A conceptual framework for integrated information privacy protection

Hanifa Abdullah
School of Computing, College of Science, Engineering and Technology (CSET)
University of South Africa (UNISA)
Florida, Roodepoort, Johannesburg, South Africa
abdulh @unisa.ac.za

L. Labuschagne
Research Administration Department
University of South Africa (UNISA)
Pretoria
South Africa
llabus @unisa.ac.za

J. Young
Centre for Business Management
University of South Africa (UNISA)
Pretoria
South Africa
youngj@unisa.ac.za

***Abstract*— Successful organizations strive to achieve a high degree of corporate governance, effective techniques for risk management, and an assurance regarding the fulfilment of compliance requirements. This effort bears the Governance, Risk and Compliance (GRC) label, which entails integrating these three disparate disciplines to achieve effectiveness and efficiency in meeting the organization's strategic objectives. An interesting development has been the integration of privacy within a GRC context. Privacy has a number of elements, including governance, management, legal, technical aspects, compliance, risk management, information security, business processes and organizational issues which fall into the GRC processes. A large number of privacy breaches and a growing number of privacy regulations will steer organizations in the realm of managing privacy protection within a GRC context. There are a number of privacy facets but the focus of this paper is specifically on information privacy protection.**

This paper seeks to develop a formalized and repeatable conceptual framework to address information privacy protection within a GRC frame of reference.

Keywords*— *Information privacy, data protection, corporate governance, risk management, compliance, Governance, Risk and Compliance (GRC)

I. INTRODUCTION

In 1986, [1], espoused that the Information Age would lead to four major concerns regarding the use of information, namely, privacy, accuracy, property and accessibility (PAPA). This assertion proved to be valid for each area, particularly privacy, which has become the focus of concern over the years [2]. Ubiquitous computing has facilitated the collection, processing, distribution and usage of personal information freely and this has prompted consumer worries [3]. The "information society" according to [4] renders the exchange of vast amounts of personal information via the Internet raising the importance of data protection.

A new development has been the rise of privacy within a Governance, Risk and Compliance (GRC) market niche [5]. The three keywords, governance, risk and compliance are commensurate with GRC, an acronym that has infiltrated the business community over the last years [6]. According to [7], "GRC is an integrated approach overseeing people, processes and technology in order to deliver stakeholder value while managing risk and complying with regulations and laws".

978-1-5090-2576-3/16/$31.00 ©2016 IEEE.

Many organizations get their first experience of a GRC program when they begin to implement a privacy program as privacy is an enterprise issue that spans legal, information technology (IT), compliance and business operations [8]. This paper considers the concept of GRC as a meaningful approach to information privacy protection by embedding the individual components of information privacy protection within a GRC frame of reference.

Reference [9], states the purpose of a conceptual framework is to explain the foremost things to be studied and the relationships between them. The conceptual framework presented in this paper is an outline of GRC items interlinked to support information privacy protection. The approach and application of each item of GRC provides a unique contribution to information privacy protection. When applied in a well-designed, planned and coordinated manner, GRC provides a distinctive solution for the proactive planning of information privacy protection which is the objective of this paper.

This paper is structured as follows. Section II provides an overview of information privacy with a view of identifying the various information privacy protection elements that can be integrated within a GRC conceptual framework. Section III provides a discussion of the various information privacy protection elements. Section IV focuses on the development of the conceptual framework for integrated information privacy protection. Section V provides the conclusion to this paper with reflections on future research.

II. BACKGROUND ON INFORMATION PRIVACY

A. Information Privacy

Privacy is the "right of individuals to control the collection and use of personal information about themselves" [10]. Reference [11], defines four dimensions of privacy including privacy of the person (bodily privacy), privacy of personal communication, privacy of personal data (information privacy) and media privacy which relates to aspects of behavior such as political activities and religious practices in both private and public places.

The focus of this paper is on information privacy. According to [11], information privacy refers to an individual's claim that data about themselves should not automatically be available to other individuals and organizations, and where

another party possesses data, the individual must be able to exercise a substantial degree of control over that data and its use.

