ADDRESSING THE INCREMENTAL RISKS ASSOCIATED WITH SOCIAL MEDIA BY USING THE COBIT 5 CONTROL FRAMEWORK

By

Petro Gerber

Thesis presented in partial fulfilment of the requirements for the degree of Master of Commerce (Computer Auditing) in the Faculty of Economic and Management Sciences at
Stellenbosch University

Supervisor: Mrs G Steenkamp
March 2015

DECLARATION

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof, that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: March 2015

ACKNOWLEDGEMENTS

I would like to express my gratitude to:

- Our Heavenly Father who gave me the willpower and determination to complete this research;
- My husband, family and friends for their continuous words of encouragement;
- My supervisor, Gretha Steenkamp, for her patience and guidance throughout the process.

ABSTRACT

Social media offers great opportunities for businesses and the use thereof will increase competitiveness. However, social media also introduce significant risks to those who adopt it. A business can use existing IT governance control framework to address the risks introduced by social media. However a business should combine existing control frameworks for adequate and complete IT governance.

This study was undertaken to help businesses to identify incremental risks resulting from the adoption of social media and to develop an integrated IT governance control framework to address these risks both at strategic and operational level. With the help of the processes in COBIT 5, this study provides safeguards or controls which can be implemented to address the IT risks that social media introduce to a business. By implementing the safeguards and controls identified from COBIT 5, a business ensures that they successfully govern the IT related risks at strategic level. This study also briefly discuss the steps that a business can follow to ensure IT related risks at operational level is addressed through the implementation of configuration controls.

OPSOMMING

Sosiale media bied groot geleenthede vir besighede en die gebruik daarvan sal mededingendheid verhoog. Sosiale media hou ook egter beduidende risiko's in vir diegene wat dit aanneem. 'n Besigheid kan bestaande Informasie Tegnologie (IT) kontrole raamwerke gebruik om die risiko's wat ontstaan as gevolg van die gebruik van sosiale media aan te spreek. Vir voldoende en volledige IT korporatiewe beheer moet 'n besigheid egter bestaande kontrole raamwerke kombineer.

Hierdie studie is onderneem om besighede te help om die toenemende risiko's wat ontstaan as gevolg van die gebruik van die sosiale media, te identifiseer en om 'n geïntegreerde IT kontrole raamwerk te ontwikkel om hierdie risiko's op strategiese sowel as operasionele vlak aan te spreek. Met die hulp van die prosesse in COBIT 5 voorsien hierdie studie voorsorgmaatreëls of kontroles wat geïmplementeer kan word om die IT-risiko's waaraan die besigheid, deur middel van sosiale media blootgestel is, aan te spreek. Deur die implementering van die voorsorgmaatreëls en kontroles soos geïdentifiseer uit COBIT 5, verseker 'n besigheid dat hulle die IT-verwante risiko's op strategiese vlak suksesvol beheer. Hierdie studie bespreek ook kortliks die stappe wat 'n besigheid kan volg om te verseker dat IT-verwante risiko's op operasionele vlak aangespreek word deur die implementering van konfigurasie kontroles

TABLE OF CONTENT

LIST OF FIGURES, TABLES AND APPENDICES

List of figures

List of tables

List of appendices

CHAPTER 1

INTRODUCTION

1.1 Background

Social media is mobile and web-based technologies that enable people to communicate and interact freely with each other (Kietzmann, Hermkens, McCarthy & Silvestre, 2011:241). The business use of social media has experienced exceptional growth over the last few years with some businesses allocating a separate budget to social media (Nielson, 2013:5). Business' uses include marketing, market research, customer service etc. When a new technology such as social media is introduced, new risks at strategic and operational level are also introduced to the business. Although most organisations acknowledge the advantages of using social media, most of them do not implement governance strategies and structures for its use (Petty & Van der Meulen, 2011).

The King III report which became operational in South Africa on 1 March 2010 specifically addresses the implementation of information technology (IT) governance principles (Goosen & Rudman, 2013:835). One of the key focus areas of the IT governance in King III is strategic alignment, whereby the business strategic objectives and operations should be aligned with IT's strategic objectives and operations. If the policies and procedures defined by executive management is miscommunicated to the IT professionals, IT's understanding and implementation thereof will be different, thus leading to IT gap.

In order to implement IT governance principles and structures and at the same time overcome the IT gap a business-IT alignment process must be implemented (Goosen & Rudman, 2013:839). There are several existing control frameworks such as Control Objectives for Information Technology and Related Technology

(COBIT) or Information Technology Infrastructure Library (ITIL) which can assist a business with the business-IT alignment process. According to Goosen & Rudman (2013:17), in order to achieve business-IT alignment and successfully implement IT governance principles, a business will need to use existing control frameworks and combine them to develop an entity-specific integrated control framework which can be implemented to address business strategies and operations as well as IT strategies and operations.

Goosen (2012:34) developed a seven step integrated control framework to ensure that business-IT alignment is achieved and that IT risks are addressed at strategic and operational level. Goosen's (2012:34) seven step integrated control framework could be used in order to address the risks of social media at strategic and operational level.

1.2 Research objective

The objective of this study is to develop an integrated IT governance control framework to identify and manage the incremental IT risks which arise when a business uses social media. This study will focus mainly on developing controls or safeguards for IT risks at a strategic level and to a lesser extent on addressing the IT risks at an operational level.

1.3 Research motivation

Social media has become an integral part of most businesses. Social media introduces many IT risks to the business, both at strategic and operational level. Businesses need to have governance policies and structure in place to govern these risks. Defining these governance policies and structures can be complex and difficult and if not done correctly it can lead to an IT gap. This study was undertaken to help businesses to identify incremental risks resulting from social media and to develop an integrated IT governance control framework to address these risks both at strategic and operational level.

1.4 Design and methodology

A non-empirical study was conducted by reviewing existing literature from academic published articles, whitepapers, theses and websites. A thorough literature review was done which enabled the author to acquire a better understanding of the following:

- IT governance principles
- IT governance structures, processes and mechanisms
- IT gap and business-IT alignment
- Integrated control framework for IT governance
- Social media categories
- Business use of social media
- Risks relating to social media

From the literature review the author was able to identify that a control framework (a system of control categories that covers all fundamental internal controls expected within a business) could be applied to achieve IT governance, however a business should combine existing control frameworks for adequate and complete IT governance. Goosen (2012:34) developed a seven step integrated control framework for IT governance, which could be followed for IT governance of social media. The steps identified in Goosen's framework and applied to social media is as follows:

Step 1: Identify business imperatives for social media.

Step 2: Identify the incremental risks derived from the business imperatives for social media.

Step 3: Identify COBIT 5 as a relevant IT governance control document.

Identify the processes in COBIT 5 that is relevant to governing social media risks.

Map the identified incremental risks of social media against the relevant processes to identify controls that a business should implement.

Step 4 – 7: Explain the process a business should follow to address risks for social media on operational level.

1.5 Organisation of the research

Chapter 2 and 3 contains a literature study on IT governance and social media respectively. Chapter 2 provides an understanding of IT governance concepts, the IT governance principles of King III and to identify how to develop an integrated framework which can assist with the implementation of IT governance principles when a new technology is introduced to the business. Goosen (2012:34) developed an integrated framework which simplifies the business-IT alignment process, overcomes the IT gap and ensures that IT governance is achieved both at strategic and operational level. This framework can be applied by a business on any new technology introduced to the business. One of the technologies that a business can use is social media. Chapter 3 provides an understanding of what social media is, its business uses and which risks it introduces to a business.

In chapter 4 of this study, the business imperatives for social media are identified. From the business imperatives the incremental risks introduced by social media are identified. This represents step 1 and 2 of the integrated control framework.

Chapter 5 presents a discussion of the COBIT 5 control framework. The processes which are linked to social media are then identified (Appendix A). Each incremental risk as identified in chapter 4 is then mapped to the processes that are applicable to specific risk. From each of the processes safeguards or controls are identified to address each incremental risk at a strategic level (Step 3). Other literature was also reviewed to ensure a comprehensive list of safeguards.

Chapter 6 discuss the steps a business should follow to ensure that IT risks relating to social media is also addressed on an operational level (Steps 4 – 7). The study presents a discussion of access paths, IT architectural components and the configuration controls that should be identified.

Chapter 7 contains an overview of the research with a summary of the research findings and a discussion of possible future research.

1.6 Limitations of the research

The research is subject to the following limitations:

- This study did not include all possible business imperatives but only the main ones as identified from the business use of social media by the author. Every business can have different business imperatives depending on their requirements and the business imperatives can change over time.
- This study did not research the effective and efficient governance of all risks relating to social media. It only focuses on the incremental risks as identified by the business imperatives.
- This study did not deal with pre-adoption issues of social media, the choice of which social media network is more suitable for business use or changes from one social media network to another. For this study it was assumed that social media networks were already in use by the business.
- This is a general study and therefore do not deal with specific compliance with legal, regulatory and contractual requirements.
- Only the processes of COBIT 5 that have an influence on the identified risks were evaluated. It can be that a business can have other risks and that other processes can be applicable.
- The focus of this study was on the business use of social media and not the personal use of social media by the employees. Only controls which the business can implement for their own use were therefore identified and not any controls for personal use of social media networks by employees. Only the access paths for business use of social media was identified and not any access paths from personal devices of employees.
- For the purpose of this study the business is a third party using social media networks and not the provider thereof.
- This study does not address any risks or provide any controls regarding service level agreements between the business and social media provider.

- This study does not focus on a specific business continuity plan for social media.
- No case study was done thus operational risks cannot be discussed in detail.

CHAPTER 2

INFORMATION TECHNOLOGY GOVERNANCE CONCEPTS

2.1 Background

Companies rely greatly on IT to achieve their business goals. When a new technology is introduced, new risks are also introduced to the business. According to Badenhorst (2009:7) the risks relating to IT have become substantial and therefore governance of these IT related risks are important.

The King III report which became effective in South Africa on 1 March 2010 specifically addresses the implementation of IT governance principles (Goosen & Rudman, 2013:835). However, the King III report only addresses the IT governance requirements at a general level without giving guidance on the implementation thereof (Goosen & Rudman, 2013:835). A number of control frameworks such as COBIT or ITIL are available to assist businesses with the development and implementation of IT governance strategies and structures.

Chapter 2 aims to provide an understanding of what IT governance entails including the IT governance principles as contained within King III. It further aims to provide and understanding of how to use existing control frameworks in order to develop an integrated control framework which will assist with the implementation of IT governance principles when a new technology is introduced to the business.

2.2 Corporate governance

Corporate governance is defined as the structures and relationships which determine a company's direction and performance. It includes relationships between the board of directors, management and all other stakeholders (McRitchie, 1999). Good corporate governance is achieved through ethical, responsible, accountable, fair and transparent management (IODSA, 2009).

After the collapse of international high-profile companies, such as WorldCom and Enron, various laws, practices and regulations have been published to ensure good corporate governance. Corporate governance should be a tool used to monitor and achieve the objectives of the company (Fleming as cited by Terblanche, 2011:6). However, there is a risk that companies might turn the laws and regulations on corporate governance into an objective only for the purpose of annual reporting, instead of applying the governance principles to achieve their objectives (Kaselowski, 2008:12).

2.3 IT governance

IT has become an essential part of business. It is used to conduct, support, sustain and grow the business. Information systems are now part of the strategy of a business and introduce significant risks both at operational and strategic level (IODSA, 2009). IT governance has therefore become an integral part of corporate governance (Badenhorst, 2009:5).

