# IT Governance Auditing in Virtual Organizations

**Dr. Konstadinos Kutsikos**
Department of Business Administration
University of the Aegean
kutsikos@aegean.gr

**Dr. Michail G. Bekiaris**
Department of Business Administration
University of the Aegean
m.bekiaris@aegean.gr

***Abstract***

*The collapse of a number of high-profile firms (such as Enron, WorldCom, and Parmalat) acted as the shaking news that turned the focus upon Corporate Governance (defined as the total of operations and controls of an organization). The Sarbanes-Oxley Act of 2002 constituted a reaction against those facts by stressing out the significance of corporate controls and auditing. At the same time, new forms of corporate structure are emerging. Their key characteristic is their nature of interconnected and distributed business entities that collaborate for value creation.*

*It therefore becomes imperative to develop the right auditing framework in the context of such corporate structures. In this article, we describe our research findings from the first phase of development of our auditing framework. We initially describe current developments in Corporate and IT Governance and briefly focus on relevant IT Governance frameworks that are widely used, such as COBIT. We then analyze and explain current trends and developments in organizational structures; especially, the evolution from monolithic corporate structures to more distributed ones. Finally, the effects of this evolution on IT Governance are modeled through a new auditing framework. The latter aims to track changes to a number of auditing parameters and requirements that depict the aforementioned evolution path.*

Keywords: auditing, IT governance, virtual organizations, COBIT, financial statements

JEL Classification: M15, M40, O30

## Introduction

A key success factor of many modern organizations is their capability to exploit available information in their decision-making processes. The latter are thus increasingly dependant on the quality of information which, at the same time, is characterized by constant and dynamic flow.

As a result, there is an ever increasing level of corporate investments in information technology infrastructures of ever increasing complexity. Such complexity leads to risk exposure that could result in financial or moral damage or even damage of a

company's reputation and client base. Such risks can be internal or external threats, including unintentional mistakes, malicious attacks, malfunctions or other shortcomings.

Auditing is the discipline that that brings discipline to the above factors through rigorous frameworks and guidelines that: a) help auditors support their opinions in internal audits; b) help them define the minimum necessary auditing points; c) guide them in the management of internal audit; and d) provide them with standardized sources for the planning of an audit.

However, this well-defined environment is in a state of prolonged change due to two key developments: new legislation and evolving corporate structures.

First of all, a number of accounting scandals and the collapse of the likes of Enron and WorldCom turned the spotlight on Corporate Governance (defined as the total of operations and controls of an organization). The Sarbanes-Oxley Act of 2002 constituted the legislative movement that signalled the beginning of a new audit culture.

At the same time, new forms of corporate structure are emerging that are made possible because of data networks and internet technologies. A new business architecture, termed by a host of names like virtual organizations or business webs (Tapscott, 2004), is enabled by the Internet discontinuity. Its key characteristic is its nature of interconnected and distributed business entities that collaborate for value creation. Such an architecture can be defined as a system composed of suppliers, distributors, service providers, infrastructure providers, and customers that use the Internet for business communications and transactions. The main benefit is the potential for reducing search, coordination, contracting, and other transaction costs between firms.

It therefore becomes imperative to develop the right auditing framework in the context of corporate structures that are transformed by technological discontinuities of this kind. Such a framework should aim to minimize risk exposure while safeguarding the managerial and accounting benefits of IT investments.

In this article, we describe our research findings from the first phase of development of our auditing framework. We initially describe current developments in Corporate and IT Governance and briefly focus on relevant IT Governance frameworks that are widely used, such as COBIT. We then analyze and explain current trends and developments in organizational structures; especially, the evolution from monolithic corporate structures to more distributed ones. Finally, the effects of this evolution on IT Governance are modeled through a new auditing framework. The latter aims to track changes to a number of auditing parameters and requirements that depict the aforementioned evolution path.

## Corporate and IT Governance

There are several definitions of Corporate Governance from a number of authors and organizations. According to (Shleifer and Vishny, 1997), Corporate Governance deals with the ways in which suppliers of finance to corporations assure themselves of getting a return on their

investment. It can be also defined as the total of operations and controls of an organization (Fama and Jensen, 1983) or as an overall structured system of principles (Dey Committee, 1994; OECD, 1999) according to which an enterprise operates and is organized, managed and controlled. The purpose of this system is to ensure the promotion of an organisation's collective interest as well as the unimpeachable character of its procedures. The goal is to provide senior executives with accurate and timely information about the firm's internal and external environment.