As the use of IT systems has become highly accessible and present in both business and government operations, there has been an increase in the number of failures to protect personal information [12]. The protection of personal information called privacy protection or data protection has emerged as a critical issue due to rapid technological changes fostering the free flow of personal information [13]. The focus of this paper is therefore on the protection of personal data (information privacy).

The following section provides an overview of privacy management activities, practices and privacy research areas that must be taken cognizance of when implementing a privacy initiative within an organization. The privacy initiative in the context of this study is information privacy protection and hence the activities, practices and research areas are referred to as information privacy protection elements as discussed in the ensuing section.

B. Information Privacy Protection Elements

Reference [14] identifies privacy program management activities as being located from the highest cited activity to the lowest cited activity as legal, IT, compliance, risk management and security according to a survey conducted in 2011. Reference [15], identifies the factors that must be taken into consideration when implementing privacy practices into the broad categories of legal requirements, available technologies, social norms and business processes. Reference [16], asserts that privacy is an area that involves governmental, legal, social, managerial and technical matters. Reference [17], states that laws, policies, management and practices of organizations and the behavior of individuals all impact information privacy research without a single area being neglected. According to [18], information privacy has captivated corporate attention. The rise of almost instantaneous collection, analysis, use and sharing of data has encouraged policymakers, privacy experts, business and regulators to search for novel approaches to securing and governing the data [19].

Thus, by analyzing the above views, information privacy protection elements, can be placed in the broad categories of governance, managerial, legal, technological aspects, compliance, risk management, information security, and business processes and organizational issues, as depicted in Figure 1.

Governance is examined in the context of corporate governance (E1) because the best-known use of governance is at the corporate level [20].

Corporate privacy policies, management and practices of organizations, social issues which could be interpreted as collaboration between people and the behavior of individuals which could, in turn, be interpreted as organizational culture are collectively grouped under the broad term of business processes and organizational issues (E8).

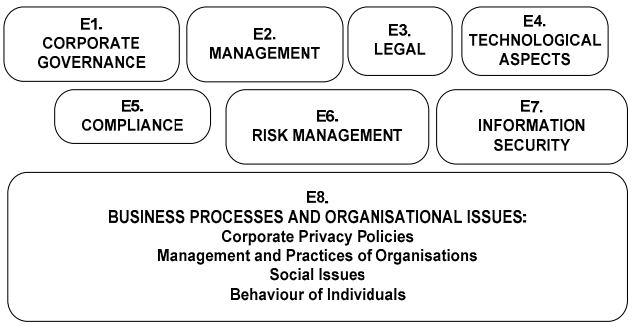

Fig 1: Information privacy protection elements

The following section expands upon the information privacy protection elements identified in Figure 1 by providing a general overview of the specific element as well as its relationship to information privacy.

III. Discussion Of Information Privacy Protection Elements

A. Corporate Governance (E1)

According to [21], the responsibility on organizations to implement good corporate governance places an obligation on directors to ensure that data protection measures are in place, failing in which can lead to imprisonment. In the past data protection would rarely feature on the agenda of board meetings but now data protection is seen as requiring end-to-end compliance throughout an organization and has climbed up the agenda [22].

Reference [23], defines a governance structure as a system of management tools and structures that assist to "steer" and identify how the organization operates through rules of engagement. South African organizations must align operations and governance with the principles set by the King III code of corporate governance [24] which, although non-legislative, is the country's official code of governance best practices [25]. The King III report on corporate governance [26] expands on the principles of the King III code of corporate governance.

With specific regard to personal information, there is a need to heed to the provisions of King III. Chapter 5 of the King III code of corporate governance deals with the governance of IT based on seven principles [24]. Specifically, principle 5.6 states that the board should ensure that information assets are managed effectively [24]. Recommended practice 5.6.1 of the King III code of corporate governance elaborates on principle 5.6 by stating that the board should ensure there are systems in place for the management of information, which should include information security, information management and information privacy [24]. Recommended practice 5.6.2, states "The board should ensure that all personal information is treated by the company as an important business asset and is identified" [24]. Thus the treatment of personal information is considered a corporate governance imperative.

The next section discusses the second information privacy protection element, management (E2).

