A Context Adaptive Framework for IT Governance, Risk, Compliance and Security

Shree Govindji, Gabrielle Peko(✉), and David Sundaram

Department of Information Systems and Operations Management,
University of Auckland, Auckland 1142, New Zealand
bgovl53@aucklanduni.ac.nz,
{g.peko,d.sundaram}@auckland.ac.nz

Abstract. The technological solutions offered today evolve at a rapid pace, as this happens, risk management and security practices are becoming more relevant and in fact, now a necessity for most growing organisation. Governance, Risk management and compliance (GRC) are established and well-adhered functions in a business which have individually always been very important in business management. As individual topics, the application of all concepts have been fundamental for businesses in order to manage risks. However, over the years, the term GRC was developed and applied to describe the integration between the various areas due to the reason that a monolithic approach between the functions was no longer feasible in successful management of business risk. However IT GRC has been dealt with an isolated manner from IT Security. In this paper we explore IT GRC and Security and propose an integrated context adaptive framework that addresses the problems of monolithic approaches.

Keywords: Governance · Risk management · Compliance
Information technology · Security · Context adaptive

1 Introduction

According to De Smet and Mayer [2], the main challenge of GRC is to have an approach which is as integrated as possible. Integrated GRC was developed to manage the increasing business complexity due to new legal requirements enforced as a result of various financial scandals and business failures. Racz [3] proposed the first scientific definition to the term stating that "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". This definition however, does not consider the security aspect of GRC and so we will consider other suitable definitions too as security is an important aspect of GRC, but it has failed to be mentioned by most researchers exploring GRC topics and concepts. A GRC approach does assist organisations in their approach for IT security and IT Security can benefit from an integrated GRC view [4]. Security vulnerabilities have risks which must be constantly monitored and evaluated in order to reduce the opportunity of a breach [1]. Managing the security

P. Cong Vinh et al. (Eds.): ICCASA 2017/ICTCC 2017, LNICST 217, pp. 14–24, 2018.
https://doi.org/10.1007/978-3-319-77818-1_2

architecture is important in managing a global risk and compliance platform, IBM acknowledges this and provides their own solutions to GRC which considers the security aspect and also fills the gap missed by most researchers. Many other consulting companies have also proposed similar solutions, identifying that there is indeed a strong, inseparable link between GRC and security capabilities. Vicente and Da Silva [5] have identified the young age of scientific research around GRC. In more recent studies, Racz [6] has also mentioned that there is a lack of a scientifically grounded definition, stating that most GRC related definitions are published by software vendors and consultants and are suited to their products and services. During the time of this writing, Racz [3, 6] claim is supported by the research contributed by De Smet and Mayer [2] who have identified that more research is still needed to define the integration between various terms.

In the next section we define the significant terms in GRC and security before discussing IT GRC in Sect. 3 and IT security in Sect. 4. Section 5 introduces the integration between IT GRC and IT security. Then, in Sect. 6, an Integrated IT GRC Security (GRCS) framework synthesizing ideas, theories, and models from these two concepts is presented. The paper concludes in Sect. 7.

2 GRC and Security

In order to better understand the integration between GRC, we need to first define each individual term and so the following provides a brief definition of governance, risk management and compliance.

Governance/Corporate Governance: Defined as a set of processes, policies and laws affecting the way an enterprise or corporation is directed or controlled. Corporate governance principles which are well defined and enforced provide a structure that suits all stakeholders concerned, ensuring the company follows regulations, ethical standards and best practices [7]. It deals with internal and external aspects of an organization [8]. The past failure of many large organisations has prompted policy makers to initiate legislative reforms which require disclosure and reporting of organisational risks. The Sarbanes-Oxley Act, for example, was the government's response to the Enron scandal, the large US energy company which collapsed due to a reduced perception of debt and risk and overstatement of revenues as a result of undisclosed ownership structures [9].

Risk Management: An enterprise wide risk management approach supports corporate governance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) provide a suitable definition for enterprise wide risk management which is widely accepted, defining ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and mange risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives" [10].

Compliance: According to Fowler-Rians [11], regulatory compliance is achieved through meeting expected behaviors in processes and practices. It refers to adherence to

established guidelines, internal policies, regulations or legislative obligations by an organization. i.e. company compliance with the Sarbanes-Oxley legislation and a growing body of other regulations and laws.