IT governance is based on the same fundamental principles as corporate governance (Terblanche, 2011:12). Several definitions exist for IT governance. Table 2.1 presents some of the definitions used for IT governance.

Table 2.1: IT governance definitions

Defined by	Definition
Gartner (s.a.)	IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organisation to achieve its goals.
IT Governance Institute (ITGI) (2003:10)	IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.
Van Grembergen	IT governance is the organisational capacity to control the

(2000:41)	formulation and implementation of IT strategy and guide to proper direction for the purpose of achieving competitive advantages for the corporation.
Hardy (2006:56)	IT governance is the responsibility of the board of directors and executive management. The overall objective for boards and executives driving IT governance should be to understand the issues and the strategic importance of IT so their enterprises can sustain operations and expand upon activities as they move into the future. IT governance activities should focus on ensuring whether expectations for IT are met, and that IT risks are addressed.

(Sources: As indicated in table)

From Table 2.1 it is evident that IT governance is achieved when the board members understand the IT environment and risks surrounding the IT, thus aligning the IT strategy with the business strategy when implementing structures and processes.

Entities which implement IT governance principles are likely to experience the following advantages (Bowen, Cheung and Rohde, 2007:192; Hardy, 2006:56):

- The entity's reputation is improved,
- Trust is enhanced with internal and external parties,
- IT and business goals and processes are strategically aligned, resulting in a competitive advantage, and
- Risks management is improved.

2.4 IT governance in South Africa and the King III report

The King reports have formed the basis of corporate governance in South Africa and aims to be one of the world's leading corporate governance standards. While the first two reports focused on corporate governance, risk management and sustainability, the King III report introduces a new focus area, namely IT

governance. The King III report was issued on 1 September 2009 and became effective on 1 March 2010.

The King III report (IODSA, 2009) defines IT governance as:

> *"A framework that supports effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives"*.

Chapter 5 of the King III report contains seven IT governance principles that South-African companies listed on the Johannesburg Stock Exchange (JSE) should implement and other companies can do so voluntarily. Table 2.2 lists the seven IT governance principles listed in Chapter 5 of the King III report (IODSA, 2009).

Table 2.2: King III's IT governance principles

Principles (Chapter 5)	Description of principle
Principle 5.1	The board should be responsible for IT governance
Principle 5.2	IT should be aligned with the performance and sustainability objectives of the company
Principle 5.3	The board should delegate to management the responsibility for the implementation of an IT governance framework
Principle 5.4	The board should monitor and evaluate significant IT investments and expenditure
Principle 5.5	IT should form an integral part of the company's risk management
Principle 5.6	The board should ensure that information assets are managed effectively
Principle 5.7	A risk committee and audit committee should assist the board in carrying out its IT responsibilities

(Source: IODSA, 2009)

The four key focus areas of the IT governance principles are (Badenhorst, 2009:8):

1. Strategic alignment (Principle 5.2 and 5.3)
2. Value delivery (Principle 5.4)
3. Risk management (Principle 5.5)
4. Resource management (Principle 5.6)

2.4.1 Strategic alignment

Strategic alignment focus on aligning the investment in IT with the strategic objectives of the business. When formulating the IT strategy, the business must take the business objectives into consideration (ITGI, 2003:22-23).

2.4.2 Value delivery

Value delivery concentrate on ensuring that IT delivers the promised benefit against the strategy while optimising costs. IT should thus provide on-time benefits of the appropriate quality as were promised, while at the same time staying within budget (ITGI, 2003:24).

2.4.3 Risk management

Risk management address the safeguarding of IT assets, disaster recovery and continuity of operations (ITGI, 2003:26).

2.4.4 Resource management

Resource management focus on optimising knowledge and IT infrastructure by the optimal investment in IT resources, the optimal use of IT resources and the proper management of IT resources. IT resources includes applications, information, infrastructure and people. (ITGI, 2003:28).

In order to achieve strategic alignment (one of the four key focus areas of IT governance principles) business and IT professionals must communicate to ensure that their strategies are aligned. If this is not done properly, it will give rise to an IT gap.

2.5 IT gap and business-IT alignment

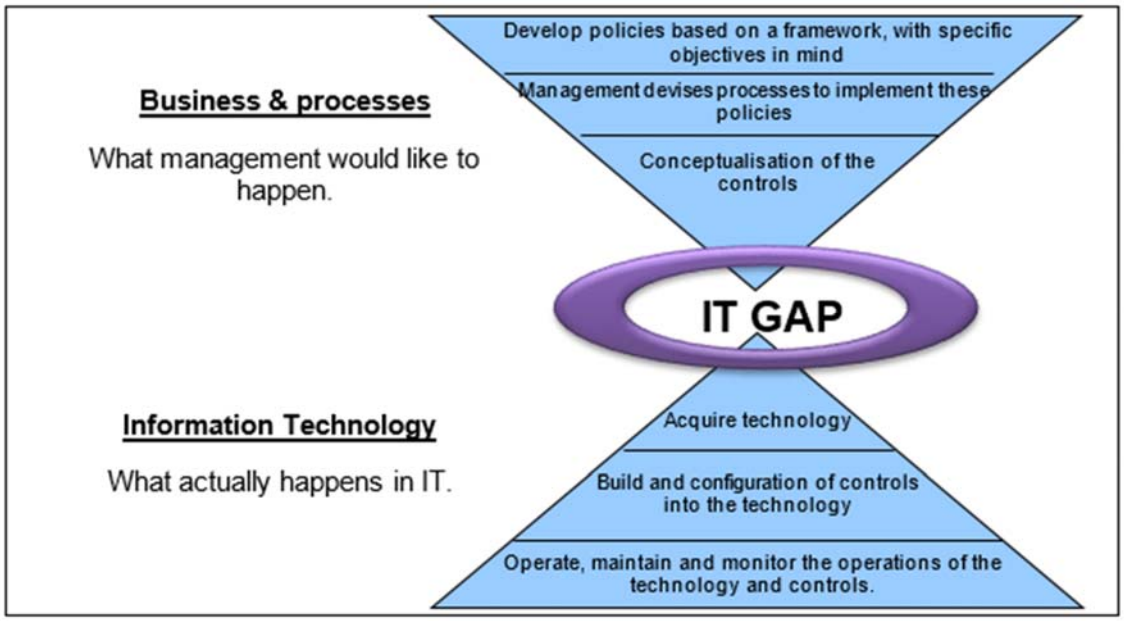
2.5.1 IT gap

According to the ITGI (2003:7-8):

> *"Board and executive management generally expect their enterprise's IT to deliver business value, i.e., provide fast, secured, high-quality solutions and services; generate reasonable return on investment; and move from efficiency and productivity gains towards value creation and business effectiveness. In many enterprises, expectations of IT and reality often do not match and boards are faced with:*
>
> - *Business losses, reputational damage and a weakened competitive position*
> - *Inability to obtain or measure a return from IT investments*
> - *Failure of IT initiatives to bring the innovation and benefits they promised*
> - *Technology that is inadequate or even obsolete*
> - *Inability to leverage available new technologies*
> - *Deadlines that are not met and budgets that are overrun."*

The reason for this problem is that there is a miscommunication between the executive management and the IT professionals of a business. The board and executive management do not understand the technologies in use by the business or the control techniques that should be implemented to address the associated risks, whereas the IT professionals do not understand the control model (focus on design, implementation and maintenance of risk controls) or operational framework (a system of control categories that covers all fundamental internal controls expected within a company to mitigate risk) implemented by executive management (Rudman as cited by Goosen & Rudman, 2013:839). The difference between management's perspective of policies and procedures and IT's understanding and implementation thereof is referred to as the 'IT gap' as illustrated in Figure 2.1

Figure 2.1: IT gap



(Source: Kruger & Rudman, 2013:1242)

When an IT gap exist in a business, it is not possible to achieve strategic alignment (which is one of the key focus areas of IT governance according to the King III report).

2.5.2 Business-IT alignment

In order to address and overcome the IT gap, a business-IT alignment process must be implemented (Goosen & Rudman, 2013:839). Business-IT alignment is only achieved when the IT strategic objectives and operations support the enterprise's strategic objectives and operations (ITGI, 2003:22). The IT strategy should thus be formulated based on the business requirements.

The following are some of the advantages from a successful business-IT alignment (IBM, Innotas as cited by Goosen & Rudman, 2013:839):

- IT strategies will support business strategies and goals
- Risks are reduced (both business and IT-related)
- Decision-making is improved by reliable real-time data
- Increased strategic flexibility

Many companies rely on existing best practice control frameworks such as COBIT or ITIL to assist them with the alignment process. A control framework is a system of control categories that covers all fundamental internal controls expected within a business to mitigate risk (Rudman, as cited by Goosen, 2013:839). The existing control frameworks each address different internal controls for example, COBIT describes IT controls that should be implemented on strategic level in the day-to-day operations, while ITIL describes best practices specifically for IT service management. According to Goosen & Rudman (2013:17), in order to achieve business-IT alignment and successfully implement IT governance principles, a business will need to use existing control frameworks and combine them to develop an entity-specific integrated control framework which can be implemented to address business strategies and operations as well as IT strategies and operations. To combine these existing control frameworks can be time consuming and costly and therefore a business should only identify the areas and control techniques that are applicable to the organisation.

2.6 Integrated control framework

Goosen (2012:34) developed an integrated framework by combining different existing best practice control frameworks and as a result provided a seven step integrated control framework. This seven step integrated control framework of Goosen (Goosen's framework) enables a business to simplify the integration process of different frameworks and it enables the business to achieve IT governance both at strategic and operational level. The steps identified in Goosen's framework is as follows:

IT governance at strategic level

1. Determine the business's business imperatives
2. Identify the incremental risks derived from the business imperatives
3. Link the relevant risk to an existing globally accepted control framework's processes to identify possible mitigating controls

IT governance at operational level

4. Implement the applicable control techniques as identified at a strategic level (step 3)
5. Determine the access paths which are affected by the selected business imperatives
6. Identify the IT architectural components which form the relevant access path
7. Implement relevant configuration controls over each IT architectural components

2.7 Development of the integrated framework

To develop the seven step integrated framework of Goosen (2012:34) for a specific business, a better understanding is needed of each of the steps listed above.

2.7.1 Business imperatives

A business should distinguish between their basic business assumptions and business imperatives.

Business assumptions are the objectives set by a business in order to perform its basic everyday functions. Examples of basic business assumptions as listed by Goosen (2012:17) include:

- A profit-driven business
- Good internal controls and standards
- Resource management procedures
- Business continuity policies and procedures
- Data security

Business imperatives are those critical and fundamental business drivers, selected at a strategic level, which are necessary for a business to achieve its stated objectives and which give the organization its competitive advantage in its specific environment (Boshoff, 2012). Business imperatives are the foundation of

the business-IT alignment process. Business imperatives are specific to each business environment (Goosen & Rudman, 2013:840).

2.7.2 Identify incremental risks

The business imperatives of a company would lead to a specific IT requirement (technology to be implemented) to meet this imperative. When this technology is introduced to the business, it introduces strategic and operational IT risks.

Incremental risks are specific risks arising from the business imperatives (strategic risks) and the type of technology that the business is using (operational risks) to achieve the business imperatives.

Strategic risks can be subdivided into the following main categories (Boshoff, 2013):

- Obsolescence
- Integration
- Interoperability
- Security
- Scalability
- Retrofit

2.7.3 Link the risks to processes of a control framework

The risks identified are then mapped to an existing globally accepted control framework's processes to identify mitigating controls. Examples of existing frameworks are COBIT, ITIL, International Organisation for Standardisation (ISO), Projects in Controlled Environments (PRINCE2) etc.