While many laws, codes, committees and discussion groups have been working on corporate governance since decades, a series of extraordinary accounting scandals and the collapse of a number of high-profile firms (such as Enron, WorldCom, and Parmalat) acted as the shaking news that turned the focus upon Corporate Governance. The Sarbanes-Oxley Act of 2002 constituted a reaction against those facts that aimed at preventing any repetition of similar phenomena and stressed out the significance of corporate controls and auditing. It was the legislative key movement that signalled the beginning of a new audit culture. The Act includes a wide variety of measures that lay the foundations for a legislative approach of effective Corporate Governance by stressing out those issues that deal with control of financial information.

Many things have been written about the significance of the Sarbanes-Oxley Act and about internal audit in general. However, there are not many references to the significance of IT, even though financial reports are produced by IT systems. Such systems usually cover the input, authorisation, recording, execution and reporting of financial transactions. As such, they are directly related to the overall process of creating financial reports and should be assessed with the same attention paid to all important projects, according to the Sarbanes-Oxley Act (ITGI, 2006).

IT Governance is a responsibility of both Board of Directors and Executive Management. IT Governance (ITG) consists of the leadership, organizational structures and processes for planning and organizing, acquiring and implementing, delivering and supporting, and monitoring IT performance (ITGI, 2003; Schwarz and Hirschheim, 2003). Its goal is to help business executives ensure that a company's IT infrastructure and information flows: a) are aligned with the company's corporate goals, strategies and profitability measures; b) can be assessed for incurring risks and mitigating actions.

In fact, the responsibilities of both Board Directors and Executive Management regarding IT have evolved and become even more complicated. This evolution of responsibilities took place from the level of estimating the impact of specific technology issues within an enterprise to the level of IT governance as the main source for achieving business objectives (Trites, 2004). Both Board Directors and Executive Management should become aware of their evolving role in terms of IT Governance, since their tasks depend on the information they receive (Hardy, 2006).

**Control frameworks**

The need to strengthen IT Governance and closely relate it to Corporate Governance is assuming central role in today's business management (Shleifer et al, 1997; Van Grombergen, 2004). The Bank of

International Settlements (BIS) recommends that company directors should address IT as an integrated item of their strategic agendas and not as a support function of business strategy. Indeed, the majority of board members recognise the vital importance of IT Governance for their organisation as well as the significant negative effects that may derive form IT (violations, thefts, mistakes).

However, putting IT Governance into action remains a challenging issue for business executives and IT experts alike. In a 2001 survey by (PriceWaterhouseCoopers, 2001), almost two thirds of the surveyed members of Boards of Directors do not feel comfortable answering questions concerning IT. They further consider that these questions should only be directed to their CIOs and/or their IT departments. In a similar 2005 survey by (ITGI, 2006), almost three out of four companies do not examine IT-related risks on a regular basis. From the corporate managers' point of view, the reason for that should be sought in: a) difficult to comprehend technical descriptions of IT systems; b) mostly administrative/accounting approach to IT risks by business executives.

Beyond issues of understanding IT, organizational data moves between multiple business groups and IT systems on its way from initial transactions to the reports that senior executives must attest to. Attesting to the accuracy of the data requires confidence in accounting procedures and controls. Attesting to the confidence in IT systems that house, move and transform data requires confidence in the processes and controls for those IT systems.

Control frameworks have been trying to give an answer to these problems. In general, there are two categories of control models: business control models and IT control models.

The most well-known business control model is COSO. COSO Internal Control-Integrated Framework was published by the Committee of Sponsoring Organisations of the Treadway Commission, in order to define a framework that would improve the quality of financial statuses and ethics by means of an effective system of internal audit. The aim is to enable higher level employees to set appropriate internal controls for ensuring that a company's mission and targets for profit-making are achieved. The second COSO framework is COSO Enterprise Risk Management – Integrated Framework. It was published in order to assist enterprises to evaluate and improve risk management (effective identification, evaluation, risk management), while COSO ERM is the next step towards the expansion of the process "Added Value" of the Sarbanes–Oxley Act.

COBIT (Control OBjectives for Information and related Technologies) is an open standard published by the IT Governance Institute (ITGI) and the Information Systems Audit and Control Association (ISACA). It is an IT Governance framework built in part upon the COSO framework. COBIT was first published in 1996. COBIT 3 version, which was published in 2000, was the one that become widely known and was adopted by many companies. COBIT 4 was published in 2005.

