A Risk-Based Framework For New Products: A South African Telecommunication's Study

Submitted in partial fulfilment
of the requirements of the degree of

Master of Science

of Rhodes University

Michael Jeffries

Grahamstown, South Africa
May 2016

Abstract

The integrated reports of Vodacom, Telkom and MTN — telecommunication organisations in South Africa — show that they are diversifying their product offerings from traditional voice and data services. These organisations are including new offerings covering the financial, health, insurance and mobile education services. The potential exists for these organisations to launch products that are substandard and which either do not take into account customer needs or do not comply with current legislations or regulations.

Most telecommunication organisations have a well-defined enterprise risk management program, to ensure compliance to King III, however risk management processes specifically for new products and services might be lacking. The responsibility usually resides with the product managers for the implementation of robust products; however they do not always have the correct skillset to ensure adherence to governance requirements and therefore might not be aware of which laws they might not be adhering to, or understand the customers' requirements. More complex products, additional competition, changes to technology and new business ventures have reinforced the need to manage risk on telecommunication products. Failure to take risk requirements into account could lead to potential fines, damage the organisation's reputation which could lead to customers churning from these service providers.

This research analyses three periods of data captured from a mobile telecommunication organisation to assess the current status quo of risk management maturity within the organisation's product and service environment. Based on the analysis as well as industry best practices, a risk management framework for products is proposed that can assist product managers analyse concepts to ensure adherence to governance requirements. This could assist new product or service offerings in the marketplace do not create a perception of distrust by consumers.

Acknowledgements

I wish to thank:

- Jesus Christ, for giving me the health, strength and direction throughout this journey.
- My wife, Abigail Jeffries for always being at my side, through the ups and downs and allowing me the space to try and balance between home, work and studies, for always supporting me. I will always love you.
- My supervisors, Prof. Karen Bradshaw and Prof. Barry Irwin for their guidance and answering my questions in a timely fashion.
- Emile Swanson for assisting me through my technical challenges.
- To my employer, for giving me the support required to reach this goal.
- To all candidates which I interviewed throughout the research period.

Contents

List of Figures

List of Tables

Glossary

Acronyms

AML Anti-Money Laundering

BBM BlackBerry Messenger

BCM Business Continuity Management

BOD Board of Directors

CMM Capability Maturity Model

DR Disaster Recovery

DRP Disaster Recovery Plans

ERM Enterprise Risk Management

FICA Financial Intelligence Centre Act

IPR Intellectual Property Rights

ISO International Organization for Standardization

IT Information Technology

MB Megabyte

NPS Net Promotor Score

OTT Over The Top

PDLC Product Development Lifecycle

POCA Prevention of Organised Crime Ac

RA Revenue Assurance

ROI Return on Investment

SIM Subscriber Identity Module

SLA Service Level Agreement

Chapter 1

INTRODUCTION

1.1 Context of research

Innovation is critical to ensure telecommunication organisations remain competitive for their survival. Risk management is equally important in improving innovative practices and ensuring the continued sustainability of the business. Increased competition, faster innovation cycle times, improved technology, developing business model complexity and new business ventures have reinforced the need to manage risk.

For organisations to remain competitive they need to ensure that they are innovative and creative (Lee *et al.*, 2015). Lee *et al.* (2015) further state that telecommunication innovation is important as it drives national competitiveness and economic growth. Mayle & Henry (2010) state that, in general, the starting point for creativity and innovation is dissatisfaction with the status quo. This dissatisfaction forces the organisation to search for solutions to a failure or changes in response to external factors such as competition, government regulation and changes in technology, resource shortages or new ways of perceiving a target. Keeley (2009) states that if the organisation is not moving at the speed of the market place, the business is already dead and operational excellence is no longer differentiating enough. Henry (2010) says that due to globalisation, organisations need to ensure that they are more responsive to change in order for them to remain competitive within the environment.

With globalisation trending, telecommunication organisations are competing not only within the local market, but also with global organisations. In January 2015, some telecommunication organisations in South Africa lobbied in parliament that over the top

(OTT) applications should be regulated (Alfreds, 2016), demonstrating that telecommunication organisations are aware of these global trends and emerging global competition. Organisations need to respond more quickly to changes in the market, which is why creativity and innovation are so important, as seen by an exponential increase in the use of smartphones year on year. Vodacom has seen a 26% rise in the use of smartphones to 6 million devices from 2012 to 2013 and a 51.1% increase of up to 138 MB of data used per device (Vodacom, 2013). In 2015, Vodacom had 26.5 million active data customers and its data usage grew by 25% (Vodacom, 2015). Likewise MTN reported a 108.5% increase in data traffic, over 30 million active data subscribers and a 37.2% increase in data revenue in their South African operations (MTN, 2015). Owing to the mobile market having passed its saturation point — it was over 150% capacity in mid-2015 (Lancaster, 2016) — telecommunication organisations have been forced to look for different streams of revenue.

Henry (2010) states that organisations should change, have fewer rules, and share leadership by flattening the organisational structure, which will also empower staff to be more accountable. Leaders should allow and encourage teamwork between different resources and departments thereby responding to customer behaviour. Although this could increase innovation, it could also be problematic as it creates additional concerns with regard to governance and compliance. For example, without a multifunctional team, key stakeholders such as the legal, regulatory, risk management or technology security departments might not be kept abreast of changes within the organisation timeously, which could result in scope creep or substandard products existing in the market place.

Additional concerns arise when organisations develop products too fast, or adapt too quickly to competitive pressures, which could impact on an organisation's strategy and its product quality. Some telecommunication companies have taken the approach to outsource some of their product development and functions; this could create even more potential problems as they do not control or fully understand the mechanism behind the developmental approach that was adopted (Summerfield, 2013b).

Another example within the telecommunication space is applications hosted beyond the borders of South Africa, where customers upload personal information without looking at the ramifications such as data leakage, privacy and the potential on-selling of their personal information to third-parties. Laws such as the Protection of Personal Information (POPI) Act (The Republic of South Africa, 2013) normally impact these types of projects and it cannot always be left in the hands of the product managers and owners to make the correct decisions to ensure compliance.

According to the Vodacom annual report for 2014 (Vodacom, 2014), Vodacom's strategy was to drive market penetration into existing markets and pursue opportunities within new markets. This approach included bundling products outside the traditional telecommunication landscape such as life insurance, mobile finances and enterprise services. MTN's integrated report for 2013 (MTN, 2013) shows similar trends, with investment in financial-type services and the development of a mobile money solution.

Considering the growing expansion within these markets, telecommunication organisations are moving into areas where they might not have the required skillsets to ensure compliance and governance. Adler & Kranowitz (2005) says problems that are diagnosed early through anticipated strategies and are then averted through proper project planning and early interactions allow for more robust projects. However, projects that are protracted, entrenched, politicised and unpredictable could fail.

It is therefore the responsibility of the risk management department to ensure that governance practices are implemented, while ensuring that the organisation takes a risk-based approach. This approach includes the identification and evaluation of risks related to information security, customer experience, regulations and privacy to ensure that sound decisions are made in order to sustain the competitive environment of the telecommunication industry.

1.2 Current landscape

Large telecommunication companies do perform a level of risk management, as shown in their integrated reports (MTN, 2015, Telkom, 2015, Vodacom, 2015). Processes need to be put in place to ensure that risks are identified and mitigated on products and services before impacting the organisation's reputation and brand value.

Furthermore, with the constant introduction of new products and services, there is a need to ensure that new services do not create additional risks, which could result in customers losing their trust in the brand. Therefore, it is very important that organisations ensure that governance structures are in place and are being followed to ensure robust projects are launched.

Although South Africans generally believe that online retailers and service providers have security systems in place to protect them against fraud, they still do not believe that

organisations protect their personal information and financial data from hackers (BusinessTech, 2014). The latter belief can be mitigated by organisations confirming in their annual integrated reports that continuous risk assessments are carried out. These reports however deal with strategy and although they do show that governance is taken into account, should customers trust the organisation to always make the correct decisions all the time, especially when it needs to balance organisational strategy and risk?

Service providers should do more to build trust into their brands as they build credibility with the customers (Siegel *et al.*, 2000). They further state that trust can be built with better governance, risk and compliance controls to ensure that proper controls are implemented and that the correct stakeholders are involved in making business decisions, as this could impact on the security of customer information. However, since product managers are responsible for all aspects of a project, including the legal, security, privacy and marketing aspects, they are required to ensure that they are in fact skilled to make these decisions.

Considering risk management from the perspective of combined assurance shows that risk managers are the second line of defence when it comes to ensuring that risks within the organisation are identified, managed and mitigated. Line management (product management) is the first line of defence and internal/external audits should be the third line of defence to ensure that the implemented controls work as they were intended (Soh & Martinov-Bennie, 2015).

Although combined assurance does play an important role in the assurance that risks are managed, there are still concerns that line managers are not skilled in terms of the issues that they need to identify (Soh & Martinov-Bennie, 2015). Therefore, the onus currently lies with the risk management department to identify the risk on behalf of line management.

1.3 Problem statement

Telecommunication companies can damage their brand as a result of not adhering to good governance principals and rushing products to market in order to obtain larger market share. We aim to develop a risk-based framework which will influence the behaviour of the product development teams when developing their products. The risk-based framework should assist with the early identification of risks and controls which ensure that they do not impact on the product development timelines if identified later in the project.

1.4 Research objectives

The primary objective of the research is to propose a risk-based framework which assists product managers in the telecommunication industry to identify risks which can impact on the success of their products.

The primary objective is supported by the following secondary objectives:

1. To identify the perceived risks telecommunication organisations are facing when developing products.
2. To identify the key success factors for robust products.
3. To identify a process which telecommunication companies use as a bench-mark for their risk maturity.
4. To propose a model to implement a product risk-based framework.

1.5 Scope of study

The following section describes what is included and excluded in the scope of this study.

- The study focuses on telecommunication organisations in South Africa. With some modifications, due to different markets, legal or regulatory landscapes, the proposed framework could, however, be used within both different organisations and countries.
- The study analyses the internal processes of an organisation to determine what organisations are doing to build trust in their services.
- In the study, a few assumptions are made about the external customer environment, however the study focus on an organisational point of view to determine what companies are doing to enhance their processes and skills to build customers' trust.
- This study does not attempt to compare all listed telecommunication organisations in South Africa, but rather focuses on the major mobile telecommunication organisations.

- This study does not attempt to design, build, implement or evaluate what policies and procedures or processes need to be in place in an organisation. It does, however, refer to examples that can be used by the organisation.
- The study does not review all the different types of services offered by telecommunication service providers; a few samples of different areas within the organisation are considered to create a general picture of the environment.

1.6 Assumptions of study

The following are assumed in this report:

- Most South African consumers who are using smart mobile devices are to some extent aware of the need for basic information security and the protection of their data, due to an increased awareness of the POPI Act (The Republic of South Africa, 2013), which was passed into law in 2013. In South Africa, over the past few years, there has also been an increase in the amount of fraud related to subscriber identity module (SIM) swops and fraudsters are targeting banking customers (Jacobs, 2015, PWC, 2015). This should make users more aware of their security needs.
- With the passing of the Consumer Protection Act (The Republic of South Africa, 2008), consumers are more aware of their rights and who is responsible and liable for the protection of their information. Therefore most South Africans who use smart mobile devices believe that the responsibility to protect their personal information resides with the service provider or the application developer.
- Improvements in telecommunication applications are becoming more prevalent, including improvement of security and privacy issues. These improvements can be seen in South African telecommunication companies' integrated reports.
- Telecommunication organisations are attempting to increase their footprint in the market by creating new applications and services that are not strictly related to the telecommunication industry, including banking and insurance (MTN, 2013, 2014, 2015, Telkom, 2015, Vodacom, 2013, 2014, 2015).
- Assumptions related to the collection of data are addressed in Chapter 3.

1.7 Document structure

The remainder of the document is organised as follows:

Chapter 2 includes a literature review of related work within this field, both from industry standard documents and academic literature. To ascertain the impact on telecommunication service providers, the review analyses problems by using relevant theoretical considerations and models.

Chapter 3 describes how the datasets were collected over a three-year period as well as the research methodologies used during this study.

Chapter 4 analyses the data collected over the three-year period and describes how it relates to the field of study.

Chapter 5 reviews the findings of the research and presents a framework that product managers could use to ensure the organisation provides customers with a robust service offering. The proposed framework is analysed based on interviews conducted with experts in the field of products and services in the telecommunication industry to evaluate whether a risk framework could be adopted by a telecommunication organisation.

Chapter 6 summarises the main contributions of the thesis and considers these in the light of potential future work that can be performed in the field of products and services risk management.

Chapter 2

LITERATURE REVIEW

The aim of this chapter is to provide the academic foundation for the research topic. This research is exploratory in nature and the research includes academic literature to identify and define the areas that form part of the study.

With the aim of ensuring that the literature review is logical, the researcher has broken it down into three different segments according to the sub-problems and research objectives discussed in Section 1.3.

This chapter looks first at the consumer landscape, risk management methodologies and what current South African telecommunication organisations are doing with regard to risk management. The chapter goes further to look at trust models and why customers purchase products and services. Finally, the chapter concludes with a risk maturity model that can be used to implement risk management for products and services.

2.1 Risk management within telecommunication organisations

Altman & Cooper (2004) state that risk management can be defined within two streams. Firstly, traditional risk management focuses on financial and hazard risk and secondly, enterprise risk management (ERM), deals with the operational and strategic risks of the organisation. The value of risk management is to enhance shareholder value and give the organisation a competitive advantage by ensuring that the company complies with

regulatory requirements. Risk management is also used as the tool for a company's decision-making processes.

The King III Report (Institute of Directors in South Africa, 2009) on corporate governance informs organisations that are listed on the Johannesburg Stock Exchange that they need to put appropriate processes and systems in place to report to stakeholders and provide them with a complete picture of the organisation. The report needs to confirm reliability internally and it should build trust in the organisation externally. Section 4 of the King III report states that the Board of Directors (BOD) should exercise leadership to ensure good corporate governance. Risk should be the cornerstone of the corporate governance and the organisation should ensure that on-going and effective risk assessments are performed. The report further emphasises that the BOD should ensure that they are satisfied with the management of risk within the organisation. The King III report goes on to state that a systematic, documented and formal risk assessment should be conducted in an organisation at least once a year. The draft King IV (Institute of Directors in South Africa, 2016) adds in an additional aspect for risk management, namely opportunity management, this draft advises BODs that both risk and opportunity management need to be considered when making strategic decisions. The draft King IV (Institute of Directors in South Africa, 2016) goes further to state that risk is necessary within businesses and should not only be viewed negatively, but rather that risk should be reviewed for the reward that it can offer the organisation. The draft King IV report does not discourage risk taking, however they caution against excessive risk taking. The draft King IV report cites (Mitchell, 2011) which states that organisations that build ethical cultures normally outperform those that do not and this reduces the organisation's exposure to ethical concerns which could cause breakdowns. This means that unethical behaviour by organisations can damage the trust in the organisation by customers and stakeholders.

Vodacom (2014) states: *"There is no opportunity without risk, we have the right structures in place to identify, monitor and manage our risk effectively"*. Within this integrated report, Johan Van Graan, Chief risk officer for Vodacom states: *"Balancing risk and reward is an everyday thing for you and I as individuals, exactly the same must be for well-managed companies that aim to survive and succeed no matter the challenges and changes in the environment"*. This statement is important as it demonstrates that organisations need to take risks to remain competitive. Risk management should, however, be used as a tool to understand what risks the organisation might face, thereby ensuring that appropriate mitigation plans are in place to manage the risk.

Vodacom (2013) states that it reviews more than 4 000 operational, tactical and strategic

risks during a financial year. Vodacom (2015) further defines its critical strategic risks as:

- Regulatory decisions and changes in regulation;
- Increased competition;
- Unpredictable political, economic and legal risks;
- Major network and billing infrastructure failures;
- Complying with competition legislation;
- Customer privacy, and
- Consumer protection.

Similarly, according to MTN's integrated report (MTN, 2013) it is clear that risk management is an integral part of the organisation. The report states that *"MTN's objective is to instil greater risk awareness throughout the organisation; to standardise the approach to risk management and to embed the process into the day-to-day running of the business."* It further states that the organisation ensures that adequate efforts are made at all levels to ensure that risk management practices are instilled in the business across all MTN's operations. This ensures that information security risks, such as cyber security and data privacy, are proactively addressed. The top five risks facing MTN (2014) are similar to those identified by Vodacom (2015):

- Adverse regulatory changes or non-compliance with the laws and regulations;
- Creation and maintenance of a competitive advantage;
- Network performance;
- Financial performance targets, and
- Compromised information security.

Although both organisations have seen the impact of risk management and have put processes in place to ensure that these risks are mitigated, it is clear that the common themes underlying the risks are strategic and tactical. This leaves a huge gap covering operational and project-related risks. These project-related and operational risks can occur and could

potentially impact the organisation's strategy if they are not identified early and managed well. For example, a project-related risk occurred when a product manager made a decision to enable header enrichment of Vodacom uniform resource locator strings to enable a charge-to-bill service to work in a seamless manner. This development could have been seen as an enhancement to assist customers to interact with the service more efficiently, however the risks related to it were not taken into account. There was some negative media against Vodacom stating that they were passing on customer information in clear text (Fin24Tech, 2014). As these types of decisions never reach an executive board level, they are never tracked. Therefore, this 'small' change to the operational environment created a security vulnerability, which resulted in the leaking of many subscribers' information to the Internet.

2.2 Consumer landscape

More effective awareness is required to educate consumers about information security to change their behaviour (Bada *et al.*, 2015). Consumers do not always take their own privacy or security issues into account when dealing with large telecommunication companies. The assumption is made that customers have built trust in these organisations to ensure that their needs are sufficiently managed. The draft King IV (Institute of Directors in South Africa, 2016) states that trust can take a long time to build, however it can be lost very quickly. The draft King IV cites Rossouw & Van Vuuren (2001) who state that the loss of trust can threaten the organisation's licence to operate and could destroy intangible assets such as reputation. The draft King IV therefore stresses that organisations should engage more with stakeholders in new ways to build their trust and reputation.

Reviewing the scenario in 2013 where Blackberry announced that it was releasing BlackBerry Messenger (BBM) for the official Android and iPhone operating system platforms, there was a flood of rogue applications available on the official Android PlayStore[1]. Figure 2.1 is an example of the rogue blackberry applications on the Android PlayStore taken from an Android device in 2013. In the Apple iTunes store[2], which was more controlled through its development process (Apple Corporation, 2016), no evidence was found that these rogue applications were available to the general public.

[1]https://play.google.com/store
[2]http://www.apple.com/itunes/charts/

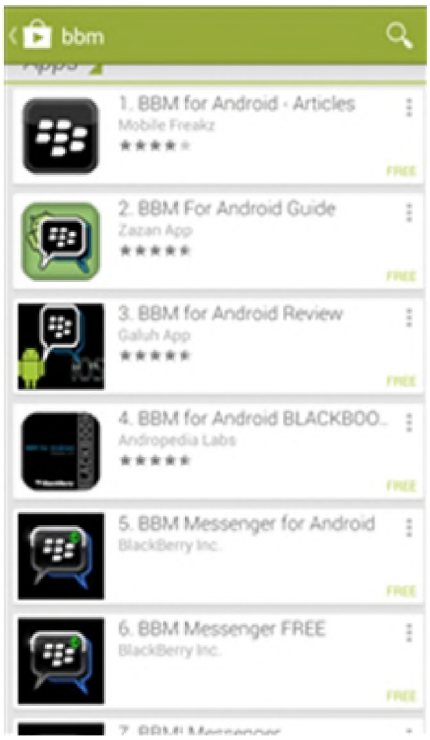

Figure 2.1: Screenshot from an Android device displaying rogue BBM applications

It could be investigated whether Apple gained more trust in its application store than Google did. Furthermore, did this phenomenon actually bother consumers or did they still continue to purchase and download from these service providers? Does trust in these service providers actually play a role in the decisions that customers make? Do the decisions that are made by telecommunication service providers actually influence customers to turn to other more trusted organisations or are they happy with the level of service they receive?

Another example of risks not being taken into account is from March 2013, where South African websites including Woolworths, Sasol and Postnet were hacked. Personal customer information was posted to websites such as pastebin.com (Swart *et al.*, 2013). There was some media coverage (Waqas, 2013, Selvan, 2013) of the data compromise but no evidence was found of the organisations informing their customers of this breach in security and there was no available information showing a financial or reputational damage to the organisations or any outcry from the affected consumers regarding their information leakage. This could however change in future when the South African information regulator is formed, as the POPI Act (The Republic of South Africa, 2013) requires organisations to disclose any breaches of their customers information, and further studies would be required to understand the South African consumers' understanding of the potential

impact to them of these types of data leakages.

There is a growing concern from consumers about the protection of their personal data that now exists on smartphones, including their bank account numbers, emails and contact numbers. Additionally, there are growing concerns by corporations as mobile devices and services have become an integrated part of their environment and are used to store or access company-sensitive information, such as customer records, intellectual property and the internal operations of the organisation (KPMG, 2013). KPMG states that trust will become a byword of the mobile era, because consumers will need to trust that telecommunication companies and service providers keep their data and information secure.

Vodacom operates in South Africa, Tanzania, the Democratic Republic of Congo, Mozambique and Lesotho and has a large customer base using similar types of technology (Vodacom, 2015). Vodacom is also part of a larger enterprise that is based in the United Kingdom (Vodafone). Vodafone operates in Europe, the Middle East, Africa, Asian Pacific and the United States (Vodacom, 2015). Based on the large footprint of Vodacom and that South African consumers use similar services and mobile devices to those available in the rest of the world, Vodacom could use the lessons learnt in different parts of the world to create more robust products. Similarly, MTN has a large footprint within the African market (MTN, 2014) and thus could collaborate and share their lessons learnt in these markets to develop 'risk-free' products and services.

2.3 Risks in application and service development

Telecommunication companies are currently branching out from traditional services of only telecommunication type services, into broader fields such as banking, insurance, education and health (MTN, 2014, Telkom, 2015, Vodacom, 2015) as seen from the creation of companies such as Telkom Business[3], MTN Banking[4] and Vodacom Mobile Money[5] and Vodacom Insurance company[6]. With this multifaceted product approach, the complexity of the business model increases. Business decisions therefore, need to be made promptly to ensure competitive advantage is either maintained or increased.

Benta *et al.* (2011) state that risk management should be proactive, because uncertainty is inevitable, as all projects are unique and temporary and are based on different assump-

[3]http://business.telkom.co.za
[4]https://www.mtn.co.za/everydayservices/usefulextras/Banking
[5]http://www.vodacom.co.za/vodacom/services/financial-solutions/m-pesa
[6]http://www.vodacom.co.za/vodacom/services/financial-solutions/insurance/insurance

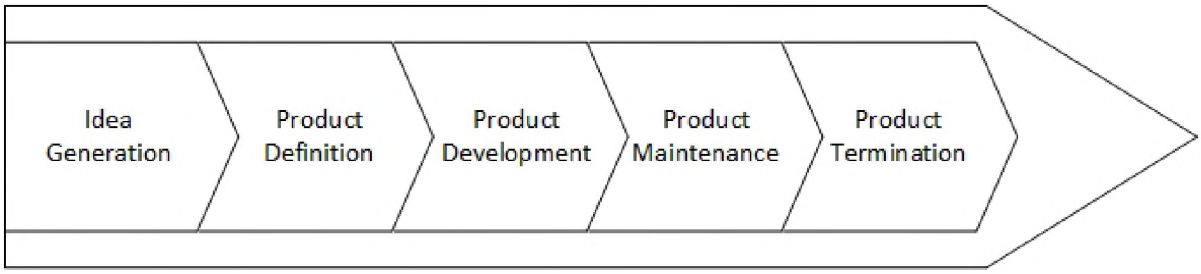

Figure 2.2: Generic product development model adapted from PMBOK (Project Management Institute, 2000) and Prince II (Office of Government Commerce, 2009)

tions and constraints. Project management is seen as an attempt to control the environment by implementing planning, cost control, task allocation and monitoring processes. Organisations use different project management approaches to implement products and services, such as PMBOK (Project Management Institute, 2000), PRINCE II (Office of Government Commerce, 2009) or in-house developed methodologies for a more structured approach.

A generic model for product development is shown in Figure 2.2. This would normally follow a structured approach ensuring that governance and robust projects are delivered to the market. Although the executive board would normally review high and critical risks for the organisation, there could be gaps or risks introduced at a more operational level or project level, which could impact on the organisation's strategic objectives.

