Corporate governance of information technology

Information technology (**IT**) **governance** is a subset discipline of corporate governance, focused on information technology (IT) and its performance and risk management. The interest in IT governance is due to the ongoing need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders. It has evolved from The Principles of Scientific Management, Total Quality Management and ISO 9001 Quality management system.

Historically, board-level executives deferred key IT decisions to the company's IT management and business leaders. Short-term goals of those responsible for managing IT can be in conflict with the best interests of other stakeholders unless proper oversight is established. IT governance systematically involves everyone: board members, executive management, staff, customers, communities, investors and regulators. An IT Governance framework is used to identify, establish and link the mechanisms to oversee the use of information and related technology to create value and manage the risks associated with using information technology.

Various definitions of IT governance exist. While in the business world the focus has been on managing performance and creating value, in the academic world the focus has been on "specifying the decision rights and an accountability framework to encourage desirable behavior in the use of IT."[1]

The IT Governance Institute's definition is: "... leadership, organizational structures and processes to ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."[2]

AS8015, the Australian Standard for Corporate Governance of Information and Communication Technology (ICT), defines **Corporate Governance of ICT** as "The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation."

Contents

Background

The discipline of information technology governance first emerged in 1993 as a derivative of corporate governance and deals primarily with the connection between an organisation's strategic objectives, business goals and IT management within an organization. It highlights the importance of value creation and accountability for the use of information and related technology and establishes the responsibility of the governing body, rather than the chief information officer or business management.

The primary goals for information and technology (IT) governance are to (1) assure that the use of information and technology generate business value, (2) oversee management's performance and (3) mitigate the risks associated with using information and technology. This can be done through board-level direction, implementing an organizational structure with well-defined accountability for decisions that impact on the successful achievement of strategic objectives and institutionalize good practices through organizing activities in processes with clearly defined process outcomes that can be linked to the organisation's strategic objectives.

Following corporate governance failures in the 1980s, a number of countries established codes of corporate governance in the early 1990s:

- Committee of Sponsoring Organizations of the Treadway Commission (USA)
- Cadbury Report (UK)
- King Report (South Africa).

As a result of these corporate governance efforts to better govern the leverage of corporate resources, specific attention was given to the role of information and the underpinning technology to support good corporate governance. It was soon recognized that information technology was not only an enabler of corporate governance, but as a resource, it was also a value creator that was in need of better governance.

In Australia, the AS8015 Corporate Governance of ICT was published in January 2005. It was fast-track adopted as ISO/IEC 38500 in May 2008.[3]

IT governance process enforces a direct link of IT resources & process to enterprise goals in line of strategy. There is a strong correlation between maturity curve of IT governance and overall effectiveness of IT.

Problems

IT governance is often confused with IT management, compliance and IT controls. The problem is increased by terms such as "governance, risk and compliance (GRC)" that establish a link between governance and compliance. The primary focus of IT governance is the stewardship of IT resources on behalf of various stakeholders whose ranking is established by the organisation's governing body. A simple way to explain IT governance is: *what* is to be achieved from the leveraging of IT resources. While IT management is about "planning, organizing, directing and controlling the use of IT resources" (that is, the *how*), IT governance is about creating value for the stakeholders based on the direction given by those who govern. ISO 38500 has helped clarify IT governance by describing a model to be used by company directors.

While directors are responsible for this stewardship it is not unusual that will delegate this responsibility to management (business and IT) who are expected to develop the necessary capability to deliver the performance expected. Whilst managing risk and ensuring compliance are essential components of good governance, the primary focus is on delivering value and managing performance (i.e. "Governance, Value delivery and Performance management" (GVP)).

Frameworks

There are quite a few supporting references that may be useful guides to the implementation of information and technology (IT) governance. Some of them are:

- AS8015-2005 Australian Standard for Corporate Governance of Information and Communication Technology. AS8015 was adopted as ISO/IEC 38500 in May 2008

- ISO/IEC 38500:2015 Corporate governance of information technology,[4] (very closely based on AS8015-2005) provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organizations' use of IT. ISO/IEC 38500 is applicable to organizations from all sizes, including public and private companies, government entities, and not-for-profit organizations. This standard provides guiding principles for directors of organizations on the effective, efficient, and acceptable use of Information Technology (IT) within their organizations.
- COBIT5 is regarded as the world's leading IT governance and control framework. COBIT5 provides a reference model of 37 IT processes typically found in an organization. Each process is defined together with process inputs and outputs, key process activities, process objectives, performance measures and a maturity model. ISACA published COBIT5 in April 2012 as a "business framework for the governance and management of enterprise IT". COBIT5 consolidates COBIT4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with TOGAF and ITIL.
- IGPMM- The Information Governance Process Maturity Model [5] depends on maturing 22 processes that help identify – and improve the management of – information value, cost and risk. CGOC updated the IGPMM in March 2017.[6] The processes reflect the needs of the key information stakeholders, including legal, records information management (RIM), privacy and security, lines of business and IT. The maturation for each business process moves through four stages:
  - Stage 1: Ad hoc and inconsistent
  - Stage 2: Siloed and manual
  - Stage 3: Siloed, consistent and instrumented
  - Stage 4: Integrated, instrumented and optimized

Other frameworks offer a partial view on IT Management & IT Governance Processes:

- CMM - The Capability Maturity Model: focus on software engineering
- ITIL - Focus on IT Service management
- ISO/IEC 20000 - Focus on IT Service management
- ISO/IEC 27001 - Focus on Information Security Management
- ISO/IEC 27005 - Focus on Information Security Risk Management
- ISO/IEC 29148 and IREB - Focus on Requirement Engineering
- ISO/IEC 29119 and ISTQB - Focus on Software Testing

Non-IT specific frameworks of use include:

- PRINCE2 and PMBOK - Focus on Project Management
- ISO 22301 - Focus on Business Continuity
- The Balanced Scorecard (BSC) - method to assess an organization's performance in many different areas
- Six Sigma - Focus on quality assurance
- The Open Group Architecture Framework (TOGAF) - methodology to align business and IT, resulting in useful projects and effective governance

Professional certification

- Certified in the Governance of Enterprise Information Technology (CGEIT) is a certification created in 2007 by ISACA. It is designed for experienced professionals, who can demonstrate

5 or more years experience, serving in a managing or advisory role focused on the governance and control of IT at an enterprise level. It also requires passing a 4-hour test, designed to evaluate an applicant's understanding of enterprise IT management. The first examination was held in December 2008.

- COBIT5 Foundation, COBIT5 Assessor and COBIT5 Implementation are certifications created in 2012 by ISACA.

See also

- Computer security
- Data governance
- Enterprise architecture
- Information governance
- Information technology management
- IT portfolio management
- IT service management
- Project governance
- Service governance

References

1. Weill, P. & Ross, J. W., 2004, *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*", Harvard Business School Press, Boston.
2. "Board Briefing on IT Governance, 2nd Edition" (http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf) (PDF). IT Governance Institute. 2003. Retrieved June 24, 2014.
3. Introduction to ISO 38500 (http://www.itsmf.nl/imagesfile/PRESENTATIES%20JC%2008%20tbv%20publicatie/Christophe%20Feltus%20Introduction%20to%20ISO%2038500%20v1_0.pdf)
4. [1] (http://www.iso.org/iso/pressrelease.htm?refid=Ref1135) Archived (https://web.archive.org/web/20081205091528/http://www.iso.org/iso/pressrelease.htm?refid=Ref1135) December 5, 2008, at the Wayback Machine
5. Smallwood, Robert F. (2018-10-01). *Information Governance for Healthcare Professionals: A Practical Approach* (https://books.google.com/books?id=7FFuDwAAQBAJ&q=cgoc+igpmm&pg=PT38). Taylor & Francis. ISBN 9781351339728.
6. "New IGPMM Essential in Confronting Data Challenges - Corporate Compliance Insights" (https://www.corporatecomplianceinsights.com/new-igpmm-essential-in-confronting-data-challenges/). *Corporate Compliance Insights*. 2017-03-03. Retrieved 2018-11-21.

Further reading

- Blitstein, Ron, 2012. "IT Governance: Bureaucratic Logjam or Business Enabler" (http://www.cutter.com/promotions/bitu1210.html), Cutter Consortium.
- Brown, Allen E. and Grant, Gerald G. (2005) "Framing the Frameworks: A Review of IT Governance Research," Communications of the Association for Information Systems: Vol. 15, Article 38.
- S. De Haes, and W. Van Grembergen, “Exploring the relationship between IT governance practices and business/IT alignment through extreme case analysis in Belgian mid-to-large size financial enterprises”, *Journal of Enterprise Information Management*, Vol. 22, No. 5, 2009, pp. 615–637.

- Georgel F., *IT Gouvernance : Maitrise d'un systeme d'information*, Dunod, 2004(Ed1) 2006(Ed2), 2009(Ed3), ISBN 2-10-052574-3. "Gouvernance, audit et securite des TI", CCH, 2008(Ed1) ISBN 978-2-89366-577-1
- Lutchen, M. (2004). *Managing IT as a business : a survival guide for CEOs.* Hoboken, N.J., J. Wiley., ISBN 0-471-47104-6
- Renz, Patrick S. (2007). "Project Governance." Heidelberg, Physica-Verl. (Contributions to Economics) ISBN 978-3-7908-1926-7
- Van Grembergen, W., *Strategies for Information technology Governance*, IDEA Group Publishing, 2004, ISBN 1-59140-284-0
- Van Grembergen, W., and S. De Haes, *Enterprise Governance of IT: Achieving Strategic Alignment and Value*, Springer, 2009.
- Wim Van Grembergen, and S. De Haes, “A Research Journey into Enterprise Governance of IT, Business/IT Alignment and Value Creation”, *International Journal of IT/Business Alignment and Governance*, Vol. No. 1, 2010, pp. 1–13.
- Weill, P. and Ross, J.W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results,* Boston, MA, Harvard Business School Publishing, ISBN 1-59139-253-5
- Wilkin, C.L. and Chenhall, R.H. (2010). A Review of IT Governance: A Taxonomy to Inform AIS, Journal of Information Systems, 24 (2), 107–146.
- Wood, David J., 2011. "Assessing IT Governance Maturity: The Case of San Marcos, Texas". Applied Research Projects, Texas State University-San Marcos. (This paper applies a modified COBIT framework to a medium sized city.) (http://ecommons.txstate.edu/arp/345)