COBIT helps business managers bridge the gap between control requirements, technical issues and business risks. A recent study by (ITG/PriceWaterhouseCoopers, 2006) showed that:

- The awareness and knowledge of COBIT has increased from 18% in 2003 to 27% in 2006. In addition, one out of seven executives surveyed said that they have a very good knowledge of that framework.
- The application of COBIT, according to those asked, is not an easy procedure and must be adapted to a company's particularities.
- One out of ten companies covered in the study use the COBIT framework. In addition, one out of three of the surveyed companies are "secret" users of COBIT - they either use parts of COBIT or use it as a foundation for their internally developed IT Governance framework.
- Almost half of COBIT users regard it as an important tool for IT Governance.

In terms of its capabilities, COBIT helps business managers have end-to-end control on IT through:

- Maturity models, for evaluating the current state of IT Governance in their organizations and benchmark it against best-practice principles and standards.
- Critical success factors, for determining key drivers of control on IT processes.
- Key goal/performance indicators, for assessing whether an IT process has accomplished relevant business demands.
- Activity domains, categorized as: a) plan and organize; b) acquire and implement; c) deliver and support; d) monitor and evaluate.

COBIT deals mainly with what should be done and not with how it should be done. For this reason, it is necessary to supplement COBIT by other IT systems security standards. Such a framework is not restrictive nor is it always the same, since it is supplemented by other processes and systems, while at the same time it keeps changing (Broderick, 2006). Likewise, it does not expand analytically to technical issues regarding IT systems themselves.

## Corporate Structures and IT Governance

As Corporate and IT Governance become established practices, Boards of Directors are pressed to undertake an increasing number of auditing tasks. The latter can be grouped into two key supervision categories: a) Design of disclosure controls and procedures and internal control over financial reporting; b) Evaluation of effectiveness of such disclosure controls and procedures, especially as they pertain to the integrity of the company's management information systems.

These tasks are well understood by auditing experts, as they have been repeatedly executed and refined within the classic organizational structure exhibited by the majority of enterprises: monolithic, vertically integrated firms.

This fairly close link between auditing and organizational structures may face a challenging future due to technological discontinuities, such as Internet-related technologies. The latter may help (or even force) executives identify new opportunities in terms of how to best allocate their resources and thus define organizational (and auditing) boundaries accordingly.

Indeed, over the past decade, a clear business trend is emerging, indicating a move away from large, rigid enterprises and well-

established supply chains. Instead, companies increasingly focus on their core competencies, while engaging in flexible alliances for supplementing their strengths and exploiting specialized expertise of other firms. Examples abound, across different industries:

- in the automotive industry, with traditionally strong supplier-OEM relationships, speed to market leads to demand for flexibility in supply chain configurations. As a result, Mercedes-Benz does not build its own E-Class cars; Magna Corporation does the work, including final assembly
- in knowledge-intensive industries (e.g. software engineering, pharmaceutical research), it is almost typical nowadays to find freelancers, small firms and specialized enterprises (onshore or offshore) to form project-specific coalitions for creating new products and services. Tom Siebel, of Siebel Systems Inc., the software maker, claims that such a virtual organization is the most important element in Siebel's success: the company has 8,000 people on payroll, but more than 30,000 people work for Siebel
- in relatively new industry sectors that are technology-intensive (e.g. biotechnology), innovation is achieved by many small research-based companies engaging in co-opetitive relationships that require flexible, ad-hoc and temporary cooperation.

In order to describe this evolution of organizational structures, a number of terms have been coined, such as adhocracy (Mintzberg, 1980), cluster organization (Mills, 1991), network organization (Imai & Itami, 1984), and organizational marketplace (Williamson, 1975). All these concepts share certain common characteristics, like flatter hierarchies, dynamic structures, empowerment of individuals, high esteem of individuals' capabilities, intellect and knowledge.

Despite the proposed new models, the basic duality between a hierarchical (bureaucratic) and a networked structure remains. In (Nonaka & Takeuchi, 1995), the authors argue that what is necessary for knowledge-driven organizations today is a smart combination of both. They propose the concept of the hyperlinked organization, which is able to maximize corporate-level (hierarchical) efficiency and local flexibility (networked teams) as it grows in scale and complexity while maintaining its basic capability to create value.