2.3.1 Defining risk management

According to the International Organization for Standardization (ISO 31000) (International Standards Organisation, 2009), risk is the "effect of uncertainty on objectives" where an effect is a positive or negative deviation from what is expected. Risk management is defined as a set of coordinated activities or methods that are used to direct an organisation to control the risks it is facing, since these prevent the organisation from achieving its objectives. It is commonly accepted that risk management involves both the management of potentially adverse effects and the realisation of potential opportunities.

Risk management can also be described as the collection of deliberate actions and activities that organisations carry out at all levels to identify, understand and manage risks to achieve their objectives. When defining a risk, the product owner needs to look at the probability of the risk occurring and what the impact of the risk would be.

2.3.2 Risk management benefits

The benefits of embedding risk management at all levels of the company, as taken from ISO 31000 (International Standards Organisation, 2009) are:

- An increased likelihood of an organisation achieving its objectives;
- Proactive management is encouraged;
- An awareness of the need to identify and treat risk throughout the organisation is created;
- Improving the identification of opportunities and threats;
- Complying with relevant legal and regulatory requirements, both internationally and locally;
- Improved mandatory and voluntary reporting;
- Improved governance;
- Improved stakeholder confidence and trust;
- A reliable basis for decision-making and planning is established;
- Improved controls;
- Effective allocation and use of resources for risk treatment;
- Enhanced health and safety performance, as well as environmental protection;
- Improved loss prevention and incident management;
- Minimised losses;
- Improved organisation learning, and
- Improved organisation resilience.

Reviewing the benefits of good governance and risk management, it is important that organisations start embedding a structure for risk management from the onset. To ensure that corporate governance is part of the organisation's targets, it is very important that risk management is embedded within the PDLC of a business.

2.3.3 Risk management structure

For product risk management to be adopted by an organisation, a structured approach to enterprise risk management should already be in place. This enables buy-in for the risk program at all levels. (International Standards Organisation, 2009) states *"Risk management requires strong and sustained commitment by the management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels."*

Figure 2.3: Vodacom risk management structure (Vodacom, 2014)

As shown in the Vodacom risk management structure, Figure 2.3, risk management can be broken into five different areas:

- Strategic risk, which is managed by the chief officers and executive committee;
- Tactical risk, which is managed by the managing executives and group executives;
- Operational risk, which is managed by the executive heads of departments;
- Process risk which is managed by line management; and
- Project risk, which is managed by the project and product team.

The decision in the example of the header enrichment incident described in Section 2.1, was made at the project level by the product and project management team. The risks

associated with this project would not have been on the radar of the Vodacom BOD, with the result that a vulnerability could have been introduced into the organisation at a lower level in the structure, which could have impacted the strategic intent and objectives of the organisation.

According to ISO 31000 (International Standards Organisation, 2009), before the design and implementation of a framework for managing risk is considered, both the internal and external context of the organisation need to evaluated. The external context could include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment;
- Key drivers and trends affecting the objectives of the organisation;
- Relationships, perceptions and values of the external stakeholders.

When looking at the internal context, it should include, but is not limited to:

- The governance, organisational structures, roles and accountabilities of the organisation;
- Policies, objectives and strategies to meet the organisation's objectives;
- Capabilities, resources, knowledge;
- Information systems, information flows and decision-making processes;
- Relationships, perceptions and values of internal stakeholders.

To ensure that both the internal and external contexts of an organisation are understood while performing a risk assessment, ISO 31000 (International Standards Organisation, 2009) defines a model for risk management (Figure 2.4), which begins by ensuring that there is communication and consultation within the area of new product development. This implies the need for engagement with different stakeholders, including the customer, the organisation and shareholders to understand and communicate the risks related to the product.

The second step in the model is understanding the context to which the risk relates within the product development environment. The market in which the product will be sold needs

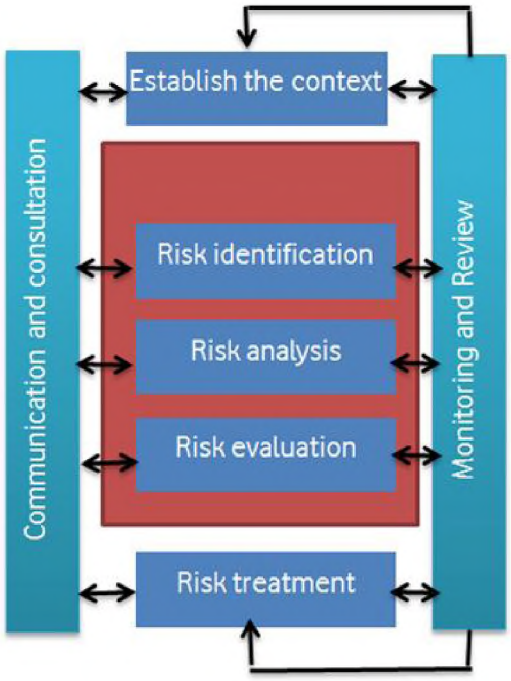

Figure 2.4: Risk management process (International Standards Organisation, 2009)

to be understood as well as what the objectives of the product are; what influence the product can have on other existing products; what the competition is currently doing and finally; what technology and platforms are used by the product or service. Only after these aspects, which have an impact on the service delivery of the product, are defined can a risk assessment be performed on the product.

Risk assessment consists of three main components:

- **Risk identification:** This is the process of finding out what the risks are that can impact the organisation, the different departments or the proposed product. Sources of risks can be internal or external or can be brought about by changes within the process, the organisation and systems.
- **Risk analysis:** This is the process of identifying the causes, the sources and contributing factors of the risks. It also involves looking at the consequences of the risk, what controls are currently in place to manage the risks and how effective these controls are.
- **Evaluation of the risks:** This component analysis the organisation's risk appetite and compares it to the assessment. If the risk is within the organisation's appetite,

it may be decided not to add additional controls for this risk. This process is one of the key processes of risk management, because it allows the organisation to make decisions based on the outcome of the risk analysis to define which risks are acceptable and where treatments would be required.

Once the risks have been evaluated, treatments or controls can be identified and implemented if the risk does not reside within the organisation's tolerance level. Throughout this process, there is constant monitoring, reviewing of the environment and consultation with both the internal and external parties.

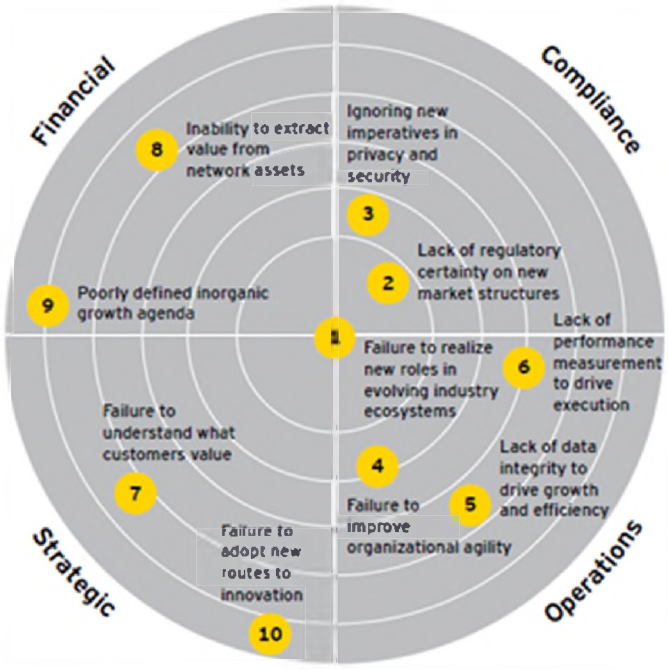

Figure 2.5: Top ten risks in 2014 for telecommunication organisations (Ernst & Young, 2014)

The top ten risks for telecommunication companies as identified by Ernst & Young (2014) are shown in Figure 2.5. There are four main quadrants: Compliance, Operations, Strategic and Financial. These four areas all have an impact on the development of products and services. Therefore, a failure or risk that is not managed can have a direct impact on the objectives of the organisation.

These four categories of risk are deconstructed into ten different categories shown in Table 2.1 and Figure 2.5.

These internal and external risks would be some of the key risks that telecommunication companies would have on either their strategic radar or on the tactical risk register. It is

Table 2.1: Top ten Ernst & Young risks for 2014 deconstructed

Category	**Risk**	**Definition of Risk**
All	Failure to realize new roles in evolving industry ecosystem	As a telecommunication organisation evolves, with new value propositions this creates new risks, within the telecommunication industry specifically; issues around OTT players has created new risk for the organisation, as well as the growth in financial services.
Compliance	Lack of regulatory certainty on new market structures	The telecommunication industries are changing and facing new challenges. Examples of some of these uncertainties are net neutrality and how to regulate OTT, additionally with new products such as mobile money, banking type legislation has now become a requirement. There is also no clarity regarding POPI and exactly what requirements should be put in place for compliance.
Compliance	Ignoring new imperatives to privacy and security	Within South Africa the POPI Act (The Republic of South Africa, 2013) has been passed into law; there has been wide spread media around the impact of this legislation. POPI brings with it a new risk category, for example, how do operators deal with big data, or marketing campaigns directed at specific customers.
Operational	Failure to improve organisation's agility	As the ecosystem within telecommunication organisations changes, and operators are moving from network-centric to customer facing models, changes in processes, which now need to be more simplified and streamlined, are required.
Operational	Lack of data integrity to drive growth and efficiency	As organisations are moving towards big data strategies, if the integrity of the information is questionable, this can affect the efficiencies and data growth strategies of the organisation.
Operational	Lack of performance measurements to drive execution	Without established internal metrics that can show progression in the organisation, or external metrics that can show financial and operational performance to show direction, this can impact the absence of accountability and what appropriate actions might be required to reach targets.
Strategic	Failure to adopt new routes to innovation	Telecommunication organisations need to ensure that they are on the forefront of technology. Normally telecommunication organisations would have the footprint and network to support different types of services; but how do they ensure that these different markets are sustainable with new innovations. The second issue relates to the skillsets required by organisations to maintain innovation.
Strategic	Failure to understand the customer	Organisations need to understand what the customer wants and then provide a service that is more relevant to the customer requirements.
Financial	Inability to extract value from network assets	Telecommunication organisations have started moving in the direction of sharing mobile networks or constructing fibre networks together; however they still need to try and maintain differentiated services.
Financial	Poorly defined inorganic growth agenda	What used to be the core service of telecommunication organisation a few years back, could be moving to non-core type service as the telecommunication environment grows. New partners and new services have changed the market.

important, therefore, that risk management becomes more structured and that a culture of risk management is introduced throughout an organisation. This will ensure that each employee understands his/her role and the potential impact of not implementing controls.

2.4 Trust within telecommunication organisations

In 2011, Vodacom stated in its integrated report that its three operational principles would be speed, simplicity and trust (Vodacom, 2011). This declaration shows that telecommunication companies, such as Vodacom, understand that trust is one of the main factors required to ensure market leadership and excellent service to the customer.

Trust is defined from the consumer's viewpoint as the perception of the degree to which an exchange partner will fulfil its transactional obligation in situations characterised by risk or uncertainty (Joubert & Van Bell, 2013). Trust is important in risky situations to which the customer may be exposed by the telecommunication organisations. According to Joubert & Van Bell (2013), South African consumers are often not aware of who the vendors or third-parties are that are accountable for delivering the service and therefore the consumer is not sure whom to trust. Due to skill shortages in the development of non-traditional telecommunication services, organisations are using various third-parties when they develop products and services.

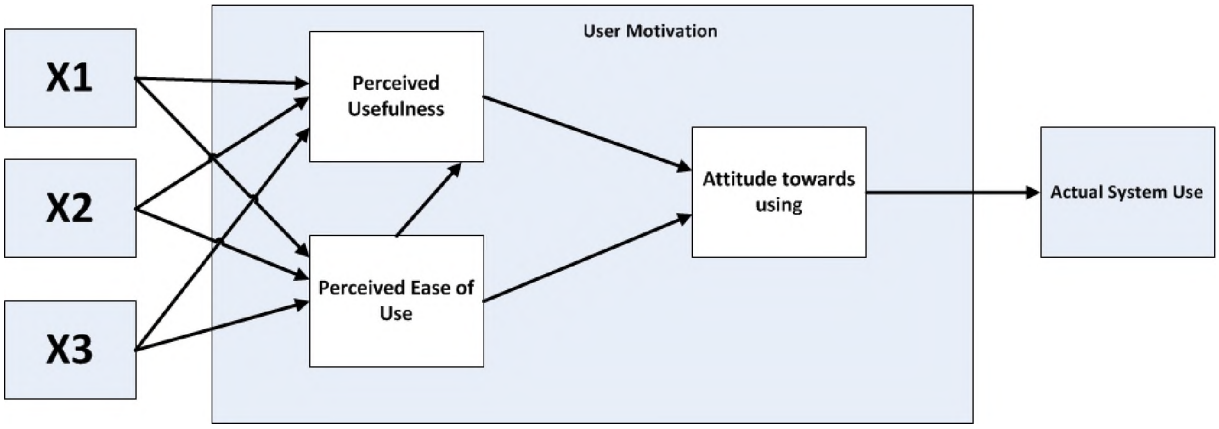

Figure 2.6: Perceived usefulness of a product or service (Davis, 1989)

From the model in Figure 2.6, we can see that trust is initially established by the user's perception of the risk of the service, the usefulness of the service and its ease of use. It is therefore important that organisations understand the customer's requirements during the conceptualisation of the product to ensure the intended results are achieved. This

would in turn ensure that the product or service aligns with the organisation's strategic objectives.

In the comprehensive literature review undertaken by Rousseau *et al.* (1998) it is clearly shown that, regardless of the authors, the two main components of trust are confident expectation and a willingness to be vulnerable. Mayer & Gavin (1995) summarise trust as *"The willingness of a party to be vulnerable to the action of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that party"*. This means that the "trustor" makes himself/herself vulnerable, which could result in something important being lost as a result of the relationship.

Akbar & Parvez (2009) discuss the telecommunication industry in Bangladesh, where there are six different telecommunication companies. South Africa has a similar marketplace with six telecommunication organisations (four mobile and two fixed-line operators). In Bangladesh, the high number of service providers has resulted in aggressive competition in the market, which has forced the telecommunication operators to change their strategies and business models with the aim of sustaining or improving their respective competitive advantages. Due to the emerging market in Bangladesh not being particularly loyal to a specific company, organisations need to establish a loyal customer base. Akbar & Parvez (2009) further state that telecommunication companies are now looking at different antecedents such as service quality, switching, cost, trust, corporate image and customer satisfaction to maintain their customer base and keep the customers loyal.

In South Africa, this scenario holds true as well, because at any given time there are a large number of promotional offers from different organisations with the aim of gaining customer loyalty. For years Vodacom has been announcing that it has the best cellular network in South Africa (Mybroadband, 2015). On the other hand MTN (2014) advertised that it would pursue a customer experience strategy called "Perfect 10" which would require an investment of R8 billion. This shows that MTN has become responsive to this type of conduct, and this is one of the controls it has implemented to ensure that customers can trust the brand.

Organisations therefore understand that to sustain the business, they need to ensure that consumers trust them. However, to understand trust, organisations need to be aware of the three characteristics on which trust is built, as discussed by Mayer *et al.* (1995):

Ability can be described as someone's competence or expertise in making good decisions. For telecommunication organisations, the customer must make the choice of who they

believe has the ability not only to deliver a service, but also to protect their information, because customers are continuously giving these organisations more and more control over their data, their service and their billing and privacy information. To maintain this trust from the customers, a proper governance program is required from the organisation.

Benevolence is the attitude or intent of the organisation to show customers that they can be trusted. MTN's integrated report (2014) stated that the corporation's reputation has come under scrutiny with regard to corporate governance over the past few months. MTN has now confirmed that it includes responsive corporate governance issues. By doing so, MTN is trying to ensure that customers can aspire to the trusted brand. Similarly, Vodacom (2011), with its three principles (speed, simplify and trust), is trying to show customers that telecommunication organisations do focus on having good governance structures in place so that customers can trust the brand.

Integrity is defined by Mayer *et al.* (1995) as the decision-maker's belief that the party it is contracting with adheres to a set of principles that the trustor finds acceptable. In other words, integrity deals with showing the customer that the organisation is devoted to the customer, that it does protect customer information, that it does deliver products as intended and that the organisation acts in a manner that allows the customer to trust it.

Morgan & Hunt (1994) state that trust can only exist when one party has confidence in the other party's reliability and integrity. Therefore, it is integral that telecommunication organisations gain customers' trust and confidence if they want to remain sustainable in a highly competitive market. Practically, this means that within the products and services development lifecycle, telecommunication organisations can no longer deploy products that have not been tested. Moreover they can no longer deal with third-parties if they have not ensured that those third-parties can offer the same level of trust. Furthermore, with the deployment of new types of services, such as insurance, m-health, education or mobile money, telecommunication companies now need to establish a deeper level of trust with the customers, as is the case with banking institutions.

2.5 Analysing customer adoption and trust

It is important to understand trust from a consumers' perspective, as this guides the consumers spend on specific products or brands. Organisations need to embrace the trusted approach to sustain their brand.

2.5.1 Definition of customer trust

Consumers' trust levels are declining according to Ernst & Young (2014), as regulators are implementing stricter guidelines for data protection. Due to the spotlight on data protection and privacy, there are many more headline articles related to telecommunication companies and data privacy. In Figure 2.7, the declining trend in trust is clear.

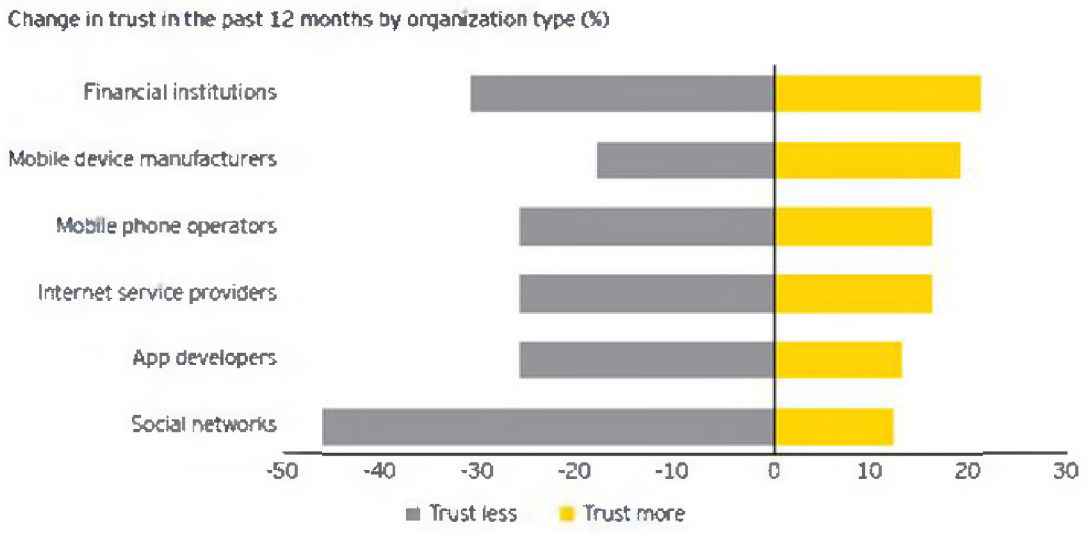

Figure 2.7: Changes in consumers' trust levels in organisations (Ernst & Young, 2014)

IBM (2011) states that executives have been using phrases such as "customer first" for years, and now, due to the fact that communication service providers are investing heavily in loyalty and customer satisfaction programs to increase advocacy, it rings even truer. Putting the customer first is mainly a focus, because by maintaining customers for longer and by their purchasing of more services, the company tends to generate more profit. Organisations are also measuring the "Word of Mouth" aspect of customer satisfaction, because customers will inform their friends about both the positive and negative experiences they have with an organisation. Although the data provided in Figure 2.7 shows that the level of trust in mobile operators is declining, trust levels in social networks and financial institutions are declining even faster. Large organisations such as Vodacom use metrics such as net promotor score (NPS) to measure customer satisfaction; these values are given in the integrated reports (Vodacom, 2014).

IBM (2011) goes further to state that for organisations to strengthen customer advocacy and drive growth they need to:

- Improve customer experience insights by focusing on attributes that drive customer

advocacy;

- Apply a social behaviour-driven perspective and become part of a two-way dialogue with consumers;
- Profile and target customers' advocacy segments to improve advocacy levels;
- Build multilevel capabilities to support an approach to customer advocacy.

2.5.2 User acceptance model

The technology acceptance model from Davis (1989), as adapted from the theory of reasoned action, has been tailored for modelling user acceptance of information systems. This model uses three factors to explain users' motivations in using an application. These factors are: the perception of ease of use, the perceived usefulness and the user's attitude towards using the application or system, as shown in Figure 2.6.

Davis (1989) state that the attitude of a user influences whether they use or reject a system, which in turn is determined by the perceived ease of use as well as the perceived usefulness of the system. Other factors such as beliefs and motivations to comply were later added to the model. From Figure 2.6, it is clear that customers need to perceive the product or service as useful and easy-to-use, which will then motivate them to either continue using the system or discard the product or service.

Akbar & Parvez (2009) define satisfaction as the customer's evaluation of the product or service as to whether that product or service has met their needs and expectations. If the satisfaction is positive the customer will appraise the relationship of the organisation, which allows for better user acceptance. They further state that customer loyalty comprises two factors, attitude and behaviours. This can be seen by the customer's willingness to repurchase a product or service, recommend the product and service to another party, or remain loyal to the organisation. They state that there is a correlation between service quality and customer satisfaction and the stronger the relationship between service quality and customer satisfaction is, the more loyal the customer will remain to the organisation. Corbitt *et al.* (2003) support this by stating that consumer trust increases the willingness of prospective customers in using the service. Chen *et al.* (2008) mention four heightened perceived risks when it comes to telecommunication organisations:

- Publicity of data losses from telecommunication companies;

- Personal experience with identity theft or misplaced records by the organisation;
- Users suffering harm from products, such as location-based type services;
- The risk of exposure due to the nature of the search performed by the user.

To ensure that a telecommunication company does not lose its customers' trust, it is very important that the organisations in South Africa create an environment in which customers see the organisations' products as trustworthy and that the applications have sufficient quality to support the customers' needs and satisfaction. Processes therefore need to be developed to ensure that all the products that are launched by these service providers go through a series of tests and that they are reviewed by the legal, regulatory and fraud departments to finally ensure that customers are provided with the best experience when using the product.

2.5.3 Success criteria for projects

A high percentage of new products fail because organisations are forced to accept increased risks to achieve the desired returns, which is further aggravated by the increased focus on cost containment, increased demands and an overburdened workforce (Gartner, 2013). It is therefore essential to ensure that new products and services improve the organisation's strategic goals. This can be achieved by ensuring that only robust and non-risk impacting projects are launched into the market. Gartner (2013) goes further to state that organisations should accept higher failure rates using the "fail-forward-fast" method, which identifies products that might fail early in the PDLC process.

According to Gartner (2013), eight common factors are required for successful products, as defined in Table 2.2.

Davis (2002) states that product development is viewed as secondary to research in the technology industry, however product development is of strategic importance to the commercialisation of investments in the organisation. New product development can therefore predict the organisation's future. He goes further to state that robust product-development processes can make inherent risks in projects more understandable and therefore they can be mitigated or controlled better. The key effort in product development is the state-gate process where ideas are evaluated during the different lifecycles of the projects.

Table 2.2: Factors for successful products from Gartner (2013)

Upfront requirements	This is to ensure that teams spend more time, resources and effort on projects upfront which creates better projects.
Customer requirements	To ensure that products have the success rate required, the organisation should understand the market needs and try and fill the gaps.
Product advantage	The organisation needs to ensure that its product has a differentiation element and superior product offering to gain unique customer benefits, thereby increasing market share.
Stable products	An organisation needs to define the product requirements and features upfront and ensure that the product delivers on these requirements in a stable environment.
Resources and market launch	The organisation must ensure that there is a strong market launch behind a successful and tested product so that customers are aware of it, in order to drive execution.
Kill decision points	There needs to be decision points throughout the PDLC which will only allow products with the required success rates to be launched. Substandard products or products for which the market is not ready should not be launched at all, or should be put on hold.
Cross-functional product teams	To ensure products are successful, cross-functional teams need to work together. The organisation should move away from the silo approach early in the project to ensure that all teams work smoothly together.
Process and discipline	Not following proper processes, or trying to shortcut processes often leads to project failure as certain stakeholders sometimes get involved in the project too late, or it is revealed later that a shortcut process does not work as intended.

Davis goes on to divide product portfolios into four different categories. These categories can be used to determine the risk of the product, which in turn can determine the chances of success in each category of the project.