2.7.4 Implement the techniques identified at a strategic level

Each process in the control framework will provide controls and control techniques which should be implemented in order to achieve IT governance at a strategic level.

2.7.5 Determine the access paths

The access paths which are affected by each business imperative should be identified. Boshoff (1990:24) defined an access path as follows:

> *A user performs computerised activities by activating an access path. An access path is formed by the various IT components that need to be activated in order for a typical user (business, IT or otherwise) request (functionality, data or otherwise) to be executed, in order to access computer controlled resources.*

An example of an access path can be illustrated as follows:

A user wants to access the accounting system on the business' server. There are numerous ways in which the accounting system can be accessed for example:

- An employee accesses the system via the office Local Area Network (LAN);
- An employee at a branch accesses the system at head office via a Wide Area Network (WAN);
- An IT technician assists an employee at a branch on the system via remote access, etc.

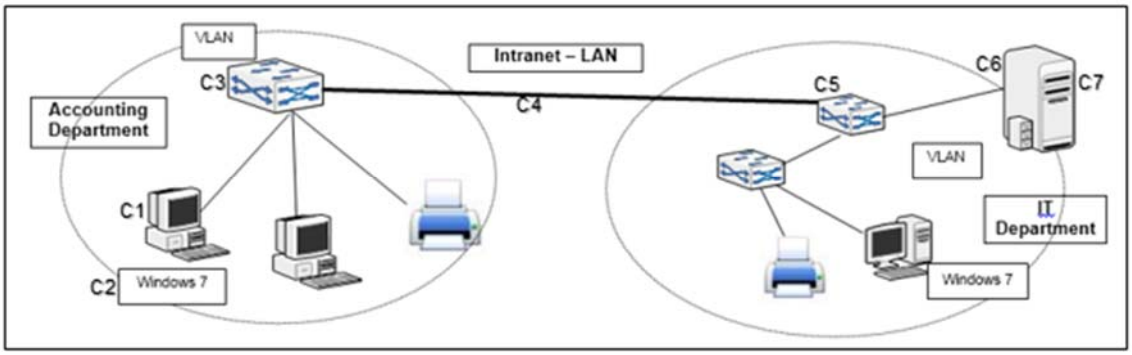
Each of the above ways are called an access path. There may be multiple access paths for the same user or activity, however the number of actual access paths available is finite (Boshoff, 1990:25). A business should identify each access path is that is affected by the business imperative.

2.7.6 Identify the IT architectural components

Each access path as identified in 2.7.5 consists of various IT architectural components which should be identified. An access path is created by joining various IT components such as computers, laptops, mobile devices, middleware, operating systems, routers, firewalls, switches, wireless networks, servers and other relevant IT components. These individual components are referred to as IT architectural components.

For the purpose of this example only the access path that the employee follows via the office LAN to the accounting system with its IT architectural components will be illustrated in Figure 2.2.

Figure 2.2: Illustration of an access path and IT architectural components



(Source: Author's own, 2014)

The access path is the route from the desktop computer of the employee to the accounting software on the server. The various IT architectural components in the access path that will be activated can be described as follows:

- Component 1 (C1) is the hardware components used to access the accounting software, for example a desktop computer that the employee uses.
- Component 2 (C2) is the operating system required to operate the desktop computer, for example Microsoft Windows 7.
- Component 3 (C3) is the switch which receives the message from the desktop computer and transmits the messages only to the server.
- Component 4 (C4) is the fixed line which is required for the connection to the server, for example Ethernet cables.
- Component 5 (C5) is the switch which receives the message from the desktop computer and allows access to the server.
- Component 6 (C6) is the business server on which the accounting software is installed.
- Component 7 (C7) is the accounting software which the user wants to access.

2.7.7 Implement relevant configuration controls over each IT architectural component

Boshoff as cited by Goosen & Rudman (2013:842) stated that each IT architectural component should be examined to ensure that they are correctly built, set up, configured, operated and/or maintained, so as to correctly control the particular access path. These controls are referred to as configuration controls. The configuration controls that would manage the risks inherent to the IT architectural components were defined as follows (Goosen, 2012:46):

> *Computer hardware is **'built'** by assembling the various components, enabling them to accept an operating system, and to function in a computer. Computer software is also **'built'**, referring either to the process of creating and converting source code files into stand-alone software artefacts that can be run on a computer, or the result of doing so. This will include the compilation process, where source code files are converted into executable code.*
>
> ***'Set up'** or **'installation'** of a program (including drivers, plugins, etc.) refers to implementing the program on a computer system and ensuring the execution thereof.*
>
> *The term **'configuration'** refers to the configuration of files, or configuring the initial settings of some computer programs. User applications, server processes and operating system settings are normally configured items.*
>
> *A computer is **'operated'** by overseeing the smooth running of a computer/device and intervening in the process by stopping and restarting services or the whole computer.*
>
> ***'Maintenance'** ensures that software is upgraded and/or computers/devices are repaired so as to ensure the optimum performance and reliability of such devices.*

According to Goosen (2012:47) if the configuration controls are correctly implemented they will address the risks surrounding the access paths, and IT governance at an operational level will be achieved.

2.8 Conclusion

The purpose of this chapter was to gain an understanding of IT governance concepts, the IT governance principles of King III and to identify how to develop an integrated framework which can assist with the implementation of IT governance principles when a new technology is introduced to the business.

A literature review was performed on IT governance concepts and King III. From the literature review it was determined that IT governance has become an integral part of corporate governance. The King III report introduced IT governance as a new focus area of corporate governance with strategic alignment as one of the main IT governance principles. In order to achieve strategic alignment the strategies of the business professionals and the strategies of the IT professionals must be aligned. If this is not done properly it leads to an IT gap. Goosen (2012:34) developed an integrated framework which simplifies the business-IT alignment process and overcomes the IT gap.

Goosen's framework can be applied by a business on any new technology introduced to the business. One of the technologies that a business can use is social media. Chapter 3 aims to provide an understanding of what social media is, after which Goosen's framework will be applied to social media over the remaining chapters of this research.

CHAPTER 3

SOCIAL MEDIA

3.1 Background

The use of social media has experienced exceptional growth over the last few years. Many organisations have introduced social media into their businesses and social media features on their agendas (Fink & Zerfass, 2010:5) with separate budgets allocated to social media (Nielson, 2013:5)

Deloitte (s.a.) states that "social media is a practice that can enable more efficient and effective connections inside and outside your organization to drive performance." Yet, there are still some businesses that do not seem to be comfortable using social media for business purposes, or offering a platform where consumers can speak freely about the specific business (Kaplan & Haenlein, 2010:59-60).

Chapter 3 aims to provide an understanding of what social media is, the different categories of social media, the use thereof by businesses and the risks it introduces to the business.

3.2 An overview of social media

Social media can be defined as mobile and web-based technologies that enable people to participate in conversations and to share and discuss content, opinions, experiences and ideas (Kietzmann, Hermkens, McCarthy & Silvestre, 2011:241). The main characteristic of social media is the interactivity. Participants can freely send, receive and process information for use by others (Aula, 2010:43). It is also characterized by open participation (can be used by anyone, including businesses, employees and individuals), discussions, community, networking and the quick and wide spread of information and other content across different communication channels (Aula, 2010:44).

From a business perspective, the biggest difference between conventional media (newspapers, magazines etc.) and social media is the ability to control information about the business or its products or services. With conventional media a business could have strategically decided which information they wanted to publish. Due to the interactivity and open participation of social media today, the business cannot control what is being said (Kaplan & Haenlein, 2010:60). Through social media, consumers can freely exchange ideas or opinions on companies, brands, products and services.

3.3 Categories of social media

To further an understanding of social media it is important to consider the different categories of social media that are available. According to Kaplan and Haenlein (2010:62) social media can be classified into six categories based on theories in the field of media research (social presence, media richness) and social processes (self-presentation, self-disclosure). The following table represents the six categories of social media according to Kaplan and Haenlein (2010:62):

Table 3.1: Categories of social media

		Social presence(1) / Media richness(2)		
		Low	**Medium**	**High**
Self-presentation(3) / Self-disclosure(4)	**Low**	Collaborative projects	Content communities	Virtual game worlds
	High	Blogs	Social networking sites	Virtual social worlds

(Source: Kaplan & Haenlein, 2010:62)

Kaplan & Haenlein (2010:62) defined the theories used in Table 3.1 as follows:

(1) Social presence: Sound, visual and physical contact that can be achieved
(2) Media richness: Amount of information transmitted in a certain period of time
(3) Self-presentation: The desire to control the impressions that other people form (usually done through self-disclosure)

(4) Self-disclosure: Disclosure of personal information (conscious or unconscious)

The six categories mentioned in Table 3.1 are described in more detail in Table 3.2 and linked with examples of social media networks and technologies. Because new social media networks and technologies are developed daily, it is impossible to provide a complete list of examples. The examples used in the table were derived from the Kaplan & Haenlein (2010) study as well as the top social networks identified in a survey conducted by Nielsen (Nielsen, 2012).

Table 3.2: Classification of social media examples according to categories

Social media category	Description	Examples
Collaborative projects	Collaborative projects enable users to create content jointly. There can be distinguish between two types of collaborative projects: 1. Wikis: Websites which allow users to add content or to remove and modify content that has been placed by previous users. 2. Social bookmarking: Websites which enable group-based collection of Internet links or media content.	Wikipedia Delicious Pinterest Wikia
Blogs and microblogs	Blogs are websites that display the specific entries made by an individual. It provides interaction through additional comments that readers can add. Only the person managing the blog can add or remove content. A micro blog only allows users to publish short text updates.	Twitter Blogger WordPress Tumblr

Content communities	It is where a group of people share media content about a common object of interest. It can be video's, photos etc.	YouTube (video's) Flickr (photos) Slideshare (power point presentations) BookCrossing (books)
Social networking sites	It is a website that allows subscribers to create a profile with their personal information. Interaction starts when a subscriber invites friends to add them to the subscriber's visible list of contacts.	Facebook MySpace Google+ LinkedIn
Virtual game worlds	It is an online interface where multiple users can appear in the form of personalised avatars and interact with each other. Virtual game worlds are strongly influenced by fantasy and science fiction. In this type of virtual world users are required to behave according to strict rules.	World of Warcraft EverQuest
Virtual social worlds	Virtual social worlds are similar to virtual game worlds but offer a more open-ended experience where users can choose behaviour more freely. There are no rules restricting the range of possible interactions. The focus is on user interaction.	Second Life

(Sources: Kaplan & Haenlein, 2009; Kaplan & Haenlein, 2010; Nielsen, 2012)

3.4 Business use of social media

Each of the categories mentioned above can be of specific use for business. Table 3.3 below discuss examples of how each category can be used by a business.

