

Achieving It Governance Of Social Media At Strategic And Operational Levels


Petro Gerber, Stellenbosch University, South Africa

ABSTRACT

Social media offers great opportunities for businesses, and the use thereof will increase competitiveness. However, social media also introduces significant risks to those who adopt it. This study was undertaken to identify incremental risks resulting from the adoption of social media by businesses and to develop an integrated Information Technology (IT) governance control framework to address these risks. In order to overcome the IT gap, these risks are addressed both at strategic and operational levels. With the help of the processes in Control Objectives for Information Technology and Related Technology (COBIT) 5, this study provides safeguards or controls that can be implemented to address the IT risks that social media introduces to a business. A business can ensure that it successfully governs the IT-related risks at a strategic level through the implementation of the safeguards and controls identified from COBIT 5. This study also briefly discusses the steps that a business can follow to ensure IT-related risks at an operational level are addressed through the implementation of configuration controls.

Keywords: COBIT 5; IT Governance; Social Media

1. INTRODUCTION AND BACKGROUND

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

To implement IT governance principles and structures and simultaneously overcome the IT gap, a business-IT alignment process must be implemented (Goosen & Rudman, 2013). 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 businesses with the business-IT alignment process. According to Goosen and Rudman (2013), 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 that can be implemented to address business strategies and operations, as well as IT strategies and operations.

Goosen (2012) 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 levels. Goosen's (2012) seven-step integrated control framework could be used to address the risks of social media at strategic and operational levels.

Research Objective and 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 levels. Businesses need to have governance policies and structures in place to govern these risks. Defining these governance policies and structures can be complex and difficult and, if not done correctly, could 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 levels.

Research Methodology

To achieve the aims of this study, a literature review was performed to obtain an understanding of IT governance principles, structures, processes, mechanisms and control frameworks, as well as social media categories, business use of social media and risks relating to social media. From the literature review, the author was able to determine that an integrated control framework, such as Goosen's seven-step integrated framework (Goosen's framework), can be implemented to achieve IT alignment, both at strategic and operational levels. The remainder of the study subsequently follows Goosen's framework and applies it to social media to achieve IT governance of social media.

2. LITERATURE REVIEW

2.1 IT Governance

2.1.1 An Overview of IT Governance

Companies rely greatly on IT to achieve their business goals. 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 levels (IODSA, 2009). When a new technology, such as social media, is introduced, new risks are also introduced to the business. According to Badenhorst (2009), the risks relating to IT have become substantial, and, therefore, governance of these IT-related risks is vital.

IT Governance Institute (ITGI) (2003:10) describes IT governance as follows:

“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.”

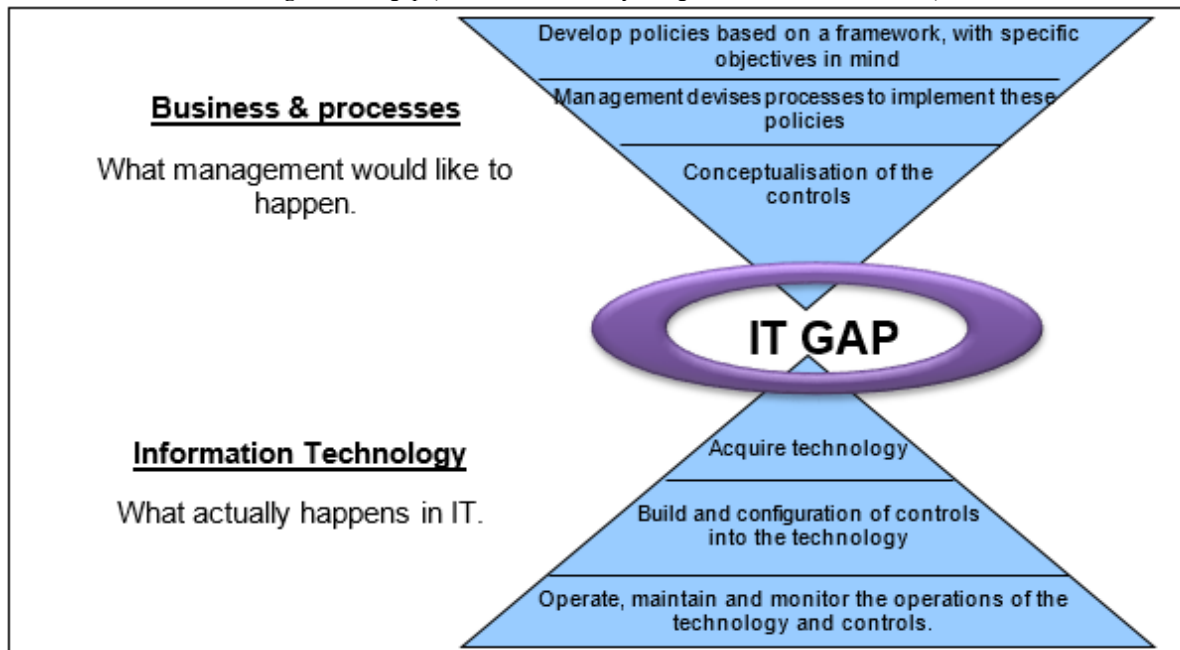
IT governance is achieved when the board members understand the IT environment and risks surrounding the IT, thus aligning the IT strategy with the business strategy when implementing structures and processes. To achieve strategic alignment, business and IT professionals must communicate to ensure that their strategies are aligned. An IT gap will result if communication is not done properly.

