Gap analysis of ICT governance in organizations: A simple implementation approach since ISO/IEC 38500

Abstract:

There are various methods available for dealing with ICT governance, most of them just describes which element in the organizations need to be considered in order to achieve the goals of ICT governance. This paper shows a simple implementation approach of a gap analysis for ICT governance in organizations since ISO/IEC 38500. The base of the method is two questions over each of the control elements that are proposed by the standard from whom quantitative performance indicators are built. The standard uses a variation of Deming management cycle (evaluate, direct and monitor). Also the standard takes account six basic issues (principles) as well as a development process. An application of the approach has been presented for the purpose of illustrating its use.

Key worlds: ICT governance, ISO/IEC 38500, gap analysis.

1. Introduction

Information technology and communication (ICT) currently play an important role in business development in different types of organizations, therefore, should be considered as a strategic element and its evaluation should be part of business management. Assessment of ICT is responsible not only for the leaders of ICT, but also for the board of directors, executive management and senior management (Weill & Ross, 2004).

Although ICTs alone do not provide a competitive advantage, it allows optimizing the use of resources of the organization, therefore an appropriate governance of ICT allows increasing the creation of value of investments in ICT. Then ICT investments should be made in coordination with the business strategy for achieving a significant impact in the organization (Alfantookh & Bakry, 2009).

ICT leaders should know about most of business processes of the organization, this will allow them to determine which investments, at what level and at what point should be performed in ICT (García, 2008; Bin-Abbas & Bakry, 2012). Critical factor to achieving improved efficiency in business process involves leveraging ICT to redesign the internal processes in order to maximize their potential.

The improvement of processes leads to improved business structures which enable the organization to create competitive advantages, which allow them to face the challenges and changes in the field in which they operate.

2. ICT governance in organization

2.1 Benefits of IT and ICT

IT (Information Technology) and ICT has become in interchangeable term. The ISO (International Standards Organization) defines IT, in its ICT governance standard (ISO/IEC 38500, 2008), as resources required to acquire, process, store and disseminate information. It adds that this includes CT (Communication Technology) and consequently ICT. This work has used ICT to mean both IT and CT or the compose term ICT.

ICT have proven a lot of benefits that include various levels: personal, business, organization, government, and society. These benefits have been viewed as consisting of five main features: i) saving time and leading to *faster achievements*; ii) saving cost through cheaper *business activities*; iii) providing services with *better quality*; iv) opening new opportunities by introducing *different capabilities* and v) enhancing trust by providing new *security measures* that are not feasible without IT. These benefits are summarized in the abbreviation ‘‘FCBDS’’ (Bakry, 2004).

2.2 Relevant ICT governance approaches

Some national and international organizations have issued a number of documents concerned with providing ICT governance recommendations in order to achieve an efficient and effective use of ICT. In this regard, the relevant initiatives among these include: ITIL (Information Technology Infrastructure Library) proposed by British Office of Government Commerce (Alfantookh & Bakry, 2009; ITIL, 2013; OGC, 2005); COBIT (Control Objectives for Information and Related Technologies) of the American Information System Audit and Control Association (Bakry & Alfantookh, 2006; COBIT 5, 2013; ITGI, 2005); ISO 20000 standard concerned with ICT services management (ISO 20000, 2005); ISO/IEC 38500 standard associated with the principle of ICT governance (ISO/IEC 38500, 2008); and MIT (Massachusetts Institute of Technology) work on ICT governance (Weill & Ross, 2004). The organization can take these recommendations as references to the assessment of its ICT governance, where the outcomes of such assessments support planning and future improvements. This paper has been focused in ISO/IEC 38500 with an assessment implementation approach.

2.3 ISO/IEC 38500

ISO/IEC 38500 is a high level, principles based advisory standard. In addition to providing broad guidance on the role of a governing body (ISO/IEC 38500, 2008), this standard encourages organizations to use appropriate actions to both improve and consolidate their governance of ICT.

A framework for effective governance of ICT is providing by the standard, to assist those at the highest level of organizations (Directors) to understand and fulfill, their legal, regulatory, and ethical obligations in respect of their organizations use of ICT (ISO/IEC 38500, 2008).

Therefore the framework has a several principles in order to evaluating, directing and monitoring (Management cycle) the use of ICT into the organizations.