Table 3.3: Business use of social media

Social media category	Business use
Collaborative projects	**1. Marketing:** Social bookmarking sites (such as Delicious) are used in marketing strategies for businesses. Businesses usually bookmark their webpages under the different categories that is applicable to the business. This is an effective way to introduce the business to the public (Chin, 2013). Wikipedia does not allow direct advertising or marketing. Everything written on Wikipedia is supposedly based on facts and not opinions. When a business is mentioned on Wikipedia it helps the readers to understand the company and its products. However, Wikipedia related content tends to show up on most Google searches, giving a business mentioned on Wikipedia a lot of exposure (Cooper, 2011; Goodwin, 2012). Pinterest is used by businesses mainly for marketing purposes where they pin relevant products and services for followers to look at and repin. A business can change the URL of their pin to direct users to the page of their choice (Bossenger, 2014a; Bossenger,

	2014b). **2. Collaboration:** Businesses also use wikis for collaboration between employees as well as customers. Employees can collaboratively create and edit documentation to improve workflow and customers can collaborate in projects (Kaplan & Haenlein, 2010:63).
Blogs and microblogs	**1. Internal process management:** Internal blogs are only accessible by employees of a certain business and are used by businesses for communication and discussions with employees (Harvard Business Review Analytic Services, 2010:8) **2. Marketing:** External blogs and microblogs are used mainly for marketing purposes. Businesses publish new product information or services on their blogs with links to specific product pages (Cohen, 2013). **3. Market research:** External blogs provides a two-way conversation with customers where customers can leave comments on the blog. This makes management of customer opinions possible (Harvard Business Review Analytic Services, 2010:12).
Content communities	**1. Marketing:** Businesses create videos or pictures to promote their products or services on YouTube and Flickr

	respectively (Harvard Business Review Analytic Services, 2010:2). **2. Customer services:** Businesses make use of videos on YouTube to answer specific customer related problems or questions with products and services (The State of Queensland, 2014).
Social networking sites	**1. Marketing:** Social networking sites are mainly used by businesses for advertising and marketing purposes. Businesses open their own accounts on social networking sites to promote their products and services. Through their profiles they can advertise their products and communicate with customers and employees (Harvard Business Review Analytic Services, 2010:8). **2. Human resource management:** LinkedIn is used for networking with business professionals and is used as a recruitment tool (Vanover, 2009).
Virtual game worlds	**1. Marketing:** Virtual game worlds are used for in-game advertising where their products are placed in the game (Kaplan & Haenlein, 2010:63).

Virtual social worlds	Virtual social worlds can be used by businesses for the following (Kaplan & Haenlein, 2009:566-568): **1. Marketing and communication with customers:** In Second Life, for example, it can be done in the following ways: A business can buy advertising space in virtual malls or radio stations or they can advertise on virtual billboards. A business can also sponsor an event in the virtual world. A business can get publicity through the activities they perform within Second Life. **2. Virtual product sales:** Businesses can sell digital versions of their existing real life products and services. **3. Market research:** When a business develops a new product they can get the residents of the virtual world to actively help with the customisation process. New products can also be launched virtually to gather customer opinions and make the necessary changes before it is launched in real life. **4. Human resource management:** Virtual social worlds can be used to organize recruitment events and facilitate interviews especially for businesses that need candidates who are technologically advanced. It can also be used to create awareness of real life recruitment campaigns through virtual advertising media as mentioned in

	point 1. **5. Internal process management:** Businesses use virtual social worlds for internal meetings and knowledge exchange.

(Sources: As indicated in table)

3.5 Risks relating to social media

Although there are many business uses for social media, as with any technology the use thereof introduces risks to the business. According to ISACA (2010:6) risks are introduced in three ways, by employees using social media in the workplace, employees using social media outside the workplace and through business use. ISACA (2010:7-8), Fink & Zerfass (2010:19) and Shullich (2012:9-35) identified the following risks of a corporate social media presence:

Table 3.4: Risks of a corporate social media presence

Threats and vulnerabilities	Risks
Malware such as trojans, viruses and spyware can be introduced to the organisational network	• Data leakage, theft and corporate espionage • System downtime • Resources required to clean systems
Exposure to customers and the enterprise through a fraudulent or hijacked corporate presence	• Customer backlash/adverse legal actions • Breach of privacy due to exposure of customer information • Reputational damage • Targeted phishing attacks on customers or employees

Unclear or undefined content rights to information posted to social media sites	• Difficulty to determine the ownership of published content • Difficulty to control the published data • Reputational damage
A move to a digital business model may increase customer service expectations	• Customer dissatisfaction with the responsiveness received in the arena, leading to potential reputational damage for the enterprise and customer retention issues • Difficulty to control the communication process with customers • Reaction is too slow or not responding timeously • Reputational damage
Mismanagement of electronic communications that may be impacted by retention regulations or e-discovery	• Regulatory sanctions and fines • Adverse legal actions
Use of personal accounts to communicate work-related information	• Privacy violations • Reputational damage • Loss of competitive advantage
Employee posting of pictures or information that link them to the enterprise	• Brand damage • Reputational damage
Excessive employee use of social media in the workplace	• Network utilisation issues • Productivity loss due to a distraction from core duties • Increased risk of exposure to malware due to longer duration of sessions

Employee access to social media via enterprise-supplied mobile devices (smartphones, personal digital assistants (PDAs))	• Infection of mobile devices • Data theft from mobile devices • Circumvention of enterprise controls • Data leakage
Content management	• The risk that someone can change or delete content on a social media site • Content on social media is permanent of nature and if outdated content is downloaded it can create a problem • Difficulty in determining the representation of published content (does it represent the employee or customer's opinion or that of the organisation)
Breach of privacy	• Publishing of confidential information or locations by uneducated and negligent employees • Lack of awareness that privacy can be breached • Breach of privacy can lead to harassment such as blackmailing, extortion, cyber bullying and cyber stalking

(Sources: ISACA, 2010:7-8; Fink & Zerfass, 2010:19; Shullich, 2012:9-35)

3.6 Conclusion

The purpose of this chapter was to perform a literature review on social media in order to gain an understanding of the term social media, its business uses and the risks it introduces to the business.

Social media is web-based technologies that enable people to communicate and interact freely with each other (Kietzmann, Hermkens, McCarthy & Silvestre, 2011:241). The main characteristic of social media is the interactivity. Kaplan & Haenlein (2010:62) divided social media into six main categories namely, collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds and virtual social worlds.

Social media can be a positive business tool to enhance the business. Businesses use social media for marketing, market research, customer service, internal process management, human resource management, virtual product sales and collaboration. Although it is a positive business tool, social media also introduces a lot of risks to a business, such as reputational risks, security risks for example malware and breach of privacy.

According to the King III report, the board are responsible for IT governance and IT should form an integral part of the company's risk management. A business that uses social media should comply with the IT governance principles as discussed in Chapter 2. In order to gain an advantage from the use of social media, a business should successfully mitigate the risks introduced by it. An integrated control framework for IT governance of social media should be developed. Chapter 4 to 6 aims to develop this integrated control framework based on Goosen's framework as identified in Chapter 2.

CHAPTER 4

DEVELOPING AN INTEGRATED CONTROL FRAMEWORK FOR IT GOVERNANCE OF SOCIAL MEDIA AT A STRATEGIC LEVEL: DETERMINE BUSINESS IMPERATIVES AND IDENTIFY INCREMENTAL RISKS

4.1 Background

As discussed in Table 3.3 there are a lot of different uses for social media within business. By making use of social media a business can reach its basic business objectives (business assumptions) as well as its strategic objectives (business imperatives). However, at the same time social media introduces risks to the business. Therefor a business which uses social media needs to apply an integrated control framework in order to address the risks and to comply with the IT governance principles as required by King III.

Chapter 4 to 6 aims to develop an integrated control framework for the IT governance of social media. The development of the framework is based on Goosen's framework (2012:34) as discussed in chapter 2. This chapter presents the first two steps of achieving IT governance at strategic level. Later chapters will address the remaining five steps.

4.2 Business imperatives

Business imperatives are the foundation of the business-IT alignment process (refer to Chapter 2). As previously mentioned business imperatives are specific to each business environment, therefore there is no one set of imperatives that would apply to all businesses. The imperatives listed below are possible business drivers. They are not necessarily all applicable to an entity and there can be other business imperatives besides the ones listed. It can also be that as technology develops, the business imperatives for an entity can change. Each imperative was formulated by taking the business use for social media into consideration as well as previous literature which lists basic business imperatives. The specific

literature taken into consideration is mentioned at each business imperative listed below. Apart from the business imperatives listed, all other business uses for social media such as collaboration, internal process management etc. was assessed and for the purpose of this study found to be normal business assumptions and thus will not be discussed further. The following business imperatives were identified as the key business imperatives for a business that uses social media:

4.2.1 Marketing and product innovation

The business needs to be innovative with its marketing strategy to increase brand awareness, develop target marketing activities and to ultimately increase sales. Furthermore the competitive market that businesses find themselves in nowadays require them to constantly develops new products to address customers' changing needs (Goosen, 2012:35) When a business develop a new product, it is crucial that they develop the exact product that the customer requires and they market it properly through innovative ways in order to increase awareness and the sales of the new product.

4.2.2 Customer service

Customer service levels should be of superior quality to gain a competitive advantage in the business environment. In order to increase customer satisfaction levels it is necessary to gather information about customers' perceptions and requests about the products or services (Goosen, 2012:35; ISACA, 2010:5).

4.2.3 Pro-active management

Real time information needs to be available to the business to evaluate customer needs, discussions and perceptions. This would enable the business to address customer issues quickly and to adjust strategies, products or services appropriately to gain a competitive advantage (Goosen & Rudman, 2013:846).

4.2.4 Pro-active recruitment

The businesses recruitment processes need to be pro-active to find the most suitable candidate for a vacancy before its competitors. To be pro-active, the recruitment practices should look at formal applications received and also focus on candidates who do not apply for a vacancy but advertise themselves via social media networks. Human resources should aim to become experts in using social networking technology (such as LinkedIn) to track candidates that would be suitable for their business (Nigel Write Recruitment, 2011:5).

4.3 IT impact of business imperatives

A business imperative is defined at strategic level. However each of these imperatives will have a direct impact on the IT that is required by the business in order to achieve the business imperative. Risks are introduced to the business due to the specific IT requirement. Table 4.1 identifies the impact that each of the imperatives has on the IT environment and lists the relevant business and strategic risks (incremental risks as described in 2.7.2 of the literature review) that are introduced by each imperative as identified by the author. Although social media introduces numerous risks to a business, only the specific risks introduced by each imperative will be considered in this study. A detailed description of each risk follows in 4.4.

Table 4.1: Impact of business imperative on IT environment and incremental risks

Business Imperative	Impact on IT environment	Incremental risks
Marketing and product innovation	The IT system must be able to facilitate inbound marketing where the customer can have input, share ideas The IT used to advertise the product must be set up in such a way that the advertisement reaches the target	• Reputational • Security • Privacy • Obsolescence

	market and that the content pulls the customers to the relevant product sites. The IT system must provide a platform where customers can help co-produce new products.	
Customer service	Direct and interactive contact with customers must be available so that the business can identify customers' opinions and requests on products or services. The system must provide a private interface, which can only be seen by the business, where customers can comment about the products or services and where the business can correspond in a timely manner. The IT system must have the ability to monitor discussions about the business.	• Reputational • Security • Privacy • Obsolescence
Pro-active management	The IT system must be able to provide real time information and discussions about the business to enable management to make quick appropriate adjustments to strategies, products and services. It must also provide a private and secured interface where management can communicate with customers and respond to any negative comments about the business.	• Reputational • Security • Privacy • Obsolescence
Pro-active recruitment	The IT system must be able to provide a list of suitable candidates based on a specific skill set or specific requirements for a vacancy. It must	• Security • Privacy • Obsolescence

	also provide an interface where management and potential employees can communicate with each other. All personal information shared between the business and potential employees must be safeguarded by the IT system.	

(Source: Author's own, 2014)

4.4 Risks relating to social media

The second step in the business-IT alignment process (refer to Chapter 2) is to identify the incremental IT risks that social media introduces to a business.

The risks as identified by the business imperatives can be summarised into two main categories, namely business risks and strategic risks (as described in 2.7.2 of the literature review).