2.1.2 IT Gap

The board and executive management of a company usually expect that the company's IT resources will add value to the business for example provide fast solutions and services, improve efficiency and productivity. In many businesses this expectation of IT is often not met (ITGI, 2003). The reason that this expectation is not met, is that there is a miscommunication between executive management and the IT professionals of a business.

An IT gap, as illustrated in figure 1 below, exists when 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. While simultaneously, 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).

Figure 1. IT gap (Rudman, as cited by Kruger & Rudman, 2013:1242)



When an IT gap exists in a business, it is not possible to achieve strategic alignment.

2.1.3 Business-IT Alignment

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

Many companies rely on existing best practice control frameworks 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). The existing control frameworks each address different internal controls. For example, COBIT describes IT controls that should be implemented at a strategic level in the day-to-day operations, while ITIL describes best practices specifically for IT service management. According to Goosen and Rudman (2013), to achieve business-IT alignment, a business will need to combine existing control frameworks to develop an integrated control framework that can be implemented by the business. The implementation of an integrated control framework will address both business and IT strategies and operations, thus achieving business-IT alignment. Combining these existing control frameworks can be time-consuming and costly and, therefore, a business should only identify those areas and control techniques that apply to the organisation.

2.2 Integrated Control Framework

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

IT Governance at a 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 an Operational Level

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

2.3 Development of the Integrated Framework

The development of Goosen's framework for a specific business requires a better understanding of each of the steps listed above.

2.3.1 Business Imperatives

A business should distinguish between their basic business assumptions and business imperatives. Business assumptions are the objectives set by a business to perform its basic everyday functions. 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 that give the organisation its competitive advantage in its specific environment (Boshoff, 2012). Business imperatives are specific to each business environment (Goosen & Rudman, 2013).

2.3.2 Identify Incremental 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

2.3.3 Link the Risks to Processes of a Control Framework

The risks identified are 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.

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. COBIT 5 thus provides an integrated control framework for the governance and management of enterprise IT (ITGI, 2012). COBIT 5 recognises that there is a clear distinction between governance and management of IT, as 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 five processes.

The management area consists of four domains:

- Align, Plan and Organise (APO) subdivided into 13 processes
- Build, Acquire and Implement (BAI) subdivided into ten processes
- Deliver, Service and Support (DSS) subdivided into six processes
- Monitor, Evaluate and Assess (MEA) subdivided into three processes

These processes are enablers that can assist an organisation with IT governance and management.

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.

2.3.3 Implement the Techniques Identified at a Strategic Level

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

2.3.5 Determine the Access Paths

The access paths that are affected by each business imperative should be identified. Boshoff (1990:24,92,100) defines 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.”

There may be multiple access paths for the same user or activity. However, the number of actual access paths available is finite (Boshoff, 1990). A business should identify each access path that is affected by the business imperative.

2.3.6 Identify the IT Architectural Components

Each access path, as identified in 2.3.5, consists of various IT architectural components, which must 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.

2.3.7 Implement Relevant Configuration Controls Over Each IT Architectural Component

Boshoff, as cited by Goosen & Rudman (2013), stated that each IT architectural component should be examined to ensure that they are correctly built, set up, configured, operated and maintained, so as to correctly control the particular access path. These controls are referred to as configuration controls. The configuration controls that manage the risks inherent to the IT architectural components are defined as follows (Goosen, 2012:46-47):

“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.”

