A Proposed Best-practice Framework for Information Security Governance

Ghada Gashgari, Robert Walters and Gary Wills
School of Electronics and Computer Science, University of Southampton, SO17 1BJ, Southampton, U.K.

Keywords: Information Security Governance, IT Security Governance, Critical Success Factors, Governance Principles.

Abstract: Information security (IS) must be integrated into corporate governance and regarded as a governance challenge that includes reporting, accountability and adequate risk management. Good implementation of information security governance (ISG) delivers strategic alignment, risk management, resource management, performance measurement and value delivery. Several publications have addressed this field. However, the critical success factors (CSFs) that ensure the improvement from a high level across the essential governance areas for effective governance, have not been identified. Based on the literature review, this research identifies seventeen initial CSFs for ISG that affect the long-term success of organisations. For clear high-level guidance of ISG practices, a comprehensive set of ISG rules has been developed based on the principles of ISO/IEC 27014 and COBIT for IS. A best-practice framework for ISG has been proposed across the essential governance areas for effective governance of IS that support the organisations to survive and thrive.

1 INTRODUCTION

Data and information held on IT systems are valuable and critical to the business of the organisation because the value of a business is concentrated in the value of its information. In the ever-changing technological environment, the threats to information security (IS) from viruses, hackers, criminals, and terrorists are increasing, as well as the threats to information from errors, loss, misuse, or disclosure (ITGI, 2006). Consequently, organisations need to incorporate effective IS into their everyday practice that must be proactive, and cope effectively with the technological changes and the growing cybersecurity risks (ITGI, 2006). This can only successful and effective with the active involvement of executives and senior management who can evaluate emerging security threats and the organisation's response to them, and provide strong cybersecurity leadership. This involvement is the integration of IS with corporate governance (CG) (ITGI, 2006; Johnston and Hale, 2009; Entrust, 2004; Mears and Von Solms, 2004; National Cyber Security Summit Task Force, 2004; Johnston and Hale, 2009; Westby and Allen, 2007; Abu-Musa, 2010).

The integration of IS with CG is called Information Security Governance (ISG). ISG deals with the security of information assets in a comprehensive manner, involving every stakeholder in the organisation. Therefore, IS should not be regarded as just a technical issue by the IT department but a governance challenge (ITGI, 2006; National Cyber Security Summit Task Force, 2004). Governing IS is the responsibility of the highest levels of the organisation, who need to use all their resources securely and efficiently, with accountability and in compliance with laws and regulations, in order to sustain successful operations, support organisational strategy and objectives (ITGI, 2006), and sustain a security culture (Allen, 2005). Consequently, ISG should be effectively implemented in order to achieve all its required objectives.

The CSFs are the limited key areas of practice, appearing at several levels in the organisation, where things must go right in order to ensure successful competitive performance and achievement of objectives. Therefore, attention must be paid to those activities that make the difference between success and failure (Bullen and Rockart, 1981).

Gashgari, G., Walters, R. and Wills, G.
A Proposed Best-practice Framework for Information Security Governance.
DOI: 10.5220/0006303102950301
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 295-301
ISBN: 978-989-758-245-5

Despite the significance of the CSFs that are concentrated on the most important aspects for success, no research has explored them in a comprehensive manner from the top to the bottom of the highest levels of the organisation including Board of Directors, executives and management among the essential governance areas.

This research aims to develop a best-practice framework for implementing effective governance of IS. Thus, the following objectives need answering.

Objective1: develop a foundation that guides the implementation of ISG at all organisational levels (high-level guidance).
Objective2: identify a high-level critical success factors (CSFs) for governing IS based on the guidance.
Objective3: ensure the holistic view of CSFs across the essential ISG areas for effective governance of IS.

These three objectives were met by analysing both academic and practice-oriented literature, which is used as a basis for the proposed framework that need to be reviewed and validated.

The rest of the paper is structured as follows: section 2 is the literature review then section 3, constructing the framework that consists of three stages followed by the conclusion.

2 LITERATURE REVIEW

2.1 The Concept and Benefits of ISG

IBM Global Business Service (2006) defines ISG as an "organisation's management responsibilities and practices that provide strategic vision, ensure objectives are achieved, manage risks appropriately, use organisational resources responsibly, and monitor the success or failure of the information security programs" (Abu-Musa, 2010).

