Classification of IT Governance Tools for Selecting the Suitable One in an Enterprise

Fatemeh NasserEslami[1]*, Mehdi Fasanghari[1] and Ali Abdollahi[1]

ABSTRACT

The Information Technology (IT) governance arrangements refer to the patterns of authority for key IT activities in organizations, including IT infrastructure, IT use, and project management. During the last 20 years, three primary modes of IT governance have become prevalent: centralized, decentralized, and the federal mode. These modes vary in the extent to which corporate Information System (IS), divisional IS, and line management is vested with authority for the key IT activities. In order to making integrity in information systems, reducing redundancy of information in organizations, managing of information security and IT services, and standardizing of software producing, a suitable framework for organizations is needed. Thus, this study investigates to comparison the IT governance tools and males solutions which helps an organization in selection of the best IT Governance tools fit to its structure.

Keywords: Internet, management, Corporate Governance, IT Governance, Framework, Guidance.

1. Introduction

IT is essential to manage transactions, information and knowledge necessary to initiate and sustain economic and social activities. These activities increasingly rely on globally cooperating entities to be successful. In many organizations, IT is fundamental to support, sustain and grow the business. While many organizations recognize the potential benefits that technology can yield, the successful ones also understand and manage the risks associated with implementing new technologies [1]. The IT governance is an integral part of enterprise governance that consists of the leadership, organizational structures, processes that ensure the organization's IT sustains, and extends the organization's strategies and objectives [1]. The IT governance drives strategic alignment between IT and the business and must judiciously measure performance [2]. So, is an integral part of enterprise governance which operates model for how organization will make decisions about use of IT, Involves external relationships for obtaining IT relationships, Involves authority, control, accountability, roles, and responsibilities, Involves processes and methods for making decisions and Involves judgments about how well use of IT enables strategic direction [2].

Today businesses rely on information technology (IT) as an integral part of their overall enterprise strategy. A new field of thought called IT governance has been under development for several years. Just as business management is governed by generally accepted good practices, IT should be governed by practices that

[1] The End of North Kargar- Iran Telecommunication Research Center (ITRC), Iran
* *Corresponding Author* (Email: F_eslami@itrc.ac.ir, Telephone: 989122844209)

help ensure an enterprise's IT resources are used responsibly, its risks are managed appropriately and its information and related technology support business objectives [13]. In other word IT governance is the process by which decisions are made around IT investments. How these decisions are made, who makes the decisions, which is held accountable, and how the results of the decisions are measured and monitored are all parts of IT governance [3]. While there is no 'standard' definition, in general, IT governance involves specifying the decision rights, the accountability and authority framework for important IT decisions, with the objective of encouraging 'desirable behavior's in the use of IT [14].

According to the IT Governance Institute, IT governance is the responsibility of the board of directors and the executive management, and is an integral part of enterprise governance. It elevates information as a key organizational asset and treats governance of information at par with governance of other assets like human, financial, intellectual, and relationship assets [13]. As larg number of IT Governance tools, it is a big problem for optimizations to select the suitable one. In order to classify the IT Governance tools and interviewing some parameters to selection, we first review the theoretical background of the tools. Available standarsds and importance of COBIT standard will be presented afterward. Then the table of tools comparison will be illustrate. Next, the validation process will be described and the conclusion will be presented at the end.

2. IT Governance Definition

Many definitions of IT governance have been presented. As the demands made on service recipients changed, so did these definitions. The most important of them will be briefly discussed here. At first only the place IT governance should have in the organization was included [2]. Then decision-making processes were added [3]: which IT decisions should the IT and business managers take, and which priorities should they define? The next addition was that the return on their IT investments should be monitored [4]. And then it was stressed that companies should ensure the organizational capacity to formulate and implement an IT strategy, in order to align IT and business [5]. Meanwhile, two interesting observations were made. The first is that the set-up of a company's IT governance structure depends to a large degree on its environment, which means that there is no one way of doing it right [6]. A more dynamic environment requires a more flexible IT governance structure, for example. The second observation concerns the importance of the perceptions that the IT organization and the rest of the company have of one another [6]. These perceptions play a serious role in the realization of a good governance structure. Communication is, therefore, an important success factor – but not necessarily something at which IT professionals excel. And so it is all the more important to achieve a good alignment between business and IT.