The configuration controls can manage the risks inherent to the IT architectural components. According to Goosen (2012), 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.

Goosen’s framework can be applied by a business to any new technology introduced to the business. One such technology that a business can use is social media.

2.4 An Overview of Social Media

The use of social media in business has increased remarkably over the past few years. Many organisations have introduced social media into their businesses and social media features on their agendas (Fink & Zerfass, 2010) with separate budgets allocated to social media (Nielsen, 2013).

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). The primary characteristic of social media is the interactivity thereof. Participants can freely send, receive and process information for use by others (Aula, 2010). It is also characterised by open participation (can be used by anyone, including businesses, employees and individuals), discussions, community, networking and the rapid and widespread of information and other content across different communication channels (Aula, 2010). Examples of social media networks include Facebook, Twitter, LinkedIn, Instagram, Google Plus+ and YouTube.

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. In the case of conventional media, a business could strategically decide which information it 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). Through social media, consumers can freely exchange ideas or opinions on companies, brands, products and services.

2.5 Business Use of Social Media

Social media can be a positive business tool to enhance the growth, profitability and image of the business. Businesses use social media for marketing, market research, customer service, internal process management, human resource management, virtual product sales and collaboration.

2.6 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 the Information Systems Audit and Control Association (ISACA) (2010), 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), Fink and Zerfass (2010) and Shullich (2012) identified the following risks of a corporate social media presence:

- Malware such as trojans, viruses and spyware introduced through social media can cause data leakage, theft and system downtime,
- Breach of privacy due to exposure of customer information,
- Targeted phishing attacks on customers or employees,
- Reputational damage due to customer backlash, adverse legal actions, difficulty to control published data, difficulty to control the communication process with customers,
- Customer service expectations increase that can lead to customer dissatisfaction with the response of the enterprise (not timeously), leading to reputational damage,
- Reputational damage due to employees posting pictures or information that link them to the enterprise,
- Privacy violations due to employees using personal accounts to communicate work-related information,
- It may be difficult to determine ownership of published content,
- 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,
- Excessive use of social media in the workplace by employees can lead to network utilisation issues, unproductive workers and an increase in exposure to malware attacks,
- Employees accessing social media via enterprise devices can cause malware attacks or infection of devices, data theft from devices or data leakage,
- Loss of competitive advantage,
- Publishing of confidential information or locations by uneducated and negligent employees, and
- Breach of privacy by employees due to lack of awareness can lead to harassment such as blackmailing, extortion, cyber bullying and cyber stalking.

3. FINDINGS AND DISCUSSIONS/APPLICATIONS

3.1 Overview

To develop an integrated IT governance control framework for social media, the business's strategic objectives and operations should be aligned with IT's strategic objectives and operations. By applying Goosen's seven-step framework to social media, businesses can identify incremental risks resulting from the adoption of social media and can develop an integrated IT governance control framework to address these risks, both at strategic and operational levels, thus bridging the IT gap.

3.2 Implementation of Goosen's Seven-Step Framework

3.2.1 Step 1: Identify the Business Imperatives for Social Media

Business imperatives are the foundation of the business-IT alignment process. The following business imperatives were identified as the key business imperatives for a business that uses social media:

Marketing and Product Innovation

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

Customer Service

Customer service levels must be impeccable to gain a competitive advantage in the business environment. To increase customer satisfaction levels, it is necessary to gather information about customers' perceptions and requests about the products or services (Goosen, 2012; ISACA, 2010).

Pro-Active Management

Real-time information must be available to the business to enable the evaluation of customer needs, discussions and perceptions. Real-time information will enable the business to address customer issues quickly and to adjust strategies, products or services appropriately to gain a competitive advantage (Goosen & Rudman, 2013).

Pro-Active Recruitment

Pro-active recruitment processes are required to ensure that the business can find the most suitable candidate for a vacancy before its competitors. For a business’ recruitment processes to be pro-active, the recruitment practices should consider 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 Wright Recruitment, 2011).

3.2.2 Step 2: Identify the Incremental Risks Derived from the Business Imperatives for Social Media

Each of the business imperatives will have a direct impact on the IT that is required by the business to achieve the business imperative concerned. Risks are introduced to the business due to the specific IT requirement. The impact of each imperative on the IT environment was evaluated to identify the incremental risks at a strategic level (refer to 2.3.2 and 2.6) derived from each business imperative. The incremental risks identified are summarised in Table 1 below.