B. Management (E2)

In order to operate a business, it is necessary to have both good governance and management [27]. Reference [27],

highlight the difference between governance and management by asserting that governance is about who makes the decisions whereas management has to do with making and implementing the decisions. Thus, management is required to implement the decisions regarding information privacy as stipulated by the board. The role of management regarding information privacy protection is discussed in the ensuing sections. This is because the King III code of corporate governance covers all of the information privacy protection elements as outlined in Figure 1 [24]. Therefore, the outstanding information privacy protection elements are examined in relation to corporate governance and management as a preliminary build-up to the conceptual framework for integrated information privacy protection that is discussed in Section IV.

The next section provides an overview of the legal aspects (E3) of information privacy protection.

C. Legal aspects (E3)

According to the Business Dictionary [28], privacy law is defined as a "regulation or statute that protects a person's right to be left alone, and governs collection, storage, and release of his or her financial, medical, and other personal information". In South Africa, the regulation for the protection of personal information is the Protection of Personal Information (POPI) Act [29].

According to the King III code of corporate governance, good governance does not exist in isolation from the law, and it is not appropriate to separate governance from legislation [24]. The King III report states that personal information should be processed according to applicable laws [26]. The applicable law in this instance is the POPI Act. This implies that the protection of personal information is a corporate governance imperative.

The next section provides an overview of the fourth element of information privacy protection, namely technological aspects (E4).

D. Technological aspects (E4)

Technology has become a huge business enabler placing enormous pressure on the board for ensuring that their organization's technology resources are adequate to carry out the organization's business activities [30]. Organizations need to consider a legion of privacy protection tools including Privacy Enhancing Technologies (PETs), encryption, steganography, Platform for Privacy Preferences (P3P), access control systems, privacy seals for Web sites, blind signatures, biometrics, firewalls, pseudonyms and anonymous systems, trusted sender stamps, Enterprise Privacy Authorization Language (EPAL), anti-spam tools and pop-up blockers [31, 32].

According to the King III code of corporate governance, the pervasiveness of IT requires the governance of IT as an important corporate initiative [24]. IT governance is about the policies and procedures that prescribe how an organization will direct and control the effective and efficient use of its technology resources to accomplish the realization of business goals [30, 33]. The King III code of corporate governance has an entire chapter (Chapter 5) dedicated to IT governance [24]. Specifically, principle 5.1, states that the board should be responsible for IT governance while principle 5.3 states that management should be responsible for the implementation of an IT governance framework [24]. This indicates that IT governance is an important corporate governance and management imperative.

The next section provides an overview of the compliance element (E5) of information privacy protection.

E. Compliance (E5)

Compliance (E5), encompasses adherence with legislation as well as the organizations' internal policies, which may be based on best practices [34]. Principle 6.1 of the King III code of corporate governance states that the board should ensure that the company complies with applicable laws and considers adherence to nonbinding rules, codes and standards [24]. Furthermore, the board should task management with the implementation of an effective compliance framework and processes (principle 6.4) [24]. In the context of this study, the applicable legislation is that of privacy law since the context of this study is on information privacy protection. This indicates that compliance with the law (E3) is an important corporate governance and management imperative.

The next section provides an overview of the risk management element (E6) of information privacy protection.

F. Risk Management (E6)

Information privacy risk is the collective term to describe risks that lead to breaches of information privacy [35]. For the effective management of these risks, Privacy Risk Management (PRM) endeavors to eliminate risks before a breach rendering this approach preventative in nature [36].

The use of an efficient, logical, easy to comprehend risk management framework is an innate part of a successful risk management process in organizations [37]. Principle 4.1 of the King III code of corporate governance states that the board should be held accountable for the governance of risk and should empower management with the responsibility of designing, implementing and monitoring the risk management plan (principle 4.4) [24]. This indicates that risk management is an important corporate governance and management imperative.

The next section provides an overview of the information security element (E7) of information privacy protection.

G. Information Security (E7)

Information security is a discipline that ensures the confidentiality, integrity and availability (CIA) of electronic assets and is an important facet in the strategic management of a company [38].