ISG is "the establishment and maintenance of a control environment to manage the risks relating to the confidentiality, integrity and availability of information and its supporting processes and systems" (Moulton & Coles, 2003).

ISG is an integral part of corporate governance (National Cyber Security Summit Task Force, 2004; Rastogi & von Solms, 2006), and is not the same as IS management because governing is not managing day-to-day activity but directing and controlling the organisation, ensuring that shareholders' and stakeholders' desires are met (Love et al., 2010), and creating an appropriate organisational culture to achieve the organisation's goals(de Oliveira Alves et al., 2006)

The COBIT 5 framework (Control Objectives for Information and Related Technology) asserts that the governance processes are: evaluate, direct and monitor performance and compliance, while those of management are: plan, build, run and monitor day-to-day activities (ISACA, 2012).

ITGI (2006) indicates that ISG consists of leadership, organisational structure, and processes. Management leadership should be proactive in ensuring that the activities of IS are supported and understood at all organisational levels and aligned with organisational objectives (Love et al., 2010). Organisational structure is a rational set of arrangements and mechanisms (Weill & Ross, 2004) of how ISG functions are carried out, controlled and coordinated, and is dependent on the overall organisational structure (Bowen et al., 2006). ISG processes are the Information Security activities that support organisational objectives. These main components of ISG ensure that the confidentiality, integrity and availability of an organisation's electronic assets are maintained all the time and information is never compromised (von Solms, 2001), as well as cultivating and sustaining a security culture in the organisation (Allen, 2005).

ISG should be based on the Corporate Governance direct and control lifecycle, the core principles of CG, demonstrated by Rastogi and von Solms (2006). Therefore, governing or directing and controlling IS takes place at all management levels of the organisation. Rastogi and von Solms (2006) show that IS in the organisation is *directed* by producing policies, standards and procedures of all IS external and internal requirements from the strategic through the tactical to the operational level, and *controlled* by measuring, monitoring and reporting compliance from the operational through the tactical to the strategic level (von Solms & von Solms, 2006). Figure 1 illustrates the Direct-Control lifecycle.

Figure 1: The Direct-Control Cycle (von Solms and von Solms, 2006).

Johnston and Hale (2009) confirmed empirically that the organisations that address their Information Security from the bottom up, and isolate the governance from the management of IS, have ineffective IS programmes and can fall victim to internal and external cybersecurity attacks, in contrast to organisations whose ISG programmes have a proactive, top-down approach.

According to ITGI (2006), employing good ISG ensures that IS strategies are aligned with organisational strategy and support organisational objectives, delivers business value to all stakeholders, manages risk and resources, and measures organisational performance so that organisational objectives are achieved. It also " : 0 }, "schema" : "https://github.com/citation-style- and trust in relationships with customers and investors, while reducing operational costs and mitigating risks.

Bowen et al., (2006) claim that compliance places responsibility and accountability for IS at all levels in the organisation, so that IS is managed and risks reduced. Therefore, governance of IS uses all the organisation's resources securely and efficiently, with accountability and compliance with laws and regulations.

Thus, ISG across the organisation should be implemented for it to survive and thrive.

2.2 ISO/IEC 27014 Standard and COBIT 5 for IS Framework

The most recent and well-known ISG industrial frameworks are COBIT 5 and ISO/IEC 27014, applicable to all organisation sizes and types.

In 2013, the International Organisation for Standardization and the International Electrotechnical Commission ISO/IEC published an international standard for the governance of IS as ISO/IEC 27014, part of the 27000 series of standards that assist organisations to secure their information assets. The standard includes guidance on the concepts of ISG of aligning IS activities with organisational strategy, based on six high-level principles. The principles are the accepted rules for governance actions. The standard specifies five governance processes: evaluate, direct, monitor, communicate, and assure, that need to be implemented by the governing body and executives (ISO/IEC 27014, 2013).

The COBIT framework has been developed by the Information Systems Audit and Control Association (ISACA). This framework is both well-known and internationally accepted for IT governance (Eloff and von Solms, 2000; Lainhart, 2001).