Finally, the importance of accountability was recognized [7]. In this area, laws and regulations clearly influence the way in which IT governance is implemented. Financial scandals such as that involving the American utility company Enron have caused authorities everywhere to issue stricter laws and regulations, both on a national scale and internationally. Of course, IT governance is influenced by these developments too, since all these laws and regulations aim to increase companies' financial transparency, and to allow senior managers to be held personally responsible for any transgressions. So, IT Governance definition has been illustrated in

Table 1: Definitions of IT governance

Researchers	**IT governance definition**
Brown and Magill (1994)	IT governance describes the locus of responsibility for IT functions [].
Luftman (1996)	IT governance is the degree to which the authority for making IT decisions is defined and shared among management, and the processes managers in both IT and business organizations apply in setting IT priorities and the allocation of IT resources [].
Sambamurthy and Zmud (1999)	IT governance refers to the patterns of authority for key IT activities [].
Van Grembergen	IT governance is the organizational capacity by the board, executive

(2002)	management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT [].
Weill and Vitale (2002)	IT governance describes a firm's overall process for sharing decision rights about IT and monitoring the performance of IT investments [7].
Schwarz and Hirschheim (2003)	IT governance consists of IT-related structures or architectures (and associated authority patterns), implemented to successfully accomplish (IT-imperative) activities in response to an enterprise's environment and strategic imperatives [].
IT Governance Institute (2004)	IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives [].
Weill and Ross (2004)	IT governance is specifying the decision rights and accountability framework to encourage desirable behaviour in using IT [].

3. Available Standards

At a very broad level, organizations can approach governance on an ad hoc basis and create their own frameworks, or they can adopt standards that have been developed and perfected through the combined experience of hundreds of organizations and people. By adopting a standard IT governance framework, organizations may realize a number of benefits []. During the past two decades, a variety of standard IT governance frameworks and different assessment methods for evaluating IT impact and performance has emerged. In this section 17 tools are considered and evaluated. Some tools have developed into a set of guidelines, others into methods or best practices, and again others into de facto or de jure standards []. The reason for this listing and the subsequent evaluation is to obtain a comprehensive basis for assessing the case company's IT Governance. Also, the listing provides an interesting overview of implementation frameworks of IT Governance initiatives. Moreover, the listing shows the main differences between the tools and hereby how differently IT Governance initiatives may be pursued and adopted. Through a survey of literature the following 17 tools were found:

[8].

Table 1: Definitions of IT governance

Researchers	**IT governance definition**
Brown and Magill (1994)	IT governance describes the locus of responsibility for IT functions [9].
Luftman (1996)	IT governance is the degree to which the authority for making IT decisions is defined and shared among management, and the processes managers in both IT and business organizations apply in setting IT priorities and the allocation of IT resources [10].
Sambamurthy and Zmud (1999)	IT governance refers to the patterns of authority for key IT activities [11].
Van Grembergen (2002)	IT governance is the organizational capacity by the board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT [12].
Weill and Vitale (2002)	IT governance describes a firm's overall process for sharing decision rights about IT and monitoring the performance of IT investments [7].
Schwarz and Hirschheim (2003)	IT governance consists of IT-related structures or architectures (and associated authority patterns), implemented to successfully accomplish (IT-imperative) activities in response to an enterprise's environment and strategic imperatives [13].
IT Governance Institute	IT governance is the responsibility of the board of directors and executive

(2004)	management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives [14].
Weill and Ross (2004)	IT governance is specifying the decision rights and accountability framework to encourage desirable behaviour in using IT [15].

