", ICISS 2014*, 113–117. https://doi.org/10.1109/ ICTSS .2014 .7013160

Wilkin, C., & Chenhall, R. (2010). A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107–146.

Zarvić, N., Stolze, C., Boehm, M., & Thomas, O. (2012). Dependency-Based IT Governance Practices in Inter- Organisational Collaborations: A Graph-Driven Elaboration. *A Graph-Driven Elaboration. International Journal of Information Management*, *32*(6), 541–549.

Appendix A.1 - Semi-structuctured interview



		Question 1	Question 2	Question 3
		What is the state of IT Governance currently in the enterprise?	What is the enterprise's top IT risk? How severe is the impact?	How is the enterprise managing this risk?
Reply to Questions by Stakeholders	**Stakeholder 1**	Not effective at all.	Cybercrime - enterprise can loose lots of money.	Fire walls with the external service provider.
	Stakeholder 2	Not up to standard, the enterprise can do better.	Phising - very severe, sensitive information can be given to hackers unintentionally leading to ransom.	An initiative only taken after one incident happen. (Email notification when mail is coming from outside & awereness programs)
	Stakeholder 3	IT Governance still lacking	Loss of connectivity - loss of data processing (invoicing) which can results inaccuarate invoicing.	Nothing has been done yet.
	Stakeholder 4	In my opinion, IT Governace is no where to be found.	Access control - unathorised entry in the systems which can impact the enterprise in a huge way.	Access control measures are not satisfactory at all.
	Stakeholder 5	Not in good state, for this size of enterprise.	Data management - this could lead to unauthorised persons getting confidential data and use it against the enterprise.	Access levels are not propertly controls.
	Stakeholder 6	Governance of IT is not yet fully up to standard.	Integrity of information - this can lead to the enterprise not being trustworth leading to reputational risk.	Some modules of the ERP System are not 100% reliable, manual data interventions are sometimes needed.
	Stakeholder 7	Not as effective as it would be.	Ineffective IT risk management - could lead to operational stand still	Currently no IT Risk Management procedures.
	Stakeholder 8	Still needs to be prioritised.	Hacking	Fire walls
	Stakeholder 9	Enterprise is getting better.	Data leakage - confidential information retrieved by Hackers leading to ransom claims.	Not much have been done so far.
	Stakeholder 10	As from previous years, enterprise is improving	Ransomware	Antivirus software.
	Stakeholder 11	No IT Governace at all, enterprise needs to invest in it.	IT failure - which can result in data processing furthermore to loss of sales.	Disaster Recovery Plan
	Stakeholder 12	IT Governance is still lacking behind, enterprise should invest more to ensure that the IT infrastructure is secure.	Loss of data - this could lead to the enterprise not able to trace production details, resulting in non-compliance as per HACCP standards.	Back Ups are perfomed regularly

Appendix A.2 - Core Aspects

Core aspects	Question	Statement
Relevancy	3	Framework have covered comprehensively the components of IT risk management
	5	Framework can be used to cover the minimum basis as required by risk management phases.
Usability	1	Framework can be used as guideline for implementation of IT risk management in food manufacturing industry.
Scalability	4	Framework can be equally implemented in both large and small enterprises within the industry.
Simplicity	2	A person with limited information technology know how would be able to complete the requirements of the framework successfully.

Stakeholder's responses as per the above questions

(A - Agree, SA - Strongly Agree)