Integration of GRC: As the number of legislative rules and regulations increase, organisations have to deal with increased risks. These concerns lead companies to approach governance, risk management and compliance functions in a separate manner [8]. Growth in each specific area led to cost concerns which initiated an integrated governance, risk and compliance approach that would look across an organisations risk and control functions holistically and seek to improve both organisational efficiency and effectiveness of risk and control functions [12]. According to Rasmussen [13], an integrated enterprise view of risk and compliance means accountability is effectively managed and businesses have a complete system of record which subsequently provides visibility across multiple risk and compliance issues. This also introduces a sustainable view for business procedures as the increasing business risks and threats can be minimized with a holistic and integrated approach on GRC issues. Rasmussen [13] also mentions how a siloed GRC approach means there is less framework for managing risk and compliance as integrated business functions, this in turn leads to poor visibility across the organisation. Other outcomes of an unintegrated GRC approach includes: wasted resources and spending, poor visibility across the enterprise, overwhelming complexity, lack of business agility, greater exposure and vulnerability [13]. Recor and Hu [7] also mention that leveraged integration through the improvement of GRC processes can guide organisations to reach their overall objectives by ensuring that there is connectivity between risks, strategy and performance.

GRC and Security: In today's dynamics, the demand for accountability, regulatory compliance and security are increasing as these are mandatory areas of business which need to be covered, this leads to GRC of information security becoming a high priority goal [14]. Asnar and Massacci [14] have also identified that a process to govern security is missing at an organisational level. In their research [14], have developed on the link between GRC and information security, describing the importance of a GRC management process for information security. However, whilst there is a strong relationship between GRC and security, it is suitable to say that there is otherwise a lack of research in terms of the integration between the two topics. In contrast, there are a wide variety of organisational and industry articles mentioning the importance of integration between GRC and security. For example Rashid [15] has mentioned that GRC programs allow security professionals to gain visibility into organisational risks. Security professionals often work very closely with risk managers and both the risk and security functions interlink. Risk managers who look after GRC initiatives may be misinformed when they aren't fully briefed about information security, leading to conflicting situations [16].

AMR Research [17] shows that security purposes were fourth in reasons for companies investing in GRC solutions, this is a clear example of how GRC closely initiates with security and there is an opportunity to cover this gap in research literature. While there is a lack of research linking GRC and security together, it is easy to see how information security is involved in each aspect of the GRC components. Governance needs to be incorporated into the organizations IT security frameworks in order to ensure the effectiveness of information security governance [18].

3 IT GRC

According to Racz et al. [9], IT GRC is the term used for when GRC activities are restricted for IT operations. Risks and controls are interconnected with IT activities, resulting in a number of benefits for the organisation. The GRC integration process is streamlined through the use of technology, and IT can be a driver or enabler of integration among governance, risk management and compliance [16]. IT GRC has expanded throughout the years as technology replaces more and more manual processes. [3], found that at the time of writing their research piece, there was a lack of research on integrated approaches to IT GRC. More recent studies, however, still support the fact that there is a lack of attention on IT GRC, especially from the scientific community [2]. It is also mentioned that the link between IT governance and risk management is neglected [2].

The main reason for implementing IT GRC strategies was historically due to increasing regulatory pressure and a drive to lower the costs which were originally gained from the siloed approach [7]. Success in today's business environment requires that organisations integrate, build and support business processes which are built on a common technology backbone [13]. Information technology can streamline the GRC integration process, making it more cost effective [16]. Properly aligning IT with business strategies can enable technology to be used for value creation and competitive advantage. An IT GRC program also contributes further to each component in GRC. According to Linkous [19], an integrated IT GRC program provides value to the compliance processes and can improve the information assurance efforts. Each component of IT GRC is interrelated to each other, and therefore an IT GRC program is more effective rather than implementing just one or two of the components. For example, the attention on IT governance is captured through enforcing compliance measures. IT Governance also governs IT RM and IT Compliance activities. Through a critical analysis on prior research, Racz [3] found that none of the chosen models claiming to integrate GRC had fully covered all aspects, on top of that, none of the models elaborated on IT GRC specifically. After identifying this gap, Racz [3] proposed a detailed scientific model for integrating IT governance, risk and compliance management.

Through this research it is identified that there is a lack of research articles with an IT GRC focus within specifically the banking sector. This identifies that there is an opportunity to contribute in this area, and also contribute to IT GRC applications in various other industry-specific areas.