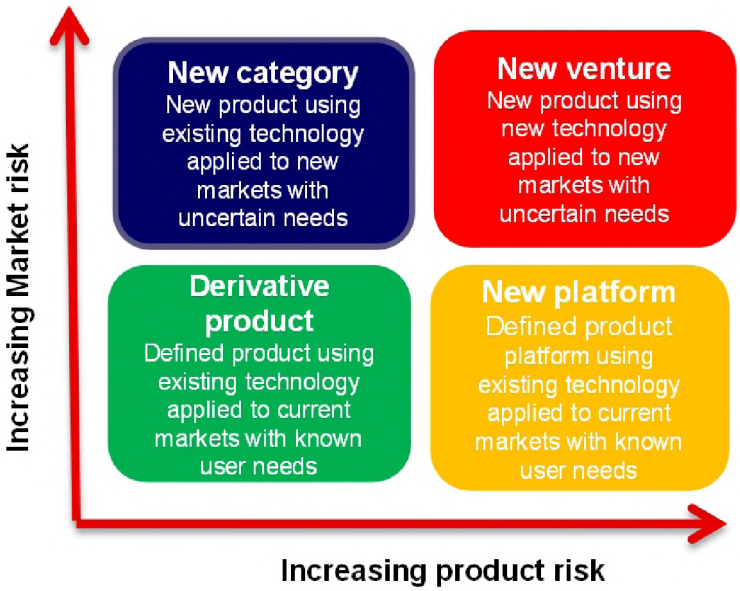

Figure 2.8: Product categories adapted from Davis (2002)

As seen in Figure 2.8, the four categories are defined as:

- **New ventures** - These types of projects are undertaken when the organisation is creating a new market outside the current market base where the project uses new technology, new processes and is radically innovative. Within this field, the organisation is using new technologies that are applied to new markets with uncertain needs. Examples of these types of projects in the South African telecommunication industry are mobile health, financial services and insurance.

- **New categories** - These types of projects are new to the company. They target an established market in which the organisation does not yet compete. This would be when the organisation has new products using existing technology, but they are applied to new markets with unknown needs. An example of this type would be when the organisation start selling technology such as cloud services for backing up customer devices.

- **New platforms** - This is where the organisation uses existing product platforms and existing technology as an addition to existing product offerings, targeting a

current market with known needs. These are deviations on products, for example when the market knowledge improves and the organisation needs to start improving its product offering. An example of this type would be when Vodacom started offering services such as airtime advance[7], which basically allows prepaid and top-up customers to "borrow" funds from the organisation and the money would be recuperated when the user recharged.

- **Derivative products** - These products use existing technology, and target existing markets. These are basically derivatives of or improvements on existing products. An example of these would be changes in tariffs, such as reducing roaming rates or data prices.

It is clear that the less an organisation knows about the technology, the product or the market, the more complex the project risk becomes. One of the examples given by Davis (2002) is when technology organisations launch new products. The product managers often get caught up in the technological detail and forget or fail to understand the user requirements or the market needs. Similarly, for commercial products, the users' needs and market strategy are well understood, however, due to the technical requirements, the product is unsatisfactory.

2.6 Maturity model for risk management in a PDLC environment

Organisations need time to change their culture. Ogbonne & Harris (2000) state that culture is both dynamic and difficult to change and that cultural change can take time to implement. Smircich (1983) debates whether culture is something an organisation "has" or something an organisation "is". If culture is something that an organisation owns, then it can be manipulated or changed to improve the effectiveness or efficiency of the organisation. However, if the culture is the organisation, it implies it can be created and recreated in a process that is continuous.

Changing the way organisations should manage risk on projects cannot simply be implemented by developing a model, getting the project management office to implement it and expecting it to work. Jose (2013) states that many organisations have tried to

[7]http://www.vodacombusiness.co.za/mobile/main/services/airtimeadvance

integrate risk management into their business practices, with different degrees of success, and they have not always achieved the full benefits of risk management practices. He goes further to support the idea that organisations should use risk maturity models to benchmark their approach against a standard level of maturity and from there, it can outline the activities required to move to the next level. A structured approach needs to be followed to ensure that the risk management models are accepted, similar to the process of product adoption depicted in Figure 2.6 and discussed in Section 2.5.2, where the product developers need to build trust in the model and see the benefits of using a risk-based approach. It is important, therefore, that a specific approach is followed for the implementation of a project risk framework within large organisations, including most of the telecommunication companies in South Africa.

Yeo & Ren (2014) define a maturity model for risk management in complex projects by looking at two layers, security and organisational "robustness". They build this model on a change management framework that considers risk planning, control processes, organisation, people and technology. The maturity model (Tables A.1, A2, A3, A.4 and A5) ensures that organisations first perform a self-control assessment of the environment to see how mature they are in the processes with regard to product risk management. This allows the organisation to use the model to identify gaps, which can be used as a roadmap for the organisation to set out improvement strategies to enhance the PDLC process.

The model (Yeo & Ren, 2014) has five levels of maturity, based on the capability maturity model (CMM) model for software (Paulk *et al.*, 1993). These levels of maturity are defined by Yeo & Ren (2014) and have been adapted within this report for a telecommunication product approach:

- **Level 1: Initial** - The process is categorised as ad hoc and sometimes chaotic. The organisation is not aware that it requires risk management and there is no structure to deal with risks. No effort has been made to identify project risks and product developers are more focused on getting products to market. The adoption of fixing issues is reactive and it is assumed that issues will take care of themselves. There are few mechanisms in place to get feedback on product issues and no way of dealing with the identified issues. The success of a project normally relies on an individual's efforts.

- **Level 2: Repeatable** - There is some level of basic risk management activities in the organisation's product management process. The organisation is aware of the potential benefits of risk management. High-level processes and risk management

policies to deal with tactical and strategic risk management have been defined, however the implementation of risk management is still lacking at a project management level. Based on the latest integrated reports for telecommunication organisations in South Africa (MTN, 2014, Telkom, 2015, Vodacom, 2015), we can see that the organisations have adopted a risk management approach, because they do report on strategic risk. However, it cannot be assumed that organisations have adopted a robust approach embedding risk management in the lower levels of the organisation or that project risk management has been included in the PDLC process.

- **Level 3: Defined** - At this level the organisation should have a formal risk management system in place which is incorporated into the product management process. The benefits of product risk management are understood by most of the higher-level management of the organisation. Risk ownership has been defined and there are risk management awareness training programs available in the organisation.

  Product managers are aware of their responsibilities for the management and mitigation of risk on their products. However due to time-to-market and other pressures, there is still a level of risk in terms of the degree of skill that goes unmanaged in the organisation.

- **Level 4: Managed** - At this level of maturity, processes and goals are established for each risk management process (including identification, assessment and response). The impact and likelihood of the risk are measured qualitatively. Detailed response strategies have been created and documented and risk mitigation outcomes and performance analysed.

  Furthermore, risk management is extended to include key stakeholders (both internal and external) within the PDLC. The organisation has a well-established risk-awareness mind-set and adopts a proactive approach to the management of risk. There are well-defined processes in place to instil robust structures and mechanisms to cope with complex tasks and emerging risks.

- **Level 5: Optimal** - The organisation has a comprehensive risk management plan in place, which includes both qualitative and quantitative ways to measure risk. There are continuous innovation and improvement processes to increase the level of risk management, which has become a norm in the product management lifecycle. The corporate culture and behaviour is that of corporate governance, which guides the corporation's rules to deal with unforeseen emerging risks. There are opportunities where project-related risks are discussed by senior level management allowing key informed decisions to be made. A supportive culture exists that allows

free communication and the escalation of identified risk, business alignment between project risk and project objectives, teamwork and the identification of innovative ideas and an appreciation to explore new technologies or methodologies.

To define the steps for a robust risk management approach for products and services, the following approach can be used by an organisation to perform a self-assessment to define its own level of maturity with regard to product and service risk management. The approach consists of four different levels: general risk management, people and culture, process requirements and processes and technology requirements.

Based on the definition of general risk management, as shown in Tables A.1 and A.2, it is important to understand the culture of the organisation. In the traditional telecommunication structure, which deals particularly with voice-type services, processes are usually well-known and defined as voice services have been in the market for years. Furthermore, changes to these services would either be synchronised with upgrades of technology, the network or changes in prices. However, with telecommunication organisations branching out into new fields such as insurance, mobile money or enterprise services (e.g. cloud, security or hosting services), the skillsets to implement and identify risk management are not always part of the processes.

In the people and culture definition (Table A.3) the approach that management uses, as well as the level of support for entrenching risk management into the PDLC, is considered. As shown in the previous category, skill levels are not always at an optimal level to ensure that risks are identified. Traditional processes do not cater for new types of services and therefore the organisation needs to adapt its approach to product development. At an ad hoc level, senior management does not support the process of risk management and can be seen making decisions that might not support the governance objectives of the organisation. However, as the process moves to a more mature level, senior management starts to understand the requirements of good corporate governance within the organisation's processes, especially when it comes to products and services, and it eventually ensures that the processes support risk. This also allows senior management to make better decisions when driving product delivery.

With regard to process requirements (Table A.4) it is clear that one cannot simply entrench risk management into the PDLC methodology, because there will be forces within the organisation that will resist the inclusion of risk. Implementing risk management has to be done step-by-step. Table A.5 shows that during the initial phases of implementing a risk management framework where simple products are developed, a risk management

system is not required. However, as the organisation moves up the capability maturity curve, it requires more advanced and innovative technology for effective risk management.

2.7 Risk assessment approaches in other industries

A literature search was conducted to review current risk management practices in other industries. Three international organisations were selected to evaluate any commonality and best practices with respect to product development approaches.

2.7.1 Tomkins group risk assessment process

Risk Visualization Tools (n.d.) performed a case study on the Tomkins Group[8]. Tomkins distribute automotive products, industrial power systems, plumbing components and construction products. They operate in 15 countries with over 52 000 employees.

Tomkins needed to ensure that the product sponsors of their investments portfolios considered risk management while designing their distribution processes. Tomkins' risk department created a potential risk factor checklist (Table 2.3) to understand the success and risk related to a project. Each project sponsor had to rate the risk which could impact their business unit, and this was used as an indicator of potential project success or failure. By balancing and aggregating the risk weights across the different product initiatives, the executive management were then able to balance a uniformed standard of risk.

This approach allows project sponsors to easily identify the different initiatives and then prioritise which product would be easier for the organisation to take on, as well as potentially identifying the success of the project.

The gap within this process is that this is discussed at a strategic level for the organisation, and the reliance on ensuring governance therefore resides with the project sponsor to ensure that governance processes are implemented at the more operational level of the project.

[8]http://www.thetompkinsgroup.com/

Table 2.3: Tomkins project risk assessment checklist

Investment risk issue	**Applicability score (No=0, Yes=1)**	**Strategic Weight**	**Risk weight (applicability score X strategic weighting**
Are you launching a new product?	1	10	10
Are you entering a new market?	1	9	0
Are you targeting a new customer segment?	0	5	0
Will you be using a new supplier/product base?	1	8	8
Will there be dependency on few large customers?	0	8	0
Is the target market highly competitive?	1	1	1
Is the competitive reaction anticipated to be vigorous?	0	2	0
Will you be using new technology?	1	5	5
Are there material regulatory issues with product or process	0	6	0
Are there any unusual health/safety requirements?	1	8	8
Are the time constraints for the project too tight?	0	5	0
Are the manpower constraints for the project too tight?	0	4	0
Is the success of this project dependent on the success of other projects?	1	3	3
Is the access to quality information or third-party verification low?	1	7	7

2.7.2 AMD risk assessment approach

AMD[9] manufactures high-performance computing, graphics and visualisation technologies, which is used mostly for gaming, datacentres and immersive platforms. They are one of the leading Fortune 500 companies with the vision of pushing boundaries where possible.

AMD moved their risk assessment to the internal audit function and performs their risk assessment with their organisation BOD and chairperson of the board to identify gaps. These identified risks are then presented to the audit committee and BOD (Corporate Executive Board, n.d.). Based on the integrated report of AMD (2015), the key themes of the risks were extracted and shown in Table 2.4.

Table 2.4: Examples of AMD top risks

Competition	Reliance on third-parties	Failure to achieve manufacturing yields
Timely delivery of products	Revenue and operating cash flow	Information and Customer loss
Global Economic uncertainty	Debt obligation	Government legislation
Logistics	Market conditions	Staff risk
Data breach and cyber-attacks	Material availability	Product compatibility
Currency fluctuation	Grey market products	Retention of intellectual property

The risk as shown in Table 2.4 for AMD relates to some aspects of product development, such as product compatibility, market conditions, logistics, data breach and cyber-attacks. These risk are presented to the audit committee and the organisations BOD. No information relating to how this is managed on specific projects was publicly available.

2.7.3 Magnolia bank risk approach

A case study was performed by Operational Council Research (2007) on Magnolia Bank operating in the United States which has more than USD50 billion in assets and provide a wide range of financial services to both individuals and businesses. They stated that there was a lack of accountability to drive development of the operational risk strategy, and

[9]http://www.amd.com/en-us

they had a series of parallel, uncoordinated and business unit specific risk management programs. This meant that risk which significantly affected the company could not be captured, assessed and escalated to the correct individual or group.

The approach Magnolia Bank took was to appoint individuals in each business unit to look at nine categories of risk. This was then discussed at a weekly business unit risk management meeting, looking at the common challenges across the business units, prioritising the risk management focus, ensuring cross-silo communication and decision-making and ultimately holding the business unit executive managers accountable for their risks.

Magnolia Bank focused on nine risk categories as shown in Table 2.5.

Table 2.5: Magnolia bank priority risks

Information Security	Fraud risk	Product risk
Compliance	Business continuity	Sarbanes-Oxley
Vendor management	Model risk	Human resource risk

The case study showed that in under a year, Magnolia Bank was able to establish a working relationship between business unit risk managers and risk owners, which allowed for their risk principles to be rolled out consistently throughout the organisation. The business units risk managers were viewed as trusted advisers on strategic initiatives and this structure furthermore allowed for rapid escalation and resolution of issues on processes and policy variances.

Magnolia Bank ensured that there was accountability for risk within the different departments within the organisation. Furthermore with weekly meetings between risk champions in the business, this allowed for a more mature risk culture. The downside for Magnolia Bank, however, is that they have defined their risk categories too specifically, which could lead them to missing out on certain opportunities or risks which the organisation could face.

2.8 Summary

In this chapter generic implementation models used by organisations when developing products and services were discussed. The risk management standard (ISO 31000) was explored, showing the benefits of using a risk management approach when designing products. Furthermore, the chapter provided guidance with regard to the top ten risks

for telecommunication organisations, thereby setting the basis for the risk framework discussed in Chapter 5.

To ensure that the process of risk management in product development is adopted, a step-by-step approach should be followed in order to get buy-in from senior management at the beginning. Managerial buy-in can be gained by ensuring that they are aware of the following requirements:

- The requirements for governance within an organisation from a legislative perspective;
- The benefits of ensuring that issues are identified upfront to ensure that these issues do not surface later in the project process, which could create additional delays;
- The cost-benefit analysis.

With regard to the maturity models listed in Appendix A, the best approach would be first to perform a benchmark exercise to identify the current maturity level within the organisation. The model can then be used as a roadmap and action plan to identify which other requirements are needed to move the organisation into a more acceptable risk management and governance compliancy.

Section 2.7 shows that there are different approachs to the managiment of risk on new products. Tomkins implemented a checklist, Magnolia bank created a risk process which allows different business units to communicate with each other, and AMD moved their risk function to the internal audit department.

Chapter 3

RESEARCH DESIGN

This chapter describes the research approach and strategy that was taken to collect the data required to analyse risk in the organisation and how the framework was developed. The essence of this chapter is the discussion of the process used to obtain the data, both qualitative and quantitative, and how these data sets were used. Crucial to this process is the explanation of how the sample was explanation of how the sample was selected and the validity issues evident with the design strategy.

Furthermore this chapter also describes the data requirements and strategy that was followed after the design of the proposed risk framework to evaluate its effectiveness and proposed implementation.

3.1 The research strategy

In order to design a risk framework for products and services, the first requirement was to benchmark the organisation and to identify what the perceived concerns were that the organisation was facing while trying to develop robust products. The research strategy adopted only considered the organisation's perceived internal issues and excluded customers' perceived concerns and risks.

Babbie & Mouton (2008) state that there are three requirements for causal research. Firstly, the cause has to precede the effect in time. Secondly, the variables need to be empirically correlated with one another, although they further state that this is a difficult requirement to meet, because there are only a few perfect correlations. The final

requirement is that the causal relationship between the two variables cannot be explained by a third variable that causes both of them.

Coldwell & Herbst (2004) state that research is important in that it reduces uncertainty by providing information that improves the decision-making process. This research took an exploratory research approach. The research to build the framework used both quantitative and qualitative approaches to use a three point validation for the collected data to ensure that the data were reliable and valid. Coldwell & Herbst (2004) however go further to explain that exploratory research involves research where particular relations exist, but the relations do not warrant a full-scale study until more clarity is gained. Babbie & Mouton (2008) agree by saying that exploratory research explores the topic and is generally undertaken when the subject is relatively new.

For the purposes of this research, an exploratory approach was used, because it was not certain that variable A (using a risk-based approach for products and services) has an effect on variable B (building trust in the organisation) as shown in Figure 3.1. Without knowing the effects of variable C (such as competitor marketplace, level of education or adoption of new technology and the different social standings of the customer) a causal research approach could not be used.

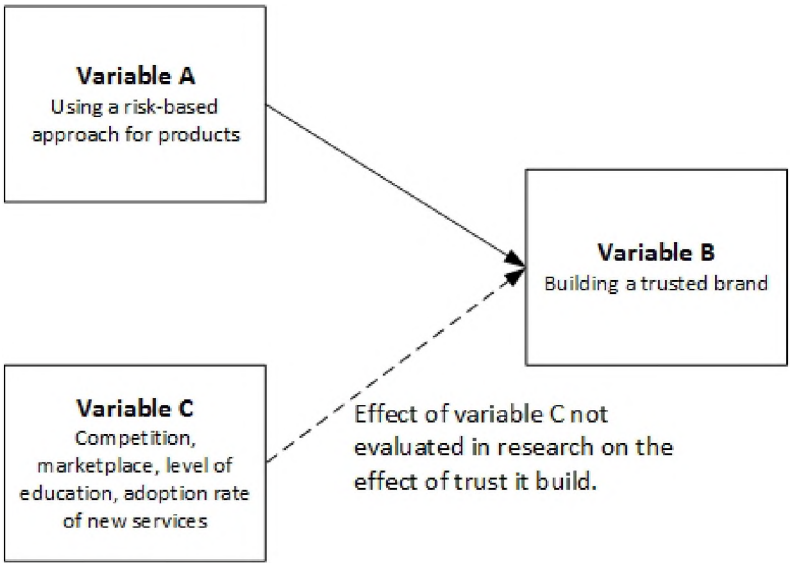

Figure 3.1: Description of causal research

As this research used both qualitative and quantitative data, the data collection methods created three point validation between the methods to ensure that the data were reliable and valid. The literature review and the collected data, over three different periods, allowed for a more robust framework for risk management to be designed. This is explained

in more detail in Chapter 5.

As discussed in Section 1.5 for the scope of the research, the framework developed was not implemented in the organisation due to the long lead-time that is required to change an organisation's culture and to get sufficient adoption for risk management. Instead, a qualitative approach was used where a number of subject matter experts were selected, based on their experience within different aspects of the PDLC, to provide their views and opinions on what the impact of the framework could possibly be and how they believed the framework should change to include their suggestions.

Table 3.1: Data collection assumptions

Assumption 1	The data collected on the risks telecommunication organisations are facing were collected from one mobile telecommunication organisation over a three-year period. It is assumed that this data reflects the population of telecommunication operators in South Africa. This assumption was based on the fact that when reviewing the different operators' integrated reports (MTN, 2014, Telkom, 2015, Vodacom, 2015), it is clear that the organisations launch similar types of products and face similar types of strategic risks. However, the level of management of the risks within the different organisations might differ.
Assumption 2	The respondents responded in a truthful manner to ensure the validity of the data. This is based on the fact that all the data collection was done in person and the assumptions that were made by the respondents were questioned to ensure that the data were reliable. The sample sizes in 2012 were larger and a total of 130 participants were interviewed, which ensured a small margin of invalidity.
Assumption 3	Due to time constraints, only the interviewees who made themselves available were interviewed. Meetings were set up with the candidates to ensure that they were available and that they had sufficient time to answer either the qualitative or the quantitative questions.
Assumption 4	The data collected from the managing executive, executive heads of departments and senior managers reflected the views of the staff who reported to them. This assumption is based on the fact that the leaders of the departments should have an understanding of the current issues faced by these departments. Based on this assumption, for the data collection period in 2015, only executive heads and managing executives were interviewed, because in the data collection period of 2012, most of the individuals in a specific department had similar views to their seniors.

3.2 Data sampling and population

Charlesworth *et al.* (2003) state that researchers must ensure that the sample selected for a study represents the entire population, especially if they want their research to

have a level of integrity or to be of any use. De Vaus (2001) states that if a sufficiently representative sample from the population is not collected, the researcher runs the risk of getting biased results. He goes further to state that the sample size depends on two key factors: the degree of accuracy required from the sample, and the extent to which there is a variation in the population with regard to the key characteristic of the study. Coldwell & Herbst (2004) describe the sample as a group of individual persons, objects or items from the population from which samples are taken for measurement.

In South Africa there are six telecommunication organisations (two fixed-line companies and four mobile operators). To ensure that the data obtained reflects the South African telecommunication organisations population, the assumptions documented in Table 3.1 regarding sample sizes were upheld.

3.3 Data collection

Data were collected in different ways over three different time periods (Figure 3.2) to understand the perceptions of both technical and commercial lower level staff as well as those of executive and higher-level management. See Table 3.2 for details. Analysis of these three datasets assisted in the design of the proposed framework.

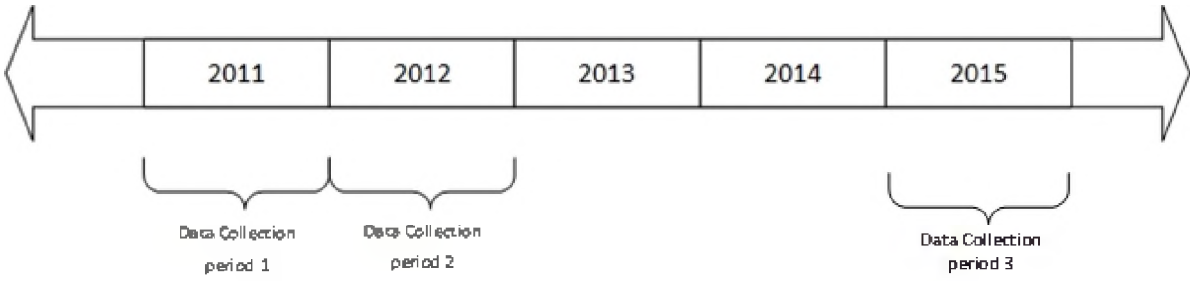

Figure 3.2: Data collection timeline

For the first data collection period in 2011, ten products were selected and stakeholders who assisted in the implementation of these products were identified. In the second period (2012), quantitative research probability sampling was used. Product managers and stakeholders who would normally be involved in the launch of any new product in the organisation were interviewed. Coldwell & Herbst (2004) define this as a method that ensures that every participant in the sample has an equal chance of being selected.

During the third data collection period in 2015, a qualitative research method that used the snowball sampling approach was used. Coldwell & Herbst (2004) describe this approach as identifying interesting people who know other people who would be good examples for the study or make good interview subjects. Initial interviewees at an executive level in the organisation were selected based on their involvement in the launch of products; they then provided additional candidates to be interviewed.

Table 3.2: Candidate list over the three periods

	Period 1 - 2011	**Period 2 - 2012**	**Period 3 - 2015**
Number of candidates	15	130	17
Sample selection was based on candidates who had been involved in the PDLC process	Product managers, technical	Product managers, Technical staff, Regulatory, Legal, Risk management, Online development, Customer experience, Billing, Information technology (IT), Engineering, Project management, Commercial teams	Executives and Managing executives from Product management, Product management, Technical departments

3.3.1 Data collection period 2011

In the first data collection period (2011), ten perceived high-risk products were selected and the product owners were provided with a structured survey that required them to rate their perceived risk on the product via a Likert scale. Candidates were interviewed in person while completing the survey and a section was also provided for any additional comments not covered by the survey questions. The participants were assigned sequential numbers that were added to the interview list to ensure that the sample was complete and that no questionnaire was omitted, while also providing a level of confidentiality. See Appendix B for the detail of this survey.