These principles are associated with six basic issues as well as a development process. The basic issues include: i) responsibility, ii) strategy, iii) acquisition, iv) performance, v) conformance and vi) human behavior. Note that the development process is not following Deming's four phases (plan–do–check–act) like several other standards mentioned above, COBIT, ITIL and ISO 20000 (De Feo & Barnard, 2004). In fact, ISO/IEC 38500 includes the three main cyclic management phases of evaluate, direct and monitor (E-D-M).

Also is important to note that the principles express preferred behavior to guide decision making. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implementing (ISO/IEC 38500, 2008).

Now, it is necessary to note that Governance is distinct form management, and for the avoidance of confusion, the two concepts are clearly defined into this standard.

By one hand the corporate governance of ICT makes reference to the system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the use of ICT to support the organization and monitoring this use to achieve plans, it includes the strategy and policies for using IT within an organization. By another hand the management refers to the system of controls and processes required to achieve the strategic objectives set by the organization's governing body. Management is subject to the policy guidance and monitoring set through corporate governance (ISO/IEC 38500, 2008).

Following the above a proper corporate governance of ICT may assist directors not only to assured conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of ICT but also to ensure that ICT use contributes positively to the performance of the organization (ISO/IEC 38500, 2008).

The propose of this standard is to promote effective efficient, and acceptable use of ICT into the organizations by assuring all stakeholders (including consumers, shareholders, and employees) that following the standard they can have confidence in the organization's corporate governance of ICT. Also by using the standard can be guaranteed not only informing and guiding directors in governing the use of ICT but also providing basis for objective evaluation of the corporate governance of ICT (ISO/IEC 38500, 2008).

3. Assessment model approach

This work has followed the standard as a guide to involved in designing and implementing a model of the assessment of management system of policies, processes, and structures that support governance of ICT.

3.1. Basics principles and management cycle

Main activities related to the six principles of the standard are suggested into the model, these activities should be developed to monitor the performance of the management of ICT. Each principle has activities which should be performed, but the standard does not indicate how, where or who should perform it. The goal of applying the proposed cycle in the standard (E-D-M) to the management of ICT is to ensure excellence in business processes and optimizing resources of the organization. The six principles of the standard are i) Responsibility (*r*): of individuals and groups; ii) Strategy (*s*): ICT satisfies the strategy of the organization; iii) Acquisition (*a*): of ICT for valid reasons; iv) Performance ((*p*): based on supporting the business of the organization v) Conformance (*c*): with mandatory legislation and regulations and vi) Human behavior (*h*): response to the needs of all people in the process.

As already mentioned, it must perform the three activities that make up the cycle defined by the standard for each of the six principles: i) Evaluate, examine and judge the present and future use of ICT, including strategies, proposals and service delivery agreements (internal and external); ii) Direct: assign responsibilities, prepare and implement plans and policies. Ensure the implementation of projects considering the impacts on the operation, processes and ICT infrastructure; iii) Monitor: supervise through adequate measurement systems, the performance of ICT, the same must be in accordance with the plans and objectives of the organization.

It is important to note that the management of ICT is part of the government of ICT, and it constitutes the essential component for the achievement of excellence and competitiveness of organizations, therefore, to study the application level of ISO/IEC 38500 framework, a model was made as described in Table 2-7 based on the summary of recommendations for good governance of ICT by Bosch (2011).

3.2. Assessment method

Following to Bin-Abbas and Bakry (2014) the proposed assessment method in this work proposes two questions on each control element: the level of importance of the element ($w_{[i]}$); and the level of its implementation ($g_{[i]}$). Five levels have been taken into account for both questions as illustrated in Table 1. Note that the two mentioned questions concerned with each issue can be assessed by different people (ICT managers, leaders, technical, etc.). Then it is needed finding averages for not only the importance but also the implementation level, as shown in Table 1. In addition, a relative measure that combines the averages of both: importance and implementation can be found. This provides this relative combined measure as a percentage value (see Table 1).

The mentioned above can be applied both to the basic ICT governance control elements mentioned in the standard and to other possible elements that may be needed for specific cases (organizational field characteristics). As will be seen below, the ICT governance requirement controls are open to further additional considerations that may be taken into account. This enhances knowledge sharing and support improvement.