Table 1. Incremental risks derived from the IT requirements of each of the business imperatives

Incremental risk	Business imperatives			
	Marketing and product innovation	Customer service	Pro-active management	Pro-active recruitment
Reputational				
1. Exposure of the business through fraudulent or criminal activities, including malware, hacking and phishing attacks				
2. Inappropriate use of social media by employees that are linked to the business	✓	✓	✓	✗
3. Insufficient response or not responding timeously to customer complaints and product-related queries				
4. Difficulty in controlling published data, changes made to published data and determining who owns the data				
Security				
1. Malware such as trojans, viruses and spyware				
2. Malicious hackers and phishing attacks	✓	✓	✓	✓
3. Uneducated and negligent users				
Privacy				
1. Unauthorised access to confidential client or employee information through hacking, phishing attacks and spyware	✓	✓	✓	✓
2. Unauthorised disclosure of information by employees of the firm because they are uneducated or unaware of the impact				
Obsolescence				
1. A social media network used by the business becomes obsolete and shuts down, or customers stop using the specific social media network	✓	✓	✓	✓
2. Software used by customers to help co-create products becomes obsolete				

3.2.3 Step 3: Link the Risks to Processes of a Control Framework

Each of the processes listed in COBIT 5 describes some implementable governance and management practices to achieve IT governance. The processes of COBIT 5 were evaluated to identify their relevance in the process of governing the incremental risks introduced by social media. The risks identified for social media in step 2 were then mapped to the COBIT 5 processes to identify mitigating controls from each process. In addition to COBIT 5, literature from Chi (2011), ISACA (2010), Briggs (2010) and Rudman (2010) was also reviewed to ensure that a comprehensive list of safeguards is available for each risk identified for social media. Appendix A contains the relevant processes, as well as detailed possible safeguards or controls for each of the identified risks.

The summarised controls are:

- 3.2.3.1 Develop and implement a social media user policy that provides guidelines on acceptable social media usage, confidentiality of information and consequences for non-compliance with the user policy.
- 3.2.3.2 Provide training to employees on the content of the social media user policy, as well as the risks involving social media, the risk of data leakage and the safeguards available to mitigate these risks.
- 3.2.3.3 Appoint a brand protection firm or employee who can scan and monitor social media sites for inappropriate communication or misuse.
- 3.2.3.4 Develop and implement a social media customer management policy to monitor customer complaints. Employ staff who is responsible to address these customer complaints, and who is responsible to ensure that all complaints are logged, reported and resolved.
- 3.2.3.5 Provide training to employees on the content of the social media customer management policy, thereby ensuring that they have sufficient knowledge of how to apply the policy and how to react to customer complaints.
- 3.2.3.6 All IT access controls (for example, passwords/firewalls/authentication logs) should be documented, implemented, monitored and regularly updated.
- 3.2.3.7 Employees should be educated on specific IT access controls that can mitigate the risks involved with the adoption of social media.
- 3.2.3.8 Continually evaluate the social media networks currently in use by the business for possible threats that could indicate that the social media network is a declining technology.

3.2.4 Step 4: Implement the Applicable Control Techniques, as Identified at a Strategic Level

The relevant controls and safeguards, as identified in 3.2.3, should be physically implemented by the business to achieve IT governance at a strategic level.

3.2.4 Step 5: Determine the Access Paths that are Affected by the Selected Business Imperatives

Access paths are used to analyse and understand the IT environment that a business should govern (Goosen & Rudman, 2013). More than one access path can 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 when engaging with a social media network (website):

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

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

An access path is created by the connection of various IT hardware, software and other IT architectural components (Goosen & Rudman, 2013). There are numerous possible connections between the different IT components. The business must identify each architectural component that forms part of the access path (Goosen & Rudman, 2013).

The following are examples of IT architectural components that may form part of the relevant access path to a social media network:

- Computers, laptops and mobile devices,
 - Operating systems,
 - Security and management software,
 - Routers,
 - Switches,
 - Firewalls,
 - Fixed lines (for example, ADSL line),
 - Wireless networks,
 - Internet service provider (ISP), and
 - Social media network
- (Goosen & Rudman, 2013; Brand, 2013).