The ten projects which were selected were based on the impact which it had on the organisation, either reputations, or that had an influence (either positive or negative)

on the organisation's financial balance sheet. The fifteen stakeholders selected had to complete the questionnaire in Appendix B.

The data collected in 2011 were used to establish a baseline of where the organisation was with regard to risk management practices for products and services. After establishing the baseline, a report was provided to management detailing embedding risk management procedures within the product development lifecycle. The results were further used to design the framework based on problem areas that were identified over the different data collection periods.

3.3.2 Data collection period 2012

In the second period (2012), quantitative research probability sampling was used; all product stakeholders who would normally be involved in the launch of any new product in the organisation were interviewed. The sample size in 2012 was increased to ensure that all products within the organisation could be reviewed. Sequential numbers were provided to all the candidates to ensure completeness. A Likert scale was used again; however the sample size was extended to all stakeholders who were involved in all product commercialisation operations. See Appendix C for the detail of this survey.

The first two data collection periods (2011, 2012) was done via structured questionnaire (Appendix B and Appendix C), this was to ensure that trends between the years could be identified.

3.3.3 Data collection period 2015

During the third period in 2015, data were collected using a qualitative approach where executive product managers were interviewed and asked similar questions to obtain a different approach to the data collected during the first two periods. The interview approach was used to broaden the scope of the data which collected. This allowed these stakeholders to identify other areas of weaknesses within the process and did not only look at specific risk related issues. See Appendix D for the details of the questions asked.

As managers would be able to provide the view of their department as seen from the data collected in 2012, where departments provided similar views, it was decided that not all stakeholders involved in the delivery of the product should be interviewed.

Coldwell & Herbst (2004) believe that one of the advantages of an interview is the ability to cover the full range and depth of a subject. It also allows the researcher to develop a relationship with the subject matter expert. The disadvantages according to Coldwell & Herbst (2004) are that it takes up too much time and comparing the qualitative data is difficult. It can be costly as it requires travel time as well as time in the interviewee's diary. Moreover, the researcher can bias the interviewee's response by influencing or leading the questions.

3.4 Validity and reliability

Results of the analysis of both the qualitative and quantitative data collection methods were compared with those obtained from the literature review and industry best practices. The gathered information tree points of validation to ensure reliability and validity. The data collected via these three methods were used to build the framework. Furthermore, data were collected after the framework was developed from subject matter experts to evaluate the risk model for products and services and to provide input regarding the approach that should be taken to implement the framework.

Coldwell & Herbst (2004) defines validity as the extent to which cause and effect can clearly be demonstrated. De Vaus (2001) defines a valid measurement as one that measures what it was intended to measure. Babbie & Mouton (2008) define validity as the extent to which a measurement reflects the real meaning of the concept under construction. For the purpose of this research, two approaches were followed. Data were collected firstly for the purpose of building a framework for risk management to be used on products and services and secondly, for subject matter experts to evaluate the proposed framework.

De Vaus (2001) states that reliability is gained by performing the research repeatedly with the same results obtained on each occasion. When considering the data over the three different periods, it can be seen that although there are some deviations in the results, they follow a similar trend. Therefore, if the same methods were applied over the same period, the results would be the same.

As both the qualitative and quantitative data used to develop the proposed risk framework were collected from only a single telecommunication organisation, the researcher cannot be certain that the data reflect the views of the entire population. Noor (2008) highlights that case studies lack of reliability and furthermore it does not address the issue of generalisation. He therefore states that data from multiple different sources can be

used to strengthen the results. The sample of data collected as part of this research does not reflect the entire population and therefore the survey was validated using different methods including interviews and available telecommunication organisations integrated reports to ensure reliability.

Appleton (1995) says that although qualitative research has increased in popularity, there still remains a critical issue of reliability and validity. Interviewees might have given their opinions rather than the actual facts relating to the question. Views could also be bias based on the interviewees' experience or opinion of an event. To mitigate bias, the researcher used the literature review to verify that the interviewees' opinions were aligned with current trends around the world. The results of the three periods under review were based on the perceptions of the candidates who were part of the PDLC and the data collected to evaluate the risk framework was based on subject matter expert experience and knowledge within the field of risk management.

3.5 Ethical considerations

Coldwell & Herbst (2004) state that ethics consists of standards of behaviour or norms that guide moral choice about behaviour and people's relationships with others.

In this study, data were collected for two purposes. Firstly, data were collected by the researcher and staff directly reporting to him as part of the organisation's continuous improvement exercise, and secondly, for the purposes of this research paper. For the preservation of the privacy and anonymity of the organisation used as the case study, no reference has been made directly to the telecommunication organisation. In addition, all respondents who participated in the research were anonymous and issued with sequential numbers to ensure the completeness of the data and the anonymity of the participants.

The selected interviewees were presented with a consent letter and confirm their voluntary participation. All the data collected were anonymised and in the thesis, the only references made to specific telecommunication organisations were obtained from the publicly available integrated reports published by the respective organisations. This ensured that no part of this research could be linked back to the specific telecommunication company used for the data collection.

Approval to use the collected corporate data was received from the following people or departments:

- The managing executive risk management declassified the data collected in 2011 and 2012 to be used for this research study;
- The chief risk officer permitted data to be collected in 2015 from interview candidates within the organisation and to be used for the evaluation of the risk management framework.
- The organisation's stakeholder relations and reputation department provided a clearance certificate to allow the data collected from the organisation to be used in the research and provided guidance to ensure that the data could not be reverse engineered to identify the organisation.

3.6 Summary

In this chapter, the process used to collect data was described to ensure the research objectives could be met. The research design was discussed and justified and the process of how the data were collected, which population and sample size were used and how the data were analysed was explained. In addition, this chapter reviewed the data collected over the three data collection periods (2011, 2012, and 2015) to identify the perceived risks faced by the organisation.

The data collected are described and analysed in the following chapter.

Chapter 4

DATA ANALYSIS

This chapter focusses on the data that were obtained through interviews and surveys with product managers, operational staff and executive managers. The chapter reviews and analyses the data collected over the three periods to identify potential weakness within the product development process. The top risks within each period are analysed, there risks are compared with those identified in the corresponding integrated reports from Vodacom, MTN and Telkom over that period. This was done to validate the findings and to determine whether these risks were prevalent within the different organisations integrated reports and whether they were identified at the organisation's BOD level.

Third-party management, privacy, fraud and revenue assurance as well as the technical implementation were identified across all periods. Thereafter further analysis was carried out looking at trends.

4.1 Overview of top perceived risks

For each of the three periods of data collection, the top risks are reviewed to analyse similarities, and changes between the different periods are discussed. These risks and identified controls form the basis for the proposed risk management framework for products and services.

4.1.1 Top ten risks perceived in 2011

Figure 4.1 shows a snapshot of the top ten risks as perceived by the product managers in the period between 2010 and 2011. The data were collected using the questions presented in Appendix B. From the dataset collected during this period, only information related to the research questions was used.

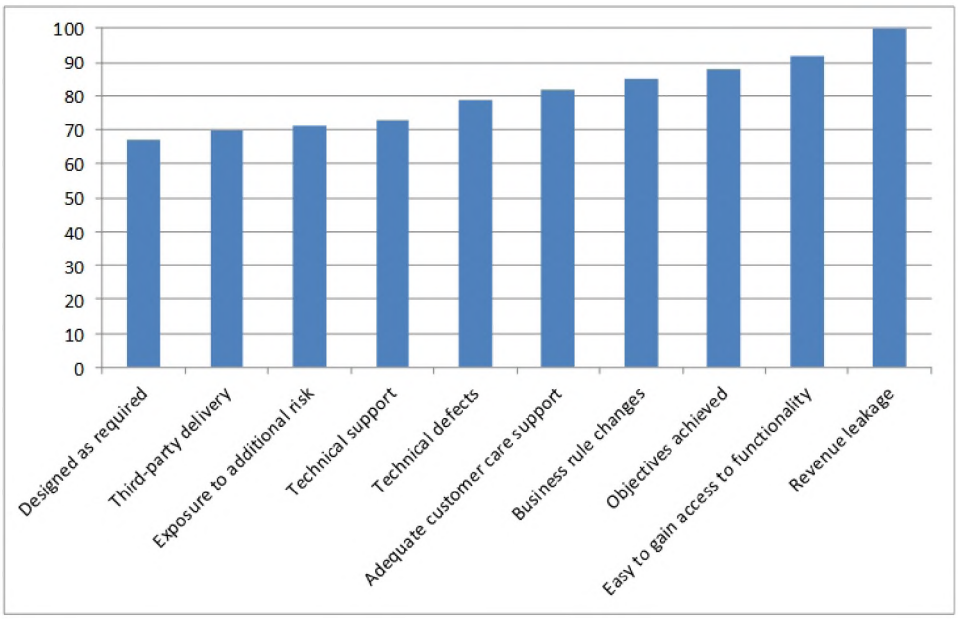

Figure 4.1: Top ten perceived project risks to the organisation in 2011

From the 2011 data, all the project managers perceived a risk to their organisation to be revenue leakage. The data show that staff were not convinced that the products deployed were fully functional with the correct revenue assurance (RA) built in. There was also a perception that the products were exposing the organisation to fraud. The majority of the product managers (88%) believed that the products did not meet the objectives of either the customer or the organisation. These findings could be directly related to the trust that the product managers placed in the functionality of their product. It can also be seen that due to technical defects and customer support, this mistrust created an additional boundary for product acceptance. There was also a concern that it was difficult for customers to gain access to the functionality of the product, or that it was not easy to find. Third-party delivery was also rated high on the list of issues challenging the deployment of projects.

The Vodacom financial report (Vodacom, 2011) shows that the organisation went through major restructuring processes. Vodacom changed its branding and logo and needed to be

sure that customers would still have trust in the brand. The financial reports also noted that customer experience needed improvement and that the organisation would undertake internal changes to deliver benefit to customers within the network, customer experience and product value. The organisation also implemented three new principles of speed, simplicity and trust. This implementation could have been driven by the fact that as the organisation had changed its branding, it needed to give some assurance to the consumers and thus, implemented these principles to gain or maintain trust. Similarly, MTN looked at improving the customer experience through a strategy focusing on convergence and operational evolution, leveraging existing scale and intellectual capacity, and looking at mergers and acquisitions to consolidate and expand on its African footprint (MTN, 2011). This broad approach is shown in Figure 4.2.

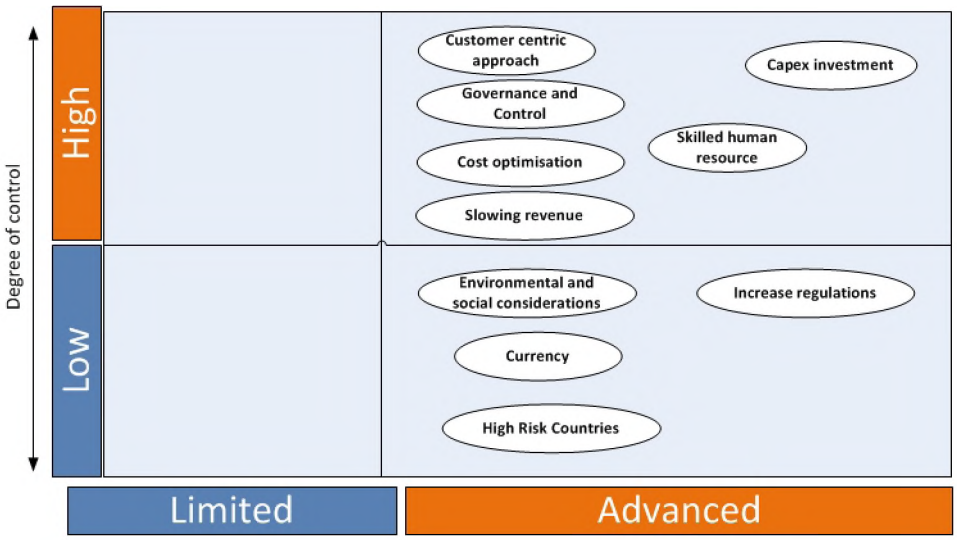

Figure 4.2: MTN risk and opportunity summary (MTN, 2011)

In MTN's report (2011) it is clear that there were enormous opportunities when considering issues over which the company had control, such as a "customer centric approach" and "governance and control". When considering a more robust strategy of implementation, MTN stated that it would provide confidence to stakeholders across the governance chain throughout their dealings with MTN. MTN also increased its training in stores for front-end staff who dealt with customers to give a better customer experience. MTN stated that in 2011 it started looking at the process of combined assurance and IT governance. The business risk management group initiated a project to implement an assurance process considering risks that the organisation was facing. MTN created a risk appetite model, which, depending on the level of risk, would be escalated to the different departments. MTN raised fraud risk as one of its biggest challenges and started implementing controls to monitor significant fraud risks.

Telkom (2011) stated that the proper management of risk drives growth and opportunity and they were proactively identifying risks and addressing these to protect and create value for its stakeholders, shareholders, employees, customers, regulators and society. In general, Telkom achieved this by integrating the ERM process into its critical operational functions and embedding risk within its business decision making.

4.1.2 Top ten perceived risks in 2012

During the period between February 2011 and January 2012, the scope of the data collection was expanded and 130 telecommunication employees were interviewed. The interviewees represented a multitude of different departments that were all stakeholders in the delivery of products and services. Data were collected using the questions presented in Appendix C. Only data pertaining to the research questions in this thesis were analysed. The results of the 2011 survey shown in Figure 4.1, were distributed to executive management and some actions were put into place to understand these issues and to see what mitigating actions could be performed to manage them.

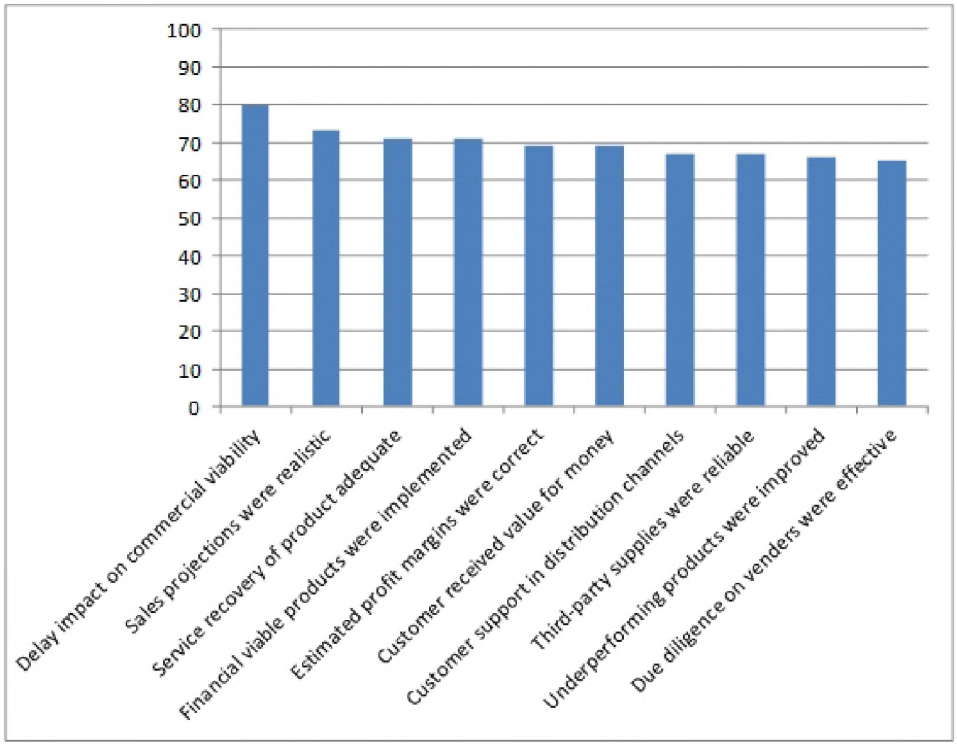

Figure 4.3: Top ten perceived project risks to the organisation in 2012

From the survey results that were obtained in 2012, one can see that there was a reduction in the perceived risks, although these were still high (Figure 4.3). Actions such as ensuring

that more emphasis was placed on ensuring that RA controls were in place decreased the perceived risk related to revenue leakages. Issues such as third-party support were highlighted again, as well as customer care support. The implementation of additional controls to ensure that more robust products went to market, explains the fact that 80% of product managers believed that project implementation was delayed, which could have an impact on the commercial viability of the products. However, looking at Vodacom's financial reports (2012), it can be seen that the customer base increased by 29.9% to 48 million customers. This report states that the organisation's most important objective for the 2011 financial year was improving customer experience, which was done by driving network quality (Vodacom, 2012). Other initiatives such as enhancing customer service and building technical in-store help centres to allow customers to set up their devices and services in-store were also implemented.

The Vodacom report (2012) further states *"Our customers are central to the sustainability of our business. To build trust among our customers, we need to manage our core operational risk around network performance and privacy. With the number of new regulations impacting our customers and our relations with them, engagement also helps us manage regulatory risks"*. MTN South Africa similarly grew its customer base in 2012 by 15.4% to 25.4 million subscribers (MTN, 2012). MTN stated that the increase in number of customers was due to the competitive data offerings and new services, such as MTN Mahala[1] and MTN Zone[2]. MTN stated that it believed in good governance and would ensure that these structures supported effective decision-making and robust controls that were aligned to best practices. Telkom grew its subscriber base by 10% by rationalising and simplifying its fixed voice portfolio (Telkom, 2012). It also introduced the first fixed mobile convergence bundle, Telkom-Mix[3], in South Africa.

None of the organisation's integrated financial statements for 2012 support the product managers' perceived risks, which shows that the organisations were operating more efficiently and with good governance models. There are two likely main drivers for the increase in subscriber numbers. Firstly, product managers who were closer to lower level operational risk issues, either did not escalate these problems to the management team, or the management team did not see these risks as being strategic to the organisation. Secondly, because there was a limited number of mobile telecommunication providers and since cell phones were no longer a commodity item, as they became integrated into South Africans' daily lives, consumers were forced to choose one of these mobile providers.

[1]http://www.mtnblog.co.za/tag/mtn-mahala
[2]https://www.mtn.co.za/everydayservices/airtime/Pages/ZoneonTopUp.aspx
[3]https://secure.telkom.co.za/today/shop/plan/telkom-mix-unlimited-anytime-plan/

4.1.3 Top perceived risks in 2015

The data collection process in 2015 took a different approach, where the executive managers for product and service delivery were interviewed to identify their perceived risks for the financial year. The questions asked during the interviews are documented in Appendix D.

During 2014, some of the smaller players (Cell-C) started a campaign to reduce pricing and mobile termination rates. This risk related to competition, in particular, was mentioned during the interviews. One of the main risks identified was revenue targets and increasing the NPS which measures customer experience and value perception. The commercial departments raised risks relating to the fact that the current PDLC processes were too extensive and therefore created delays in projects. Furthermore, they stated that there was an increase in fraud attacks, which could have an impact on the customers as well as the organisation's reputation. This was mainly due to the increase in SIM swop and upgrade fraud which the organisation identified through trend analysis. Dlamini *et al.* (2015) also identified that within the financial banking sector, criminals were by-passing the multifactor authentication and were using SIM swops, phishing and keystroke attacks to obtain banking customers credentials. The technical departments raised issues relating to system errors, which lead to poor service availability due to inadequate testing and a lack of proper disaster recovery plans (DRP). Logical access was also highlighted as a risk that could potentially lead to fraud.

The risk that was raised by most departments was that of privacy. The fact that insufficient control was being implemented was also mentioned, although this was due to time as well as budget constraints. Most organisations were waiting on the formation of the information regulator governing the POPI Act (The Republic of South Africa, 2013). This regulator would provide organisations with guidance around the implementation of controls; therefore, most employees were concerned about privacy. The legal and regulatory department raised concerns that there was the potential that the organisation could be noncompliant with regulatory requirements. These concerns were also aggravated by the fact that in some instances products were launched without the necessary approvals.

4.2 Analysis of individual risks from 2011 to 2015

While the figures in the previous sections show the main risks to the organisation in 2011, 2012 and 2015, it is important to further analyse some of the details of the risks. This

section discusses some of the data collected and correlations are drawn between the data and the annual reports for Vodacom, MTN and Telkom to see how the three companies represented the risk at a strategic and executive level. The collected data show that there were trends with regard to some risks. These risks are further analysed to determine how they impact products and services and the organisation as a whole.

4.2.1 Third-party management

Data from 2011 (Figure 4.4), show that 60% of product managers believed that there was a need for some improvement in management of third-parties. This was because firstly, third-parties did not always deliver as expected and secondly, there was a lack of governance related to third-parties.

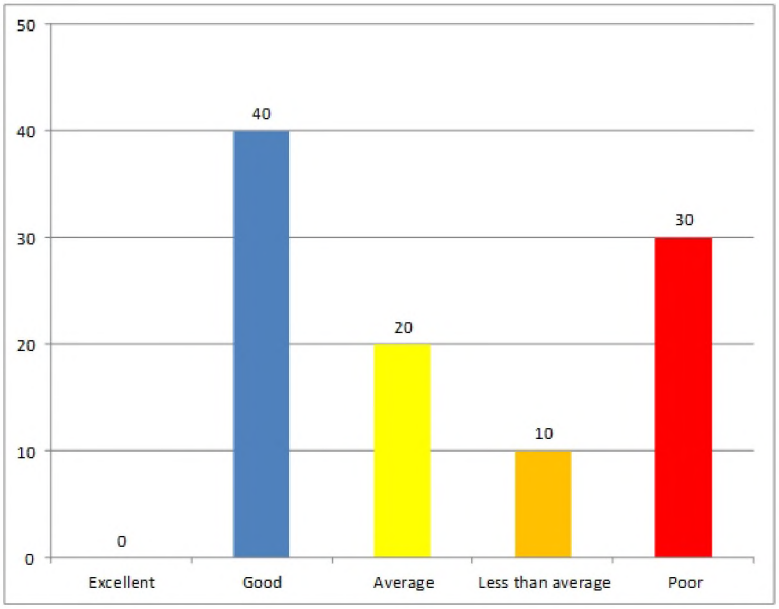

Figure 4.4: Third-party reliance 2011

Figure 4.5 shows the changed perceptions in 2012. Although poor third-party management decreased, most respondents still believed that the management of third-parties was below average. Some of the comments from the interviews conducted in 2012 reflect this well. *"Third-parties should not dictate how we should do our testing"* and *"If a third-party is involved in a product, we should ensure that they know, understand and respect our internal processes and find a way to work together in order to achieve our goals."*. Comments that reflect these gaps, such as *"There is too much reliance on third-party vendors"*, *"Insufficient formal processes are in place to manage third-parties"* and *"product*

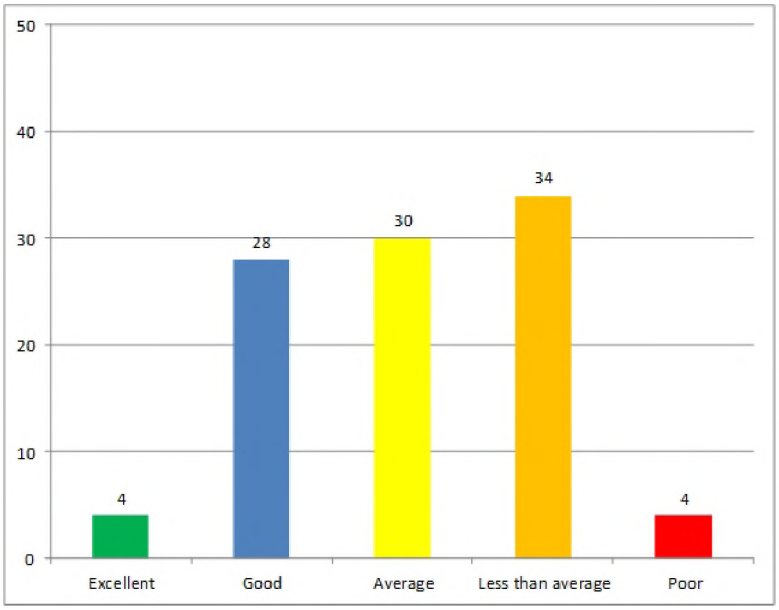

Figure 4.5: Third-party reliance 2012

insufficient support due to third-parties not allowing knowledge transfer" were captured during the interview process in 2011.