Table 1: Assessment method: importance ($w_{[i]}$) and implementation level ($g_{[i]}$).

Levels of Scale (L=5) for both importance ($w_{[i]}$) and implementation level ($g_{[i]}$).				
Poor/low	Below avg.	Average	Above avg.	Good/high
1	2	3	4	5
Average importance ($w_{[i]}$) and implementation level ($g_{[i]}$) of a control element *i* for *k* assessments.				
$w_{[i]} = \sum_{j=1}^{k} \frac{w_{[i,j]}}{k}$; $g_{[i]} = \sum_{j=1}^{k} \frac{g_{[i,j]}}{k}$ (1) and (2)				
General performance indicator *A* for each principle (*r, s, a, p, c, h*) for *N* elements of each principle.				
$A_{r,s,a,p,c,h\ [i]} = \frac{\sum_{i=1}^{N} w_{[i]} * g_{[i]}}{\sum_{i=1}^{N} w_{[i]} * L} \%$ (3)				
General performance indicator A_t: for N_t elements of the model.				
$At_{[i]} = \frac{\sum_{i=1}^{N_t} w_{[i]} * g_{[i]}}{\sum_{i=1}^{N_t} w_{[i]} * L} \%$ (4)				

3.3 ICT governance controls

Forty three ICT governance control elements have been assigned over the six principles and three stages of the management cycle proposed by the standard. These control elements are identified according to their domains (principle and stage) in Tables 2–7, where each table is concerned with one principle into the full management cycle (E-D-M). The tables allow classify both levels the importance and the implementation of each element. In order to enhance the understanding of the approach, an illustrative application is introduced in section 4.

Table 2: Principle of Responsibility

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$Ar_{[i]}$
1	E1	The organization has methods and setup options to assign responsibilities	4,33	3,00	0,60
2	D1	The organization directs that designed plans are carried out	4,00	2,67	0,53
3	M1	The organization monitors the allocation of responsibilities	4,67	3,33	0,67
4	E2	The organization evaluates the competence of those who receive responsibilities	4,67	2,67	0,53
5	D2	The organization directs that Directors receive the information they need to make decisions	5,00	2,67	0,53
6	M2	The organization monitors the proper performance of assigned responsibilities (indicators)	4,33	4,00	0,80
				Ar	**60,99**

Table 3: Principle of Strategy

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$As_{[i]}$
1	E3	The organization evaluates the development of ICT to ensure its capability support the future business needs	5,00	3,33	0,67
2	D3	The organization directs the design of policies and plans that leverage the value of ICT	4,67	2,67	0,53
3	M3	The organization monitors the achieving objectives with the planned resources	4,67	3,33	0,67
4	E4	The organization evaluates the alignment of ICT activities with a business objectives	5,00	4,00	0,80
5	D4	The organization supports ICT innovation to face new opportunities	4,33	2,33	0,47
6	M4	The organization monitors the results to verify that expected benefits have been reached	5,00	3,00	0,60
7	E5	The organization evaluates the risk management associated with the use of ICTs	5,00	2,33	0,47
				As	**60,26**

Table 4: Principle of Acquisition

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$Aa_{[i]}$
1	E6	The organization evaluates different options with ICT offers regarding to the cost and risk.	4,00	2,33	0,47
2	D5	The organization directs that the asset purchase procedure is properly performed	4,33	3,33	0,67
3	D6	The organization directs that ICT supports business needs	5,00	3,67	0,73
4	M5	The organization monitors that the investments provide the expected capabilities	5,00	4,00	0,80
5	M6	The organization monitors the understanding of internal/external needs of organization	5,00	3,33	0,67
				Aa	**67,52**

Table 5: Principle of Performance

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$Ap_{[i]}$
1	E7	The organization evaluates the operational proposals provided by ICT managers to maintain business needs	4,67	3,00	0,60
2	D7	The organization ensures that ICT resources are sufficient to meets the business needs	4,33	2,67	0,53
3	M7	The organization monitors the extent to which ICT does support for business	5,00	4,00	0,80
4	E8	The organization evaluates the ICT risk regarding to the continuity of business operations continuity of business operations	5,00	2,00	0,40
5	D8	The organization provided to Directors a correct and an update information as a decision support	5,00	2,33	0,47
6	M8	The organization monitors the prioritization of allocation of resources according on business goals	5,00	3,67	0,73
7	E9	The organization evaluates the risk of information integrity and protection of the ICT assets	4,67	2,67	0,53
8	D9	The organization directs settings of priorities and restrictions on ICT assets	4,33	2,33	0,47
9	M9	The organization monitors the compliance with established policies and standards	4,67	2,67	0,53
10	E10	The organization evaluates the effectiveness of decisions of the use of ICT as a support for the business goals	4,67	3,00	0,60
11	M10	The organization monitors the data accuracy policy and efficient use of ICTs	4,67	3,00	0,60
				Ap	**57,14**