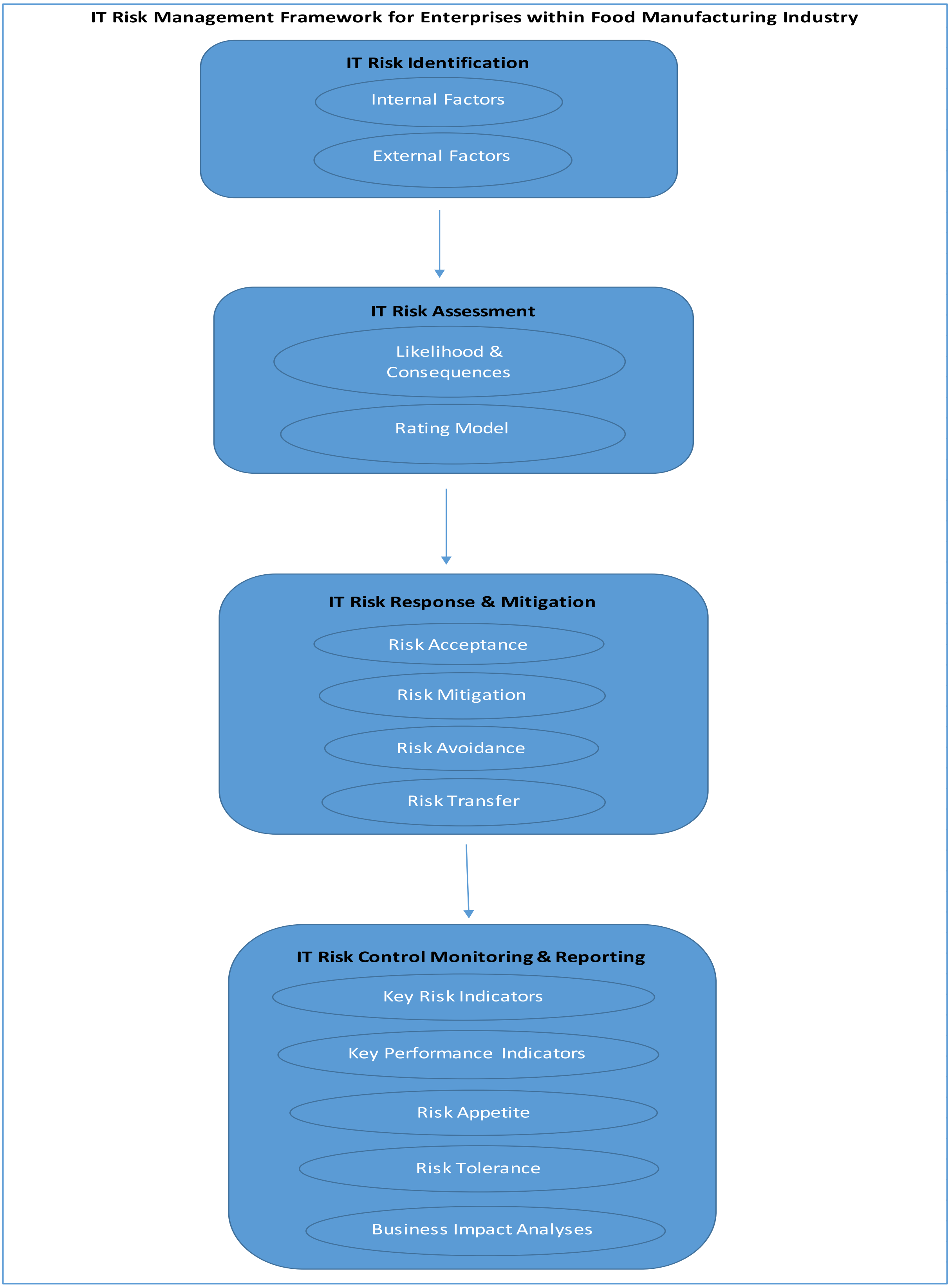
	Relevancy		Usability	Scalability	Simplicity
	3	5	1	4	2
Stakeholder 1	SA	SA	A	SA	A
Stakeholder 2	SA	SA	SA	SA	A
Stakeholder 3	SA	SA	SA	SA	A
Stakeholder 4	SA	SA	A	A	SA
Stakeholder 5	SA	SA	SA	A	SA
Stakeholder 6	SA	SA	SA	SA	SA
Stakeholder 7	SA	SA	SA	SA	SA
Stakeholder 8	SA	SA	SA	SA	SA
Stakeholder 9	SA	SA	SA	SA	SA

Stakeholder 10	SA	SA	A	SA	SA
Stakeholder 11	SA	SA	SA	SA	A
Stakeholder 12	SA	SA	SA	SA	A

Results

	Relevancy	Usability	Scalability	Simplicity
Agree	0 – 0%	3 – 25%	2 – 17%	5 – 42%
Strongly Agree	12 – 100%	9 – 75%	10 – 83%	7 – 58%

Appendix A.3 - Visual Portray of the Developed Framework


IT Risk Management Framework for Enterprises within Food Manufacturing Industry
IT Risk Identification
Internal Factors
External Factors
IT Risk Assessment
Likelihood & Consequences
Rating Model
IT Risk Response & Mitigation
Risk Acceptance
Risk Mitigation
Risk Avoidance
Risk Transfer
IT Risk Control Monitoring & Reporting
Key Risk Indicators
Key Performance Indicators
Risk Appetite
Risk Tolerance
Business Impact Analyses