Based on the interviews conducted in 2015, it seemed as if some level of governance had been put in place to manage third-parties better, although there was still much reliance on vendors and third-parties. However, it was also noted that there were still occasions when third-parties were brought on board to perform certain functions and some stakeholders, such as the technology security and risk management departments were made aware of this too late. These departments, as well as the financial departments, should ensure that a due diligence process is performed on the sustainability of these third-parties (Capron & Mitchell, 2004). In addition, a technology security review needs to be performed to ensure that the process controls and level of protection for customer information were the same or better than those of the organisation (Peltier, 2005). When stakeholders were informed late in the project phase of developing or supporting a product or service, these departments were seen as delaying the commercial department's ability to launch the product quickly. When stakeholders such as technology security requested external vulnerability assessments or penetration tests, and these were not budgeted for within the project, there was resistance from other departments, because these tests impacted the commercial viability of the projects.

By reviewing the results over the data collection periods, it can be seen that there was an improvement with regard to the management of third-parties. However, there were still

concerns that third-parties had too much influence over how the organisation implemented and performed its functions. It could also be seen that product managers understood the requirement for governance and were implementing controls for the third-parties.

4.2.2 Privacy

In 2011 the notion of privacy formed part of the regulatory and legal department and was supported by technology security, the custodian of customer information. In addition, it was assumed that privacy was managed by the organisation and therefore, no questions were asked regarding this subject in the 2011 data collection period. In 2012, there was more hype around customer privacy, because the POPI Act (The Republic of South Africa, 2013) (in 2012 it was still a Bill) was covered extensively in the media. More stakeholders in the organisation also became more aware of the importance of ensuring that customers' information was protected.

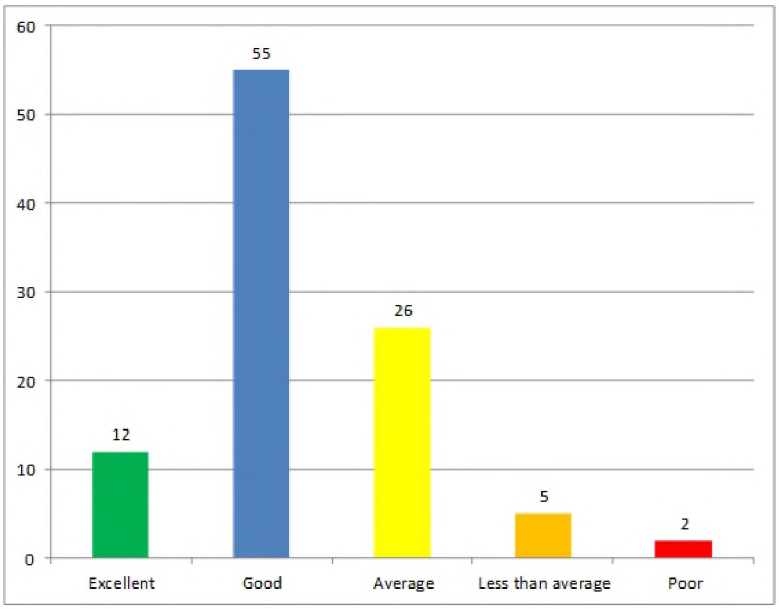

Figure 4.6: Perception of privacy 2012

Figure 4.6 shows that most respondents believed that the organisation was doing enough regarding privacy. The question asked in 2012 was *"Were customer privacy issues adequately anticipated"*. Of the 130 respondents, 66% agreed or fully agreed, 27% were uncertain about customer privacy requirements and 6% either disagreed or strongly disagreed. Figure 4.7 shows how the different departments perceived the organisation's response; it also indicates that the commercial and risk management departments had the highest

number of responses stating that privacy concerns were adequately addressed. It can be assumed that during this time period, there were no customer complaints around privacy. There was also a lack of understanding of what the requirements were to ensure that privacy concerns were addressed. All the respondents in the regulatory and legal department however, stated that they were either uncertain, or did not agree that privacy controls were implemented on all products and services development.

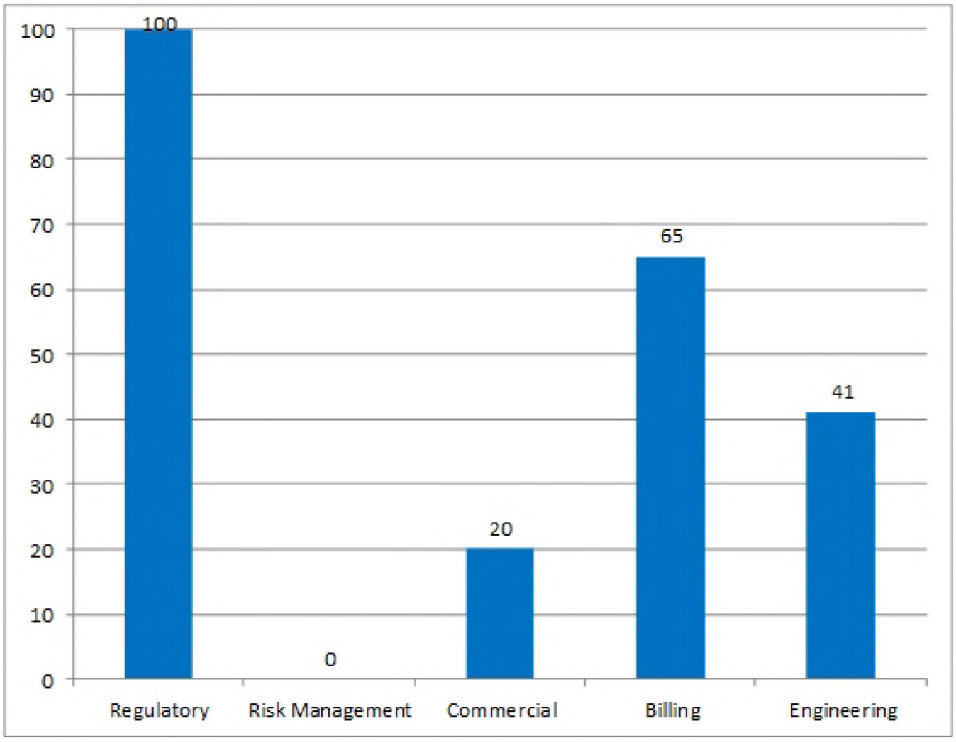

Figure 4.7: Graphical representation of departmental responses to privacy in 2011

This considerable discrepancy between the participants in the commercial department and the regulatory and legal department could indicate that there was a lack of either awareness or training around the requirements of privacy and the related POPI Act (The Republic of South Africa, 2013). In 2015, the organisation was going through an enormous transformation as a project that had been initiated in 2014 to guide the organisation to become POPI compliant. There was therefore more awareness of privacy and POPI and many of the respondents mentioned privacy as a risk. This included the marketing department that was starting to drive a campaign where it wanted to identify customers in different market segments to enable them to market specific types of services to them. They were concerned about where they would obtain new market databases that would comply with the requirements of POPI as well as how they could grow the existing marketing database and get more customers to opt into receiving marketing before the POPI

Act (The Republic of South Africa, 2013) was approved in 2014. The risk management department also stated that they noticed an increase in the number of projects where they were asked for guidance with regard to privacy-related matters.

From the collected data there is a clear improvement in the organisation's maturity from 2011, when privacy was not high on the agenda, to 2012 when, although departments were aware of privacy-related matters, they were not sure what the requirements were, to 2015 when privacy was mentioned in MTN's (2014), Telkom's (2015) and Vodacom's (2015) reports. By 2015 all three companies had started implementing plans to manage the risks that the POPI Act (The Republic of South Africa, 2013) could potentially introduce.

4.2.3 Fraud - Internal and external and RA

Fraud and RA are key to the organisation, because if customers perceive that an organisation is not managing its own assets and processes and is constantly under investigation for fraud, they could lose trust in the organisation. Therefore, it is very important that when products and services are developed, the organisation reviews and ensures that proactive measures are put in place to mitigate fraud and RA.

Based on the data from 2011, 57% of respondents stated that the new products or services introduced no additional fraud (Figure 4.8). Furthermore, 34% of respondents perceived that there was room for improvement with regard to revenue leakages. Some comments from the interviews include *"Revenue generated may not present a true reflection of the net profit/loss", "Campaigns do not generate revenue for the organisation" and "Profitability analysis for products (considering product development and operational cost) do not exist".*

Vodacom's integrated report for 2012 however, states that 3420 cases of fraud were investigated, of which 3072 were due to external causes (Vodacom, 2012). Awareness of these cases was received directly from the customers or service providers, online reports, referrals, other businesses or confidential and anonymous reports. Over the same period, 100 reports were received via the hotline hosted by KPMG. During the same period, MTN (2011) stated that it had comprehensive governance and oversight structures in place for fraud prevention and to ensure that risk management measures are established. They also had a hotline[4] in place where tipoffs could be made in support of the organisation's zero tolerance to fraud. In 2011, MTN stated that it would focus on fraud prevention to ensure that they had a more proactive approach to fraud. The focus was specifically on

[4]https://www.mtnbusiness.co.za/Support/Pages/Reportfraud.aspx

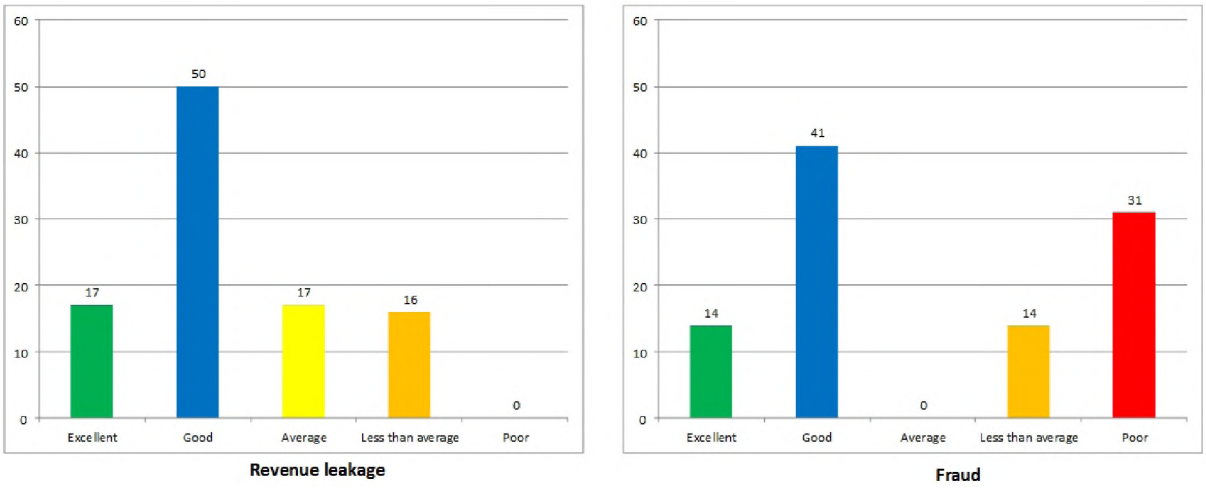

Figure 4.8: Product adequately assessed for revenue leakage and fraud 2011

mobile money, procurement fraud, airtime fraud related to IT weaknesses, standardisation of reactive investigative methodologies, creating more awareness around fraud initiatives, and formalising the proactive fraud risk monitoring. Telkom (2011) made a statement in its 2011 results that it operated in an ethical manner and that it would ensure that information would be provided to the stakeholders on all fraud-related matters. Telkom was, however, concerned that its new mobile operator, 8ta, presented new opportunities for fraudsters and that they were working with the fraud department to combat these cases. Telkom stated that it had 337 fraud cases under investigation and had arrested 466 fraudsters, of which 132 were convicted. The company suffered a total loss of R2.1 million as a result of fraud.

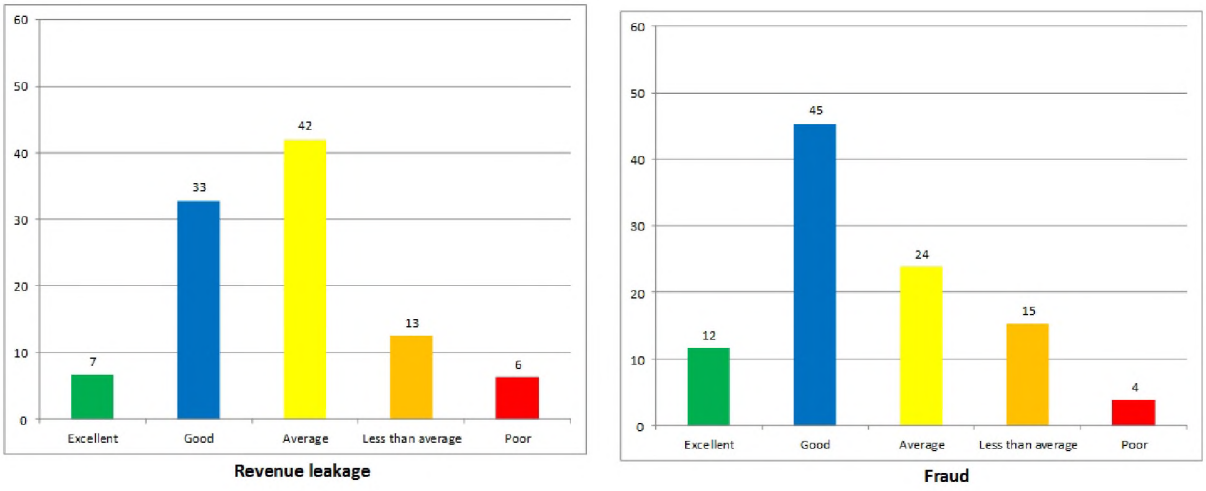

Figure 4.9: Product adequately assessed for revenue leakage and fraud 2012

Figure 4.9 shows that in 2012, 74% of the respondents stated that products were ade-

quately assessed to mitigate fraud exposure. However, only 50% stated that the products were adequately assessed to determine revenue leakages. During 2015 product managers in the online space started raising issues related to fraud on their online stores. Issues of SIM swops and identify theft were also highlighted as risks. Vodacom (2015) stated in its annual report that it would be launching products such as voice biometrics for secure customer logins to assist in the decrease of fraud. MTN (2014) stated that it had a proactive fraud risk management strategy which included running a group-wide fraud and risk awareness campaign. MTN also introduced the fraud risk universe into its ERM framework. MTN however, confirmed that products and services-related fraud was one of its top fraud risks.

Fraud is thus an important element, not only in terms of protecting the organisation's financial status, but also ensuring that trust is maintained in the organisation's client base. As seen from the results, fraud and RA are always high on the organisation's radar. Additionally, it can be deduced from the integrated reports that good governance structures were put in place in the telecommunications organisations.

4.2.4 Technical implementation

The technical component of new products and services has many different facets. These include ensuring that the product is technically sound and implemented correctly as documented in the original commercial specification; that adequate security is implemented to secure both the organisation's and the customers' information; that sufficient business continuity processes are put in place and that the capacity to run the service is sufficient. Note that this is not an exhaustive list.

In 2011, the product managers were asked three technical questions, the results of which are summarised in Figure 4.10.

1. Were controls, resolutions and release processes adhered to?
2. Was there effective support from all different technical components?
3. Were technical defects identified after the product launch?

Only 38% of product managers believed that controls and release processes were adhered to. In a fast-moving environment such as a telecommunication organisation, if there are

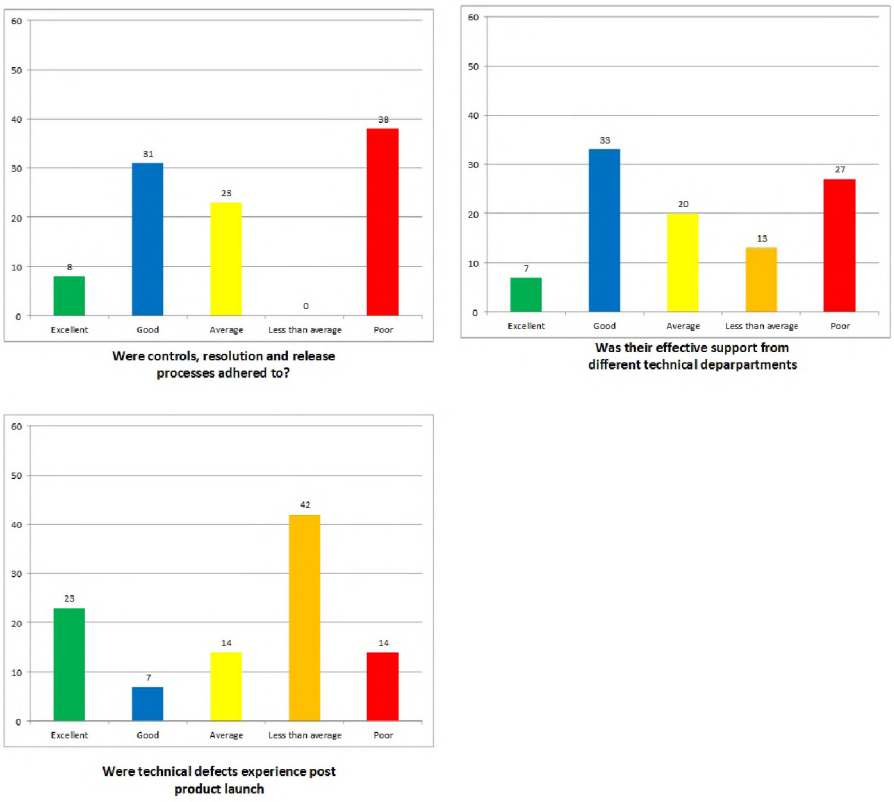

Figure 4.10: Technical questions 2011

no proper governance structures in place, it could mean that release cycles are not always adhered to. This could in turn, affect other technical developments currently in the system. In addition, 60% of product managers believed that adequate support was not provided by the technical departments. This can, however, be related to the assumption that commercial teams would almost always be dissatisfied with the length of delivery of a product, because it would normally be perceived that the technical department takes too long to develop the product. It was also noted that products had to be fixed after they had already been launched and commercialised; 48% of respondents believed that technical defects were only fixed after the product's launch. During the interviews some comments from the respondents were: *"Product was not scoped correctly"* and *"The requirements definition was inadequate"*. In 2012 the scope of the technical questions was expanded to include capacity planning, business continuity management (BCM) and information security.

The results from 2012 are summarised in Figure 4.11 where it can be seen that although, on average, 36% of respondents answered that they were uncertain of the technical implementations, 45% stated that in general, proper technical plans were adhered to and implemented. In 2015, the organisation started implementing a huge revamp of its current

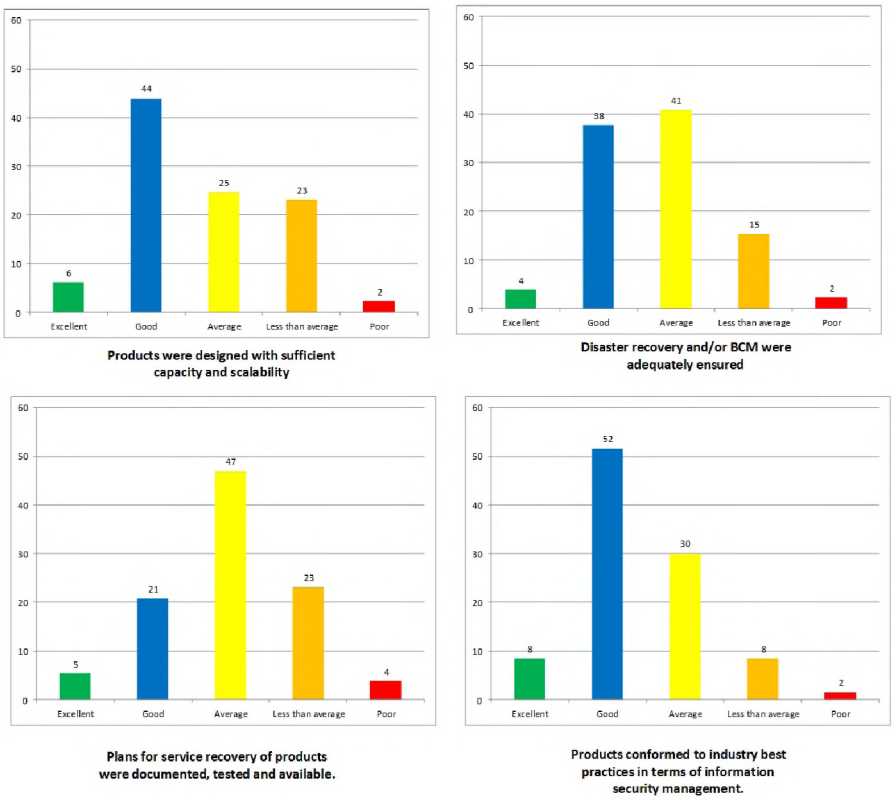

Figure 4.11: Technical questions 2012

infrastructure and was moving from legacy systems to new systems. All the candidates who were interviewed identified this migration process high on their agenda, but since this was a once-off implementation, these results were excluded from the report. To ensure stable technical implementations, a feasibility study should be performed during the early stages of product and service development. This will ensure that technical departments are not seen as delaying the launch of products or services and that the financial requirements of the technical departments are known upfront.

4.3 Summary

From the different organisations' integrated reports, it can be seen that the risks related to products and services are not always viewed in the same light by the organisation and its employees. There is a clear difference between the views of the product managers who need to ensure that revenue is growing, and support departments, such as the technical, risk and regulatory departments, who need to implement controls to manage risks for the organisation. During all the data collection periods, product managers expressed the

view that the PDLC is too cumbersome, thus leading to delays in projects which in turn hinders the commercial objectives of the organisation. Technical and governance divisions were, however of the opinion that more needs to be done prior to projects being launched commercially.

The next chapter reviews these findings and considers industry standards to develop a framework that can be used for product risk management in telecommunication organisations.

Chapter 5

DEVELOPMENT AND EVALUATION OF RISK MANAGEMENT FRAMEWORK

This chapter discusses the data that were collected over the different collection periods. Based on this information, and together with industry standards and best practice guidelines, a framework for product risk management is presented. First the different levels of where risk can be identified within an organisation based on Hopkins guidelines (2014) are discussed and thereafter a risk based framework for products and services is proposed based on the ten risks that were common over the data collection periods. The framework is also evaluated to assess its suitability for telecommunication organisations.

5.1 Trust landscape

Based on perceived risks (Section 4.2.1 - third-party management, Section 4.2.2. - privacy, Section 4.2.3 - fraud, Section 4.2.4 - technical implementation) it can be seen that there is a need for the organisation to manage risk at a project level. The risk can be categorised in five areas as defined by Hopkins (2014). These are listed below, with some examples to demonstrate each category:

- Project management risks - No executive support, conflict between stakeholders, ill-defined project scope, inaccurate cost forecasting. Inadequate support processes for projects, ill-defined processes, not well thought out project designs.

- Compliance management risks - Inadequate support for regulatory compliance, or failure to achieve compliance
- Operational risks - Incorrect development of specifications, revenue leakage or fraud controls not implemented correctly.
- Tactical risks - Project does not support business objectives, project deliverables are not based on the correct market or the market's needs.
- Strategic risk - Project does not support the strategy of the organisation.

Given the omnipresent risk, it is therefore, clear that a proper risk management approach is necessary and should be implemented from the initial engagement of a project.

The framework development methodology looked at the organisation's strategy and the governance controls and then used the datasets collected to map the key risks related to the organisation over the reporting periods. Using this analysis to link the different areas, the risk framework could be developed, focusing on key risks that were identified from the different periods analysed. These risks were then mapped according to the Deloitte (2009) and Ernst & Young (2014) risk lists to create the proposed risk framework.

5.2 Design of risk management framework

To define the risk framework, the responses to the survey questions (Chapter 4) were reviewed. The critical areas were identified and the Deloitte (2009) risk universe and Ernst & Young (2014) was modified to develop the risk approach or questions below.

The following sections cover:

1. analysis of the risks covered in the framework
2. issues inherent in the adoption of the framework
3. the checklist developed from the proposed risk management framework for products.

To ensure that all the factors of risk management are identified, the risk framework consists of ten categories that look at which area the risk resides in and whether it relates

to strategic, people, process, technology, or external factors. The proposed framework is documented in Appendix E.

The risk framework is defined in terms of the following key risk categories (Table 5.1). These are based on the data collected over the three periods, which identified perceived risks to the organisation and documented.

Table 5.1: Product risk categories

Legal and regulatory
Privacy
Competition
Customer
Reputation and brand management
Financial
Technology IT and networks with security and BCM
Internal and external fraud
Business practices
Third-party management

5.3 Analysis of the risk categories

This section presents some of the considerations that product managers need to review for the specific product or service they intend to launch. The sub-risk questions are derived from Deloitte's risk intelligence map (Deloitte, 2009) and Ernst and Young's top 10 risks in telecommunications (Ernst & Young, 2014).