Table 6: Principle of Conformance

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$Ac_{[i]}$
1	E11	The organization evaluates the extent to which ICT met the laws and established standards	5,00	2,67	0,53
2	D10	The organization have mechanisms for ensuring that the use of ICT complies with relevant obligations	4,67	3,33	0,67
3	M11	The organization monitors the compliance and agreement (audit/reporting) that are timely, complete and appropriate	4,67	3,00	0,60
4	E12	The organization evaluates the compliance of internal procedures for Governance of ICT	4,67	3,00	0,60
5	D11	The organization directs that policies are established to meet internal obligation in the use of ICT	4,33	3,67	0,73
6	M12	The organization monitors that ICTs preserves privacy and strategic knowledge	4,67	3,00	0,60
7	D12	The organization monitors that ICY processes are suitable to meet business goals demeanor and respect the procedures	4,67	2,67	0,53
8	M13	The organization monitors compliance with internal processes of ICT	4,33	2,67	0,53
9	D13	The organization directs that has been realized ethical use of ICT	4,67	2,00	0,40
				Ac	**57,65**

Table 7: Principle of Human Behavior

i	Stage	Activities	Importance ($w_{[i]}$)	Implementation level ($g_{[i]}$)	$Ah_{[i]}$
1	E13	The organization evaluates that the human component is identified and taken into account in all ICT activities	4,33	3,00	0,60
2	D14	The organization directs that the activities of ICTs are consistent with human component	4,33	3,00	0,60
3	M14	The organization monitors ICT activities in order that human behavior remain relevant (training/coaching)	4,67	3,33	0,67
4	D15	The organization monitors work practices in order to be consistent with the use of ICTcan be identified and reported (policies and procedures) to directors	5,00	3,00	0,60
5	M15	The organization monitors the application of appropriate practices to be consistent with the use of ICT	4,67	3,33	0,67
				Ah	**62,71**

4. An illustrative application

In order to illustrate the use of the proposed approach, it has been applied to the ICT governance of a commercial organization, whose identity is kept concealed for business reasons. Three ICT managers and 20 technical staff members of the technology center of the organization, ‘‘K = 23’’, have assessed all 43 control elements presented in Tables 2–7 according to model above. The results of the gap analysis are given in the importance as well as implementation fields of every control element in these tables in terms of the number of staff who adopted a specified level for each field. Tables 2-7 also show the averages of the importance weights and implementation grades of all control elements according to the six standard principles. Note that the collective weighted implementation indicators for the standard principles are also given in the same Tables.