4.4.1 Business risk

Reputational risk

Reputational risk refers to the possibility or danger of losing one's reputation (Aula, 2010:44). The use of social media ensures that businesses are more visible to the public and can promote brand awareness. The downfall of being more visible is that every action the business takes is known publicly. Something that would previously not have been published is now open for everyone to see. This can cause reputational damage to a business. Loss of reputation can have several consequences for a business including financial implications, procurement problems and issues surrounding the maintenance of customers or the loyalty of employees (Aula, 2010:45).

The following (derived from Table 3.4 of the literature review) may result in reputational damage for a business that uses social media:

i. Exposure of the business through fraudulent or criminal activities including malware, hacking and phishing attacks
ii. Inappropriate use of social media by employees that are linked to the business
iii. Insufficient response or not responding timeously to customer complaints and product related queries
iv. Difficulty in controlling published data, changes made to published data and determining who owns the data

4.4.2 Strategic risks

Security

According to Ross as cited by Brand (2013:13) IT security risk is defined as: "the risk relating to the loss of confidentiality, integrity and availability of information or IT resources". Each of the components of security risk is defined as follows:

> *Confidentiality is concerned where access to protected information is only made available or disclosed to authorised individuals, entities, systems or processes.*
>
> *Availability refers to timely and reliable access to and use of information, software and hardware upon demand by an authorised user.*
>
> *Integrity concerns ensuring that information is only created, modified or destroyed by authorised users in authorised ways to protect the accuracy, completeness, non-repudiation and authenticity of the information.*

(ISO/IEC, 2012; Ross, 2011; Zissis and Lekkas, 2012:586 as cited by Brand, 2013:13-14)

The following (derived from Table 3.4 of the literature review) may result in a security risk for a business that uses social media:

i. Malware such as trojans, viruses and spyware
ii. Malicious hackers and phishing attacks
iii. Uneducated and negligent users

Privacy

The use of social media enables the businesses to provide the public with information and at the same time it enables the company to gather information about customers and prospective employees. This information is the property of the business and must be safeguarded.

The following (derived from Table 3.4 of the literature review) may result in a privacy threat to the business:

i. Unauthorised access to confidential client or employee information through hacking, phishing attacks and spyware
ii. Unauthorised disclosure of information by employees of the firm due to the fact that they are uneducated or unaware of the impact

Obsolescence

According to the Oxford English Dictionary (2014), obsolescence is when machinery, consumer goods, etc., become obsolete as a result of technological advances, changes in demand, etc.

The need for businesses to be innovative in order to improve competitiveness, sales growth, efficiency and productivity cause them to adopt new advanced technology systems quicker than their competitors, thus reducing the lifecycle of technologies (Pantano, Iazzolino & Migliano, 2013:225). A technology is obsolete when it is out of date (both hardware and software) or out of use measured by the acceptance level of the users (Pantano, Iazzolino & Migliano, 2013:227).

The following may result in obsolescence for a business that uses social media:

i. A social media network used by the business becomes obsolete and shuts down or customers stop using the specific social media network
ii. Software used by customers to help co-create products becomes obsolete

4.5 Conclusion

The purpose of this chapter was to start with the development of an integrated control framework for the IT governance of social media. The development was based on Goosen's framework as identified in the literature review in chapter 2. This chapter applied the first two steps of Goosen's framework on social media.

In step 1, the business imperatives for social media was identified as marketing and product innovation, customer service, pro-active management and pro-active recruitment. Each of these imperatives have a direct impact on the IT that is required by the business. The author identified the IT impact of each imperative and from there was able to identify the incremental risks (step 2 of Goosen's framework) at strategic level introduced by social media. The incremental risks are reputational risk, security risk, privacy risk and obsolescence.

According to Goosen's framework, in order to govern these risks, a business needs to identify possible mitigating controls as part of step 3. Chapter 5 aims to link each risk to an existing globally accepted control framework in order to identify possible mitigating controls for the identified incremental risks.

CHAPTER 5

DEVELOPING AN INTEGRATED CONTROL FRAMEWORK FOR IT GOVERNANCE OF SOCIAL MEDIA AT A STRATEGIC LEVEL: MAPPING OF SOCIAL MEDIA INCREMENTAL RISKS TO AN EXISTING CONTROL FRAMEWORK

5.1 Background

The purpose of this chapter is to continue with the development of the integrated control framework for the IT governance of social media by identifying possible mitigating controls for each of the incremental risks of social media as identified in section 4.4. This is done through identification of an appropriate existing control framework and then the mapping of the incremental risks identified to the processes of the control framework. Each process will provide mitigating controls for the identified risks. This represents step 3 of Goosen's framework.

5.2 Existing control frameworks

There are a number of existing control framework to address IT governance. Examples include COBIT, ITIL, ISO standards, PRINCE2 etc. COBIT was issued by the ITGI and has become a best practice control framework for IT governance (Hardy, 2006:59). Some writers believe that COBIT is a *de facto* control framework for IT governance (Robinson, 2005:48; Sallé, 2004; Soomro & Hesson, 2012:273 as cited by Brand). According to Steenkamp (2011) a business which implements COBIT will comply with the requirements of King III relating to IT governance.

COBIT 5 was released during 2012 and integrates other control documents and frameworks such as COBIT 4.1, Val IT, Risk IT, BMIS, ITIL, TOGAF and ISO standards. The governance enablers listed in COBIT 5 was derived from other relevant governance standards and frameworks. COBIT 5 thus provides an integrated control framework for the governance and management of enterprise IT

(ITGI, 2012). By maintaining a balance between benefits, risk levels and resource use, it helps enterprises to create optimal value (ITGI, 2012). COBIT 5 provides a holistic view on governance and therefore for the purpose of this study it is the most appropriate control framework to use when addressing IT governance of social media.

5.3 COBIT 5

COBIT 5 is the most suitable integrated control framework for the governance and management of enterprise IT. COBIT 5 is based on the following five key principles (ITGI, 2012):

Principle 1: Meeting stakeholders needs

Enterprises exist to create value for their stakeholders. Stakeholder needs must be transformed into an actionable strategy by the enterprise through COBIT 5's goal cascade. The goal cascade is based on four steps:

Step 1: Stakeholder drivers influence stakeholder needs

Step 2: Stakeholder needs cascade to enterprise goals

Step 3: Enterprise goals cascade to IT-related goals

Step 4: IT-related goals cascade to enabler goals

Enablers are discussed in detail under Principle 4.

Principle 2: Covering the enterprise end-to-end

COBIT 5 provides a holistic view on governance and management of an organisation's information and related technology. It is holistic because it covers everything (including activities and responsibilities of both IT functions and non-IT business functions) and everyone (both internal and external) that is relevant to governance and management of the organisation's information and related technology.

Principle 3: Applying a single integrated framework

COBIT 5 is an overarching governance and management framework because it is an integrated source of governance enablers derived from other relevant governance standards and frameworks.

Principle 4: Enabling a holistic approach

Enablers are an organisation's resources for governance through which its governance objectives are achieved. These resources include frameworks, principles, structures, processes and practices, as well as service capabilities, people and information.

COBIT 5 defines seven categories of enablers that can assist an organisation with IT governance and management. The seven categories are:

1. Principles, policies and frameworks
2. Processes
3. Organisational structures
4. Culture, ethics and behaviour
5. Information
6. Services, infrastructure and applications
7. People, skills and competencies

Each enabler has specific stakeholders, goals, a life cycle and good practices that support the achievement of the enabler goals.

Principle 5: Separating governance from management

COBIT 5 recognise that there is a clear distinction between governance and management of IT because they encompass different types of activities, require different organisational structures and serve different purposes. COBIT 5 divides governance and management processes of IT into the following domains:

The governance area consists of one domain named "Evaluate, Direct and Monitor (EDM)" which is subdivided into 5 processes.

The management area consists of four domains:

- Align, Plan and Organise (APO) subdivided into 13 processes
- Build, Acquire and Implement (BAI) subdivided into 10 processes
- Deliver, Service and Support (DSS) subdivided into 6 processes
- Monitor, Evaluate and Assess (MEA) subdivided into 3 processes.

The 27 processes listed above are also listed as one of the enablers in principle 4. A process is defined in COBIT 5 as:

> *A collection of practices influenced by the enterprise's policies and procedures that take inputs from a number of sources (including other processes), manipulates the inputs and produces outputs (e.g. products, services).*
>
> (Source: ITGI, 2012:19)

5.4 COBIT 5 processes applicable to social media

Each of the processes listed in COBIT 5, describes a number of implementable governance and management practices to achieve IT governance. As part of step 3 of Goosen's (2012:34) integrated control framework, the processes of COBIT 5 were evaluated to identify if each specific process is relevant in the process of governing the incremental risks introduced by social media. Appendix A contains a complete list and description of all the processes and its application to social media. The following processes in each domain were identified as relevant in the process of governing the incremental risks introduced by social media:

Table 5.1: COBIT 5 processes applicable to social media

Evaluate, direct an monitor (EDM)	
	EDM01 Ensure governance framework setting and maintenance
	EDM02 Ensure benefits delivery
	EDM03 Ensure risk optimisation
	EDM04 Ensure resource optimisation
Align, Plan and Organise (APO)	
	APO01 Manage the IT management framework
	APO02 Manage strategy
	APO04 Manage innovation
	APO07 Manage human resources
	APO08 Manage relationships
	APO11 Manage quality
	APO12 Manage risk
	APO13 Manage security
Deliver, Service and Support (DSS)	
	DSS01 Manage operations
	DSS02 Manage service requests and incidents
	DSS03 Manage problems
	DSS05 Manage security services
	DSS06 Manage business process controls

(Source: ITGI, 2012:24)

5.5 Mapping of incremental risks introduced by social media to relevant COBIT 5 processes

As part of step 3 of Goosen's framework, the risks identified for social media in section 4.4 should be mapped to COBIT 5's processes in order to identify mitigating controls from each process. Table 5.2 contains a detailed mapping of the risks to the relevant processes as identified in Table 5.1.

Table 5.2: Mapping of social media risks to COBIT 5 processes

COBIT 5 PROCESS	Risk 1				Risk 2			Risk 3		Risk 4	
	i	ii	iii	iv	i	ii	iii	i	ii	i	ii
EDM01 Ensure governance framework setting and maintenance	X	X		X	X	X	X	X	X	X	X
EDM02 Ensure benefits delivery										X	X
EDM03 Ensure risk optimisation	X	X	X	X	X	X	X	X	X	X	X
EDM04 Ensure resource optimisation		X	X	X			X			X	X
APO01 Manage the IT management framework	X	X	X	X	X	X	X	X	X		
APO02 Manage strategy										X	X
APO04 Manage innovation										X	X
APO07 Manage human resources	X	X	X	X	X	X	X	X	X		
APO08 Manage relationships			X	X							
APO11 Manage quality	X	X	X	X						X	X
APO12 Manage risk	X	X	X	X	X	X	X	X	X	X	X
APO13 Manage security	X				X	X	X	X	X		
DSS01 Manage operations	X				X	X		X	X		
DSS02 Manage service requests and incidents	X	X	X	X	X	X	X	X	X		
DSS03 Manage problems	X	X	X	X	X	X		X	X		

DSS05 Manage security services	X				X	X	X	X	X		
DSS06 Manage business process controls	X	X		X	X	X	X	X	X		

(Source: Author's own, 2014)

Table 5.2 key:

Risk 1	**Reputational risk**
i	Exposure of the business through fraudulent or criminal activities including malware, hacking and phishing attacks
ii	Inappropriate use of social media by employees that are linked to the business
iii	Insufficient response or not responding timeously to customer complaints and product related queries
iv	Difficulty in controlling published data, changes made to published data and determining who owns the data
Risk 2	**Security risk**
i	Malware such as trojans, viruses and spyware
ii	Malicious hackers and phishing attacks
iii	Uneducated and negligent users
Risk 3	**Privacy risk**
i	Unauthorised access to confidential client or employee information through hacking, phishing attacks and spyware
ii	Unauthorised disclosure of information by employees of the firm due to the fact that they are uneducated or unaware of the impact

Risk 4	Obsolescence risk
i	A social media network used by the business becomes obsolete and shuts down or customers stop using the specific social media network
ii	Software used by customers to help co-create products becomes obsolete
X	The process is applicable in governing the specific risk

(Source of risks: Section 4.4)

5.6 Identifying safeguards for each incremental risk

Each of the processes listed in COBIT 5 describes a number of implementable governance and management practices to achieve IT governance. The relevant control process of COBIT 5 which was matched to each risk in section 5.5 was investigated to identify possible safeguards or controls for the specific risks. In addition to COBIT 5, literature from Chi (2011); ISACA (2010); Briggs (2010) and Rudman (2010) were also reviewed to ensure that a comprehensive list of safeguards is available for each risk. Table 5.3 provides possible safeguards or controls for each of the identified risks.