Privacy and security emanated as distinct problems in the computer field in the 1960's [39]. Reference [40] cites [41] as stating that privacy refers to a set of legal requirements and good practices regarding the handling of personal information whereas security refers to the technical aspects ensuring that the legal requirements and good practices with respect to privacy will be met. The privacy of information as well as the security of information systems is a focal point of concern for both the research community and the public and attempts to deal with these issues separately have produced inconsistent and weak results[42].

Information security within organizations is implemented by creating and maintaining an effective Information Security Management System (ISMS) [43]. Reference [44], defines an ISMS as an information assurance framework specifically to

manage information security based on a structured business risk approach, and to establish, implement, operate, monitor, review, maintain and improve information security.

The ISO 27001 standard is an example of a "specification for an Information Security Management System (ISMS)" [45]. The codified requirements in ISO 27001 are elaborated and explained in ISO 27002 and requirements for data security and data protection are cited in this standard [46]. This links to principle 6.1 of the King III code of corporate governance [24] which states that the board should comply with standards as discussed in section E.

The King III code of corporate governance in recommended practice 5.6.3 states that the board should ensure that an ISMS is developed and implemented [24]. The King III report on corporate governance states that IT management is responsible for the implementation of the ISMS [26]. The ISMS includes the confidentiality of information, the integrity of information and the availability of information and information systems in a timely manner [26]. Thus, information security implementation is a corporate governance and management imperative.

The following section focuses on a discussion of business processes and organizational issues (E8), the final element of information privacy protection.

H. Business processes and organisational issues (E8)

In relation to information privacy, a privacy governance program must be built around people, policies, processes and awareness and training [32]. Policies must be developed to detail how data must be stored, accessed, manipulated, processed, managed, transferred and deleted [47, 48]. A data privacy policy details senior management's willingness to safeguarding personal information and complying with legislation [31].

Implementing a privacy training and awareness program for the board and management fosters a sense of privacy culture that will permeate the entire organization. Principle 6.2 of the King III report on corporate governance states that both the board and each director must have an understanding of the effect of applicable laws as well as codes and standards of the organization [26]. Recommended practice 6.2.1 of the King III code of corporate governance states, that the induction and training programs of directors should involve an overview as well as changes to laws, rules, codes and standards [24]. Thus, business processes and organizational issues are corporate governance and management imperatives.

The next section provides an overview on how the various information privacy protection elements (E1 – E8) discussed in sections A - H above are integrated within an GRC frame of reference with a view of creating a conceptual framework for integrated information privacy protection.

IV. A CONCEPTUAL FRAMEWORK FOR INTEGRATED INFORMATION PRIVACY PROTECTION

For the purpose of this paper, the frame of reference and definition as espoused by [6] are used as both these items may be used when approaching the topic of GRC in a structured, scientific manner. Comprehensively, "GRC is an integrated, holistic approach to organization-wide governance, risk and compliance ensuring that an organization acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people thereby improving efficiency and effectiveness" [6]. Reference [6] incorporated the above definition into a high-level frame of reference indicating the key items that should be addressed when researching the integrated concept of GRC.

According to the GRC frame of reference proposed by [6], governance, risk management and compliance are the core subjects of GRC. Each of these subjects consists of the four basic components of GRC, namely; strategy, processes, technology and people. The organization's risk appetite, internal policies and external regulations comprise the rules of GRC. Figure 2 depicts the conceptual framework for integrated information privacy protection within [6]'s frame of reference. This conceptual framework is derived by embedding the information privacy protection elements (E1 – E8) within the GRC frame of reference.

The information privacy protection elements (E1 – E8) are adapted to subjects, components and rules according to [6]'s frame of reference. S1, S2, and S3 depict the overarching subjects of corporate governance and management, risk management and compliance respectively. The information privacy protection elements of corporate governance (E1), management (E2), compliance (E5) and risk management (E6) are now subjects S1, S2 and S3 according to [6]'s frame of reference. Corporate governance and management are collectively grouped under the subject S1 as management is contingent on corporate governance as explained by [49]. Reference [49] states that corporate governance regulations require the board to exercise due diligence in their roles of establishing a strategy and ensuring that management implements this strategy.

Table I depicts the mapping of the information privacy elements depicted in figure 1 to the core subjects of [6]'s GRC frame of reference.