3. Available Standards

At a very broad level, organizations can approach governance on an ad hoc basis and create their own frameworks, or they can adopt standards that have been developed and perfected through the combined experience of hundreds of organizations and people. By adopting a standard IT governance framework, organizations may realize a number of benefits [16]. During the past two decades, a variety of standard IT governance frameworks and different assessment methods for evaluating IT impact and performance has emerged. In this section 17 tools are considered and evaluated. Some tools have developed into a set of guidelines, others into methods or best practices, and again others into de facto or de jure standards [17]. The reason for this listing and the subsequent evaluation is to obtain a comprehensive basis for assessing the case company's IT Governance. Also, the listing provides an interesting overview of implementation frameworks of IT Governance initiatives. Moreover, the listing shows the main differences between the tools and hereby how differently IT Governance initiatives may be pursued and adopted. Through a survey of literature the following 17 tools were found:

ITIL: Information Technology Infrastructure Library (ITIL) is the world-wide de facto standard in Service Management. ITIL provides a comprehensive, consistent volume of best practices drawn from the collective experience of thousands of IT practitioners around the world. ITIL focuses on critical business processes and disciplines needed for delivering high-quality services. Out of the ITIL framework, the British Standard BS15000 has emerged. BS15000 is the world's first standard for managing IT services. All activity is classified under two broad umbrellas, i.e. Service Management and Service Delivery. This approach defines IT quality as the level of alignment between IT services and actual business needs. As a result, organizations can mature their best practices without regard to specific technologies [18].

COSO: Committee of Sponsoring Organizations (COSO) defined internal control as a process, affected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in categories; Effectiveness and efficiency of operations, Reliability of financial reporting Compliance with applicable laws and regulations. Indeed COSO (1992) makes recommendations to management on how to evaluate, report, and improve control systems [19].

ISO 17799: The ISO 17799 or the counterpart of British Standard BS 7799 is a standard for information security including a comprehensive set of controls and best practices in information security. The standard is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce. Compliance with ISO 17799 and BS7799 ensures that an organization has established a certain compliance level for each of the ten categories covered, i.e. security policy, security organization, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance (ISO 2000, BS 2002) [20].

ISO/IEC 17799:2000: The Code of Practice for Information Security Management is an international standard, based on BS 7799-1. It is presented as best practice for implementing information security management [21].

ISO/IEC TR 13335: The technical report Guidelines for the Management of IT Security contains information on IT security management not only from the planning perspective, but also from the implementation and maintenance perspectives [22].

ISO/IEC 15408: Security Techniques—Evaluation Criteria for IT Security is used as a reference to evaluate and certify the security of IT products and services [23].

TickIT: TickIT provides a scheme for the certification of the software quality management system. It intends to improve the effectiveness of the quality management system and targets customers, suppliers and assurance professionals [24].

NIST 800-14: The special publication Generally Accepted Principles and Practices for Securing Information Technology Systems contains information for establishing a comprehensive IT security program [25,26].

ASL: Application Services Library (ASL) is a collection of best practice guidance for managing application development and maintenance. It is the public domain standard for application management, separate from the IT Infrastructure Library (ITIL), but linked to it in terms of adherence to standards for managing processes and providing a coherent, rigorous, public domain set of guidance. ASL is a part of the IT Service Management (ITSM) Library. ASL recognizes three types of control, i.e. functional, application and technical control. Where Information Technology Infrastructure Library (ITIL) is a generally accepted standard for organizing technical management, the Application Services Library (ASL) offers a framework for the organization of application management [27].

SAC: SAC defines the system of internal control, describes its components, provides several classifications of controls, describes control objectives and risks, and defines the internal auditor's role [28].

SAS70: SAS70 is an auditing standard designed to enable an independent auditor to evaluate and issue an opinion on a service organization’s controls. Statement on Auditing Standards, No. 70 (SAS70) for Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A SAS70 audit (www.sas70.com) is widely recognized, because it represents that a service organization has been through an in-depth audit by an independent accounting and auditing firm of their control activities, which generally include controls over information technology and related processes. Organizations must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. Control objectives and control activities should also be organized in a manner that allows the user auditor and user organization to identify which controls support the assertions in the user organization’s financial statements, e.g. existence, occurrence, completeness, valuation, etc.

SASs: provide guidance to external auditors regarding the impact of internal control on planning and performing an audit of an organization's financial statements [29,30].

COBIT: Control Objectives for Information and Related Technology (COBIT) has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices. The tools include: (1) Performance Measurement elements, i.e. outcome measures and performance drivers for all IT processes, (2) A list of Critical Success Factors (CSF) that provides succinct, non-technical best practices for each IT process, and (3) Maturity Models to assist in benchmarking and decision-making for capability improvements [31].