5.3.1 Regulation and legal

There are cases where organisations were fined for non-compliance with legal and regulatory requirements. Organisations could find themselves on the brink of bankruptcy due to large damage claims imposed by regulators who sometimes seek fines or restitution to remediate issues. For example, Siemens was charged with violating the Foreign Corruption Practice Act and fined $1 billion. Similarly, in 2007 Baker Hughes paid a fine of $44.1 million and incurred costs of over $850 million for an independent investigator to conduct their own investigation (Conversano, 2013).

To ensure that the telecommunication organisations do not put their licence agreements at risk, the legal and regulatory department needs to ensure that the new product or

service complies with all relevant laws. With the introduction of products outside the traditional telecommunication environment, product managers have to ensure that other laws impacting the product are also taken into account. This is necessary to safeguard the current revenue, their potential future revenue and protect the organisation against liability claims and penalties. Reviewing MTN (2014), Telkom (2015) and Vodacom (2015) integrated reports, it can be seen that regulatory compliance is identified as one of the strategic risks for the organisation. Therefore from a product and service development perspective, it is important to ensure that product managers are aware of how the products they develop comply with to applicable legislation.

To ensure that product managers are aware of the requirements that could affect their products under development, requirements stipulated in Table E.1 could guide the product manager to ensure that they have the required input from the legal departments and documentation, to assist them in designing products compliant with applicable laws. Examples include having the correct terms and conditions available to customers and being aware of which legislative and regulatory changes could impact their products in future.

5.3.2 Privacy

Privacy normally relates to the regulation and legal compliance category. It warrants its own category, however, due to the POPI Act (The Republic of South Africa, 2013) that was passed into law in 2013 and clarity is required to ensure compliance. This risk recommends controls required to protect the privacy rights of the customer. Consideration of how information is communicated to the customer, who the information is passed to, where the information resides and how the information is processed, within the context of POPI is required. Attention needs to be paid if the organisation performs unsolicited marketing of the subscriber base by asking questions such as where and how the organisation obtained the customer database. If the marketing database was bought from a third-party, what process was used by the third-party for collecting the information? A survey compiled in 2013 by Cibecs (2014) states that protecting data is imperative for organisations, as organisations with an ineffective data protection strategy could find themselves vulnerable to data theft, unauthorised access to confidential information and therefore could be liable for legal penalties, which could have an impact on corporate governance compliance.

Many telecommunication organisations should already have a privacy policy available

such as MTN [1], Telkom[2] and Vodacom[3]. Changes within products however may not comply with these privacy statements and policies if the product manager is not aware of the privacy requirements and what to comply with. A lack of privacy controls on products could lead to reputational damage and fines when the POPI Act (The Republic of South Africa, 2013) is enacted. Table E.2 shows some considerations and questions that product managers need to ask about their products to ensure compliance with the privacy requirements of the POPI Act (The Republic of South Africa, 2013) as well as the organisation's privacy policy.

5.3.3 Competition

Increase in competition leads to volatility in the market and profit reduction; however, an increase in market size allows for gain to reduce costs and increase incentives (Raith, 2003). Summerfield (2013a) states that in recent years many big brands have fallen victim to market competitive pressures, including Kodak, BlackBerry and Nokia. He further states that although competitive risks might sound defensive, pushing back new entrants and responding to competition should be considered a top priority for all organisations. Organisations stagnate if they do not track competition risks and become over reliant on their current product experience. He explains that an organisation has to ensure that it has plans in place and can respond accordingly to counteract competition. He does, however, warn that organisations should analyse and manage their core competencies to ensure that they cannot easily be duplicated, to ward off competition. In turn, by doing this the organisation can gain a competitive advantage.

It is important that organisations adequately measure compliance and comply with competition laws and regulations. Failure to comply could lead to penalties and personal consequences for directors, as well as damaging the organisation and the brand's reputation. If a product is launched and the organisation is not aware of market intelligence or what the competition is doing, it could lead to the product not achieving its objectives. Reviewing the competition's offerings can lead to the creation of products that diversify the organisation's offering with the aim of gaining market share and remaining competitive. Products that are already in the market should be benchmarked against the competition for identifying current weaknesses and understanding where improvements can be made.

[1] www.mtn.com/MTNGROUP/Pages/privacy-statement.aspx
[2] www.telkom.co.uk/privacy.html
[3] www.vodacom.co.za/vodacom/terms/privacy-policy

Products that do not align with the organisation's strategy might not get the correct or enough resources required for them to be successful. Furthermore, in the worst-case scenario, a product could affect the organisation's reputation if it does not align to the organisational culture. For example, a reputable telecommunication organisation launching products that could be perceived by the public as disreputable, such as adult or gambling services, could have an adverse effect on existing products. Table E.3 lists to the questions that product managers need to ask to ensure they have considered competition as a risk.

5.3.4 Customer

This risk describes the ability of the organisation to understand the customers' needs and for identifying how well they understand the market segment. How does the organisation ensure both that it builds trust in the brand and that the product generates revenue. The risk also relates to changes that the organisation makes to products and the effect on the customer base. Organisations need to ensure that they have adapted to new consumer trends. If organisations stick with flawed or unreasonable pricing strategies, or fail to embrace new technology effectively, they run the risk of not being able to compete (Summerfield, 2013a). Table E.4 lists the questions that product managers need consider when looking at customers' requirements.

5.3.5 Reputation and brand management

When planning the best ways to communicate and engage with the customer, it is important to not only identify the problem, but to understand the different perspectives of the stakeholders and how they view the problem and the possible solutions. Adler & Kranowitz (2005) state that understanding the nature of the risk and how the customers' perceive the risk is important to understand how to communicate the risk to customers. The way that the risk is communicated serves many roles: it increases trust in the organisation, reduces the length and impact of the perceived risks, and reduces misunderstandings by the consumer. Adler & Kranowitz (2005) designed seven golden rules to communicate risk effectively. These rules are:

1. Accept and involve the public as a partner;
2. Plan and evaluate performance;

3. Listen to the audience;
4. Be open and honest;
5. Coordinate and collaborate with creditable sources;
6. Meet the needs of the media;
7. Communicate clearly and with compassion.

Table E.5 focuses on questions that product managers need to consider to ensure that they do not negatively affect the brand reputation of the organisation.

5.3.6 Finance

This risk analyses two different aspects of finance: project budget and revenue generation. The project budget helps the product manager ensure that the project is kept within the required budget and overspending is avoided. It is important to ask what planning and data analysis went into the budget for near actual results.

Based on trend analysis, the project manager needs to look at the anticipated revenue of the product and how to prevent revenue leakages and the cross-cannibalisation of existing products. Product reporting would also fall into this category if any funds need to be reported to the regulator. It could be that different products have different tax requirements that need to be considered. Table E.6 lists questions that product managers need to consider to ensure that they have thought about the impacts of the product development from a financial perspective.

5.3.7 Technology, networks, security and BCM

During the development stages of the product, a close eye needs to be kept on the technology that was chosen to provide the service. Technology could affect whether the organisation is perceived to be innovative and adaptable to change. Product managers also need to consider the ease-of-use of the technology they are implementing as well as the key users of this technology. Technology plays an important role in the sustainability of an organisation, because it can help accelerate innovation (Summerfield, 2013b). Furthermore, the technology department is the enabler for a business to map its processes and can suggest ways to transform these processes.

This risk reviews different technology-related issues, including BCM, architectural design and technology security as shown in Table E.7 and E.8 and the factors that need to be considered to ensure that the technology aspects of the product are risk-free. These considerations should be made to ensure that the products are robust enough to service the customers' needs and to ensure the confidentiality, availability and integrity of the customers' private information such as billing information.

5.3.8 Internal and external fraud/anti-money laundering/RA

For robust products, fraud (both internally and externally), RA and anti-money laundering (AML) has to be reviewed. Hamman (2015) says that South Africa organisations are governed by two statutes regarding AML: the Financial Intelligence Centre Act - FICA (The Republic of South Africa, 2001) and the Prevention of Organised Crime Act - POCA (The Republic of South Africa, 1998), which assist organisations to be vigilant and accountable in fighting against money laundering. It is therefore important that during the product development phases the product manager ensures that these laws are complied with. Special attention needs to be given to these laws for services such as Vodacom's MPESA and MTN's mobile money, which must comply with these laws; however other services, such as airtime transfer and airtime vouchers could be affected by these types of legislations as well.

As shown in Table E.9, this risk category covers what is in place to mitigate fraud and revenue leakages, and also what controls need to be put in place to monitor these types of risks.

5.3.9 Business practices

This risk analyses how the organisation currently operates and how different departments would need to operate to support the product or service. It reviews the business model to understand how the product can be profitable and ensures that the product generates revenue. Table E.10 refers to considerations that must be made for the product to be supported by the entire business.

5.3.10 Third-party management

Voice and data type services would normally be the core product offerings of telecommunication companies. Thus, they would either need to acquire additional skillsets or outsource some of the non-core business functions such as insurance, mobile money and value-added services to third-parties. The management of third-parties is therefore important to ensure that controls applied to the organisation also apply to third-parties. This can mostly be done via legal contracts and service level agreements with third-parties. However, in the event that an incident does happen to one of these third-parties, it can still create legal, reputational and financial impacts on the company. Table E.11 gives a list of questions that need to be considered by product managers to ensure compliance with the management of vendors and third-parties. This ensures that outsourced products are robust before launching into the market.

5.4 Adopting a risk management framework

Each risk category discussed in the previous section should have an assigned risk owner, however the overall risk for the product should remain with the product owner. It is the responsibility of the product and project manager to engage with the relevant stakeholders to ensure that they have provided input and have answers to these statements and questions.

An organisation may not be able to implement all the controls as discussed in the risk framework at once due to the following constraints:

- Education, the scope of the risk framework is broad the product manager will not be familiar with all aspects relating to each risk. It is therefore necessary that the product manager engages with subject matter experts to provide guidance when developing a product. Further training may also be required for product managers to ensure that they have a high-level overview of potential pitfalls of products to persuade them to consult with the correct departments and subject matter experts.
- Stakeholder engagement, not all the stakeholders as defined by this model, will be readily available to assist the product manager and ensure that their aspects are completed. By implementing a risk framework, the product manager may inundate some departments with additional request for inputs, whereas in other cases the

subject matter expert may not be required to provide consultation. An example of this is when the product makes a simple change to tariffs, the product manager will send the concept document to the privacy manager. A process therefore needs to be defined as to which stakeholders should be engaged on which products.

- Time, because there will be a delay in implementing the product as the project manager would now need to focus on the governance aspect of the project. With the implementation of the risk framework, the product manager needs to consult more widely and therefore more stakeholders will be involved in the process. This could cause a delay, as more approvals are now required before launching a product.

- Cost, as there will be additional cost requirements added to the project to ensure that all the controls are working as required. Examples of these could be that additional security controls would need to be implemented for protection of sensitive data; this could affect the business case of the product resulting in it no longer being profitable to implement.

Therefore, it is suggested that a maturity approach such as the risk maturity model, as discussed in Section 2.6, should be implemented. Prior to a telecommunication organisation implementing risk management for products and services, they should already have a mature ERM policy and framework for operational, tactical and strategic risk in place to ensure that governance is implemented. Only when the ERM culture is partially or fully entrenched within the organisation can the organisation start looking at product and services risk management. The approach should be the introduction of "light-weight" risk checklists for management to understand the benefits of product and service risk management. Awareness should be continuous and training around product and service risk management should be provided. The risk framework needs to be piloted on a high-risk and high-profiled product which would have high inherent risks. If the implementation is successful, it can show the executives' support and be used for demonstrating the return on the investments (ROI).

5.5 Risk management checklist

A good reason for adopting the checklist approach instead of the full framework for risk management is to prevent the product manager from being overwhelmed by having to handle the potential large number of risks. The second reason why a checklist should

be used is that in the absence of in-depth risk management training and the fact that the project manager may not be skilled on all the different aspects of risk, these types of checklists can be used for identifying which stakeholders to consult. The third reason to use the checklist is that not all products are similar in design and could have different risks related to them. Therefore, category specific checklists can be designed for each type of product to assist the product managers.

This example of a checklist (Table 5.2) consists of a few questions that the product owner should be able to answer. However, by answering these questions the product manager could start to think about how the risks relate to the product. The example in Table 5.2 is a subsection of the product and service risk framework discussed in Section 5.3, although the basis of this type of checklist is to look at the major critical risks that the project can face. In all the cases where the product manager answers "No" to one of the questions, action plans such as "monitoring" should be provided or dates should be determined by when these issues can be mitigated. The example in Table 5.2 should be modelled and updated depending on what the specific product is. Whether it is new technology, a new market segment or a new business model, as shown in Figure 2.8, the checklist needs to become more detailed as the risks on the new products increase. Once the risk list is completed and the product is launched commercially, it is important that the product manager constantly monitors the performance of the product and incidents, such as security breaches, or RA leaks, and makes sure that the risk department is aware of these new risks. The product manager then needs to ensure a process is stated to close these gaps in order to contain the risks.

5.6 Evaluating the proposed risk management framework

The primary objective of the research was to produce a proposed risk management framework that could assist product managers with a tool to identify risk on their products and to ensure that governance is adhered to when developing these solutions. This section reviews the proposed risk framework, which was evaluated by subject matter experts. The results of these interviews are analysed to evaluate if a risk framework could be adopted by a telecommunication organisation.

Table 5.2: Example of a risk checklist for products

Description	**Yes**	**No**	**Comment**
Has all product documentation been approved?			
Was the business case for the product approved and was product development within budget?			
Has the regulatory department confirmed that all regulatory issues have been addressed?			
Does the product use any customer personal information, and have you consulted with the privacy officer?			
Have the customer communication and marketing messages been approved?			
Are all business rules for the product defined and approved?			
Have the legal department updated the terms and conditions for the product?			
Has all information security issues been identified and addressed?			
Does the product require input from business continuity and is there a DR in place?			
Has competition analysis been performed and does the product offer a differentiated service?			
Was a technical assessment performed and was this approved?			
Have unit testing, functional testing and customer experience testing been completed?			
Has the impact of fraud/AML/RA been assessed?			
Are any third-parties or vendors providing a service to deliver the product and have these vendor agreements been assessed by the legal department?			
Does the product have the correct support structures in place to assist customer queries			

5.6.1 Qualitative evaluation

The risk management framework presented could not be implemented during this research, as it takes time to change an organisation's culture to become more risk-adverse. Furthermore, stakeholder buy-in is critical for a framework of this nature to be adopted by senior management, as it could affect the time of delivery of the new product, which can in turn affect the financial viability of the product. A number of internal and external subject matter experts were interviewed to evaluate the framework and to determine what impact a risk framework could have on the organisation and to identify potential weaknesses and strengths of the framework.

The list of responses are documented in Appendix F.

The interviewees, as shown in Table 5.3, were selected on the basis of their positions within the organisations they represented, their influence with regard to the PDLC process, and the role they currently played within the PDLC process.

These candidates were interviewed to gain a deeper understanding of the following objectives:

- What their thoughts were regarding the impact risk management for products and services would have on the organisation, both positive and negative.
- What the challenges would be in implementing a products and service risk framework in a telecommunication organisation's PDLC process.
- After reviewing the product and service risk framework, what should be changed, what additional categories should be added and what should be removed from the framework.

The candidates were all at a senior level in their respective areas, ranging from senior managers and executive heads of departments to managing executives. The structure of the interview was first to determine what these subject matter experts believed would be the impact of a risk framework and how to implement one. Thereafter the proposed risk management framework was presented and discussed to identify any gaps in or changes required to the framework

Table 5.3: Interview list to analyse the risk management framework and approach

Position	**Key requirement for being selected as an interview candidate**
Executive head of corporate communications.	To provide a view of how a risk framework will assist an organisation to grow or maintain its level of trust from consumers.
Executive head of technical product development.	To analyse the additional technical intervention required and how the risk framework could assist the technical departments in developing controls upfront within the PDLC process.
Executive head of mobile product management for business customers. Executive head of project management for consumer products. Executive head of project management for enterprise products.	To analyse the approach needed to implement the risk framework and what the perceived impact would be from a time, financial and resource perspective.
Managing executive for corporate security. Senior manager for risk management. Executive head for corporate security in a different telecommunication organisation Senior risk manager in a different industry	To analyse the implementation of the risk framework and what they could see as perceived benefits to the organisation.

5.6.2 Results of qualitative evaluation

From the data collected (Appendix F), all interviewees were supportive of the implementation of a risk management framework for products and services. Most interviewees noted, however, that this would not be a simple task of creating a framework and then quickly implementing it within the telecommunication organisation. The one caution against implementing a risk framework is that it could give management a false sense of security that the products they launch are robust and secure, if product implementation teams are simply working around the risks or are introducing other possible risks.

The subject matter experts agreed that with the implementation of a risk management framework, not only would staff understand what is required from them to ensure that robust and secure products are launched by the organisation, but the framework would also build a risk aware culture within the organisation which is supported by policies and procedures. A risk management framework would assist the organisation in identifying risks upfront so that it would not be exposed to issues later during the product lifecycle or post-launch. These could lead to costly mitigation controls being put in place, or potential reputational damages to the brand which could have been avoided.

Concerns related to the potential negative impact of the risk management framework were identified. These included the speed of delivery to products; and that the framework could dilute concepts and products to the extent that the product is no longer fit for the purpose. These comments came from both project managers as well as technical departments. The interviews identified that, as the proposed risk framework had not yet been implemented, it would be difficult to measure the positive effect a risk aware culture would have on the organisation. However they believed an introduction of the framework would be positive as it would allow the organisation to launch products which were more robust and error free.

Once the proposed risk management framework was presented to the subject matter experts to identify potential gaps and changes to the framework, most of the interviewees believed that it was sufficient as a start to the process.

The risk management departments questioned why privacy was not part of the regulatory and legal compliance section, since POPI is only one of the regulations in South Africa and why emphasis within the framework was put on this regulation only. One of the risk management subject matter experts supported the notion that privacy remains separate in the event where someone takes this framework and implements it in a country that

does not have a POPI Act (The Republic of South Africa, 2013). In other words, it is still important that customers' privacy be maintained. Key concerns were that the framework did not measure the effectiveness of mitigation controls which were to be implemented and did not measure the cost/benefit of these controls.

Clarity was required from commercial subject matter experts as to the purpose of the finance section in the framework and what it focused on. Different interviewees suggested that finance should look at the following:

1. the cost to implement the product
2. the ROI of the product and
3. the cost of implementing controls.

If these financial values could be determined for a product, the risk associated with the product could be calculated and the proposed framework used as a decision-making tool. The comments showed that the subject matter experts understood risk management, as they were alluding to the principle of risk management, which is to assist the business in making sound decisions. This principle is discussed in Section 2.3.2, as one of the benefits of risk management.

Both the product development teams and the risk management teams had similar concerns regarding the implementation of a risk framework. They shared the opinion that it is important to get buy-in from senior stakeholders. Some product subject matter experts advised that despite senior management buy-in, the implementation of the framework must be constantly communicated throughout the organisation to ensure compliance. The requirement for a strong risk culture theme was identified, as most respondents stated that for an organisation to adopt a risk-based approach, it needs to already have a mature ERM process in place. With this in place, a risk framework for products and services risk would support the existing ERM process.

Although the intention was not to implement the framework in the organisation as part of the research, all the subject matter experts were asked what they believed the challenges were for implementing the framework, as well as what they believed would be the best approach for implementing the framework. The most common answer related to stakeholder buy-in. The second common theme was that the framework can initially be seen as additional bureaucracy and programs would need to be put in place to change

the culture of the organisation and mind-sets of individuals. All the interviewees were positive about implementing a risk management framework for products and services, however there were cautions such as the adoption and rollout of the framework.

5.7 Proposed implementation plan

In Section 2.6, a capability maturity model for risk management within products and services is proposed. For the implementation of a risk management framework, it is therefore important that organisations firstly identify at what level of maturity the organisation is and thereafter identify actions to move between maturity levels. As seen from the results of the evaluation of the proposed risk management framework, it is important that there is already a culture and adoption of ERM within the organisation prior to the implementation of a product and service risk evaluation. The adoption of ERM assists the product risk implementation as stakeholders would have already been exposed to risk management and senior executives would be aware of the benefits of risk management.

It is therefore proposed that once the ERM process is embedded within the organisation and buy-in for the proposed product risk framework has been obtained from senior executives, only then can the organisation start with the initiation of a risk management process for products and services. This could fail, however, if the organisation attempts to adopt the framework too rapidly, as the product managers could see this as additional bureaucracy and reject or work around the risk process.

The proposed risk management framework should therefore be modified and adopted based on the skillset of product managers as well as the organisation's needs. It is nonetheless important to be able to measure the benefits of implementing this new approach.

5.8 Summary

In this chapter, development of the risk framework was discussed based on the top ten issues that product managers need to consider to ensure that their products comply with relevant regulations and that only robust products enter the market. The framework is intended to be used as a skeleton and needs to be modified and adopted based on the particular product that the telecommunication organisation is considering for development. In addition, the results of the qualitative evaluation of the risk management framework were discussed and a proposal for implementation of the framework was presented.

Chapter 6

CONCLUSION AND FUTURE WORK

Telecommunications organisations who want to ensure sustainability or to compete within the South African market, need to ensure that they launch robust products that allow the consumer to build trust within the brand. The primary objective of the research was to propose a risk management framework to assist product developers in the identification of risk throughout the PDLC process. This chapter reviews the objectives set in Chapter 1 and provides additional avenues for research which could be explored further.

6.1 Summary of thesis

This thesis has provided evidence through interviews and questionnaires with stakeholders in different business units that assist in the launching of new telecommunication products and services, that there are concerns from a governance perspective about the robustness of the products. A risk framework were proposed to assist product managers to evaluate and identify these risks and implement controls to mitigate these risks early in the PDLC process. Through interviews, the risk framework was evaluated to identify whether it would be successful and what potential impact it could have on the organisation.

6.2 Contribution of the research

This study aims to add value to telecommunication service providers currently operating within the South African environment by proposing a risk-based approach as a tool to create a more risk aware culture which support robust products and services. This approach can then be communicated to customers to strengthen the brand's value and to ensure that knowledge is shared and easily available, thereby building trust in the organisation, which in turn impacts on the organisation's competitive advantage.

As described in Chapter 1, the research topic addressed in the study is: "A Risk-Based Framework For New Products: A South African Telecommunication's Study ".

In terms of the primary objective, a risk management framework for a telecommunication organisation was proposed in Section 5.3 based on the responses from the data collected over the three periods. This framework incorporated the risks proposed in the Deloitte (2009) intelligence map. Further amendments to the proposed risk framework was made when reviewing the top ten risks for telecommunication organisations, as presented in the Ernst and Young (2014) top ten risks report. Senior management subject matter experts, both within and outside the organisation, evaluated the risk framework in (Section 5.6) and provided input on how the framework could be improved as well as an implementation strategy for the proposed risk framework.

The study was supported by secondary objectives:

1. To identify the perceived risks telecommunication organisations are facing when developing products.
2. To identify the key success factors for robust products.
3. To identify a process which telecommunication companies use as a bench-mark for their risk maturity.
4. To propose a model to implement a product risk-based framework.

In response to secondary objective 1, the data collected in Chapter 4, over three periods, shows which areas the organisation could mature in risk management and the identification of key perceived risks. The management of these key risks could increase the consumer's trust in the organisation. The maturity of risk management and creating and maintaining trust by the consumer cannot be implemented overnight as discussed in

Section 2.6. Furthermore, customers could see telecommunication products as 'grudge purchases' and as such, these consumers may only be looking for the cheapest deal and not yet considering their level of trust within the organisation. Telecommunication organisations may still need to mature to a level where they can use the process of trusted applications to their competitive advantage.

Based on secondary objective 2, as organisations increase risk appetites to increase returns, they have to look at how products are designed to ensure that it is accepted by the market. Section 2.5.3 looks at four product portfolios and describes a method, including defined upfront requirements and kill point decisions which should be implemented during the PDLC process.

In relation to secondary objective 3, a maturity model for the implementation of a product risk management framework was presented in the report in Section 2.6. Organisations need to modify this model to suit their organisation structure. The proposed strategy for implementation is to first benchmark the organisation to a maturity model to understand where the current gaps are in product and service risk management, and thereafter implement incremental changes to mature the organisation.

In response to secondary objective 4, during discussion with subject matter experts in Section 5.6, additional considerations were identified for a successful implementation of a risk-based framework. An example of this is to start with a risk checklist as proposed in Section 5.5 and thereafter mature the culture and improve the checklist. Once the organisations sees the benefits of a risk-based approach, these checklist could mature with new and emerging risks.

Based on the research conducted over the different periods of data collection, it can be stated that although enterprise risk management structures in products and services are mature as seen in Section 2.1, there are still milestones for organisations to overcome with regard to product risk management maturity, before the consumer's level of trust in the organisation is fully developed.