COBIT 5 aids organisations in achieving their goals for IT governance. This framework has the advantage of being integrated with several best practices and standards of ISACA frameworks, guidance and research, such as COBIT, the Business Model for IS, the IT Assurance Framework, Val IT, and Risk IT (ISACA, 2012). Within COBIT 5, is COBIT 5 for IS with four features: an up-do-date view on governance, clear distinctions between governance and management, an end-to-end view, and holistic guidance. This framework focuses on IS and provides more detailed and practical guidance for governing IS at all levels of the organisation. The framework specifies 12 principles that communicate the organisational rules, and five governance processes that ensure: framework setting and maintenance, benefit delivery, risk optimisation, resource optimisation, and stakeholder transparency (ISACA, 2012).

2.3 ISG Research on Critical Success Factors

The CSFs are "the few key areas where things must go right for the business to flourish and for the managers goals to be attained" (Bullen & Rockart, 1981).

Although ISG has become essential in most organisations, little research on ISG has been published. Most academic and practice-oriented literature have just discussed the CSFs for effective governance of IS in different terms such as key, essential, successful, and critical; and within related topics such as enterprise security (Westby & Allen, 2007), business ISG (BISG) (Bobbert & Mulder, 2015), ISG (Allen, 2013; de Oliveira Alves et al., 2006; ITGI, 2006; Love et al., 2010; National Cyber Security Summit Task Force, 2004; Paul Williams, 2001; Rastogi & von Solms, 2006;) and IS (Bowen et al., 2006).

Only one study was found focusing on the CSFs: Bobbert and Mulder (2015). This identified 22 CSFs for BISG that function only at one level of the organisation which is the strategic level. Additionally, the factors are for BISG which is more general than ISG, since it focuses on more than the IT business area. A list of practices was specified, which were then examined and validated by an expert panel.

3 CONSTRUCTING THE FRAMEWORK

There are several CSFs that organisations need to adopt for effective governance of IS. The framework proposed here is intended to explore the high-level CSFs that function as the core principles of ISG and have an impact on effective governance.

Task Force and Entrust (2004) confirmed that adopting an ISG framework is an important action in assisting organisations in integrating ISG into their CG practices, securing information in the face of growing cybersecurity risks, improving the efficiency of organisational processes, complying with regulations, and cultivating an acceptable IS culture.

The development of the framework consists of three stages to accomplish the three objectives and aim of the research, summarised in Figure 2.

3.1 Stage 1: Forming the Guidance

This stage is about developing the foundation that guides the implementation of ISG, so accomplishing the first objective.

The six high-level principles of ISO/IEC 27014 are for the Board of Directors and executive management. The principles are the accepted rules for governance actions that guide its implementation. Further, it supports the organisation to align their IS activities with their overall business objectives (ISO/IEC 27014, 2013).

The twelve high-level principles of COBIT for IS are aimed at IS professionals at all levels. They are a mechanism for communicating with the Board of Directors and management instructions and directions that support the governance objectives. Additionally, the principles aid IS professionals in optimising the value of the organisation, as well as supporting and defending the business, and cultivating responsible behaviour of IS (ISACA, 2012).

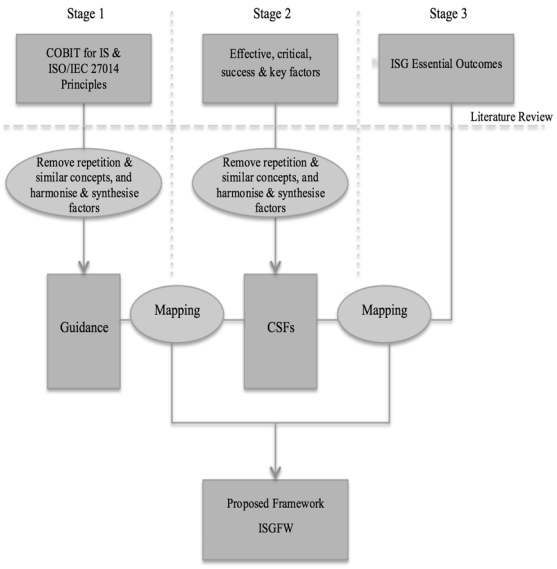

Figure 2: Developing stages of the proposed framework.

When the principles of both frameworks are used together, they provide synergy that is beneficial for all high organisational levels. By integrating these principles, a comprehensive set of rules that supports and defends the business, and cultivates IS culture will be developed for ISG implementation.