4 IT Security

With the adoption of IT security being a mandatory task for most, if not all, organisations in today's environment, experts are finding it increasingly difficult to apply holistic measures across different domains. Adopting a risk management perspective is not enough to completely eliminate the security risk, hence the reason we are not integrating security within GRC, but rather taking a separate approach to consider security on its own. Very often, there is insufficient knowledge about the security

domain, threats, countermeasures and company infrastructure, leading to wrong decision making [20]. Ekelhart et al. [20] identify that the main reasons for this happening is due to the vaguely defined security terminology and because managers who make decisions are often not understanding the complexity of underlying IT infrastructure [20]. Damianides [21] also identifies how there is little consideration given to organisational requirements and priorities and in the past, information security would be dealt as a solely technological issue. Damianides recommends that information security should be addressed in all phases of a project. According to Grob et al. [22], Information security management (ISM) is focused on organisations information systems operating at a faultless service level. Traditionally, ISM focuses on the consideration of technical systems, such systems can cause operational business risks and therefore these IT related risks must be identified and adequate countermeasures must be defined. Analyzing threats within the scope of ISM is occasionally defined as risk management [22]. Grob et al. [22] have also identified that there needs to be a functional alignment between operational risk management (ORM) and ISM as ISM has more of a system-based focus and therefore can capture possible threats better, whereas ORM focuses more on the overall amount of damage impacting business processes. The perception of risks in an organisation is influenced by the lack of security culture and training. Grob et al. [22] have depicted the misalignment between ORM and ISM.

The human element which challenges information security involves a number of aspects. Firstly, security risks not only need to be effectively communicated to stakeholders but also require a mutual understanding between the stakeholders. Human errors also threaten best security practices. Human errors are defined by Kraemer and Carayon [23], as non-deliberate accidental cause of poor computer and information security. Kraemer and Carayon [23] have also identified the main factors which causes errors in information security, these errors can be traced back to poor communication, security culture and security policy, including a number of other issues which the authors have identified through their study. Humans are the cause for many information security breaches, and decision makers can make decisions which contribute to risk and impact an organisations response to threats. In fact, the biggest IT security risk is the human element [2] and many prior events such as the Enron and WorldCom scandals reaffirmed this.

The organisational element refers to factors such as organisational size, top management support and type of industry which has an influence on how effective information security controls are within organisations [24]. Other factors such as uncertainty of environmental elements, rapid change of technology, competitors' behaviours and customers' security requirements, and changes in legislation also have an impact on the way security is managed in an organisation [24]. Top management support has been identified as an important factor which is critical for implementing security controls within organisations [25]. Werlinger et al. [26] have identified through their own research how a lack of security culture in an organisation makes it difficult to change existing security practices.

The technological complexities are another challenge which contribute to not being able to maximize full security efforts. Testing security systems are a costly, lengthy and a complex process which is why many organisations have difficulty in this area. Werlinger et al. [26], have identified that network and system complexity is challenging

for organisations who are even wanting to implement security controls. Other IT complexities involve decentralization of IT management, mobility and distribution of user access, security updates and consistent installation and a lack of support for using security tools [26] which all contribute to the complexity of IT security related changes.

Regardless of all the available frameworks, many organisations are struggling with implementing IT security measures for two reasons: (1) they may not have a comprehensive security strategy, (2) their security strategy isn't updated to reflect changes in their business, cyber security practices and IT platforms [1]. The resulting threat to IT security includes a costly security breach.

5 IT GRC and IT Security

Executive boards and management have a number of fundamental responsibilities associated with information security governance, including understanding why information security need to be governed, and ensuring it fits in the IT governance framework [21]. IT GRC is similar to GRC in the sense that it has been identified that there is minimal research articles conducted on the integration of IT GRC and IT security. However, when looking at articles outside of the research field, we are able to identify that there is in fact integration between IT GRC and security in the current business world. According to PwC (2017), IT GRC is defined as "Combining disciplines for better enterprise security. Adopting a unified IT governance, risk management and compliance (IT GRC) approach, and managing the associated activities coherently will create efficiencies, provide a holistic view of the IT environment and ensure accountability". An IT GRC program links with security in a number of ways and in order to support effective communications, the IT GRC program should provide the ability to allow different categories of users to view risk and compliance data in their own relevant ways, these users may range from IT operations, risk managers, auditors and even security operations [19]. While security is a distinct function, it is still very much interrelated with risk-related functions and so it is important to consider security as a distinct part of IT GRC functions too.