TABLE I: MAPPING OF INFORMATION PRIVACY PROTECTION ELEMENTS TO CORE SUBJECTS OF [6]'S FRAME OF REFERENCE

Information privacy protection elements		**Subjects**
Corporate Governance (E1)	→	Corporate governance and Management (S1)
Management (E2)		
Compliance (E5)	→	Compliance (S3)
Risk Management (E6)	→	Risk Management (S2)

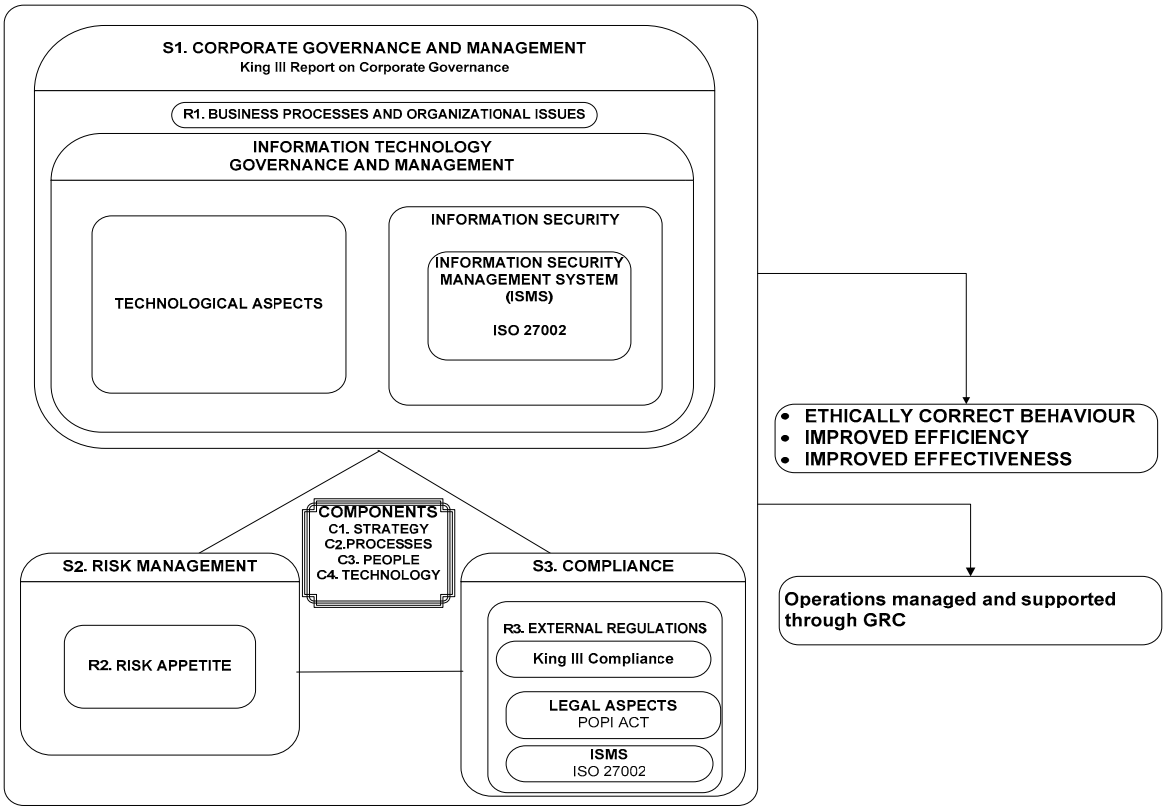

Fig 2: Conceptual framework for integrated information privacy protection

S1 incorporates two information privacy protection elements. The first information privacy protection element is technological aspects as discussed in section D. This element is enveloped within an IT governance and management framework because the pervasiveness of IT requires the governance of IT, the responsibility of which rests with the board and the implementation thereof to management as discussed in section D. IT governance responsibilities are an aspect of a larger framework of enterprise governance responsibilities ensuring that IT is aligned with business goals and delivers value through investments in IT [50, 51]. Figure 2 depicts this with IT governance and management being a subset of corporate governance and management.

The second information privacy protection element incorporated by subject S1 is information security as discussed in section G. The board must ensure that an ISMS is developed in order to implement information security within the organization and IT management should be delegated the task of implementing the ISMS as discussed in section G and depicted in Figure 2.