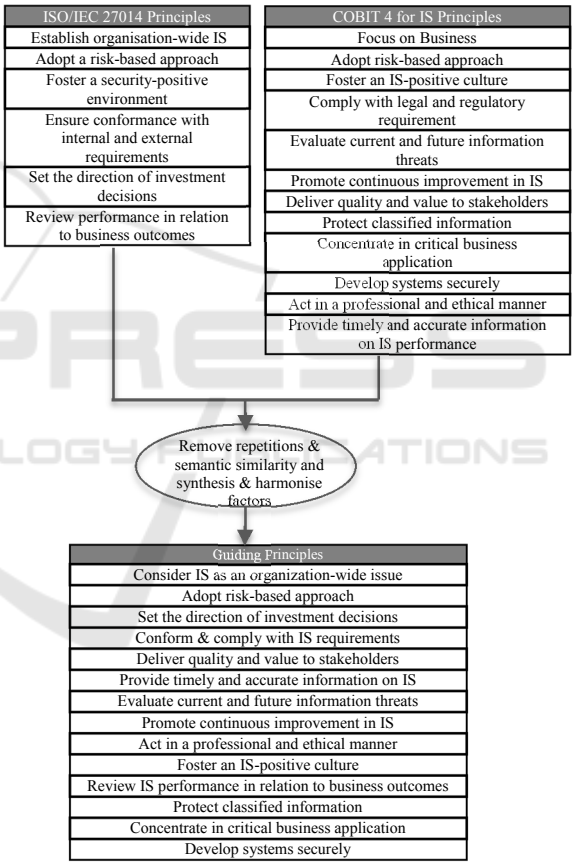

Figure 3: Forming the guidance.

This is our main contribution, as it establishes a framework for ISG, based on internationally recognised standards and frameworks of the governance of IS that can be used by all organisations types and sizes. Figure 3 clarifies Stage 1 and the guiding principles for ISG implementation.

Table 1: The Identified CSFs.

	CSF	Source
1	Integrate IS with business activities	(Westby & Allen, 2007); (Allen, 2013); (Bobbert & Mulder, 2015); (Bowen et al., 2006); (ITGI, 2006)
2	Determine clear IS responsibility and be held accountable	(Allen, 2013); (Bowen et al., 2006); (ITGI, 2006); (Paul Williams, 2001); (Westby & Allen, 2007)
3	On-going strategic alignment	(Bobbert & Mulder, 2015); (ITGI, 2006); (Rastogi & Solms, 2006)
4	Visible involvement & leadership	(Allen, 2013); (Bowen et al., 2006); (de Oliveira Alves et al., 2006); (ISACA, 2012); (ITGI, 2006); (Paul Williams, 2001); (Westby & Allen, 200)
5	Ensure IS policies and practices comply with law & regulations and relevant requirements	(Allen, 2013); (Bowen et al., 2006); (ITGI, 2006);(Love et al., 2010); (Paul Williams, 2001); (Westby & Allen, 2007)
6	Ensure timely and transparent reporting of IS performance and issues	(Bobbert & Mulder, 2015); (ISO/IEC 27014, 2013); (ITGI, 2006); (National Cyber Security Summit Task Force, 2004);
7	Constant review of IS performance	(Bowen et al., 2006); (ITGI, 2006); (National Cyber Security Summit Task Force, 2004); (Westby & Allen, 2007)
8	Improve IS on an on-going basis	(Allen, 2013); (ITGI, 2006); (National Cyber Security Summit Task Force, 2004);
9	Effective communication	(Bowen et al., 2006); (Bobbert & Mulder, 2015); (ITGI, 2006); (ISACA, 2012); (National Cyber Security Summit Task Force, 2004)
10	Effective business continuity/disaster recovery plan	(Allen, 2013); (ITGI, 2006); (National Cyber Security Summit Task Force, 2004); (Paul Williams, 2001)
11	Determine risk appetite	(Allen, 2013); (Bobbert & Mulder, 2015); (Paul Williams, 2001); (Love et al., 2010);
12	Ensure regular risk & threats assessment	(Bobbert & Mulder, 2015); (ITGI, 2006); (Love et al., 2010); (National Cyber Security Summit Task Force, 2004); (Westby & Allen, 2007);
13	Protect critical and sensitive assets	(ITGI, 2006)
14	Identify critical applications & information systems	(ITGI, 2006); (National Cyber Security Summit Task Force, 2004)
15	Integrate IS with systems lifecycle	(Allen, 2013); (Westby & Allen, 2007)
16	Effective IS awareness and training	(Allen, 2013); (Bowen et al., 2006); (Bobbert & Mulder, 2015); (de Oliveira Alves et al., 2006); (ISACA, 2012); (ITGI, 2006); (Paul Williams, 2001); (Westby & Allen 2007);
17	Adequate IS investment & resource commitment	(Allen, 2013); (de Oliveira Alves et al., 2006); (ISACA, 2012); (ITGI, 2006);