6.3 Future work

As risk management for products and services is still a young field of study, there are many potential additional avenues of research that could be explored. The research presented in this thesis describes an approach for telecommunication organisations in South Africa

to build more robust products and services. While the research is broad in terms of the areas of research, there are still large margins of improvement that can be considered for the developed risk framework.

Within this section of the thesis the reader is presented with possible future research that can be conducted to expand the scope of the research, or to enhance the proposed risk framework:

- For the purposes of this research, a risk framework was created and proof tested by subject matter experts. Although the initial results of the framework were positive, the framework was only discussed in theory. A study should be conducted after the risk framework has been implemented in an organisation to address the following: how the framework impacted the organisation, either positively or negatively; how the influence of the framework can be measured; and what improvements can be made to the framework for optimal implementation in a telecommunication environment.

- The risk framework developed in this study focused on telecommunication organisations in South Africa, however further research on how it could be adapted for other industries or countries could be performed.

- The research in this thesis considered only one stakeholder (the organisation) and looked at the perception of internal risks. Further studies could be conducted to review the perceived risks from the customer's perspective, government's perspective and that of other stakeholders. The framework could then be modified to include these stakeholders' perceived risks.

- Further checklists could be created and enhanced to streamline the implementation of products and services risk management. A study could be conducted to test how to optimally implement this framework in the telecommunication industry.

- Research to map the framework based on the organisation's risk appetite could be performed. Based on the results from testing the framework with the subject matter experts, there are still concerns that the framework analyses risk in terms of a worst-case scenario, which could stifle the product. If the organisation has a defined risk appetite, the risk framework for products and services could be modified to ensure that only critical risks, which could have an effect on the organisation, are reviewed.

- Projects such as combined assurance and the impact that a risk management framework could have on this practice could be investigated. This would provide the first

line of assurance (line management) with a solid understanding of what is required from them.

- Based on the insights from the subject matter expert interviews, the fact that product managers would require the correct skillset was raised a few times. A study should be conducted to determine: what the best approach is to create awareness around products and services risk management; the required skills needed to implement a framework; and what the best approach would be to educate and train the necessary staff to obtain this skillset.

References

Adler, P., & Kranowitz, J. L. 2005. A primer on perceptions of risk, risk communication and building trust. *The Keystone Centre, Keystone.* Retrieved October 2015 from http://www.netl.doe.gov/File%20Library/Research/Coal/carbon-storage/TKC-Risk-Paper-fin.pdf.

Akbar, M., & Parvez, N. 2009. Impact of service quality, trust, and customer satisfaction on customer loyalty. *Assumption Business Administration College*, **29**, 24 – 38.

Alfreds, D. 2016. Vodacom calls for OTT regulation. Retrieved March 2016 from http://www.fin24.com/Tech/News/vodacom-calls-for-ott-regulation-20151109.

Altman, W., & Cooper, G. 2004. Integrating enterprise-wide risk management. *Engineering Management*, **14**, 12 – 13.

AMD. 2015. AMD 2015 Annual Report on Form 10-k. Retrieved September 2016 from http://phx.corporate-ir.net/External.File?item=UGFyZW50SUQ9MzI5MDQ0fENoaWxkSUQ9LTF8VHlwZT0z.

Apple Corporation. 2016. App distribution guide. Retrieved July 2015 from https://developer.apple.com/library/ios/documentation/IDEs/Conceptual/AppDistributionGuide/AppDistributionGuide.pdf.

Appleton, J. 1995. Analysing qualitative interview data: Addressing issues of validity and reliability. *Journal of Advanced Nursing*, **22**(5), 1365–2648.

Babbie, E., & Mouton, J. 2008. *The practice of social research.* 8th edn. Oxford University Press. ISBN 978-1133049791.

Bada, M., Sasse, A., & Nurse, J. R. C. 2015. Cyber security awareness campaigns: Why do they fail to change behaviour? *Pages 118 – 131 of: International Conference on Cyber Security for Sustainable Society.*

Benta, D., Podean, I., & Mircean, C. 2011. On best practices for risk management in complex projects. *Informatica Economica*, **2**, 142 – 152.

BusinessTech. 2014. South Africans don't trust online security. Retrieved December 2015 from http://businesstech.co.za/news/internet/63619/south-africans-dont-trust-online-security/.

Capron, L., & Mitchell, W. 2004. Where firms change: Internal development versus external capability sourcing in the global telecommunications industry. *European Management Review*, **1**, 157 – 174.

Charlesworth, J., Lawton, A., Lewis, J. Martin, V., & Taylor, P. 2003. *Toolkit 1: Study guide for MBA B736.* Open University Press.

Chen, J. V., Ross, W., & Huang, S. F. 2008. Privacy, trust, and justice considerations for location-based mobile telecommunication services. *Info*, **10**, 30–45.

Cibecs. 2014. *2014 Data loss survey.* Technical report. IDG Connect. Retrieved April 2016 from http://cibecs.com/wp-content/uploads/2014/05/Data-Loss-Survey-2014.pdf.

Coldwell, D., & Herbst, F. J. 2004. *Business research.* Juta and Company Ltd. ISBN 0-7021-6635-9.

Conversano, J. 2013. The upfront costs of compliance are looking more like a bargain every day. *Pages 34–37 of:* Williams, M (ed), *Risk and Compliance Magazine.* 4, vol. Oct-Dec. Finacier Worldwide Ltd.

Corbitt, B. J., Thanasankit, T., & Yi, H. 2003. Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research and Applications*, **2**, 203 – 215.

Corporate Executive Board. AMD's Risk Assessment Survey. Retrieved September 2016 from https://www.cebglobal.com/member/risk-management/research/case_study/07/amd-s-risk-assessment-survey.html.

Davis, C. R. 1989. User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, **35**, 982 – 1003.

Davis, C. R. 2002. Calculated risk: A framework for evaluating product development. *MIT SLOAN Management Review.* Retrieved October 2015 from http://sloanreview.mit.edu/article/calculated-risk-a-framework-for-evaluating-product-development/.

De Vaus, D. 2001. *Research design in social research.* London: SAGE Publications. ISBN 0-761-5347-7.

Deloitte. 2009. *Risk intelligence map - technology sector.* Retrieved November 2015 from http://www2.deloitte.com/global/en/industries/technology-media-and-telecommunications.html.

Dlamini, M., Venter, H. S., & Eloff, J. H. P. 2015. An innovative risk-based authentication mechanism for closing the new banking vault. *Pages 72–80 of: The proceedings of the 3rd International Conference on Innovation and Entrepreneurship (ICIE).*

Ernst, & Young. 2014. Top 10 risks in telecommunications 2014. Retrieved November 2015 from http://www.ey.com/Publication/vwLUAssets/EY_-_Top_10_risks_in_telecommunications_2014/$FILE/EY-top-10-risks-in-telecommunications-2014.pdf.

Fin24Tech. 2014. Vodacom subscriber details leaked. October. Retrieved November 2015 from http://www.fin24.com/Tech/News/Vodacom-subscriber-details-leaked-20141030.

Gartner. 2013. Gartner says smart organizations will embrace fast and frequent project failure in their quest for agility. *In: Gartner project and portfolio management & IT governance summit.* Retrieved December 2015 from http://www.gartner.com/newsroom/id/2477816.

Hamman, A. J. 2015. *The impact of anti-money laundering legislation on the legal profession in South Africa.* Masters thesis, University of the Western Cape.

Henry, J. 2010. *Creativity, cognition and development.* Milton Keynes, UK: Open University Press. ISBN 0749295945.

Hopkins, P. 2014. *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management.* 3rd edn. The institute of risk management. ISBN 978-0749465391.

IBM. 2011. Building advocacy in telecommunications. Retrieved November 2015 from http://www-05.ibm.com/cz/telecommunications/resources/Building_advocacy_in_telco_GBE03447USEN.PDF.

Institute of Directors in South Africa. 2009. King Code of governance principles for South Africa. Retrieved December 2015 from https://www.iodsa.co.za/resource/collection/94445006-4F18-4335-B7FB-7F5A8B23FB3F/King_III_Code_for_Governance_Principles_.pdf.

Institute of Directors in South Africa. 2016. Draft King IV report on governance principles for South Africa 2016. Retrieved April 2016 from http://www.iodsa.co.za/?page=KingIV.

International Standards Organisation. 2009. *SANS 31000 / ISO 31000 - risk management - principles and guidelines.* Retrieved November 2015 from http://www.iso.org/iso/home/standards/iso31000.htm.

Jacobs, C. J. 2015. *A prototype to improve the security and integrity of mobile banking.* Masters thesis, University of Johannesburg.

Jose, I. 2013. *Developing a risk management maturity model: A comprehensive risk maturity model for Dutch municipalities.* Masters thesis, Universiteit Twente.

Joubert, J., & Van Bell, J. 2013. The role of trust and risk in mobile commerce adoption within South Africa. *International Journal of Business, Humanities and Technology*, **3**, 27 – 38.

Keeley, L. 2009. Complex, strategy and innovation. 2009 Innovation summit. Retrieved December 2015 from https://vimeo.com/4964720.

KPMG. 2013. Mobile security: From risk to revenue. Retrieved December 2015 from https://www.kpmg.com/LV/en/IssuesAndInsights/ArticlesPublications/Press-releases/Documents/Mobile-security-risk-to-revenue-v2.pdf.

Lancaster, H. 2016. South Africa - mobile infrastructure, operators and broadband - statistics and analyses. Oct. Retrieved May 2016 from http://www.budde.com.au/Research/South-Africa-Mobile-Infrastructure-Operators-and-Broadband-Statistics-and-Analyses.html.

Lee, S., Kim, D., & Son, H. 2015. The impact of mobile broadband infrastructure on technological innovation: An empirical analysis. *International Telecommunications Policy Review*, **22**, 93–108.

Mayer, R. C., & Gavin, M. B. 1995. Trust in management and performance. Who minds the shop while the employees watch the boss? *Academy of Management Review*, **20**, 709–734.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. 1995. An integrative model of organisational trust. *Academy of Management Review*, **20**, 709–734.

Mayle, D., & Henry, J. 2010. *Changing Organisations.* Milton Keynes, UK: Open University Press. ISBN 978-1848735378.

Mitchell, J. A. 2011. The ethical advantage: Why ethical leadership is good for business. Retrieved April 2016 from http://www.cebcglobal.org/wp-content/uploads/2015/02/The_Ethical_Advantage_Why_Ethical_Leadership_is_Good_Business.pdf.

Morgan, R. M., & Hunt, S. D. 1994. The commitment-trust theory relationship of marketing. *Journal of Marketing*, **58**, 20–38.

MTN. 2011. MTN Group limited integrated report for year ending December 2011. Retrieved November 2015 from https://www.mtn.com/Investors/FinancialReporting/Documents/INTEGRATEDREPORTS/2011/ar_integrated_report2011.pdf.

MTN. 2012. MTN Group limited integrated report for year ending December 2012. Retrieved November 2015 from https://www.mtn.com/Investors/FinancialReporting/Documents/INTEGRATEDREPORTS/2013/ar_Annual_Financials_Statement_2013.pdf.

MTN. 2013. MTN Group limited integrated report for year ending December 2013. Retrieved November 2015 from https://www.mtn.com/Sustainability/Documents/MTN_Group_Integrated_Report_2013.pdf.

MTN. 2014. MTN Group limited integrated report for year ending December 2014. Retrieved November 2015 from https://www.mtn.com/Sustainability/Documents/MTN_Group_Integrated_Report_2014.pdf.

MTN. 2015. MTN Group limited integrated report for year ending December 2015. Retrieved November 2015 from https://www.mtn.com/Investors/FinancialReporting/Documents/ANNUALREPORTS/2015/Booklet/Annual_results_booklet_2015.pdf.

Mybroadband. 2015. Does Vodacom really have the best network in South Africa? Retrieved December 2015 from http://mybroadband.co.za/news/cellular/126694-does-vodacom-really-have-the-best-network-in-south-africa.html.

Noor, K B M. 2008. Case Study: A strategic research methodology. *American Journal of Applied Science*, **11**(5), 1602–1604.

Office of Government Commerce. 2009. *An introduction to PRINCE2: Managing and directing successful projects.* The stationary office. ISNB 978-0113311880.

Ogbonne, E., & Harris, L. C. 2000. Leadership style, organisational culture and performance: Empirical evidence from UK Companies. *The International Journal of Human Resource Management*, **11**, 766–788.

Operational Council Research. 2007. Case study 5: Risk management matrix. 60 – 65. Retrieved September 2016 from https://www.cebglobal.com/member/risk-management/assetviewer.html?filePath=/content/dam/risk-management/us/en/General/PDF/09/09/Operational_Risk_Management_Case_5_Risk_Management_Matrix(1).pdf.

Paulk, M. C., Curtis, B., Chrissis, M., & Weber, C. V. 1993. *Capability maturity model for software, Version 1.1.* Technical report. Software Engineering Institute. Retrieved November 2015 from http://www.sei.cmu.edu/reports/93tr024.pdf.

Peltier, T, R. 2005. *Information security risk analysis.* Auerbach Publications. ISBN 978-1439839560.

Project Management Institute. 2000. *A guide to the project management body of knowledge.* Project Management Institute. ISBN 860-1200917796.

PWC. 2015. *Shaping the bank of the future South African banking survey 2013.* Technical report. PWC. Retrieved November 2015 from http://www.pwc.co.za/en/assets/pdf/south-african-banking-survey-2013.pdf.

Raith, M. 2003. Competition, risk and managerial incentives. *The American Economic Review*, **4**, 1425–1436.

Risk Visualization Tools. Tomkins PLC. *A Compendium of Planning, Budgeting, and Risk Communication Templates*, 136 –137. Retrieved September 2016 from https://www.cebglobal.com/member/risk-management/assetviewer.html2.

Rossouw, D, & Van Vuuren, L. 2001. *Business ethics.* 5th edn. Oxford University Press. ISBN 978-0199048113.

Rousseau, D., Sitkin, S., Burt, R., & Camerer, C. 1998. Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, **23**, 387–392.

Selvan, S. 2013. #ProjectSunRise: Team ghostShell leaks 700,000 accounts of South African institutions. Retrieved March 2016 from http://www.ehackingnews.com/2013/01/projectsunrise-team-ghostshell-leaked.html.

Siegel, R., McDaniel, M., & Keuschner, K. 2000. *A communication strategy for residual risk.* Technical report. Retrieved November 2015 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.201.4501&rep=rep1&type=pdf.

Smircich, L. 1983. Concepts of culture and organizational analysis. *Administrative Science Quarterly*, **28**, 339–358.

Soh, D., & Martinov-Bennie, D. 2015. Internal auditors perceptions of their role in environmental, social and governance assurance and consulting. *Managerial Auditing Journal*, **30**(1), 605–622.

Summerfield, R. 2013a. Successfully managing competition risk. *Pages 13–18 of:* Williams, M (ed), *Risk and Compliance Magazine.* 4, vol. Oct-Dec. Finacier Worldwide Ltd.

Summerfield, R. 2013b. Tackling innovation risks. *Pages 7–12 of:* Williams, M (ed), *Risk and Compliance Magazine.* 4, vol. Oct-Dec. Finacier Worldwide Ltd.

Swart, I.P., Grobler, M. M., & Irwin, B. 2013. Visualization of a data leak: how can visualization assist to determine the scope of an attack? *Pages 1 – 8 of: Information Security for South Africa (ISSA).* South Africa.

Telkom. 2011. Integrated report for year ending 31 March 2011. Retrieved November 2015 from http://www.telkom.co.za/flipping-books/annual-report-2011/index.html.

Telkom. 2012. Integrated report for year ending 31 March 2012. Retrieved November 2015 from http://www.telkom.co.za/flipping-books/annual-report-2012/index.html.

Telkom. 2015. Integrated report for year ending 31 March 2015. Retrieved November 2015 from http://www.telkom.co.za/ir/apps_static/ir/pdf/financial/pdf/Telkom%20IR%202015%20Final.PDF.

The Republic of South Africa. 1998. Prevention of Organised Crime Act No 121 of 1998. Retrieved April 2016 from http://www.paab.co.za/index.php/component/docman/doc_download/1144.

The Republic of South Africa. 2001. Financial Intelligence Center Act 38 OF 2001. Retrieved April 2016 from http://www.banking.org.za/docs/default-source/default-document-library/financial-intelligence-centre-act-38-2001.pdf?sfvrsn=8.

The Republic of South Africa. 2008. Consumer Protection Act. Retrieved November 2015 from http://www.gov.za/sites/www.gov.za/files/32186_467_0.pdf.

The Republic of South Africa. 2013. Protection of Personal Information. Retrieved November 2015 from http://www.justice.gov.za/legislation/acts/2013-004.pdf.

Vodacom. 2011. Integrated report for year ending 31 March 2011. Retrieved November 2015 from http://www.vodacom.co.za/cs/groups/public/documents/document/pocm01-584703.pdf.

Vodacom. 2012. Integrated report for year ending 31 March 2012. Retrieved November 2015 from http://www.vodacom.co.za/cs/groups/public/documents/document/pocm01-584702.pdf.

Vodacom. 2013. Integrated report for year ending 31 March 2013. Retrieved November 2015 from http://vodacom.onlinereport.co.za/vodacom_ir_2013/wp-content/themes/vodacom/downloads/Vodacom_2013_integrated_report.pdf.

Vodacom. 2014. Integrated report for year ending 31 March 2014. Retrieved November 2015 from http://vodacom.onlinereport.co.za/vodacom_ir_2014/wp-content/themes/vodacom/downloads/Vodacom_2014_integrated_report.pdf.

Vodacom. 2015. Integrated report for year ending 31 March 2015. Retrieved November 2015 from http://vodacom.onlinereport.co.za/vodacom_ir_2015/.

Waqas. 2013. #ProjectSunRise: Team ghostShell leaks 700,000 accounts of South African Institutions. Retrieved January 2016 from https://www.hackread.com/projectsunrise-team-ghostshell-leaks-700000-accounts-of-south-african-institutions/.

Yeo, K. T., & Ren, Y. 2014. Risk management capability maturity model for complex product systems (CoPS) projects with an Asian perspective. *Journal of Engineering, Project, and Production Management*, **4(c)**, 81–98.

Appendices

Appendix A

CMM models for complex projects

Table A.1: General risk management CMM model part A
(reproduced from Yeo & Ren 2014)

Ad hoc	The organisation is unaware of the need for the management of risk. No culture of risk management is evident within the organisation. There is no structural approach to dealing with uncertainty (risks). There is no understanding of risk management principles or language. Almost no executive-level support for risk management exists. There is no attempt to recognise the benefits of risk management. No investment in risk management (e.g. training and education) is made. Risk events are dealt with reactively, no proactive risk management.
Initial	Organisation recognition of the benefits of risk management. A risk management policy is defined. Some initial recognition of risk management process and methodology. Some risk management training are conducted. There is experimentation on some aspects of the risk management processes.
Defined	Align risk management objectives with the objectives of the organisation. Relationships with stakeholders are built and maintained. Communicate with stakeholders to ensure risk management framework remains appropriate. Integrated risk management process is defined. Create methods and opportunities to ensure risk management is communicated to the business. Management supports a formal risk management program. Risk management is implemented on certain selected projects. Proactive behaviour to risk and threats. Lessons learned from past projects. Effective management of known/predictable risks.

Table A.2: General risk management CMM model part B
(reproduced from Yeo & Ren 2014)

Managed	Appointment of a risk manager —formal or informal — with assigned responsibilities within the organisation at appropriate levels. Education and risk sharing with other parties. Double loop learning is implemented. Institution arrangements (service level agreement (SLA) and contracts). Networked or leveraged risk management capabilities and network innovation capabilities. Focus on dealing with front-end engineering or planning departments. High risk awareness. Capable of managing most predictable risk and managing some emerging risks. An institutionalised risk management process exists.
Optimizing	The use of risk management by the organisation to gain a competitive advantage. Emphasis on opportunity management (positive risk management). Double loop learning is optimal. Cross-organisational and cross project risk management collaboration and multi learning exist. There is involvement of affected parties and internal stakeholders in risk management processes. Develop strategic alliances and create partnerships with external stakeholders. Ability to manage both known risks and emergent risks.

Table A.3: People and culture requirements CMM model
(reproduced from Yeo & Ren 2014)

Ad hoc	Lack of senior management support or involvement. The project success depends on individual efforts. The organisation is unaware of the need for management of risk and uncertainty. There is little or no attempt to learn from past projects or prepare for future projects. Individuals have little or no risk management experience.
Initial	Review resource skill, experience and competency action plans are in place to grow and maintain skill sets. Information and training sessions are held. There is a good understanding of the organisation's internal context (legal, governance, organisation structure, roles and accountability, organisation culture, perception of value). Partial acceptance of risk management. Initial assignment of responsibilities and accountability of risk. There are weak team orientations. The organisation is good at doing repetitive work. Regular meetings to review and monitor risks. Roles are clear and responsibilities are assigned.
Defined	Reasonably high team orientation. Informal training of risk management skills and practices. There is a level of risk awareness at the organisation level. The organisation is task-oriented with management by system objectives. Cross functional structures are in place to create cross functional teams. There is emphasis on teamwork and collaboration.
Managed	Cultivate a culture of risk by design. Strong teamwork, including external parties. Continuous formal project management and risk management training for project teams. Strong project driven organisation. Organisation is flexible with willingness to accept change. Adaptive leadership and management style.
Optimizing	Strong risk-aware culture with proactive approach to risk and opportunity management in the project leadership team. Active use of risk information and prior experience is used to gain an advantage. Strong project-driven organisation that is dynamic and energetic and flexible. Strong negotiation skills and ability to influence other parties. Strong organisational learning to facilitate innovation and new ideas. Enlightened leadership and management style.

Table A.4: Process requirements CMM model
(reproduced from Yeo & Ren 2014)

Ad hoc	No formal project management process or practice is available. No project management data are collected or analysed. No document of project lessons. No risk management tools are being used.
Initial	Informal project management processes are defined. Project management problems are seldom systematically identified or analysed. Fragmented risk data are collected.
Defined	Formal project planning and controls systems are established and applied. Real time monitoring of project and schedules use a defined model. Formal project database is maintained. Well established templates, software tools for quantitative analysis are used.
Managed	Consistent and systematic risk management for project portfolios. Specific methodologies used for specialised projects which is incorporated in the generic risk management framework. Define methods to ensure risk management performance is measured and reported. Project management data and process are integrated internally. Conduct post project reviews and capture lessons learned.
Optimizing	Project management and risk management data are quantitatively analysed, measured and stored. KPI's are defined and aligned to the organisation. Risk management processes are continuously improved and performance optimised. Develop a network system of coalition and partnership with external vendors and contractors. Leverage good relationships with governance structures (executive management authorities). Cultivate goodwill in communities. Risk management process is integrated into project management process. Use sophisticated tools for quantitative and qualitative analysis with proper interpretation.

Table A.5: Technology requirements CMM model
(reproduced from Yeo & Ren 2014)

Ad hoc	Basic and narrow-range technology. Single and simple products.
Initial	Simple templates and spreadsheet tools are used in some activities. Mid-range products.
Defined	Formal risk management systems defined to identify, evaluate or mitigate risk. Involvement of complex project assembly and integration.
Managed	Sophisticated software simulation tools for qualitative analysis is used. Involve large scale multiple complex assemblies and installation.
Optimizing	Advanced and some innovative technology.

Appendix B

Survey Questions from 2011

The questionnaire below was modified to ensure the anonymity of the organisation. Ten high profile products were selected and the key stakeholders who interacted with the product was interviewed. The phrase "*organisation*" replaced the organisations name within the survey.

Resources that are responsible for developing products, services, promotions and campaigns in *organisation* are interviewed. Your willingness to complete the survey can assist us in establishing improvement areas for product development.

Even if you are not directly involved in the specific area that the question address, your input will be valuable to determine how much you agree or disagree with a specific statement. Note that the final statistical analysis will ensure that the opinions of people directly involved with the area, will be captured separately.

The Likert scale is used for analysis and it is specifically designed to determine the opinion of a subject. The scale includes five response categories. When answering the questions, you will notice a middle value which is labelled as 'uncertain'. The label of 'uncertain' can also be interpreted as 'neutral', 'undecided' or even 'not applicable'. If at all possible, try to determine whether you lean more towards the 'agree' or 'disagree' end of the scale.