The implications of the above trends for organizations have led to a proliferation of adjectives applied primarily to enterprises, among others, the agile enterprise, networked organization, virtual company, extended enterprise, knowledge enterprise (Nonaka & Takeuchi, 1995), learning organization (Senge, 1990), ambidextrous organization (O'Reilly & Tushman, 2004). The definitions all have their nuances, deriving from the emphasis on one or another combination of the aspects above. Ultimately, however, they all point to the need to respond to the changing landscape of the digital economy in dynamic and innovative ways.

This evolution of organizational structures into more distributed and collaborative entities is fueled by relevant technological innovations, such as web services and the semantic web. (Wen et al., 2005) used web robots to discover the latest knowledge on the Internet for better service of collaborative design. Furthermore, XML is used to make this system more efficient. Extensive work has been carried out to provide solutions for collaborative and distributed product development. (Li & Qiu, 2006) reviewed related works from three

aspects: a) visualization-based collaborative systems; b) co-design collaborative systems; and c) concurrent engineering-based collaborative systems. Based on the review of 130 cases, they concluded that the major issues for future collaborative system development are as follows:

- integration of various collaborative manners and systems
- security and interoperability of collaborative systems
- effective sharing of knowledge and information, which includes financial information and risk management procedures.

Collaboration between partners in a virtual organization from a wide variety of domains will result in the need to share knowledge from varied sources, with different data types, file formats and software tools. To cope with this, (Mostefai et al, 2005) proposed an ontology-based approach to enable semantic interoperability. The case study proves the effectiveness of ontologies in collaborative product development to support the product data exchange and information sharing. For interoperability to be achieved effectively it is essential that the semantic definitions of the knowledge objects, processes, contexts and relationships are defined based on a mathematically rigorous ontological foundations (Lin & Harding, 2007). Much current work utilizes the Web Ontology Language for the representation of semantic objects, but this has a very limited capability in terms of process definition. Similarly, the Process Specification Language has a strong process representation capability but is weak in its representation of objects. Researchers are therefore increasingly identifying the need for heavyweight ontologies and improved knowledge formalism (Young et al., 2007).

## The Auditing Perspective

Bringing together the concepts of the previous sections may prove to be a significant challenge for auditors enforcing IT Governance principles and directives within a virtual organization structure. The role of such auditors may need to expand in order to address new forms of business and IT risks that will require proper checks and controls for their containment. For example, the need for IT systems interconnection and integration in a virtual organization may by itself be a very complex and continuous activity. Both the implementation and operation of such an activity will need to be monitored, tested and acted upon discrepancies in order to ensure that information flows (especially financial) satisfy typical control objectives (accuracy, validity, compliance).

Thus, the relationship between IT Governance, virtual organizations and auditing will need to be defined at multiple levels:

- on the financial side, the nature of evidence and the way it is accumulated in such a distributed environment of business entities may need to be altered. In addition, timing of accumulation may need to become continuous, thus adding a grounded need to the arguments of (Percy, 1997). These may, in turn, lead to another cycle of changes in the IT infrastructure of an organization, with potential changes in the flow of financial information
- on the operational side, a number of IT and business processes will need to be reengineered to account for cross-entity involvement in their execution. Developing and monitoring control objectives for such processes may not be under the sole control of an organization

any more. This, in turn, necessitates new auditing approaches in process testing and correction of control problems.

In order to address these challenges for IT Governance and auditing within a networked corporate structure like a virtual organization, our research aims: a) to analyze how IT Governance auditing parameters and requirements change as an organization evolves from a monolithic corporate structure to a more distributed one; b) to provide relevant recommendations and solutions.

The first phase of our research is focused on identifying the auditing parameters whose changes we will follow in the aforementioned evolution path. In order to ensure a methodological approach, these parameters are investigated through three layers of our Auditing Framework: *Corporate Strategy*, *Processes*, and *Technology* (see figure 1).