IT Governance and IT Security: IT governance and information security are linked through the development of information security governance practices. According to Da Veiga and Eloff [27], Information security governance can be defined as the overall manner in which information security is deployed to mitigate risks. The concept arises when it was found that communication of the information security culture and control frameworks is the responsibility of company executives. Da Veiga and Eloff [27] also mention that organisational risks can only be addressed when a governance framework for information security is in place. While there is a large link between the two concepts, there is a lack of research on the integration of IT governance and IT security management elements, while IT governance is viewed as a component of the wider IT management model [2]. Certain characteristics of IT governance and security governance contribute to more effective alignment and execution of IT programs. In relation to certain regulations, for example the SOX, security is no longer just an IT issue, an effective IT and security governance program is essential. Security and risk management are a key part of the IT governance framework, but more research is still needed

to guide how this integration should occur [2]. In order to meet the Sarbanes Oxley requirements, it should not be considered as just a compliance process, but also an opportunity to develop strong governance models.

IT Risk Management and IT Security: The relationship between risk and IT security is inseparable, in essence, IT security is solely performed to mitigate risks [4]. According to Parent and Reich [28], there are three primary areas which IT risk management targets: the security of data and information, the integrity of hardware and systems and IT project implementations [28]. The management of technology risk is synonymous with information security, leading to an under appreciation of both concepts. [2] Have also proposed through their research, that integrating IT risks in the decision making framework will accommodate for information security aspects. As Grob et al. [22] have identified, the IT risk analysis function within IT risk management serves as a basis for identifying and implementing measures for risk governance. Risk governance is achieved by avoiding, passing, decreasing or accepting risks and in the context of information systems, IT security experts can conduct such measures for risk governance due to their competencies [22]. A number of standards and best practices for IT security management have been established and offer extensive improvements within IT risk management efficiency [22].

IT Compliance and IT Security: IT security can be driven by IT compliance and appears with regulations which assist with data protection and privacy. Frameworks such as HIPAA, COBIT and ISO17799 help organisations establish a comprehensive approach to both privacy compliance management and information security [19]. Linkous [19] also mentioned how the SOX helped organisations adapt a holistic approach to security and privacy compliance as having SOX in effect as boards of directors began to be interested in security compliance. In essence, as the landscape for information security becomes more complex, organisations have to ensure their compliance requirements address any regulatory and non-regulatory changes. Many employees in IT security departments are acting without the knowledge of the regulatory requirements and what these require in terms of regulatory compliance, hence the reason it is important to strengthen the connection of IT security and compliance requirements [4]. In this environment, information security initiatives are faced with increasing regulatory and compliance pressures, this is leading to the development of security-specific compliance frameworks. Such actions are directing security managers into more IT GRC based activities.

6 An Integrated IT GRCS Framework

As recommended by [2], more research is still needed to define how well to integrate both security and risk management into organisations IT governance frameworks. In contrast to this however, they are many organisational resources which can be useful in identifying the link between IT GRC and security. Most organisations adopting an IT GRC program are often missing the security component, therefore addressing this

problem through the development of their own IT GRC/IT Security based solution. We can see from this that it is not possible to separate the two, and often, if not mentioned as a separate topic, IT security is already embedded into IT GRC in one way or another. Past research has already begun to demonstrate how effective compliance initiatives are linked to direct benefits with company revenue, profits and customer retention, therefore it has been predicted that a baseline for security activities will include information security moving towards mandated and standardized frameworks. Based on our findings, we propose our own framework which addresses some of the identified gaps in our research. The bottom line is that there are not enough research papers that address GRC and security given the very important and blatant link between the two, especially in the context of IT. Therefore, we firstly present a high level framework for IT GRCS in Fig. 1.