Table 5.3 Safeguards or controls to mitigate social media risks

RISK		SAFEGUARD OR CONTROL
Risk 1	**Reputational risk**	
i	Exposure of the business through fraudulent or criminal activities including malware, hacking and phishing attacks	• Use a brand protection firm that can scan the internet for misuse of the enterprise brand or appoint a person who is solely responsible for brand protection. • Each social media network used by the business should have a separate email account and distinctive security questions to prevent malicious attackers from gaining access. • Refer to the controls listed at risk 2 (security risk) for specific controls over malware, hacking and phishing attacks.
ii	Inappropriate use of social media by employees that are linked to the business	• Develop a policy that specifies how employees may use business assets and intellectual property in their online presence. • Users must be informed of the details of the policy and they must sign the policy to indicate that they take responsibility for non-compliance with it. • Use a brand protection firm that can scan the internet for misuse of the enterprise brand by employees or appoint a person who is solely responsible for it. • Communication by employees on social media networks should be monitored on a regular basis and acted on immediately if identified as inappropriate. • Communication by former employees or employees who had any dispute with the

		business should be monitored closely. • Employees should be trained about the impact that inappropriate use or comments via social media networks can have on the business. They should also be trained on the consequences they face if it occurs. • Provide employees with a private and safe platform where they can report any inappropriate use of social media by co-workers. • Provide employees with a guideline of examples of suitable and inappropriate behaviour. • Identify possible solutions or recovery actions that can be taken if inappropriate behaviour already occurred.
iii	Insufficient response or not responding timeously to customer complaints and product related queries	• Ensure that staffing is adequate to handle the increase in the amount of traffic that could be created from a social media presence. Appoint personnel who is solely responsible to monitor all customer complaints and who can monitor social media networks for possible complaints. • Regularly review whether appointed employees are following up on all customer complaints and follow up on any discrepancies. • Ensure that employees is adequately trained and have sufficient knowledge about social media and how to use it. • Ensure that employees are adequately trained on how to react to customer complaints and that they have resources such as knowledge repositories with

		examples of response plans available to help them. • Train employees to report any brand-related posts that they see on social media which can influence the business's reputation immediately. • Create notices on social media sites that provide clear windows for customers to log their responses with regards to existing products and services and for customers to log expectations and views. This will enable the business to keep all responses private so that the business can react on it before it goes viral. Address all customer queries in a timely manner based on business policies. • All incidents of customer complaints should be logged and reported. If there is no current solution for a complaint it should be investigated immediately. Use these incidents to identify problem areas with the products or services. • Perform customer satisfaction analysis with the help of social media by providing links to secure private websites where customers can complete a survey that is not open for everyone to see. • Ensure that all quality related queries are documented, resolved, followed up and improved.
iv	Difficulty in controlling published data, changes made to published data and determining who owns the	• Establish clear policies that dictate to employees and customers what information is acceptable to be posted as part of the enterprise social media presence. • Users must be informed of the social media use policy and they must sign the policy to indicate that they take personal responsibility for non-compliance.

	data	• If feasible, ensure that there is a capability to capture and log all communications. • Communication by employees and customers on social media should be monitored on a regular basis and acted on immediately if identified as unauthorised or inappropriate. • All unwanted posts/tweets/videos should be cleared regularly by a responsible person. • Ensure that legal and communications teams carefully review user agreements for social media networks that are being used. • Create notices on social media sites that provide clear windows for customers to log their responses with regards to existing products and services and for customers to log their expectations and views. This will enable the business to keep all responses private and easier to keep track of so that the business can react on it before it goes viral.

Risk 2	**Security risk**	
i	Malware such as trojans, viruses and spyware	• The business should have a policy that states that all computers and similar devices should have antivirus and antispyware software installed on them. • Anti-malware software should be updated regularly and distributed centrally to ensure that all devices are protected. • Regular spot checks should be done on employee's devices to ensure that all anti-malware software is up to date. • Employees should be trained to identify malware attacks, regarding the impact that it can have on the business and how to prevent malware attacks from taking place. • Firewalls should protect the business from outside intruders. • Logs of malware attacks or alerts detected by antivirus and antispyware software should be reviewed regularly to identify possible sources of the threats. Recurring incidents should be investigated in depth.
ii	Malicious hackers and phishing attacks	• All computers should be password protected. The passwords should be unique, strong and should be changed regularly. • Employees should be educated not to share their passwords with anyone. • All computers should have screensaver timeout to protect it from inside and outside attackers. • Employees should be trained to be aware of phishing attacks and that they should

		delete all suspicious messages and avoid clicking on links. • Users should be educated to access a website directly and not through a third party website. • Employees should be trained to become aware of the risks involved with using social media networks. • The business should have a policy that states that all data should be encrypted. • Authentication services need to be implemented to detect when unauthorised users want to connect to the network. Incidents must be addressed immediately.
iii	Uneducated and negligent users	• Employees should be trained to identify malware attacks, regarding the impact that it can have on the business and how to prevent malware attacks from taking place. • Employees should be educated not to share their passwords with anyone. • Employees should be trained to be aware of phishing attacks and that they should delete all suspicious messages and avoid clicking on links to websites. • Users should be educated to access a website directly and not through a third party website. • Employees should be trained to become aware of the risks involved with using social media networks. • The personnel in the IT department should have sufficient knowledge about social media and the risks it introduce in order to address any attacks on the business, to

		effectively execute policies and to train and assist other employees. • All employees must have access to knowledge repositories which contains information regarding the risks and remedies of social media as well as knowledge repositories of all training provided to enable self-support. • Users must be informed of the social media use policy and they must sign the policy to indicate that they take personal responsibility for non-compliance and negligence. Disciplinary actions should be in place to address any negligence.
Risk 3	**Privacy risk**	
i	Unauthorised access to confidential client or employee information through hacking, phishing attacks and spyware	• Refer to controls listed at risk 2 (security risk). • Monitor social media networks for imposter accounts and report them immediately to the service providers. • Monitor social media accounts for change notifications, login notifications and upload notifications that may be suspicious or not from an acceptable source. • Authentication services need to be implemented to determine which user created the data. • Maintain an audit trail of access to information that is sensitive or private. • Provide specific instructions to employees for use and storage of sensitive or private information.

ii	Unauthorised disclosure of information by employees of the firm due to the fact that they are uneducated or unaware of the impact	• An acceptable user policy for social media must be in place to prevent users from revealing confidential information. • Users must be informed of the social media use policy and they must sign the policy to indicate that they take personal responsibility for non-compliance. • Employees should be trained about the impact that data leakage could have on the organisation, how it occurs and the consequences they face if it occurs. • Communication by employees on social media should be monitored on a regular basis and acted on immediately if identified as unauthorised or inappropriate. • Authentication services need to be implemented to determine which user created the data. • Assign access rights to sensitive or private documents. • Maintain an audit trail of access to information that is sensitive or private.

Risk 4	**Obsolescence risk**	
i	A social media network used by the business becomes obsolete and shuts down	• Continually evaluate the existing social media networks used by the business to determine whether customer use of that specific network is declining. • Continually evaluate the external environment for threats of declining technologies. • Expand the social media portfolio by making use of different networks. An interconnected social media presence can create a sustainable engagement. • Evaluate emerging social media networks for innovation which can influence the technical health of the current portfolio.
ii	Software used by customers to help co-create products becomes obsolete	• Continually evaluate the existing social media portfolio to determine whether customer use is declining and whether it still meet the needs it was acquired for. • Encourage customers and employees to provide innovative ideas for potential new social media investments that the business can make. • Evaluate customer satisfactory levels and whether customer expectations are met. • Evaluate emerging social media networks for innovation which can influence the technical health of the current portfolio.

5.7 Conclusion

The aim of this chapter was to continue with the development of the integrated control framework for the IT governance of social media by applying step 3 of Goosen's framework on social media. Step 3's aims are to identify an appropriate existing control framework, mapping the incremental risks identified to the processes of the control framework and then identifying possible mitigating controls for each of the incremental risks of social media.

COBIT 5 was identified as the best existing control framework because it integrates other frameworks and provides a holistic view on governance. The relevant control processes of COBIT 5 were matched to each risk identified for social media in section 4.4. From the applicable processes various safeguards and controls were identified which can be implemented in order to address incremental risks of social media. The main controls identified from COBIT 5 were that employees of the business should be educated regarding the risks and proper use of social media, the business should make use of general IT controls such as passwords, firewalls and anti-virus software and the business should actively monitor their social presence. These controls can be included in a business' existing information security policy and security training programs for end-users.

The controls identified in table 5.3 however only address IT related risks at a strategic level. According to Goosen's framework, in order to ensure successful IT governance, IT related risks at an operational level must also be addressed. Chapter 6 aims to complete the integrated control framework for social media by briefly explaining how to address IT related risks at an operational level.

CHAPTER 6

DEVELOPING AN INTEGRATED CONTROL FRAMEWORK FOR IT GOVERNANCE OF SOCIAL MEDIA AT AN OPERATIONAL LEVEL

6.1 Background

In order for a company to successfully govern social media, the business must address and overcome the IT gap. As discussed in chapter 2, this can only be achieved when the IT strategic objectives and operations support the enterprise's strategic objectives and operations (ITGI, 2003:22).

Chapter 4 and 5 discussed the steps to achieve IT governance at strategic level for social media. IT governance frameworks, like COBIT 5 used in chapter 5, sufficiently address IT governance at strategic level. However they provide little guidance on addressing risks at operational level. The last 4 steps of Goosen's framework addresses IT governance at operational level. A specific case study would be needed in order to discuss these steps in detail, therefore this chapter aims to briefly discuss the steps to achieve IT governance for social media at an operational level.

6.2 IT governance at operational level

Step 4 to 7 of Goosen's (2012:34) integrated control framework must be applied to social media in order to achieve IT governance at operational level.

Step 4: Implement the applicable control techniques as identified at a strategic level

The relevant controls and safeguards as identified in Chapter 5 should be physically implemented by the business.

Step 5: Determine the access paths which are affected by the selected business imperatives

Access paths, as defined in chapter 2, are used to analyse and understand the IT environment which a business should govern (Goosen & Rudman, 2013:842). A number of access paths exist for a user who accesses a social media network. The focus of this study is on business use of social media and therefore only the main access paths followed by the business will be identified.