The rule (R1) for corporate governance and management is the organization's internal policies regarding information privacy protection. This means that the information privacy protection element business processes and organizational issues (E8) now becomes rule (R1) according to [6]'s frame of reference for integrating GRC. Both the board and management are responsible for the organization's business processes as discussed in section H.

The risk subject (S2), and compliance subject (S3), must be governed by the board and implemented by management as discussed in sections E and F. Figure 2 represents this with the link between corporate governance and management to risk and compliance. The rule for risk management according to [6]'s frame of reference is the organization's risk appetite (R2). The rule (R3) for compliance, deals with external regulations, such as, adherence with the King III code on corporate governance, privacy law (legal aspects of information privacy protection as discussed in section C) and the ISO 27002 code of practice for information security management as discussed in section G. There are also standards for risk management and IT governance which have not been discussed in this paper as only a few illustrative compliance examples are provided.

Compliance also refers to adherence to the organization's internal policies which includes the information privacy policy grouped under business processes and organizational issues (R1). The link between risk management and compliance is required because risk management and compliance work in tandem to enable governance as well-designed compliance programs improve accountability [52].

The subset of IT governance is intertwined with risk and compliance. Figure 2 illustrates this with corporate governance and management as well as the subset of IT governance and management linked to risk management and compliance. This is because an IT governance framework should not exist in solitude from either the corporate governance model or the Enterprise Risk Management (ERM) model or even from the

company's compliance culture [33]. Furthermore, IT governance must not only be constructed on the basis of legislation but on the principles of law, accepted security practices, risk management, audit standards and regulatory compliance and on common sense [53]. Therefore, IT governance is linked to both risk management and compliance.

Furthermore, privacy law and information privacy have always been linked to technological development [54]. Therefore, organizations need to consider a legion of privacy protection tools in order to prepare their technology environment to be compliant with data privacy legislation [31]. There is therefore a link between IT governance and compliance.

Each of the subjects, governance, risk management and compliance consists of four basic components of GRC, namely; strategy (C1), processes (C2), people (C3) and technology (C4) as depicted in Figure 2. The subjects, rules and components are consolidated in an assimilated, complete organization-wide manner aligned with the business operations and are embedded within a GRC frame of reference.

Reference [6] asserts that this approach will promote ethically correct behaviour and improved efficiency and effectiveness. The King III code of corporate governance emphasizes ethical leadership and corporate citizenship [24]. Principle 1.1 states that the board should provide sound leadership based on an ethical foundation and Principle 1.3 states that the board should make sure that the companies ethics are managed effectively.

V. Conclusion And Future Research

This paper focused on the development of a conceptual framework for integrated information privacy protection. By using this framework, an organization can proactively plan for information privacy protection and ensure accountability. Accountability relative to privacy is the ownership for personal information protection [55]. An accountable organization, according to [55] must have in place "appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws".

The conceptual framework can assist organizations to maximize performance within acceptable levels of risk and within defined precincts of internal and external compliance. However, unification of GRC is a difficult task having compatibility challenges in people, process and technology [56]. Future research will entail addressing these challenges so that organizations can have a GRC system that people will adapt to by changing the mindset of people, a well-defined process that organizations can use as a guideline for GRC and a technological solution to simplify the process as organizations have to contend to a legion of frameworks, regulations and standards.

References

[1] R. O. Mason, "Four ethical issues of the information age," *Mis Quarterly,* vol. 10, pp. 5-12, 1986.

[2] F. Bélanger and R. E. Crossler, "Privacy in the digital age: a review of information privacy research in information systems," *MIS Quarterly,* vol. 35, pp. 1017-1042, 2011.

[3] H. J. Smith*, et al.*, "Information privacy research: An interdisciplinary review," *MIS quarterly,* vol. 35, pp. 989-1016, 2011.

[4] J. Castro Edwards, "Data protection: Where are we now," *The Journal of Database Marketing & Customer Strategy Management,* vol. 15, pp. 285-292, 2008.

[5] J. Kim, "Privacy GRC taking off?," in *FierceCFO*, R. Bartley, Ed., ed, 2010.