3.2.7 Step 7: Implement Relevant Configuration Controls Over Each IT Architectural Component

Each IT architectural component should be examined to identify the configuration controls that are relevant to the component. Configuration controls are built, set up or installed, configured, operated and maintained. Configuration controls ensure that the risks identified at an operational level within each IT architectural component are sufficiently governed.

A business that 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 to identify all the architectural components. This study is 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 receive special consideration. 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, as this is a general study that does not focus 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 and should, therefore, be done with caution and precision.

If the configuration controls for each of the components in the access path are correctly implemented, including the configuration of the social media site, IT risks at an operational level will be effectively addressed and the IT gap will be bridged.

4. CONCLUSION

Social media offers great opportunities for businesses. The use of social media by businesses will increase competitiveness. However, social media also introduces 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 levels.

Goosen (2012) developed a seven-step integrated control framework to achieve IT governance and address IT risks at strategic and operational levels. By implementing Goosen's framework, the business's strategic objectives and operations are aligned with IT's strategic objectives and operations. The IT gap is thus overcome.

This study applied Goosen's framework to social media. To achieve IT governance at a strategic level, the business should identify the relevant business imperatives for social media, identify the IT impact of each imperative and then identify the incremental risks introduced by social media. The business should then identify controls which should be implemented from an existing control framework such as COBIT 5 to address these incremental risks.

To achieve IT governance at an operational level, the business should identify all the relevant access paths involving its IT architectural components. For each of these IT architectural components, the relevant configuration controls should be implemented. The social media network used by the business is one of the most important IT architectural components to be configured.

The business imperatives, together with the processes of COBIT 5, provide a method for a business to address IT governance at a 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 a strategic level and implementing the configuration controls identified at an operational level, a business ensures that they successfully govern the IT-related risks introduced by social media and, ultimately, achieve IT governance.

The following recommendations must be applied to achieve IT governance of social media:

1. Develop or expand the business' security training program to educate users regarding the risks and proper use of social media.
2. Appoint personnel who is solely responsible to monitor the business' social media presence.
3. Develop a social media acceptable use policy, communicate it to employees and monitor their compliance with it.
4. Update the existing information security policy with new policies that address specific information security risks introduced by social media.
5. Configure each social media network's settings to protect the business from the risks identified from the business imperatives.
6. Implement configuration controls for each IT architectural component that forms part of the access path to the social media network.
7. Ensure that general IT controls such as passwords, firewalls and anti-virus software are updated, maintained and implemented by all employees.

AUTHOR BIOGRAPHY

Mrs. Petro Gerber is currently a lecturer in financial accounting at Stellenbosch University. She is a qualified Chartered Accountant (South Africa). E-mail: petrok@sun.ac.za

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*. Retrieved from: <http://www.icsa.co.za/documents/speakerPres/MarleneBadenhorst/BadenhorstMakingSenseOfITGovernanceTheImplicationsOfKingIII.pdf>.
- Boshoff, W.H. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. University of Johannesburg, Johannesburg.
- Boshoff, W.H. 2012. Masters in Commerce (Computer Auditing). Unpublished class notes (Computer Auditing 871). Stellenbosch University, Stellenbosch.
- Boshoff, W.H. 2013. Masters in Commerce (Computer Auditing). Unpublished class notes (Computer Auditing 872). Stellenbosch University, Stellenbosch.
- Brand, J.C. 2013. The governance of significant enterprise mobility security risks. Unpublished Masters of Commerce (Computer Auditing) thesis. University of Stellenbosch, Stellenbosch.
- Briggs, T. 2010. *Social media's second act: Toward sustainable brand engagement*. Retrieved from: <http://onlinelibrary.wiley.com/doi/10.1111/j.1948-7169.2010.00050.x/pdf>.
- Chi, M. 2011. *Security policy and social media use*. Retrieved from: <http://www.sans.org/reading->