The following main access paths can be activated by a business to a social media network (website):

- Access through a fixed line from the business premises to a social media website
- Access through a wireless (Wi-Fi) connection to a social media website from anywhere

Step 6: Identify the IT architectural components which form the relevant access path

An access path is created by the connection of various IT hardware, software and other IT architectural components together (Goosen & Rudman, 2013:842). There are numerous possible connections between the different IT components. Each architectural component that forms part of the access path should be identified (Goosen & Rudman, 2013:842). The following are examples of IT architecture components that may form part of the relevant access path to a social media network:

- Computers, laptops, mobile devices
- Operating systems
- Security and management software
- Routers
- Switches
- Firewalls
- Fixed lines (for example ADSL line)

- Wireless networks
- Internet service provider (ISP)
- Social media network

(Goosen & Rudman, 2013:842; Brand, 2013:53)

Step 7: Implement relevant configuration controls over each IT architectural component

Each IT architectural component identified should be examined to identify the configuration controls that are relevant to the component. Configuration controls, as defined in Chapter 2, ensures that the risks identified at an operational level within each IT architectural component are sufficiently governed. Configuration controls are built, setup or installation, configuration, operated and maintenance.

A business which uses social media should evaluate each of the IT architectural components in their access path to identify configuration controls for each component. A specific case study would be needed in order to identify all the architectural components. This is just a general study and therefore the configuration controls for each of the individual components is not discussed.

The social media network (as an IT architectural component) should specifically be considered. Social media networks are mobile and web-based technologies used by a business. It is assumed that for the purpose of this study the business is a third party using social media and not the provider thereof. For this reason they do not design, build, operate or maintain the technology. They can only configure the user rights and settings of the social media network for example security settings such as the password for their social media account and privacy settings to restrict other users from accessing personal information such as telephone numbers. The configuration of each social media network is different and because of the fact that this is a general study without focusing on one specific social media network, the configuration of the social media site's settings will not be discussed in detail. The configuration of the social media network is

however one of the most important steps towards achieving IT governance at an operational level.

According to Goosen (2012:47) if the configuration controls for each of the components in the access path, including the configuration of the social media site, are correctly implemented it will effectively address the IT risks at an operational level and bridge the IT gap.

6.3 Conclusion

The aim of this chapter was to briefly discuss the steps to achieve IT governance for social media at operational level. A detailed discussion was not possible, as one would need a case study in order to address IT governance at operational level in detail. According to the last four steps of Goosen's framework all controls identified in section 5.6 should be implemented after which a business should identify all the relevant access paths with its IT architectural components that are affected by the business imperatives. For each of these IT architectural components a business should implement the relevant configuration controls. The social media network is one of the most important IT architectural components which should be configured.

The access path, its IT architectural components and the configuration controls implemented for each component provide a mechanism for a business to address IT risks at an operational level. By implementing the last four steps in Goosen's framework on social media, a business ensures that they understand the technology used, they identified all the relevant risks and they implement all necessary controls at an operational level to ensure adequate and complete IT governance.

CHAPTER 7

SUMMARY AND CONCLUSION

Social media offers great opportunities for businesses and the use thereof will increase competitiveness. However, social media also introduce significant risks to those who adopt it. This study was undertaken to help businesses to identify incremental risks resulting from social media and to develop an integrated IT governance control framework to address these risks both at strategic and operational level.

Goosen (2012:34) developed a seven step integrated control framework to achieve IT governance and address IT risks at strategic and operational level. By implementing Goosen's framework, the business' strategic objectives and operations are aligned with IT's strategic objectives and operations. The IT gap is thus overcome and strategic alignment, one of the King III focus areas, are addressed.

This study applied Goosen's framework on social media. In step 1 the business imperatives for social media was identified as marketing and product innovation, customer service, pro-active management and pro-active recruitment. Each of these imperatives have a direct impact on the IT that is required by the business. The author identified the IT impact of each imperative and from there was able to identify the incremental risks (step 2) introduced by social media at strategic level. The incremental risks are reputational risk, security risk, privacy risk and obsolescence.

In step 3 COBIT 5 was identified as the best existing control framework because it integrates other frameworks and provides a holistic view on governance. The relevant control processes of COBIT 5 were matched to each risk identified for social media. From the applicable processes various safeguards and controls were identified to address IT risks at a strategic level. The main controls identified from COBIT 5 were that employees of the business should be educated regarding the risks and proper use of social media, the business should make use of

general IT controls such as passwords, firewalls and anti-virus software and the business should actively monitor their social presence. These controls can be included in a business' existing information security policy and security training programs for end-users.

All safeguards and controls identified should be implemented (step 4) after which a business should identify all the relevant access paths (step 5) with its IT architectural components (step 6) that are affected by the business imperatives. For each of these IT architectural components a business should implement the relevant configuration controls (step 7). The social media network is one of the most important IT architectural components which should be configured.

The business imperatives together with the processes of COBIT 5 provide a mechanism for a business to address IT governance at strategic level. The access path, its IT architectural components and the configuration controls implemented for each component provide a mechanism for a business to address IT risks at an operational level. By implementing the safeguards and controls identified from COBIT 5 at strategic level and implementing the configuration controls identified at operational level, a business ensures that they successfully govern the IT related risks introduced by social media and ultimately achieve IT governance.

Areas for possible further research include:

- A more in-depth study of addressing social media risks on operational level derived from the access paths and IT architectural components;
- A case study on the implementation of IT governance principles for social media by South African companies.

LIST OF REFERENCES

Aula, P. 2010. Social media, reputation risk and ambient publicity management. *Strategy & Leadership,* 38(6):43-49.

Badenhorst, M. 2009. *Making sense of IT governance: The implications of King III* [Online]. Available: http://www.icsa.co.za/documents/speakerPres/MarleneBadenhorst/BadenhorstMakingSenseOfITGovernanceTheImplicationsOfKingIII.pdf [2014, September 21].

Boshoff, W.H. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: University of Johannesburg (previously: Rand Afrikaans University).

Boshoff, W.H. 2012. Masters in Commerce (Computer Auditing). Unpublished class notes (Computer Auditing 871). Stellenbosch: Stellenbosch University.

Boshoff, W.H. 2013. Masters in Commerce (Computer Auditing). Unpublished class notes (Computer Auditing 872). Stellenbosch: Stellenbosch University.

Bossenger, A. 2014a. *3 ways any business can market on Pinterest*. [Online]. Available: http://www.socialmediaexaminer.com/3-ways-to-market-on-pinterest/#more-63076 [2014, August 28].

Bossenger, A. 2014b. *How to use Pinterest messages for marketing.* [Online]. Available: http://www.socialmediaexaminer.com/pinterest-messages-marketing/#more-67594 [2014, August 28].

Bowen, P.L., Cheung, M.D. & Rohde, F.H. 2007. Enhancing IT governance practices: A model and case study of an organization's efforts. *International Journal of Accounting Information systems,* 8:191-221.

Brand, JC. 2013. The governance of significant enterprise mobility security risks. Unpublished Masters of Commerce (Computer Auditing) thesis. Stellenbosch: University of Stellenbosch.

Briggs, T. 2010. *Social media's second act: Toward sustainable brand engagement.* [Online]. Available: http://onlinelibrary.wiley.com/doi/10.1111/j.1948-7169.2010.00050.x/pdf [2014, June 20].

Chi, M. 2011. *Security policy and social media use.* [Online]. Available: http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749 [2014, September 24].

Chin, A. 2013. *Two ways social bookmarking can improve your business.* [Online]. Available: http://spinnakr.com/blog/ideas/2013/04/social-bookmarking-to-help-your-business/ [2014, August 28].

Cohen, H. 2013. *7 tips for making your blog a content marketing magnet*. [Online]. Available: http://www.socialmediaexaminer.com/7-tips-for-making-your-blog-a-content-marketing-magnet/ [2014, August 28].

Cooper, J. 2011. *How do I use Wikipedia for SEO purposes?* [Online]. Available: http://pointblankseo.com/wikipedia-seo-purposes [2014, August 28].

Deloitte. s.a. *Social Business*. [Online]. Available: http://www.deloitte.com/view/en_us/us/services/consulting/social-business/index.htm [2013, May 20].

Fink, S. & Zerfass, A. 2010. *Social Media Governance 2010.* [Online]. Available: http://www.ffpr.de/newsroom/2010/09/09/study-social-media-governance-2010-2/#hype [2014, June 25].

Gartner. s.a. *IT Governance (ITG).* [Online]. Available: http://www.gartner.com/it-glossary/it-governance [2014, September 21].

Goodwin, D. 2012. *Wikipedia appears on page 1 of Google for 99% of searches [study]*. [Online]. Available: http://searchenginewatch.com/article/2152194/Wikipedia-Appears-on-Page-1-of-Google-for-99-of-Searches-Study [2014, August 28].

Goosen, R. 2012. The development of an integrated framework in order to implement information technology governance principles at a strategic and operational level for medium-to-large sized South African businesses. Unpublished Masters of Commerce (Computer Auditing) thesis. Stellenbosch: University of Stellenbosch.

Goosen, R. & Rudman, R. 2013. An Integrated Framework To Implement IT Governance Principles At A Strategic And Operational Level for Medium-To Large-Sized South African Businesses. *International Business & Economics Research Journal,* 12(7):835-854.

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information security technical report,* 11:55-61.

Harvard Business Review Analytic Services (HBR-AS). 2010. *The new conversation: Taking social media from talk to* action. [Online]. Available: http://www.sas.com/resources/whitepaper/wp_23348.pdf [2014, June 25].

Information Systems Audit and Control Association (ISACA). 2010. *Social media: Business benefits and security, governance and assurance perspectives.* [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/Social-Media-Wh-Paper-26-May10-Research.pdf?id=45719e26-bcbe-4b48-9782-fe64fb7017cb [2013, June 24].

Institute of Directors Southern Africa (IODSA). 2009. *King Report on corporate governance for South Africa (King III)*. [Online]. Available: http://www.iodsa.co.za [2014, September 21].

IT Governance Institute (ITGI). 2003. *Board Briefing on IT Governance (second edition).* [Online]. Available: http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf [2014, September 21].

ITGI (IT Governance Institute). 2012. *COBIT 5* [Online]. Available: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx [2012, October 19].

Kaplan, A.M. & Haenlein, M. 2009. The fairyland and Second Life: Virtual social worlds and how to use them. *Business Horizons,* 52(1):563-572.

Kaplan, A.M. & Haenlein, M. 2010. Users of the world unite! The challenges and opportunities of social media. *Business Horizons,* 53(1):59-68.

Kaselowski, E. 2008. *Mitigating risk through effective information technology operations in local governments: Towards a best practice* [Online]. Available: http://www.nmmu.ac.za/documents/theses/Mitigating%20Risk%20Through%20Effective%20Information%20Technology%20Governance%20in%20Local%20Governments.pdf [2011, May 24].

Kietzmann, J.H., Hermkens, K., McCarthy, I.P. & Silvestre, B.S. 2011. Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons,* 54(3):241-251.

Kruger, W. & Rudman, R. 2013. Strategic alignment of application software packages and business processes using PRINCE2. *International Business & Economic Research Journal*, 12(10):1239-1260.

McRitchie, J. 1999. *Corporate Governance*. [Online] Available: http://www.corpgov.net/library/definitions.html [2014, September 21].

Nielsen. 2012. *State of the media: The social media report 2012.* [Online]. Available: http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2012-Reports/The-Social-Media-Report-2012.pdf [2014, June 25].

Nielsen. 2013. *Paid social media advertising. Industry update and best practices 2013.* [Online]. Available: http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2013%20Reports/Nielsen-Paid-Social-Media-Adv-Report-2013.pdf [2014, June 25].