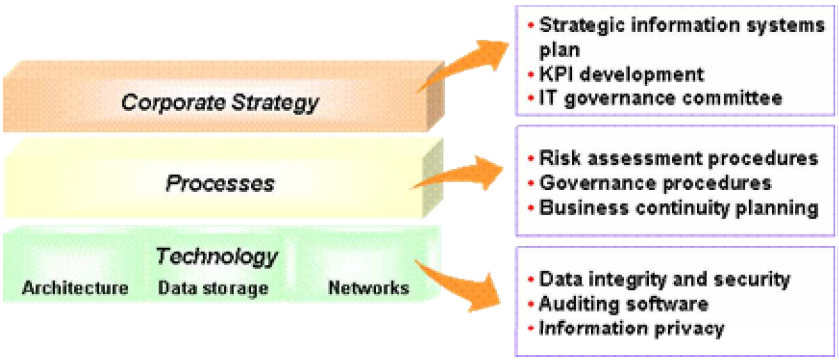


Figure 1. Our Auditing Framework

The common thread across these layers is the intrinsic delegation of partial or full control of certain operations/processes to partners. Hence, the common research question we face in each layer is how a specific auditing parameter can be controlled, given that its operation may depend on a number of external, independent entities/partners.

For example, in the Technology layer, auditors will need to be knowledgeable about the technical infrastructure underlying a virtual organization (see figure 2).

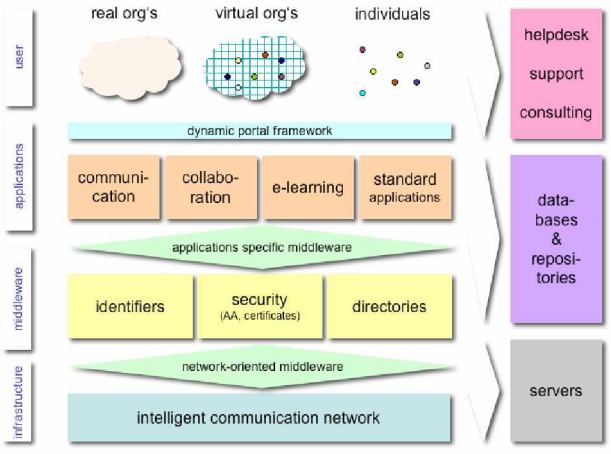


Figure 2. Typical technical infrastructure for virtual organizations

In such an infrastructure, information flows (financial or otherwise) through multiple entities create severe risks with regards to data integrity and security. New policies and procedures may need to be defined, enforced and monitored across a virtual organization. Beyond data integrity, information privacy may be jeopardized in such a distributed business environment. Policies may need to be agreed between partners but enforcement may further necessitate cooperation among auditors (internal or external).

Focusing on the security aspects, auditors should be able to test compliance against IT governance directives relevant to different policies. Policies for virtual organizations can cover almost every aspect of the virtual organization including statements of its purpose, its day-to-day operation and what is expected of various members (in terms of both resources and users). We divide virtual organization (VO) policies into three categories:

- VO-wide operational policy
- VO policy on resources
- VO policy on users.

Regarding VO-wide operational policies, they consist of statements about the intended operational state of the virtual organization - as a whole and not any single site or service. In other words, this type of policy describes the distribution of resource utilization across the whole virtual organization. For example, a policy that states “the compute load of the virtual organization is to be divided equally among all member sites” describes the virtual organization’s intended steady-state. Other policies might include:

- All work is to be performed on large queuing systems from 9 am – 5 pm and on PC clusters after hours.
- 75% of the virtual organization’s data will be stored in the virtual organization archive. The remaining 25% will be evenly distributed among partners.

Organizations can control security policies for the resources they own, but it is often difficult to map some of the social and political arrangements that are associated with shared resources in a virtual organization. Policy changes on one of the resources of the virtual organization may indirectly affect the remaining. Timely detection of such changes and taking adequate measures to notify concerned parties and rectify them is going to be a key task for the next generation of auditors.

## Future Research

The above research findings are the results of the first phase of our ongoing research initiative on corporate governance and organizational transformations. There are several directions we aim to follow in order to fully develop our aforementioned framework.

We are currently focusing on expanding the quantitative side of our research by developing relevant corporate/IT governance indices and measures. To that extent, a survey is under way, targeting the collection of data for a number of variables per organization that are significant to our frameworks:

- Corporate structure
- Corporate strategy
- Current corporate/IT governance infrastructure
- Current auditing infrastructure.

We expect that a thorough analysis of the survey findings will help us further clarify the role of the parameters that control our auditing framework.

## Conclusions

Boards of Directors are increasingly finding themselves functioning in a business environment that is constantly changing. Corporate structures are now moving from a vertical integration norm to a more distributed and collaborative way of operating. In such an environment, business factors like strategies, operations and risks will need to be shared among partner companies.