3.2 Stage 2: Identifying the CSFs

Identifying the CSFs for governing IS is the basis of the solution framework. This stage includes: exhaustively analysing the academic and practice-oriented literature concerned with the implementation of ISG and other related disciplines such as IS, enterprise security and BISG, thirteen of which discuss the effectiveness of ISG. This stage followed by extracting the key, success and effective factors based on the developed guidance; removing repetitions and semantically similar concepts; and logically harmonising and synthesising.

The CSFs have been mapped to the guiding principles in order to ensure that the identified CSFs are comprehensive in terms of including the critical practices of all organisational levels, and to ensure that each principle has the practice that is most likely to have an impact on effective governance.

Thus, this stage achieves the second objective. The CSFs identified and their sources are shown in Table1.

3.3 Stage 3: Mapping CSFs to Essential Areas of ISG

Properly implemented ISG should provide five outcomes: strategic alignment, value delivery, performance measurement, risk management, and resource management. Therefore, organisational leaders should function successfully on these essential areas (ITGI, 2006). The CSFs identified in

Table 2: The Proposed Framework.

ISG Area	Guidance		CSF
Strategic Alignment	Consider IS as an organization wide issue	1	Integrate IS with business activities
		2	On-going strategic alignment
		3	Determine clear IS roles & responsibilities and be held accountable
	Act in professional and ethical manner	4	Visible involvement & leadership
	Conform & comply with internal & external IS requirements	5	Ensure IS policies and practices comply with law & regulations and relevant IS requirements
Performance Measurement	Provide timely & accurate information on IS performance	6	Ensure timely and transparent reporting of IS performance and issues
	Review IS performance in relation to business outcomes	7	Constant review of IS performance
	Promote continuous improvement in IS	8	Improve IS on an on-going basis
Value Delivery	Deliver quality & value to stakeholders	9	Effective communication
		10	Effective business continuity/disaster recovery plan
Risk Management	Adopt risk based approach	11	Determine risk appetite
	Evaluate current & future information threats	12	Ensure regular risk & threats assessment
	Protect classified information	13	Protect critical and sensitive assets
	Concentrate on critical business applications	14	Identify critical applications & information systems
	Develop systems securely	15	Integrate IS with systems development lifecycle
Resource Management	Foster an IS positive culture	16	Effective IS awareness and training
	Set the direction of investment decisions	17	Adequate investment & resource commitment of IS

Stage 2 are deployed across these essential areas of ISG that are also component of IT governance lifecycle in (ITGI, 2003). Thus, employing the practices that ensure the improvement of all the essential areas eventually lead to effective ISG, fulfilling the third objective. Table 2 is the proposed framework that has been developed to give clear guidance on implementing the most important governance practices among the essential governance areas. The two mapping processes indicate that the CSFs are most likely to have an impact on effective governance of IS, thus achieving the research aim.

4 CONCLUSION

Information security should be considered at the highest levels of organisations including the Board of Directors, executives and management. Effective IS requires their active involvement to ensure the organisation is using all its resources securely and efficiently, with proper risk management, accountability and compliance that will sustain a successful and profitable business operation and support organisational strategies and objectives.

To implement effective governance of IS, it is necessary to identify the CSFs that are concentrated on the most important aspects for success which affect the long-term success of organisations. In the literature, CSFs for ISG have just been identified

and discussed with different terms and topics, but this is the first research has focused on ISG from a high-level CSFs that are mapped to the comprehensive ISG rules of practice which has been developed based on COBIT for IS and ISO/IEC 27014, and the essential governance areas in order to show that they are most likely to have an impact on effective governance of IS.