[6] N. Racz*, et al.*, "A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC)," 2010, pp. 106-117.

[7] S. Anand, "Technology and the integration of governance, risk management and compliance," *Financial Executive,* vol. 26, pp. 57-59, 2010.

[8] Y. Delmar, "Privacy and GRC – What the New Ponemon Study and the GAPP is Telling Us," in *InFocus Global Services Blog* vol. 2011, ed, 2011.

[9] M. B. Miles and A. M. Huberman, *Qualitative data analysis: An expanded sourcebook*: Sage, 1994.

[10] S. C. Henderson and C. A. Snyder, "Personal information privacy: implications for MIS managers," *Information & Management,* vol. 36, pp. 213-220, 1999.

[11] R. Clarke. (2013, 11th June). *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. Available: http://www.rogerclarke.com/DV/Intro.html

[12] K. Gillon*, et al.*, "Information Security and Privacy—Rethinking Governance Models," *Communications of the Association for Information Systems,* vol. 28, p. 33, 2011.

[13] C. D. Raab, "The Governance of Global Issues: Protecting Privacy in Personal Information," in *New Modes of Governance in the Global System*, ed: Springer, 2006, pp. 125-153.

[14] (2011, 19th July). *Privacy and GRC: What the New Ponemon Study and the GAPP is Telling us*. Available: http://infocus.emc.com/yo_delmar/rivacy-and-grc-%E2%80%93-what-the-new-ponemon-study-and-the-gapp-is-telling-us/

[15] A. Cavoukian, "Privacy and Government 2.0: The Implications of an Open World," Information and Privacy Commissioner of Ontario2009.

[16] W. H. Friedman, "Privacy - Dangers and Protection," in *Information security and ethics: concepts, methodologies, tools and applications*, H. Nemati, Ed., ed United States of America: Information Science Reference-Imprint of: IGI Publishing, 2008.

[17] K. Reddy and H. S. Venter, "Information Privacy in Two Dimensions - Towards a Classification Scheme for Information Privacy Research," presented at the 2010 IEEE Second International Conference on Social Computing, Minneapolis, Minnesota, USA, 2010.

[18] D. Liginlal*, et al.*, "How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management," *Computers & Security,* vol. 28, pp. 215-228, 2009.

[19] P. J. Bruening and K. K. Waterman, "Data Tagging for New Information Governance Models," *IEEE Security & Privacy,* pp. 64-68, 2010.

[20] M. N. Kooper*, et al.*, "On the governance of information: Introducing a new concept of governance to support the management of information," *International Journal of Information Management,* vol. 31, pp. 195-200, 2011.

[21] R. Rowlingson, "Marrying privacy law to information security," *Computer Fraud & Security,* vol. 2006, pp. 4-6, 2006.

[22] H. Grant, "Data protection 1998–2008," *Computer Law & Security Review,* vol. 25, pp. 44-50, 2009.

[23] S. Kavanagh and M. Suppert, "We're All in IT Together: Aligning Technology with Business through IT Governance," *GOVERNMENT FINANCE REVIEW,* vol. 23, p. 24, 2007.

[24] "King Code of Governance for South Africa," Institute of Directors Southern Africa, Johannesburg2009.

[25] L. Engelbrecht, "Implementing King III : Aligned to the Issues and Principles: Corporate Governance," *Enterprise Risk,* vol. 4, p. 30, 2010.

[26] "The King Report on Corporate Governance for South Africa," Institute of Directors of Southern Africa2009.

[27] P. Weill and J. W. Ross, *IT governance: How top performers manage IT decision rights for superior results*: Harvard Business Press, 2004.

[28] in *Business Dictionary*, ed, 2011.

[29] "Act No. 4 of 2013: Protection of Personal Information Act, 2013," vol. No. 37067, ed. South Africa, 2013, pp. 1-75.

[30] S. Posthumusa and R. Von Solms, "IT Oversight: an Important Function of Corporate Governance," *Computer Fraud & Security,* vol. 2005, pp. 11-17, 2005.

[31] G. Vrhovec, "Beating the privacy challenge," *Computer Fraud & Security,* vol. 2011, pp. 5-8, 2011.