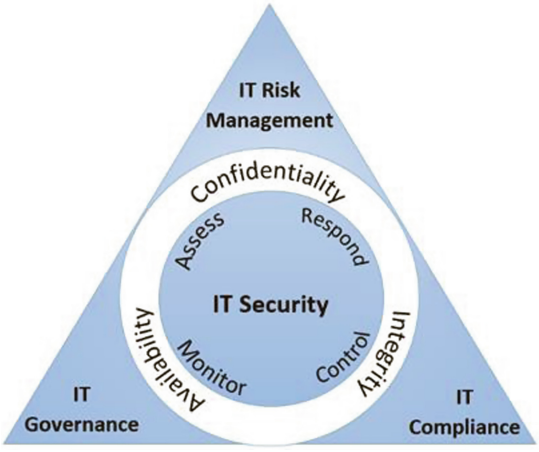

Fig. 1. Context adaptive IT GRCS framework

This framework incorporates all elements of IT GRCS into a simplified model, with IT security being in the middle as it is incorporated in each pillar for IT GRC. The CIA (confidentiality, integrity, availability) concept is a vital dimension in the model, it guides policies for IT and information security in organisations to protect all organisational assets. The process involving assess, respond, control and monitor, identified in our IT security Framework, was what we referred to when developing this model. However, we noticed that a similar process can be applied across all pillars of GRCS. These four steps helps an organisation to adapt to situation depending on context. Next we also propose a more detailed model (Fig. 2) which digs deeper into each pillar of IT GRCS and we are able to see how this framework can be applied in an organisational context. And every aspect adapts as the context changes and reacts to changes in the other elements.

Firstly, for the IT Security pillar we can see that there is an additional component which incorporates people, data, information, applications, network and infrastructure with our process model for IT security. This component has been derived from IBMs Security framework and is a good reference model as we can see that protecting IT within all these areas is vital for IT security. From the IT Security pillar, there are feedback loops to the IT GRC pillars, which shows the incorporation of IT GRCS now. The process model for IT Governance has been derived from Cobit 4.1 and has been chosen as it is both suitable and simple for our model. The process model for IT Risk Management has been derived from ISACAs Risk IT framework which includes a set of guiding principles for effective management of IT risk. It also complements COBIT

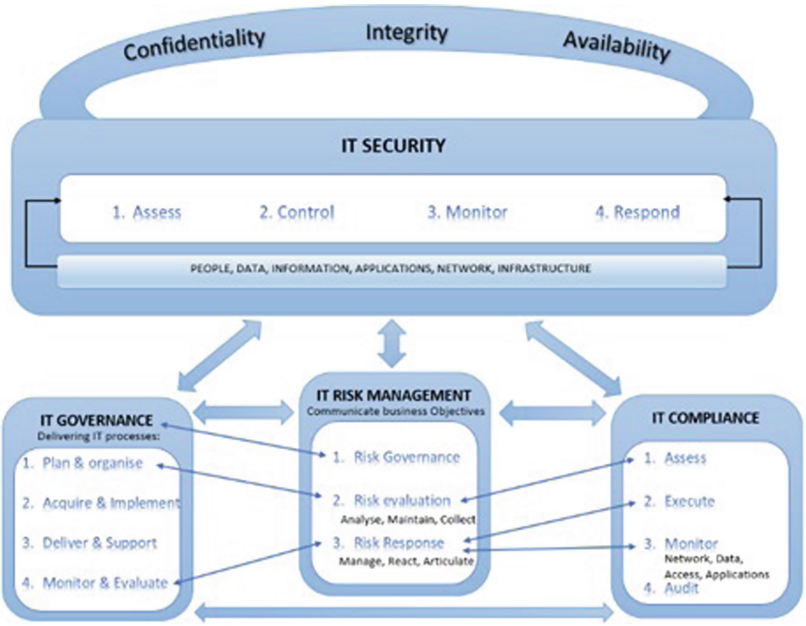

Fig. 2. Detailed IT GRCS framework

and therefore is suitable to link with our IT Governance pillar. Finally, the process model for IT Compliance is derived from a compliance process framework again by ISACA. We chose this model as it is the model suitable for IT compliance, as in our research there was a lack of frameworks and models specifically for IT compliance. We can see the link with our identified process model to IT as the monitor step refers to components from the IT security section, and also there is an audit process, which is vital for IT compliance.

7 Conclusion

In conclusion, we have identified in our research that while IT GRC has been around for a number of years now and has been an widely researched especially since the collapse of major financial organisations, there is very little literature from both academia and industry articles which propose frameworks for incorporating GRC along with IT, and especially including the IT security component. We have identified that while security is an inadmissible component in each pillar of IT GRC, it is often not mentioned – perhaps because of the assumption that it is already incorporated. Therefore we propose a framework which incorporates both IT GRC and IT Security in order to form IT GRCS. While the framework is generic, it can be applied in various sectors and there are many potential areas where further research can be done such as seeing the suitability of the framework in specific types of industries.