The CobiT Framework defines and explains a methodology for controlling and assessing the effectiveness, efficiency, integrity, reliability, availability, compliance, and confidentiality of IS resources. In a standard structure within a specific business requirement, which requires control and utilizes certain information system resources; CobiT identifies the specific controls and how to assess them .COBIT is a breakthrough Information Technology (IT) Governance tool that helps in understanding and managing the risks associated with Information and related Technology. COBIT is an authoritative, up-to date, international set of generally accepted IT control objectives for day-to-day use by business managers, users of IT and IS auditors. The COBIT Framework defines and explains a methodology for controlling and assessing the effectiveness, efficiency, integrity, reliability, availability, compliance, and confidentiality of IS resources. In a standard structure within a specific business requirement, which requires control and utilizes certain IS resources; COBIT identifies the specific controls and how to assess them [10].

4. Importance of COBIT

The Information Systems Audit and Control Foundation (ISACF) recently developed the Control Objectives for Information and related Technology (COBIT) to serve as a framework of generally applicable and IS security and control practices for information technology control. This COBIT standard allows management to benchmark the security and control practices of IT environments, allows users of IT services to be assured that adequate security and control exists, and allows auditors to substantiate their opinions on internal control and to advise on IT security and control matters. The completed phase of the COBIT project provides an Executive Summary, a Framework for control of IT, a list of Control Objectives, and a set of Audit Guidelines. Future phases of the project will provide self-assessment guidelines for management and identify new or updated control objectives through incorporations of other identified global control standards [31]. Plus, add control guidelines and identify key performance indicators. COBIT adapted its definition of control from COSO, its definition of an IT control objective from SAC, and emphasizes the role and impact of IT control as they relate to business processes; also, classifies IT resources as data, application systems, technology, facilities, and people [5].

COBIT combines the principles embedded in existing reference models in three broad categories: quality, fiduciary responsibility and security. From these broad requirements, the report extracts seven overlapping categories of criteria for evaluating how well IT resources are meeting business requirements for information. These criteria are effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information. Based on analysis of the information technology infrastructure library (ITIL) IT management practices, a UK document, COBIT classifies IT processes into four domains. These four domains are:

Planning and organizing (PO): This domain covers a whole range of topics. Included are the strategy and tactics used by IT to achieve business objectives, strategy planning, strategy communication, strategy management, risk management, and resource management, which insures that the required technology infrastructure and human capital are in place [32].
Acquisition and implementation (AI): For IT to realize its strategy, it must identify, develop or acquire, and implement solutions to business processes. Additionally, it must manage the life cycle of existing systems through maintenance, enhancements, and retirements [32].

Delivery and support (DS): On its most basic level, IT delivers services to its customers (users). This domain concerns service and support issues including performance and security, and it also includes training [32].

Monitoring (M): All IT processes need to be regularly assessed for their quality and compliance with control requirements. The monitoring domain addresses management's oversight of the organization's control processes [32].

COBIT presents a framework of control for business process owners. Increasingly, management is fully empowered with complete responsibility and authority for business processes. Furthermore, includes definitions of both internal control and IT control objectives, four domains of processes and 32 high level control statements for those processes, 271 control objectives referenced to those 32 processes and audit guidelines linked to the control objectives.

Concerning importance of Cobit and considering measuring all of Financial, customer, process, and learning indexes, its parameters (PO, AI, DS, and M) will be used for classification the tools.

5. The IT Governance Tools Classification

Cause of the number of IT Governance tools and their different charachteristic; it is hard to select the best for an enterprise. All of 13 IT Governance tools which were described are classified based on COBIT parameters. Based on a servey research, all of IT Governances was evaluated thorough scoring in 1-10 range based on COBIT standard parameters (PO, AI, DS, and M).

Table 2 shows the result of IT Governance tools scoring which is compeleted by experts of IT Governance in Iran Telecommunication Research Center (ITRC).

Table 2: IT Governance scores

	PO	AI	DS	M
ITIL	3	5	9	0
COSO	7	5	6	0
ISO 17799	5	4	8	2
ISO/IEC 17799:2000	5	4	8	2
ISO/IEC TR 13335	4	2	4	2
ISO/IEC 15408	1	3	2	2
TickIT	1	5	0	2
NIST 800-14	5	5	8	2
ASL	3	5	9	0
SAC	8	2	8	3
SAS70	8	2	5	2
SASs	8	2	5	3
COBIT	8	5	10	3

IT Governance tools are classified to 4 group which in each group there is no diverse for applying in an organization. K-means analysis was runned with SPSS software with 4 cluster and method of iterated and classify method. As a result, all of the 13 standard were alassified in 4 groups that Table 3 shows the average of each parameter for each cluster of IT Governance tools.