- room/whitepapers/policyissues/reducing-risks-social-media-organization-33749.
- Fink, S. & Zerfass, A. 2010. *Social Media Governance 2010*. Retrieved from: <http://www.ffpr.de/newsroom/2010/09/09/study-social-media-governance-2010-2/#hype>.
- 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. University of Stellenbosch, 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.
- Information Systems Audit and Control Association (ISACA). 2010. *Social media: Business benefits and security, governance and assurance perspectives*. Retrieved from: <http://www.isaca.org/Knowledge-Center/Research/Documents/Social-Media-Wh-Paper-26-May10-Research.pdf?id=45719e26-bcbe-4b48-9782-fe64fb7017cb>.
- Institute of Directors Southern Africa (IODSA). 2009. *King Report on corporate governance for South Africa (King III)*. Retrieved from: <http://www.iodsa.co.za>.
- IT Governance Institute (ITGI). 2003. *Board Briefing on IT Governance (second edition)*. Retrieved from: http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf.
- ITGI (IT Governance Institute). 2012. *COBIT 5* Retrieved from: <http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>.
- Kaplan, A.M. & Haenlein, M. 2010. Users of the world unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59-68.
- 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.
- Nielsen. 2013. Paid social media advertising. Industry update and best practices 2013. Retrieved from: <http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2013%20Reports/Nielsen-Paid-Social-Media-Adv-Report-2013.pdf>.
- Nigel Wright Recruitment. 2011. The impact of social media on recruitment. Retrieved from: <http://www.nigelwright.com/Assets/Documents/TheImpactofSocialMediaonRecruitment.pdf>.
- 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. Retrieved from: <http://www.gartner.com/newsroom/id/1550715>.
- 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*. Retrieved from: <http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940>.

APPENDIX A

Table A:1. Safeguards or controls to mitigate social media risks

	RISK	COBIT 5 PROCESS	SAFEGUARD OR CONTROL
Risk 1	Reputational risk		
I	Exposure of the business through fraudulent or criminal activities including malware, hacking and phishing attacks	EDM01 EDM03 APO01 APO07 APO11 APO12 APO13 DSS01 DSS02 DSS03 DSS05 DSS06	<ul style="list-style-type: none"> 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	EDM01 EDM03 EDM04 APO01 APO07 APO11 APO12 DSS02 DSS03 DSS06	<ul style="list-style-type: none"> 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	EDM03 EDM04 APO01 APO07 APO08 APO11 APO12 DSS02 DSS03	<ul style="list-style-type: none"> Ensure that staffing is adequate to handle the increase of traffic that could be created from a social media presence. Appoint personnel who is solely responsible to monitor social media for possible complaints. Regularly review whether appointed employees are following up on all customer complaints and follow up on any discrepancies. Ensure that employees are 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 that 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

			<p>products and services and for customers to log expectations and views. These windows 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 promptly based on business policies.</p> <ul style="list-style-type: none"> • 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 on social media websites redirecting the customer 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 data	EDM01 EDM03 EDM04 APO01 APO07 APO08 APO11 APO12 DSS02 DSS03 DSS06	<ul style="list-style-type: none"> • 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. • 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 regularly be cleared 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. These windows 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	EDM01 EDM03 APO01 APO07 APO12 APO13 DSS01 DSS02 DSS03 DSS05 DSS06	<ul style="list-style-type: none"> • 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 regularly reviewed to identify possible sources of the threats. Recurring incidents should be investigated in depth.
II	Malicious hackers and phishing attacks	EDM01 EDM03 APO01 APO07 APO12 APO13 DSS01	<ul style="list-style-type: none"> • All computers should be password protected. The passwords should be unique, strong and should regularly be changed. • 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.

		DSS02 DSS03 DSS05 DSS06	<ul style="list-style-type: none"> • 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	EDM01 EDM03 EDM04 APO01 APO07 APO12 APO13 DSS02 DSS05 DSS06	<ul style="list-style-type: none"> • 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 introduces 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	EDM01 EDM03 APO01 APO07 APO12 APO13 DSS01 DSS02 DSS03 DSS05 DSS06	<ul style="list-style-type: none"> • 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 because they are uneducated or unaware of the impact	EDM01 EDM03 APO01 APO07 APO12 APO13 DSS01 DSS02 DSS03	<ul style="list-style-type: none"> • 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

		DSS05 DSS06	<p>monitored on a regular basis and acted on immediately if identified as unauthorised or inappropriate.</p> <ul style="list-style-type: none"> • 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	EDM01 EDM02 EDM03 EDM04 APO02 APO04 APO11 APO12	<ul style="list-style-type: none"> • 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 that can influence the technical health of the current portfolio.
II	Software used by customers to help co-create products becomes obsolete	EDM01 EDM02 EDM03 EDM04 APO02 APO04 APO11 APO12	<ul style="list-style-type: none"> • 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 by the business. • 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 that can influence the technical health of the current portfolio.