References

1. IBM: SAP Security and GRC Services (2015). https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SES03016USEN
2. ISACA: The Risk IT Framework – Excerpt (2009). http://www.isaca.org/knowledge-center/research/documents/risk-it-framework-excerpt_fmk_eng_0109.pdf
3. De Smet, D., Mayer, N.: Integration of IT governance and security risk management : a systematic literature review, no. 1, pp. 143–148 (2016)
4. Racz, N., Seufert, A., Weippl, E.: A process model for integrated IT governance, risk, and compliance management. In: Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010), p. 155 (2010)
5. Kuppinger, M.: IT GRC and IT Security - Where is the link? (2010). https://www.kuppingercole.com/blog/kuppinger/grc_it_security_link180210
6. Vicente, P., Da Silva, M.M.: A business viewpoint for integrated IT governance, risk and compliance. In: 2011 IEEE World Congress on Services, pp. 422–428 (2011)
7. Racz, N., Weippl, E., Seufert, A.: A frame of reference for research of integrated governance, risk and compliance (GRC). In: De Decker, B., Schaumüller-Bichl, I. (eds.) CMS 2010. LNCS, vol. 6109, pp. 106–117. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13241-4_11
8. Recor, J., Xu, H.: GRC technology introduction. In: Tian, W. (ed.) Commercial Banking Risk Management, pp. 305–331. Palgrave Macmillan US, New York (2017). https://doi.org/10.1057/978-1-137-59442-6_14
9. Racz, N., Weippl, E., Seufert, A.: Governance, risk & compliance (GRC) software – an exploratory study of software vendor and market research perspectives, pp. 1–10 (2011)
10. Smith, R.: Seven things you need to know about IT controls. SOX Committee Integration Consortium (2004). www.integrationconsortium.org
11. COSO (2004). https://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf
12. Fowler-Rians, K.: Determinants of federal regulation compliance: a study of the employee trip reduction program. Unpublished Doctoral Dissertation, University of Houston (1997)
13. Frigo, M.L., Anderson, R.J.: A strategic framework for governance, risk, and compliance. Strateg. Financ. **90**(8), 20–61 (2009)
14. Rasmussen, M.: Value of a Common Architecture for GRC Platforms Business Burdened by Varying Risk & Value of a Common, pp. 1–8 (2010)
15. Asnar, Y., Massacci, F.: A method for security governance, risk, and compliance (GRC): a goal-process approach. In: Aldini, A., Gorrieri, R. (eds.) FOSAD 2011. LNCS, vol. 6858, pp. 152–184. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23082-0_6
16. Rashid, F.: How to Leverage GRC for Security (2013). http://www.bankinfosecurity.com/how-to-leverage-grc-for-security-a-6164
17. Anand, S.: Technology and the Integration of Governance, pp. 57–59, December 2010
18. AMR Research: November 2009 GRC in 2010 : $ 29.8B in Spending Sparked by Risk, Visibility, and Efficiency (2010)
19. Linkous, J.: Put the "i" in IT compliance. Commun. News **45**(12), 26 (2008)
20. Ekelhart, A., Fenz, S., Klemen, M., Weippl, E.: Security ontologies: improving quantitative risk analysis. In: Proceedings of the Annual Hawaii International Conference on System Sciences, pp. 1–7 (2007)
21. Damianides, M.: Sarbanes-Oxley and it governance: new guidance on it control and compliance. Inf. Syst. Manag. **22**(1), 77–85 (2005)

22. Grob, H.L., Strauch, G., Buddendick, C.: Applications for IT-risk management – requirements and practical evaluation, pp. 758–764 (2008)
23. Kraemer, S., Carayon, P.: Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. Appl. Ergon. **38**, 143–154 (2007)
24. Chang, S.E., Ho, C.B.: Organizational factors to the effectiveness of implementing Information security management. Ind. Manag. Data Syst. **106**(3), 345–361 (2006)
25. Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K.: An integrative study of information systems security effectiveness. Int. J. Inf. Manag. **23**, 139–154 (2003)
26. Werlinger, R., Hawkey, K., Beznosov, K.: An integrated view of human, organizational, and technological challenges of IT security management. Inf. Manag. Comput. Secur. **17**(1), 4–19 (2009)
27. Da Veiga, A., Eloff, J.: An information security governance framework. Inf. Syst. Manag. **24** (4), 361–372 (2007)
28. Parent, M., Reich, B.: Governing information technology risk. Calif. Manag. Rev. **51**(3), 134–152 (2009)