Nigel Wright Recruitment. 2011. *The impact of social media on recruitment*. [Online]. Available: http://www.nigelwright.com/Assets/Documents/TheImpactofSocialMediaonRecruitment.pdf [2014, April 2].

Oxford English Dictionary. 2014. [Online]. Available: http://www.oed.com/view/Entry/129926?redirectedFrom=obsolescence#eid [2014, June 25].

Pantano, E., Iazzolino, G. & Migliano, G. 2013. Obsolescence risk in advanced technologies for retailing: A management perspective. *Journal of Retailing and Consumer Services,* 20(2):225-233.

Pettey, C. & Van der Meulen, R. 2011. *Gartner says by year-end 2013, half of all companies will have been asked to produce material from social media websites for E-Discovery.* [Online]. Available: http://www.gartner.com/newsroom/id/1550715 [2014, September 28].

Rudman, R.J. 2010. Framework to identify and manage risks in web 2.0 applications. *African Journal of Business Management*, 4(13):3251-3264.

Shullich, R. 2011. *Risk Assessment of Social Media.* [Online]. Available: http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940 [2014, June 25].

Steenkamp, G. 2011. The applicability of using COBIT as a framework to achieve compliance with the King III Report's requirements for good IT governance. *Southern African Journal of Accountability and Auditing Research*, 11**:**1-8.

Terblanche, J. 2011. An information technology governance framework for the public sector. Unpublished Masters of Commerce (Computer Auditing) thesis. Stellenbosch: University of Stellenbosch.

The State of Queensland. 2014. *Benefits of YouTube for business*. [Online]. Available: http://www.business.qld.gov.au/business/running/marketing/online-marketing/using-youtube-to-market-your-business/benefits-of-youtube-for-business [2014, September 13].

Van Grembergen, W. 2000. The Balanced Scorecard and IT Governance. *Information Systems Control Journal,* 2:40-43.

Vanover, R. 2009. *Five benefits of LinkedIn for organizations (and IT pros)*. [Online]. Available: http://www.techrepublic.com/blog/data-center/five-benefits-of-linkedin-for-organizations-and-it-pros/ [2014, August 28].

Appendix A – COBIT 5 processes and application to social media

COBIT 5 DOMAIN	COBIT 5 PROCESS	DESCRIPTION	APPLICATION TO SOCIAL MEDIA
Evaluate, Direct and Monitor (EDM)	EDM01 Ensure governance framework setting and maintenance	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.	A business that uses social media wants to reach its business imperatives. It is important to put structures, principles, processes and practices in place to ensure that risks are reduced so that the business imperatives can be met.
	EDM02 Ensure benefits delivery	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT and acceptable costs.	The business must decide in which social media networks it wants to invest to get the optimal benefit to reach its business imperatives. The business must assess the technical health of the investment.
	EDM03 Ensure risk optimisation	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.	A business that uses social media should identify the specific risks they are exposed to due to the use of social media and should develop, communicate and monitor risk management practices.
	EDM04 Ensure resource optimisation	Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.	The business needs to make sure that the IT department has the necessary skills, time and knowledge to properly manage and support the use of social media. It might be necessary to appoint someone who is solely responsible for the management of the social media networks that the business uses.

Evaluate, Direct and Monitor (EDM)	EDM05 Ensure stakeholder transparency	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.	N/A – although it is important for a business to report on the success of IT and the adoption of new technologies such as social media, the focus of this research is on addressing incremental risks of social media which was already in use by the business and not on reporting to the stakeholders on the performance of each social media network.
Align, Plan and Organise (APO)	APO01 Manage the IT management framework	Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the enterprise in support of governance objectives in line with guiding principles and policies.	Social media is part of the enterprise IT and should therefore form part of the overall IT governance plan.
	APO02 Manage strategy	Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives.	A business must manage their IT strategy, specifically with regards to which social media networks they want to use and what they want to achieve with it. They must continuously update this strategy taking into account any new developments in social media to prevent obsolescence.
	APO03 Manage enterprise architecture	Establish a common architecture consisting of business process, information data, application and technology architecture layers for effectively and efficiently realising enterprise and IT strategies by creating key models and practices that describe the baseline and target architectures. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential	N/A – For the purpose of this study the business is a third party using social media networks and not the provider thereof. They therefore do not design or maintain the social media architecture.

		cost savings through initiatives such as re-use of building block components.	
Align, Plan and Organise (APO)	APO04 Manage innovation	Maintain an awareness of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.	A business that uses social media must continuously update their IT resources with new developments in social media to gain a competitive advantage and to ensure that it does not become obsolete.
	APO05 Manage portfolio	Execute the strategic direction set for investments in line with the enterprise architecture vision and the desired characteristics of the investment and related services portfolios, and consider the different categories of investments and the resources and funding constraints. Evaluate, prioritise and balance programmes and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programmes into the active services portfolio for execution. Monitor the performance of the overall portfolio of services and programmes, proposing adjustments as necessary in response to programme and service performance or changing enterprise priorities.	N/A - the focus of this research is only on social media and not the IT portfolio as a whole.

Align, Plan and Organise (APO)	APO06 Manage budget and costs	Manage the IT-related financial activities in both the business and IT functions, covering budget, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.	N/A – although it is important to identify the benefits and costs of social media, the focus of this research is only on addressing the incremental risks and thus the budget and costs are not part of this research.
	APO07 Manage human resources	Provide a structured approach to ensure optimal structuring, placement, decision rights and skills of human resources. This includes communicating the defined roles and responsibilities, learning and growth plans, and performance expectations, supported with competent and motivated people.	A business using social media needs to appoint someone who has the necessary skills and competencies to be responsible for the management of the social media. Sufficient training must also be provided to all other employees using social media.
	APO08 Manage relationships	Manage the relationship between the business and IT in a formalised and transparent way that ensures a focus on achieving a common and shared goal of successful enterprise outcomes in support of strategic goals and within the constraint of budgets and risk tolerance. Base the relationship on mutual trust, using open and understandable terms and common language and a willingness to take ownership and accountability for key decisions.	Business-IT alignment must be achieved for social media in order to comply with the King III IT governance principles.
	APO09 Manage service agreements	Align IT-enabled services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.	N/A – This study do not address any risks or provide any controls regarding service level agreements between the business and social media provider.

Align, Plan and Organise (APO)	APO10 Manage suppliers	Manage IT-related services provided by all types of suppliers to meet enterprise requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.	N/A – the use of social media does not require specific supplier management. The choice of social media networks does not fall within the scope of the research.
	APO11 Manage quality	Define and communicate quality requirements in all processes, procedures and the related enterprise outcomes, including controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.	The quality of the products as well as the social media networks used must be measured to avoid reputational damage.
	APO12 Manage risk	Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.	All risks introduced by social media should be identified, assessed and addressed.
	APO13 Manage security	Define, operate and monitor a system for information security management.	Security and privacy of information are risks introduced by social media. It is therefore very important that these risks should be managed.
Build, Acquire and Implement (BAI)	BAI01 Manage programmes and projects	Manage all programmes and projects from the investment portfolio in alignment with enterprise strategy and in a co-ordinated way. Initiate, plan, control, and execute programmes and projects, and close with a post-implementation review.	N/A – a detailed project management plan for social media is necessary, however the focus of the research is on a business which already uses social media networks and which is not the provider of the social media network, therefore the business do not build, acquire or implement social media networks and the management of programmes and projects are not necessary.

Build, Acquire and Implement (BAI)	BAI02 Manage requirements definition	Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinate with affected stakeholders the review of feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.	N/A – this research is based on a business who already uses social media and thus the pre-acquisition requirements are not within the scope of this research. The business is also not the provider of the social media network and therefore do not need to build a social media network.
	BAI03 Manage solutions identification and build	Establish and maintain identified solutions in line with enterprise requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.	N/A – this research is based on a business who already uses social media and thus the acquisition requirements are not within the scope of this research. The business is also not the provider of the social media network and therefore do not need to develop or build a social media network.
	BAI04 Manage availability and capacity	Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.	N/A – availability and capacity of social media do not fall in the scope of this research. The focus of the research is on a business which already uses social media. The business is also not the provider of the social media network and therefore do not need to develop or build a social media network.
	BAI05 Manage organisational change enablement	Maximise the likelihood of successfully implementing sustainable enterprise wide organisational change quickly and with reduced risk, covering the complete life cycle of the change and all affected stakeholders in the business and IT.	N/A – the first time adoption of social media does not fall in the scope of this research, thus it is assumed that organisational change already took place when social media was introduced the first time.

Build, Acquire and Implement (BAI)	BAI06 Manage changes	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.	N/A - A company that changes or adopts an additional social media network need to manage the change. This research does not cover the first time adoption of social media or the change to another network.
	BAI07Manage change acceptance and transitioning	Formally accept and make operational new solutions, including implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and IT services, early production support, and a post-implementation review.	N/A - A company that changes or adopts an additional social media network need to plan this carefully. This research does not cover the first time adoption of social media or the change to another network.
	BAI08 Manage knowledge	Maintain the availability of relevant, current, validated and reliable knowledge to support all process activities and to facilitate decision making. Plan for the identification, gathering, organising, maintaining, use and retirement of knowledge.	N/A – The focus of this research is only on addressing the incremental risks introduced by social media. It does not focus on the sources, using and sharing of knowledge.
	BAI09 Manage assets	Manage IT assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available. Manage software licences to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with licence agreements.	N/A – social media is a platform provided by a third party. This research only focus on the users of social media and not the providers thereof, therefore it is not the asset of the business to manage.

Build, Acquire and Implement (BAI)	BAI10 Manage configuration	Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.	N/A - social media is a platform provided by a third party who is responsible to build and configure it. This research only focus on the users of social media and not the providers thereof.
Deliver, Service, Support (DSS)	DSS01 Manage operations	Co-ordinate and execute the activities and operational procedures required to deliver internal and outsourced IT services, including the execution of pre-defined standard operating procedures and the required monitoring activities.	The management of the use of social media networks is important especially to protect sensitive business and client information.
	DSS02 Manage service requests and incidents	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.	Incidents that can harm the business such as unauthorised access and customer complaints must be diagnosed, reported, investigated and prevented.
	DSS03 Manage problems	Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.	Incident that can harm the business such as unauthorised access and customer complaints must be diagnosed, reported, investigated and prevented.
	DSS04 Manage continuity	Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the enterprise.	N/A – a business continuity plan is very important to a business but is not part of this research.

Deliver, Service, Support (DSS)	DSS05 Manage security services	Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.	Security and privacy of information are risks introduced by social media. It is therefore very important that these risks should be managed.
	DSS06 Manage business process controls	Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements and manage and operate adequate controls to ensure that information and information processing satisfy these requirements.	It is important to identify relevant controls to mitigate the risks introduced by social media.
Monitor, Evaluate and Asses (MEA)	MEA01 Monitor, evaluate and assess performance and conformance	Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.	N/A – the focus of this research is only on addressing the incremental risks introduced by social media. Performance measurement was not identified as an incremental risk and therefore assessing the performance of social media is not within the scope of this research.
	MEA02 Monitor, evaluate and assess the system of internal control	Continuously monitor and evaluate the control environment, including self-assessments and independent assurance reviews. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control assessment and assurance activities.	N/A – the focus of this research is only on addressing the incremental risks introduced by social media. The monitoring of the system of internal control was not identified as an incremental risk and is therefore not within the scope of this research.

Monitor, Evaluate and Asses (MEA)	MEA03 Monitor, evaluate and assess compliance with external requirements	Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.	N/A – the focus of this research is only on addressing the incremental risks introduced by social media and not on compliance with legal, regulatory and contractual requirements.