[32] R. Herold, "Building an Effective Privacy Program," *Information Systems Security,* vol. 15, pp. 24-35, 2006/07/01 2006.

[33] N. Robinson, "IT Excellence Starts with Governance," *Journal of investment compliance,* vol. 6, pp. 45-49, 2005.

[34] J. Salido, "A Guide to Data Governance for Privacy, Confidentiality, and Compliance," 2010.

[35] K. Reddy and H. Venter, "Using Object-Oriented Concepts to Develop a Conceptual Model for the Management of Information Privacy Risk in Large Organisations," in *Research-in-Progress track (non-peer-reviewed) of Information Security South Africa Conference, Johannesburg, South Africa*, 2008.

[36] A. Cavoukian. (2010, Privacy Risk Management. 1-22. Available: http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf

[37] A. D. Cardenas Davalos and W. Chia Chin Hui, "How is risk assessment performed in international technology projects," Umeå University, 2010.

[38] B. Von Solms, "Corporate Governance and Information Security," *Computers & Security,* vol. 20, pp. 215-218, 2001.

[39] R. Turn and W. H. Ware, "Privacy and security issues in information systems," *IEEE Transactions on Computers,* pp. 1353-1361, 1976.

[40] L. V. Casaló*, et al.*, "The Role of Security, Privacy, Usability and Reputation in the Development of Online Banking," *Online Information Review,* vol. 31, pp. 583-603, 2007.

[41] L. V. Casaló*, et al.*, "Trust: Key Concept in the Development of Virtual Communities," in *Encyclopedia of Networked and Virtual Organizations*, G. D. Putnick and M. M. Cunha, Eds., ed: Idea Group Reference, 2006.

[42] P. Dourish and K. Anderson, "Collective Information Practice: Emploring Privacy and Security as Social and Cultural Phenomena," *Human-computer interaction,* vol. 21, pp. 319-342, 2006.

[43] A. Bialas, "Information Security Systems vs. Critical Information Infrastructure Protection Systems-Similarities and Differences," 2006, pp. 60-67.

[44] B. G. Raggad, *Information Secrity Management: Concepts and Practice*. United States of America: CRC Press, 2010.

[45] W. Al-Ahmad and B. Mohammad, "Addressing information security risks by adopting standards," *International Journal of Information Security Science,* vol. 2, pp. 28-43, 2013.

[46] G. Disterer, "Iso/iec 27000, 27001 and 27002 for information security management," 2013.

[47] J. H. P. Eloff and M. Eloff, "Information Security Management: A New Paradigm," 2003, pp. 130-136.

[48] M. C. Mont*, et al.*, "Privacy Enforcement for IT Governance in Enterprises: Doing it for Real," *Trust, Privacy and Security in Digital Business,* pp. 226-235, 2005.

[49] I. Chalaris*, et al.*, "IT Governance: The Safe Way to Effective and Efficient Governance," *E-Journal of Science and Technology,* vol. 1, pp. 59-63, 2005.

[50] G. Hardy, "Using IT Governance and COBIT to Deliver Value with IT and Respond to Legal, Regulatory and Compliance Challenges," *Information security technical report,* vol. 11, pp. 55-61, 2006.

[51] S. Posthumusa*, et al.*, "The Board and IT Governance: The what, who and how," *South African Journal of Business Management,* vol. 41, pp. 23-32, 2010.

[52] S. Davis and J. Lukomnik, "Enabling Good Governance," *Internal Auditor,* pp. 28-29, 2010.

[53] M. Ulsch and J. Bamberger, "Sound IT Governance Requires Breadth & Depth," *Financial Executive,* vol. 22, p. 54, 2006.

[54] O. Tene, "Privacy: The New Generations," *International Data Privacy Law,* vol. 1, p. 15, 2011.

[55] O. o. t. P. C. o. C. (OPC) and O. o. t. I. a. P. C. O. o. A. a. B. Columbia. (2012, 11th June). *Getting Accountability Right with a Privacy Management Program*. Available: https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

[56] R. Uppaladinni and V. Chhawchharia, "Towards Assuring Enterprise-Wide Compliance," *GRC Worries? Why, when IT can Help?,* vol. 6, pp. 47-52, 2008.