Our auditing framework is part of a research effort to analyze, understand, and recommend directions to the ITI Governance auditing community on how to address the aforementioned business factors within a virtual organization setting. Our framework is designed to track changes to a number of auditing parameters and requirements that depict an evolution path from monolithic to distributed corporate structures. We eventually hope to turn it into a tool that will enable IT Governance Auditors for virtual organizations to:

- have a holistic view of auditing within such a business setting;
- provide expert opinions in internal audits;
- define minimum necessary auditing points; and
- design best-of-breed activities for managing an audit within such new corporate structures.

## Acknowledgements

The authors would like to thank Mr. George Mallikourtis, CISA, CISM, and the anonymous reviewers for their helpful comments on an earlier version of this paper.

## References

Broderick, J.S., 2006, "ISMS, security standards and security regulations", *Information Security Technical Report (II)*, pp.26-31.

Dey Report, 1994, "Where were the Directors?" Dey Committee, Toronto Stock Exchange.

Fama E. and M. Jensen, 1983, "Separation of Ownership and Control", *Journal of Law & Economics*, (26), 301-325.

Hardy, G., 2006, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges", *Information Security Technical Report (II)*, 55-61.

Imai, K. and H. Itami, 1984, "Interpenetration of Organization and Market", *International Journal of Industrial Organization,* (2), 285-310.

ITGI and PriceWaterhouseCoopers, 2006, "IT Governance Global Status Report", Information Technology Governance Institute and Price Waterhouse Coopers.

ITGI, 2006, "Serving IT Governance Professionals, Survey Results 2005, Information Technology Governance Institute.

Li, W. D. and Z.M. Qiu, 2006, “State-of-the-art technologies and methodologies for collaborative product development systems" *International Journal of Production Research*, (44), 2525-2559.

Lin, H. K., J.A. Harding and P. C. Teoh, 2005, "An inter-enterprise semantic web system to support information autonomy and conflict moderation", *Journal of Engineering Manufacture*, (219), 903-911.

Mills, D.Q., 1991, "Rebirth of the Corporation", New York: John Wiley & Sons.

Mintzberg, H., 1980, "Mintzberg on Management: Inside our Strange World of Organizations", New York: The Free Press.

Mostefai, S., A. Bouras, and M. Batouche, 2005, “Effective Collaboration in Product Development via a Common Sharable Ontology”, *International Journal of Computational Intelligence*, 2:1.

Nonaka, I. and H. Takeuchi, 1995, "The Knowledge-Creating Company. How Japanese Companies Create the Dynamics of Innovation", New York: Oxford University Press.

O’Reilly, C.A., and M.L. Tushman, 2004, "The Ambidextrous Organization", Harvard Business Review, April 2004, 74-81.

Percy, J.P., 1997, "Auditing and Corporate Governance - a Look Forward into the 21st Century", *International Journal of Auditing* 1(1), 3–12.

PricewaterhouseCoopers, 2001, "Global Data Management Survey".

Schwarz, A. and R. Hirschheim, 2003, "An Extended Platform Logic Perspective of IT Governance: Managing Perceptions and Activities of IT", *Journal of Strategic Information Systems*, 12, 129-166.

Senge, P. M., 1990, "The Fifth Discipline: The Art and Practice of the Learning Organization", London: Random House.

Shleifer, A. and R.W. Vishny, 1997, "A Survey of Corporate Governance", *The Journal of Finance*, 52(2), 737-783.

Tapscott, D., 2004, "E-government in the 21st Century", Executive Series Report, New Paradigm Learning Corporation, Ontario, Canada.

Trites, G., 2004, "Director Responsibility for IT Governance", *International Journal of Accounting Information Systems*, 5, 89-99.

Van Grembergen W. and S. De Haes, 2004, "IT Governance and its Mechanisms", IT Governance Institute.

Wen Y., L. Tian, and B. Tong, 2005, "Knowledge Discovery Based on Web Robots in Collaborative Design", *Proceedings of the Fifth International Conference on Computer and Information Technology (CIT’05).*

Williamson, O.E., 1975, "Markets and Hierarchies: Analysis and Anti-Trust Implications", New York: The Free Press.

Young, R. I. M., A. G. Gunendran, A. F., Cutting-Decelle, and M. Gruninger, 2007, "Manufacturing Knowledge Sharing in PLM: a Progression Towards the Use of Heavy Weight Ontologies", *International Journal of Production Research*, 45(7), 1505 - 1519