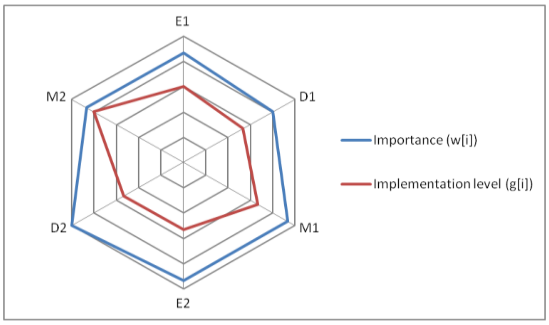

Fig.1 Assessment ICT governance control: Responsibility

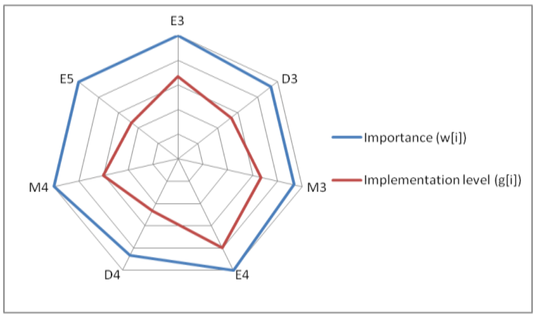

Fig.2 Assessment ICT governance control: Strategy

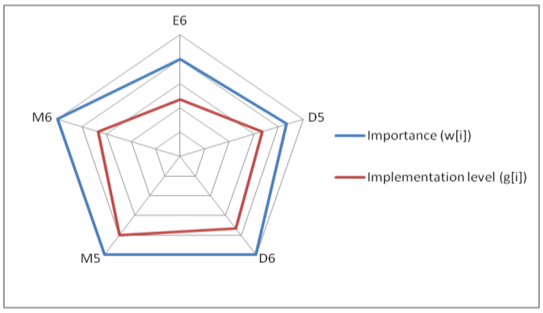

Fig.3 Assessment ICT governance control: Acquisition

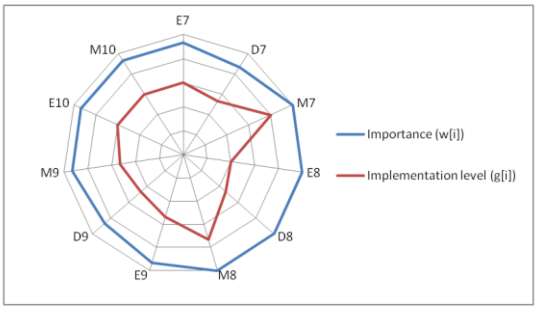

Fig.4 Assessment ICT governance control: Performance

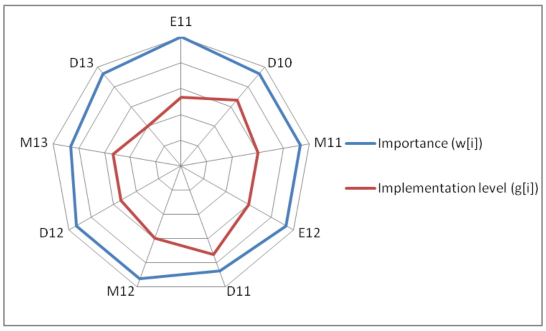

Fig. 5 Assessment ICT governance control: Conformance

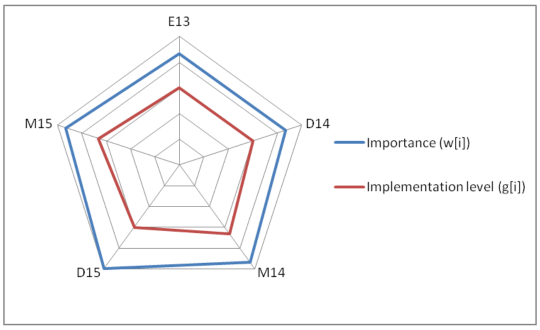

Fig.6 Assessment ICT governance control: Human Behavior

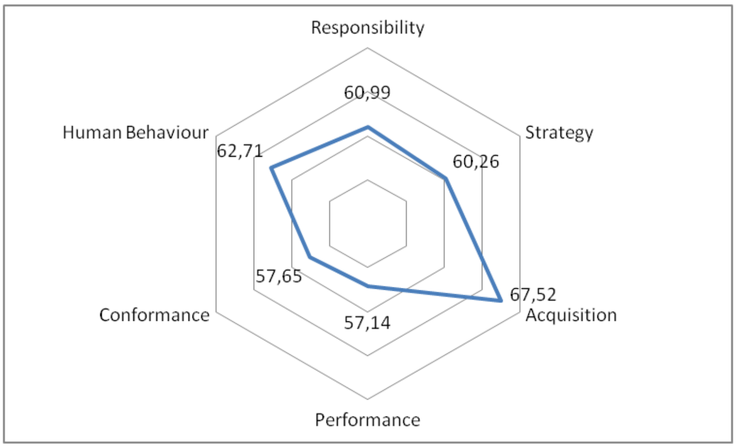

Fig.7 ICT governance performance (%)

Figures 1–6 show the results obtained for the control elements of every standard principle; and Figure 7 illustrates the results of the overall weighted ICT governance performance of the six principles. Some remarks can be derived from these results at the control element level and at the principle level. The results of the gap analysis can help specifying what need to be done for the improvement of the current state of ICT governance in the organization concerned. As an example, here are some useful observations for the illustrative case.