1. Has the product/service/campaign achieved the forecasted subscriber and revenue figures?
2. Does the product/service/campaign function as intended and documented?
3. Is the product/service/campaign easy to gain access to and function?
4. Does feedback obtained from customer care indicate customer satisfaction with the

product/service/campaign?
5.Has the product/service/campaign experienced technical defects since launch?
6. How effectively have the technical components provided the necessary support for the product?
7. Were the prescribed technical processes adhered to?
8.Have there been changes to the business rules since the product/service/campaign launched?
9.Did the project adhere to the project timelines and milestones stipulated in the project plan?
10. Was the product launched with outstanding technical and commercial issues?
11. Did all the relevant stakeholders deliver on their deliverables within the expected project timelines?
12. Has customer care support been adequate?
13. Did the third-party deliver as expected?
14. Did the product/service/campaign expose *organisation* to fraud committed by employees and customers?
15. Was there revenue leakage as a result of the product/service/campaign?

In the spaces below please list three things which:

- Went well.
- Did not go as well.

Appendix C

Survey Questions from 2012

The questionnaire below was modified to ensure the anonymity of the organisation it was used with. The phrase "*organisation*" replaced the organisations name within the survey. The survey went to all stakeholders involved within products and services launching in the organisation a list of these are shown below:

- Commercial products and service deployment product managers
- Enterprise products and Service deployment product managers
- Wholesale department
- Risk management
- Marketing department
- Legal department
- Human resources
- Procurement
- Regulatory department
- Supply chain management
- Online
- Engineering

- Billing
- Market intelligence

C.1 Introduction

The *organisation* division has established a risk management improvement framework that support leaning in product innovation though post-implementation reviews and lessons learnt. An annual lessons-learnt review is conducted which drives improvements in product innovation. The lessons learnt review on products/ services/ campaigns and promotions in 2011 has the following objectives:

- Capture key learning points for future improvement of products and services
- Review the performance of project and product management activities.

C.2 Survey methodology

Resources that are responsible for developing products, services, promotions and campaigns in *organisation* are interviewed. Your willingness to complete the survey can assist us in establishing improvement areas for product development.

Even if you are not directly involved in the specific area that the question address, your input will be valuable to determine how much you agree or disagree with a specific statement. Note that the final statistical analysis will ensure that the opinions of people directly involved with the area, will be captured separately.

The Likert Scale is used for analysis and it is specifically designed to determine the opinion of a subject. The scale includes 5 response categories. When answering the questions, you will notice a middle value which is labelled as 'uncertain'. The label of 'uncertain' can also be interpreted as 'neutral', 'undecided' or even 'not applicable'. If at all possible, try to determine whether you lean more towards the 'agree' or 'disagree' end of the scale.

The survey consist of two sections. Section A is in the format of a survey while Section 2 allows you to make specific recommendations that could improve your specific area of

involvement in new product development. These areas of improvement as mentioned by you as a primary stakeholder in the PDLC process will hopefully provide a useful starting point that can ultimately be utilised to improve *organisation* innovation processes and ensure that *organisation* is better equipped at product innovation.

The survey will take approximately 20 minutes of your time. Please be sure that your anonymity is ensured and all answers will be treated in the strictest confidence.

The survey measures your overall perception regarding products, services, promotions and campaigns that was implemented or in the process of being implemented during 2011. When the survey refers to a product, this also refers to a service, promotion or campaign. All questions should be answered within the context of the new product development environment.

C.3 Survey questions

INSTRUCTIONS: Please rate how strongly you agree or disagree with each of the following statements by placing a check mark in the appropriate box.

Competitor and marketplace

1.1 Competitor actions were adequately monitored and responded to.
1.2 New products were launched before competitors could launch comparable products.
1.3 Products provided clear competitive advantages.

Customer

2.1 The target markets were clearly defined using convincing research data.
2.2 The product specifications met customer standards and demands.
2.3 Customers were convinced that they received value for money.

Technology and innovation

3.1 *Organisation* launched innovative products.

Regulatory and legal

4.1 Legal and regulatory restrictions were adequately anticipated.
4.2 Appropriate contract arrangements with suppliers were settled.
4.3 A good awareness existed of legislation and regulations that impacts on products.

Investors and stakeholders

5.1 Support of key opinion formers for the products were assured .

Business model

6.1 The business models were generally clearly defined.

6.2 The business model would succeed in generating profitable revenue and/or market share.

6.3 Accountabilities for risks were clearly defined between different parties.

Organisation structure, management and resources

7.1 Leadership was effective to ensure that sufficient support and resources was allocated during the product lifecycle.

Intellectual property, trademarks and patents risks

8.1 *Organisation* were well protected against any IPR and trademark infringements.

Third-party risks

9.1 Past experiences with third-party suppliers were positive.

9.2 Third-party suppliers were reliable in delivering according to requirements .

9.3 Effective due diligences were conducted on vendors.

Value chain

10.1 New products were effectively communicated to trade partners.

10.2 Customer support in the delivery channels were adequately tested and measured.

10.3 Customer support in the distribution channels were of high quality.

Strategy

11.1 Products helps to achieve most of *organisation* five business strategies.

Internal governance

12.1 *Organisation* internal policies and procedures are adhered with.

Business rules and pricing

13.1 All business rules applicable to the product were known and easy to find.

13.2 The overall impact of business rules were assessed.

13.3 Knowledge of customers' price sensitivity existed.

Business Process

14.1 Existing business processes performed optimally.

14.2 Processes were monitored to ensure that they work effectively.

14.3 Processes that did not function as intended were redesigned.

Customer care

15.1 Customer care requirements are sufficiently addressed.

15.2 Customer care departments have sufficient access to info to sufficiently service customers.

15.3 Agents are well trained to support products.

Financial Management

16.1 Sales projections or uptake figures for the products were realistic.

16.2 Only the most financially viable products were implemented.

16.3 Estimated profit margins were based on convincing research data.

Project and knowledge management

17.1 Best practices were followed in terms of scope management, delivering on time, budget and quality is monitored.

17.2 Project teams learned from past experiences.

17.3 Delays in launching products did not impact on the commercial viability of products.

Financial and regulatory reporting

18.1 Financial business cases provided a clear picture of the commercial viability of products.

18.2 Volume estimates were based on clear and reliable data.

18.3 Lodgements complied to regulatory requirements.

Product management reporting

19.1 Product performance in the market was adequately tracked.

19.2 Remedial actions were applied to underperforming products.

19.3 New product performance targets were adequately measured.

Risk management methodology

20.1 Risk issues were adequately anticipated and mitigated.

Internal and external fraud

21.1 Products were adequately assessed for fraud exposures to protect *Organisation* as well as customers.

Money laundering

22.1 Products were adequately assessed to determine exposures for corruption, bribery and money laundering activities.

Revenue assurance

23.1 Products were adequately assessed to determine exposures to revenue leakages.

Physical security

24.1 Products were adequately assessed to determine physical security risks to customers and employees.

Health, safety and social responsibility

25.1 Product appealed to generally accepted values (e.g. health, safety, nature and environment).

Technology capacity and BCM

26.1 Products were designed with sufficient capacity and scalability.

26.2 Disaster recovery and/or BCM were adequately ensured.

26.3 Plans for service recovery of products were documented, tested and available.

Technology information security

27.1 Confidential information was adequately secured.

27.2 Customer privacy issues were adequately anticipated.

27.3 Products conformed to industry best practices in terms of information security management.

SLA management, control and release processes.

28.1 Service levels were monitored for adherence to timelines, quality and maintenance.

28.2 SLA's relevant to the products were well documented.

28.3 Formal processes were followed in terms of change control and release management.

Technical solution design

29.1 Products intended functionality were well known and specified.

29.2 Products met the functional requirements.

29.3 Interactions of products with other systems were well understood.

End-to-end testing

30.1 Reliable end-to-end testing was conducted before products launched.

30.2 Adverse performances as a consequence of technology or scripts changes were tested and adequately measured.

30.3 Consumer appreciation of the product was tested and measured adequately.

Public relations and communications

31.1 Products succeeded in enhancing and supporting *organisation* reputation and brand.

31.2 Public Relations for products were effective.

31.3 Possible negative external reactions were effectively anticipated.

Marketing

32.1 Marketing communication clearly conveyed the benefits and advantages of the product.

32.2 Advertising of products were effective.

32.3 Products were communicated successfully to target customers.

Product maintenance

33.1 The product is monitored and enhanced to ensure that it continues to function effectively.

C.4 Additional recommendations

Please use the space below for additional comments regarding the survey above.

34 What are the three main concerns that you have in order of importance?

35. What went well?

36. What could be improved?

Appendix D

Interview questions from 2015

The following questions were asked in 2015 to product management executives to understand their risk and how their area of responsibility.

The following areas were interviewed

- Commercial products and service deployment product managers
- Enterprise products and service deployment product managers
- Technology
- Risk management
- Online department
- Legal and regulatory departments

The following questions were asked to all interviewees:

What are your objectives of your department in relation to the organisations strategy? What are the three biggest risks facing your department related to not meeting the objectives of the organisation?

Appendix E

Proposed risk management framework for products and services

Table E.1: Legal and regulatory requirements

	Legal and regulatory
Strategic	Are there additional licence requirements needed for operating this type of service?
People	Sufficient legal and regulatory skills for support or advice on the product offering are available.
Process	Legal advisor ensures compliance with both local regulation and legislations. Terms and conditions for this service are available to the customer. How will the customer be able to view the terms and conditions? Can customer care/or agent provide advice to the customer on the product?
Technology	Contracts with suppliers are robust and signed by all parties.
External factors	Is there on-going liaison with government to keep abreast of legislative, regulatory or tax regulation changes?

Table E.2: Privacy requirements

	Privacy
People	Is a privacy awareness program in place?
Process	In the event that customer information is passed to a third-party, explicit consent is required from the customer. Privacy officer consulted with respect to all information that will be available to third-party vendors, cross border transfer, and on processing of the information. Customer privacy concerns need to be taken into account and controls to mitigate the risk of leakage need to be put in place.
Technology	Interfaces as to who has access to private/confidential information and to ensure that data cannot be tampered with need to be controlled.
External factors	Will the product be compliant with the POPI Act (The Republic of South Africa, 2013), when it comes into effect? Does the product comply with privacy principles as set out in the Constitution and Electronic Communications and Transactions Act? Does the organisation know how to deal with data leakages?

Table E.3: Competition requirements

	Competition
Strategic	Organisations need to highlight any competitive activity that the product is counteracting and indicate whether the organisation is the first in this market. Alternatively, the organisation needs to highlight the competitive advantage.
People	Is there an HR process in place to ensure that critical staff do not move to competitors?
Process	A comprehensive competitor analysis needs to be conducted including a detailed analysis of the competitors, and how the organisation's product compares with existing products and what strategy will be used to inform customers of the offering.
Technology **External factors**	Products need to be built as documented in the design. Review the current market place in terms of: What the critical success factors are to implement the solution in the market, who the competitors are, how this service differs to ensure the success thereof?

Table E.4: Customer requirements

	Customers
Strategic	What are the market trends within this sector? What are the objectives of this product offering: to ensure that the customer base grows, generate revenue or for strategic intent? Show the products competitive advantage and differentiation compared with other existing products.
People	Are sufficient sales and marketing budget and headcounts available? What customer care service will be used for supporting the queries? All support processes must be clearly documented.
Process	Review the current customer base. How will this base be affected by the implementation of the service? Well defined training manual needs to be created to support the product. Each stakeholder on product needs to have clear, measureable deliverables.
Technology	Are processes put in place for handling scenarios and reversed transactions?
External factors	An analysis of what the target market needs are, should be performed.

Table E.5: Reputation and brand management requirements

	Reputation and brand management
Strategic	The organisation executive management needs to approve products to ensure they are in line with the objectives of the organisation.
People	Sufficient resources need to be available to ensure the effectiveness of this product.
Process	The legal department needs to take due care to ensure that there are no infringements on intellectual property rights (IPR)/trademarks/patents. The product team needs to ensure that a proper communication message is sent out to prospective customers. A public relations and communication strategy needs to be created prior to the project launch. Campaign messages must adhere to communication and legal standards. A marketing plan needs to be created and approved before the service is commercially launched.
Technology	Are there technical solutions to capture complaints by customers?
External factors	How does the brand department manage perceived risk?

Table E.6: Financial requirements

	Financial
People	Ensure that there is an accountable financial advisor. Are business plans in place to ensure resource plans covering growth in different scenarios? Has forecasting been taken into account when signing off the financials?
Process	Business rules need to be robust to ensure that revenue leakages do not occur. The legal department needs to ensure that business rules for the service do not contravene any regulations or legislations. Reports and financial impacts and forecasting are monitored. Are there supporting documents for all payments made to agencies/business customers?
External factors	What impact do fluctuations in foreign exchange rates have on the service?

Table E.7: Technology requirements

	Technical, IT, network and security
People	Who is accountable for security and IT? Information on how the product supports innovation within the organisation must be documented and approved by business and the technology partners. Is there a process for training and refresher training for agents?
Process	Are there sufficient disaster recovery (DR) and BCM plans in place? All infrastructure used in the fulfilment of this service needs to undergo capacity testing to ensure the effectiveness of this service. Has the business continuity plan been tested? Is there a process in place for on-going capacity and performance requirements? Capacity planning and monitoring need to be in place for SMS and USSD. Is there a communication plan in place which details contracts, responsibilities and escalation procedures for all business functions? Is there a process and policy in place to ensure that physical access to the technology environment is restricted to authorised persons?

Table E.8: Technology requirements continued

	Robust end-to-end testing is required on the service prior to launch. This would include: (not exhaustive list) - Volume or stress testing - Negative testing - Error handling - User and customer acceptance testing - Control testing
Technical	The product manager needs to ensure the technology supports the product. Are local systems monitored 24/7 to ensure continued operations (hardware, memory, disks) ? Are there system logs and are they monitored? Is automated failover to secondary systems implemented? A vulnerability test on all infrastructure needs to be performed and a penetration test needs to be done on all front end systems. Has the local security officer approved the solution and architecture? Is there a policy in place to ensure that access is restricted to personnel that no longer requires the access (both physical and logical)? Has the appropriate physical and environmental controls been put in place to ensure prevention and/or detection of environmental hazards? Are physical access requests documented, and do these clearly indicate the level of access requested and the appropriate approval level of local management? Are operational procedures documented, such as computer start-up and shut-down, backups, equipment maintenance and media handling? Has a process been implemented to audit access to systems and changes? Are logs secured from tampering and retained for an agreed period? Is there a process in place to routinely obtain and apply security related software patches and upgrades? Is there software to detect security vulnerabilities or attacks (firewalls, intrusion detection and prevention systems, antivirus?) Is the network connectivity secure? Is there a user access policy in place to ensure logical access to technology environment to restrict unauthorised persons? Are processes and standards in place to grant/review/revoke user's access to the operating system, database? Are processes and standards in place to grant/review/revoke users' access to service? Is there security in place to protect the USSD system? Is there security in place to protect the logging service on the USSD system as banking details would normally be traversed in clear text? Is there a process in place for granting/reviewing/revoking and controlling developer and third-party access to local systems? Is there a process in place to monitor third-party activity on the local system? Is there a process to record appropriate incidents and are these stored in a repository for future use?

Table E.9: Internal and external fraud/AML/RA requirements

	Internal and external fraud/AML/RA
People	An accountable party needs to be identified for monitoring fraud activity with could potentially take place on this service. Has an AML analysis been appointed? Does the AML policy include details of relevant AML process for agent procedures i.e. know your customer, AML training for staff and suspicious activity reporting?
Process	Test cases for fraud need to be developed as well as controls for monitoring fraud and escalation. These need to be tested prior to the product being commercially available. Have AML procedures been created for staff covering all process requirements for AML systems and controls?
Technology	Reports flagging irregular activity on reversals and purchases should be automated and need to be sent to a forensics department for investigations. Is there a process to monitor transactions?

Table E.10: Business practice requirements

	Business practice
Strategic	Has appropriate sponsorship and commitment from senior management been obtained?
People	Are there processes implemented for escalation to operational teams for complex transactions cases?
Process	Support processes and escalation processes need to be clearly documented and signed off by the relevant parties.

Table E.11: Third-party management requirements

	Third-parties
Strategic	Do third-parties have strategic alliances with the organisation?
People	A list of third-party providers' needs to be identified and SLAs need to be put in place with these third-parties.
Process	Review what contracts are required with third-party vendors and check that these have been approved. Third-parties need to go through the procurement process to ensure internal governance. A list of third-parties and their subcontractors needs to be listed on the organisations database. A due diligence (financial and technical) is required prior to the contracts being signed.
Technology	How does the organisation interface with the third-party?
External factors	How are third-party liquidations managed?

Appendix F

Proposed risk framework interview

Below are some of the comments that were received during the interviews. To maintain the confidentiality of the telecommunication companies that were represented, the organisations' names are omitted from this report. Similar answers from different respondents were consolidated into one statement. The interviews were recorded as audio and only key statements were transcribed.

F.1 Interview questions and answers

The interview questions set out to determine subject matter expert's thoughts on the positive and negative impact that a risk management framework for products and services would have on an organisation.

The following section is the data which were received from the candidates which were interviewed.

F.1.1 Positive responses to implementing a risk framework for products and services

- Implementing a risk framework for products and services will ensure that the products are safe and secure. The products speak to the customers, it do not have information security issues and is marketed to the customer via the correct channel. An example of this would be the go to market strategy of a new product, via

channels such as the Internet, to low-end users who might not have access to the Internet. In this case, the chances of success of the product would be minimal.

- A positive impact of implementing a risk-based approach to product and service development, is that the organisation will know upfront what are the potential problem areas are and what the risks of preventing the project from achieving success Thereby, identifying the things that could harm the company early is positive.

- Another positive aspect of a risk management approach is an improved customer experience, because it ensures that the organisation launches products that cater to the customer's needs, that customers are protected and that customers know what to expect from the organisation. The product's functionality will meet customers' expectations, which increase trust in the product. Trust is also linked to customers purchasing more, which impacts the organisation's bottom line and revenue.

- Having a formal risk methodology in place will assist staff in understanding what is required from them to perform their job well and to ensure that a culture of risk is built into the organisation. The culture can further be supported by guidelines, policies and procedures.

- Implementing a framework will improve the governance and control of products and services and will ensure that all the "i's" are dotted and the "t's" are crossed.

- The implementation of a risk framework will assist in ensuring that the organisation's brand and image is not negatively affected. Furthermore, it will proactively prevent the organisation from contravening laws and regulations.

- A risk-based approach helps to reduce the risk of producing products that are not performing as expected.

- A framework of this nature will ensure internal alignment between different stakeholders and it will assist in breaking down silo's, which will assist in ensuring that the organisation have resources from different divisions within the organisation being able to consult on the product.

- There were times when products came to the final approval stages, only to find that the product manager did not cover the basic issues related to risk management and reputation and sometimes even from a technology perspective, and that it did not link back to the concept that was initially approved.

- The organisation always want to be top-of-mind with its customers, but being top-of-mind comes with responsibilities. Customers want to believe that the organisation is protecting their information. When a large trusted organisation makes mistakes, it causes bigger reputational damage than smaller organisations.

F.1.2 The biggest challenges of implementing a framework for risk management in products and services

- The biggest challenge for implementing a risk management framework will be to get buy in, from senior management, the product development and commercial teams as well as project managers and for them to see the overall value add of the risk framework.

- Commercial teams might see risk assessment as delaying the launch of their products by adding additional bureaucracy and controls.

- People do not understand risk management, for example, when product managers think of risk, they normally highlight budget, resources and time and do not do a proper risk assessment of the product itself.

- Product managers do not have the skills or the time to run proper risk management processes on products.

- Additional governance adds additional bureaucracy and because governance now adds new stakeholders to the decision-making process, it could have a negative impact on the fast delivery of products. The issue of risk management is that it is not that easy to work out probability and when the worst-case scenario is used in the decision-making process, it could impact on the delivery of the product.

- One of the challenges of rolling out a risk-based approach is to find out exactly where in the PDLC risk should get involved. Depending on where risk is included in the process, the creativeness of the product could be hampered. Initial concepts are sometimes great, but when all the mitigating controls are added, the product gets diluted to a level where it is not designed as initially intended and it does not have the intended impact.

- Product owners would have to factor in additional time as the risk management process might slow down the launch of products, therefore the risk process should be flexible.

- One of the biggest challenges would be the skills and resources required to implement the risk framework.
- There is a risk of a false sense of security when implementing such a framework, because it can become a check-box exercise. Management could also perceive that resources are complying with the risk framework; however they could be working around it.
- Within the telecommunication environment specifically, there are two different types of mind-sets, one is process-driven (one could say its more aligned to the IT world) and then there are the engineers who focus more on outcome. If the proper buy in from all the stakeholders and all the different type of people are not really working with the framework, it might not produce the intended benefits.

F.1.3 What is the best approach in your opinion, to implement a products and services risk management framework

- The best approach would be a collaborative effort between the product development team and the risk management team. This will increase the buy in and will ensure that the model and risk process can fit into the commercial team's PDLC process.
- Before implementing a risk framework, there has to be a mature ERM process already in place. These structures could advise the business why it is important to undergo risk management at the initial stages of the PDLC process.
- A structured approach would be the best option to ensure that stakeholders get the required training.
- Start off by having a list to identify the top twenty potential risks that would impact on most of the new products in an organisation. Thereafter, start building on that list, because as soon as one gives someone a few risks to work on, this gets their mind to start thinking of new risks. This process can undertake by using a risk universe, which should already be a part of the organisation's ERM field. The framework can be customised to target specific risks.
- One of the challenges would be how to change the culture of the organisation so that the organisation is more risk adverse. To implement a culture for the acceptance of a risk framework, there needs to be buy-in from the top, but this buy in needs to be communicated to the operational level as well.

- The framework does not need to be perfect before it gets introduced into the organisation, but it should include stakeholders from major areas who are impacted early on in the buy in process. This way they get the feeling that they were included in the introduction of the process, which will create even more buy in from them and they can then model the framework as they see fit. This approach could also give these stakeholders a sense of ownership after implementing the framework, instead of it being something they were told to do.

F.1.4 Evaluation of the risk framework

At this stage of the interview, the framework was presented to the subject matter experts to identify what was missing or needed to be changed in the framework.

- The initial risk management process should be sufficient for now, as it will not be too onerous on the product managers.
- Ensure that robust testing, including negative testing, functional testing and unit testing are added to the framework.
- Measurements of how well controls are implemented should be a part of the risk management process.
- One would assume that product managers in the organisation are aware of the legal and regulatory requirements of new products, but that is not always the case.
- Privacy and the protection of data are currently high on most organisations' agendas.
- Finance needs to look at three aspects, the budget of the project, is it worthwhile to implement the project and is there a return of investment. Also, if additional controls are implemented, what will be the cost and time implications of these controls?
- The technology aspect of the framework is too detailed, which could cause confusion when it is given to product managers. Therefore, the framework needs to be split into two aspects: How the product is built? That is: architecture and BCM; and how do the organisation go about protecting what was built? That is information security.

- With regard to the business practice category, it to speak more to the organisation's culture, because different telecommunication companies have different practices in place. Even within an organisation, different divisions have different business practices. Therefore, it means that management must be questioned and challenged if they say that "it has always been done like this".

- Because most products get built in addition to business as usual (BAU) services, the framework needs to look at how this new product would affect or change the BAU processes as well. For example, commission structures and support processes of existing products are not affected. Sometimes the existing processes are not fit for purpose, but because they are business as usual, they do not always get checked.

- The finance section in the framework should not only look at the return on invest, but it should use the organisation's risk appetite to identify which risks can be accepted and which risks should be mitigated.

- The framework should not only look at the negative aspects of risk management, but also the opportunity risk that show the benefits of risk.

- When external suppliers are being used, how does the organisation ensure that they comply with the organisation's minimum standards.

- What is missing from the framework is to review, what the organisation's capabilities are to support the product. For example, telecommunication companies recruit skillsets that are unique to a telecommunication company. As the organisation is evolving, how do the organisation know that they have the skillset to support new products, such as cloud and financial services? How will they use the existing skills in the organisation and integrate them into the company's wide range of products?

F.1.5 What are the next steps that should be taken after the initial risk framework for products and services is implemented?

- Organisations need to keep on modifying and adapting the risk framework according to the organisational needs.

- After the organisation has implemented a risk framework for product management, it need to put a process in place to measure the benefits of this approach.

- The organisation needs to review the framework to see if the controls that it identifies do actually prevent the risk from occurring. By doing a post-mortem of the project, it can be determined how effective these controls actually are.

- The lessons learnt from the process is key to ensure that the organisation consistently learns from past projects. A lot can be learned from how the organisation went about preventing some risks and it can determine whether those controls should be used in future projects. These lessons can also be used to update the framework.

- Once the product and service risk framework is put in place, measurements against certain criteria is of high importance, because it will show whether the process has had a positive effect on the organisation.