Table 3: Final Cluster Centers

	Cluster			
	1	2	3	4
PO	5	8	1	7
AI	5	4	4	2
DS	8	9	1	5
M	1	3	2	2

Table 4: ANOVA analysis

	Cluster		Error		F	Sig.
	Mean Square	df	Mean Square	df		
PO	19.6	3	2.4	9	8.0	0.01
AI	4.8	3	0.9	9	5.5	0.02
DS	32.0	3	1.2	9	27.0	0.00
M	2.5	3	0.7	9	3.4	0.06

It means provided that an IT Governance tools have been selected from the cluster 2, the average scores of its charachteristis such as PO, AI, DS, and M are 8, 4, 9, and 3 which means all of the standards in this cluster are powerfull in DS and PO, normal in AI, and weak in M. So, according to theTable 3, selecting the best tools is so much easy and confident.

To make confidence of the result of classification, ANOVA analysisi was run that has been shown in

(The F tests should be used only for descriptive purposes because the clusters have been chosen to maximize the differences among cases in different clusters. The observed significance levels are not corrected for this and thus cannot be interpreted as tests of the hypothesis that the cluster means are equal).

To concluse,

Table 5 shows the sluster that each one of tolls are belong to it.

Table 5: Cluster Membership

IT Governance tools	**Cluster**
ITIL / COSO / ISO 17799 / ISO/IEC 17799:2000 / NIST 800-14 / ASL	1
SAC / COBIT	2
ISO/IEC 15408 / TickIT	3
ISO/IEC TR 13335 / SAS70 / SASs	4

As the intention is to investigate decision-making processes in the entire business system, only 13 tools are been candidated for further evaluation. However, the IT Governance Checklist does not lead to a sufficient comprehensive analysis, but it is valuable as an indicator for a pre-analysis of IT Governance selection. The IT Governance Review is a thorough analysis of the existing IT Governance arrangements and mechanisms in an organisation leading to a future design of IT Governance by addressing the insufficiencies of the current IT Governance structure. Based on the above findings an IT Governance can be selected considering the importance of PO, AI, DS, and M parameters from the relevent cluster.

6. Concluding Remarks

An IT governance framework helps boards and management understand the issues and strategic importance of IT, and assists in ensuring that the enterprise can sustain its operations and implement the strategies required to extend its activities into the future. It provides assurance that expectations for IT are met and IT risks are addressed. In summary, IT governance ensures that IT goals are met and IT risks are mitigated such that IT delivers value to sustain and grow the enterprise. In this paper the popular standards for the IT Governance have been introduced and evaluated based on the PO, AI, DS, and M parameters (the important parameters of COBIT standard). Inorder to select the best IT Governance standar, the selected standards have been classified in to 4 clusters. So, all of the allocated standards in each cluster had the same charachteristic in action. This classification ensure easy selection of IT Governance standard based on the

enterprise specific in PO, AI, DS, and M parameters. For futer work increasing the number of parameters for evaluating will be constructive. Also, use of fuzzy clustering for dominating thye vague charachterisitic aof the standards could lead us to better results.