- The analysis result show that the given average implementation grades of all control elements range between 2.05 and 3.33 out of 5; while the given average importance weights of all control elements range between 4.50 and 4.81 out of 5. This shows that a gap is felt by the ICT staff of the organization between what is seen as important in IT governance and what is actually implemented.
- Best match between importance and implementation (0.33) exists in the control elements of ‘‘The organization monitors the proper performance of assigned responsibilities (indicators)’’, which is associated with the Responsibility principle, and of Monitoring stage of the management cycle.
- Worst match between importance and implementation (3.0) exists in the control elements of ‘‘The organization evaluates the ICT risk regarding to the continuity of business operations continuity of business operations’’, which is associated with the Performance principle, and of Direct stage of the management cycle.
- At the Performance principle has the least score, while Acquisition has the highest score, which is only around 67%.

5. Conclusions

The model principles and main tasks which sets the ISO / IEC 38500 standard provides a framework that allows us to evaluate the level of compliance of the activities to be performed for the management of ICT can be efficient and effective.

The work presented in the paper has shown a simple implementation approach of a gap analysis for ICT governance in organizations since ISO/IEC 38500. The work has focused in describe an assessment method which ask two question on each of the control elements that is proposed by the standard. These two questions help to identify the level of importance and the level of implementation in the control element by the organization. Note that the mentioned above can be applied not only to the basic ICT governance control elements mentioned in the standard, but also to other possible elements that may be needed for specific cases (organizational field characteristics).

An application of the approach has been presented for the purpose of illustrating its use. Result of the analysis shows the gaps that exist between the implementation and importance levels of each control element that could be used to identify the elements that the organization needs to improve.

Acknowledgment

This work has been supported by Escuela Politécnica Nacional, EPN, under project number: PII-DESODEH-005-2015.

References

Alfantookh, A. & Bakry, S. H. (2009). *IT governance practices: ITIL*. Saudi Computer Journal: Applied Computing and Informatics, 7(1), 56–65.

Bakry, S. H. (2004). *Development of e-government: A STOPE view*. International Journal of Network Management, 14(5), 339–350.

Bakry, S. H., & Alfantookh, A. (2006). *IT governance practices: COBIT*. Saudi Computer Journal: Applied Computing and Informatics, 5(2), 53–61.

Bin-Abbas, H., & Bakry, S. H. (2012). *Knowledge management: An instrument for building the knowledge society*. International Journal of Knowledge Society Research (IGI Publishing, USA), 3(3), 58–67.

Bin-Abbas, H., & Bakry, S. H. (2014). *Assessment of IT governance in organizations: A simple integrated Approach*. Computers in Human Behavior 32 (2014) 261–267

COBIT 5 (2013). *A business framework for the governance and management of enterprise IT*. Information System Audit and Control Association.

De Feo, J. A., & Barnard, W. W. (2004). *Juran Institute's six sigma breakthrough and Beyond: Quality performance breakthrough methods*. New York: McGraw-Hill.

Bosch, A. (2011). *Herramientas para la implantación del gobierno de las TI: ISO 38500*. TIC Comisión Sectorial de las Tecnologías de la Información y las Comunicaciones. ISBN: 978-84-935509-8-1, Madrid, España.

García, E., Rialp, A., & Rialp, J. (2008). *IT unification and integration processes in horizontal mergers and acquisitions*. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal, 19.

ISO/IEC 20000 (2005). International standards organization/international electrotechnical commission. Information Technology-Service Management, Geneva 20, Switzerland.

ISO/IEC 38500 (2008). International standards organization/international electrotechnical commission, Corporate Governance of Information Technology, Geneva 20, Switzerland.

ITGI (2005). *Information Technology Governance Institute COBIT (Control Objectives for Information and Related Technologies) 4: Control objectives, management guidelines and maturity models*. Rolling Meadows, Illinois, USA, 2005.

ITIL (2013). Information Technology Infrastructure Library. The British Office of Government Commerce. <www.itil.org>.

OGC (2005). *Office of government commerce, best practices: Introduction to ITIL*, The Stationary Office, UK, 2005.

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Boston, Massachusetts, USA: Harvard Business School Press.