The proposed framework will need to be reviewed for application to particular regions to confirm it is a suitable for local organisational structures and culture, notably because the framework is subject to local laws and regulations.

For example, ISG is lacking in Saudi organisations (Abu-Musa, 2010), therefore the next step of this research will be exploring the Saudi cultural factors by reviewing the proposed framework with experts from the Kingdom of Saudi Arabia; and then validating it by conducting case studies in several Saudi organisations in order to develop a best-practice framework for effective ISG that supports Saudi organisations in securing their assets and implementing proven security techniques and strategies.

REFERENCES

Abu-Musa, A. (2010). Information Security Governance in Saudi Organizations: an empirical Study, *Information Management & Computer Security*, 18, 226–276.

Allen, J. (2005). *Governing for Enterprise Security, Technical Note*. Pittsburgh.

Allen, J. H. (2013). *Security Is Not Just a Technical Issue*, *US-CERT: Build Security In*.

Bobbert, Y., & Mulder, H. (2015). Governance Practices and Critical Success factors suitable for Business Information Security, in *International Conference on Computational Intelligence and Communication Networks*.

Bowen, P., Hash, Joan; , & Wilson, M. (2006). *Information Security Handbook : A Guide for Managers*. National Institute of Standards and Technology (NIST).

Bullen, C. V., & Rockart, J. F. (1981). *A primer on critical success factors*, *The Rise of Management Computing*.

de Oliveira Alves, G., de Costa Carmo, L., & de Almeida, A. (2006). Enterprise Security Governance, *0*(C), 71–80.

Eloff, M. M., & von Solms, S. H. (2000). Information Security Management: A Hierarchical Framework for Various Approaches, *Computers & Security*, 19(3), 243–256.

Entrust (2004). An Essential Element of Corporate Governance, (April).

ISACA (2012). *COBIT 5 for Information Security*. IL, USA. Available at: www.isaca.org/cobit5info-sec.

ISO/IEC 27014. (2013). *Governance of Information Security*. Geneva: International Organization for Standardization and the International Electrotechnical Commission.

ITGI. (2003). *Board Briefing on IT Governance* (2nd ed).

ITGI. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd ed.). IT Governance Institute.

Johnston, A. C. & Hale, R. (2009). Improved Security Through Information Security Governance, *Communications of the ACM*, 52(1), 126.

Lainhart, J. W. (2001) An IT Assurance Framework for the Future, *The Ohio CPA Journal*.

Love, P., Reinhard, J., Schwab, A. J. and Spafford, G. (2010). GTAG Information Security Governance, *The Inistitute of Internal Auditors*, 134.

Mears, L., & Von Solms, R. (2004). Corporate Information Security Governance : A Holistic Approach.

Moulton, R., & Coles, R. S. (2003). Applying information security governance, *Computers & Security*, 22(7), 580–584.

National Cyber Security Summit Task Force (2004). *Information Security Governance : a Call To Action*, *Coroprate Governance Report*.

Paul Williams, A. (2001). Information Security Governance, *Information Security Technical Report*, 6(3), 60–70.

Rastogi, R., & von Solms, R. (2006). Information Security Governance-A Re-Definition, *Security Management, Integrity, and Internal Control in Information Systems*, 193, 223–236.

Rockart, J., & Van Bullen, C. (1981). A Primer on Critical Success Factors, *Center for Information Systems Research, Sloan School of Management, MIT, Cambridge, MA*, (February 1981).

von Solms, B. (2001). Corporate governance and information security, *Computers & Security*, 20, 215–218.

von Solms, R., & von Solms, S. H. (Basie). (2006). Information Security Governance: A model based on the Direct-Control Cycle, *Computers and Security*, 25(6), 408–412.

von Solms, S. H., & von Solms, R. (2008). *Information Security Governance*. Johannesburg: Springer.

Weill, P., & Ross, J. (2004.) *IT Governance, How Performers Manage IT Decision Rights for Superior Results.* Harvard Business Press.

Westby, J., & Allen, J. (2007). Governing for Enterprise Security (GES) Implementation Guide, *Software Engineering Institute, CERT*, (August), 1–17.