Reference

1. "Defining IT governance" http://www.zdnet.com.au/insight/soa/IT_governance_is_it_the_answer_/_0,39023731,20271444,_00.htm
2. Brown, C. and Magill, S. (1994) Alignment of the IS Functions with the Enterprise: Toward a Model of Antecedents. Management *Information Systems Quarterly*, 18, 4 (1994), 371-404.
3. Luftman, J. Assessing (2000) IT-business alignment maturity. *Communications of the Association for Computing Machinery*, 4, 14 (December, 2000), 1-51.
4. Willcocks, L. and Fitzgerald, G. (1994) A business guide to outsourcing IT, London, *Business Intelligence*, 1994
5. Ward, J. and Peppard, J. (2002) *Strategic planning for Information Systems*, West Sussex, third edition, Wiley, 2002.
6. Agarwal, R. and Sambamurthy, Z. (2002) Principles and models for organizing the IT function. *Management Information Systems Quarterly Executive*, 1, 1 (2002), 1- 16.
7. Weill P. and Vitale M. (2002) *Place to space, migrating to eBusienss models*. Harvard Business School Press. Boston, Massachusetts, 2002.
8. Erik Beulen, Pieter Ribbers (2007), Control in outsourcing relationships: governance in action, *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007.
9. Brown, C. and Magill, S. (1994) Alignment of the IS Functions With the Enterprise: Toward a Model of Antecedents. *Management Information Systems Quarterly*, 18, 4 (1994), 371-404.
10. Luftman, J. (1996) *Competing in the Information Age*. Oxford, Oxford University Press, 1996.
11. Sambamurthy, V. and Zmud, R. (1999) Arrangements for information technology governance: a theory of multiple contingencies. *Management Information Systems Quarterly*, 23, 2 (1999), 261-290.
12. Van Grembergen W. (2002) Introduction to the minitrack: IT Governance and its mechanisms. *Proceedings of the 35th Hawaii International Conference on System Science* (HICSS), IEEE, 2002.
13. Schwarz, A. and Hirschheim, R. (2003) An extended platform logic perspective of IT governance: managing perceptions and activities of IT. *The Journal of Strategic Information Systems*, 12, 2 (July, 2003), 129-166.
14. IT Governance Institute. Board Briefing on IT Governance, 2nd edition, IT Governance Institute, 2004
15. Weill, P. and Ross, J. (2004), *IT governance*, Boston, Massachusetts, Harvard Business School Press, 2004.
16. Spafford, G. (2003). The Benefits of Standard IT Governance Frameworks. *IT Management*. April 22.
17. "International Standards Provide Guidance For IT Governance By John W. Lainhart IV, Partner, Pricewaterhouse Coopers"
18. Behr, K. & Kim, G. & Spafford, G. (2004). The Visible Ops Handbook: *Starting ITIL in 4 Practical Steps*. Information Technology Process Institute.
19. W .Van Grembergen, (2004) *Strategies for Information Technology Governance*, Idea Group Publishing, 2004.
20. Ma, Q. & Pearson, J.M. (2005). ISO 17799: Best Practices in Information Security Management? *Communications of the AIS*. Vol. 15, Article 32.
21. ISO IEC 17799, International Organization for Standardization (ISO), Code of Practice for Information Security Management, Switzerland, 2000
22. ISO IEC 15408, International Organization for Standardization (ISO), Evaluation Criteria for Information Technology Security, Switzerland, 1999
23. ISO TR 13334, International Organization for Standardization (ISO), Information Technology—Guidelines for the Management of IT Security, Switzerland, 1996 – 2001
24. TickIT: Guide to Software Quality Management System Construction and Certification, British Department of Trade and Industry (DTI), London, 1994
25. Common Criteria and Methodology for Information Technology Security Evaluation, CSE (Canada), SCSSI (France), BSII (Germany), NLNCSA (Netherlands), CESG (United Kingdom), NIST (USA) and NSA (USA), 1999
26. National Institute of Standards and Technology (NIST), An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, USA, 1996

27. Meijer, M. (2003). Application Service Library (ASL) and CMM. bITa Monitor – The journal of IT Alignment and Business IT Alignment, Vol. 1(1), March, pp. 21-26.
28. "A Comparison of Internal Controls: COBIT®, SAC, COSO and SAS 55/78", By Janet L. Colbert, Ph.D., CPA, CIA, and Paul L. Bowen, Ph.D., CPA
29. COBIT 3rd Edition: Framework, IT Governance Institute, Rolling Meadows, IL, USA, 2000
30. COBIT 3rd Edition: Management Guidelines, IT Governance Institute, Rolling Meadows, IL, USA, 2000
31. Lainhart IV, J.W. (2000). COBIT[TM]: A Methodology for Managing and Controlling Information and Information Technology Risks and Vulnerabilities. Journal of Information Systems, December.
32. "Maximizing IT Value: Portfolio Management Options" by Craig Symons with Mark Cecere, G. Oliver Young, and Natalie Lambert, March 29, 2005.