

WHITEPAPER

SOFTWARE TOOLING FOR THE BEST PRACTICES OF IT GOVERNANCE

April 2004

Authors:

Menno Arentsen - Ernst and Young

Karel van der Poel - Mirror42

Contributors:

Jan van Bon - Inform IT

Harry Boonen – ISACA President of the Dutch Chapter

Pieter Goris – Westbury IT Services

Jos Mertens – WS-PlanIT

Paul Siemons - Metrific

Paul Wilkinson – Pink Elephant

This white paper is a product of the joint IT Governance project of:



Software tooling for the best practices of IT Governance

Introduction

The importance of Information Technology in organizations has become more and more critical in the past decades. It is hard to imagine a fortune 2000 company without email and communication systems, or ERP and CRM systems. These days, it is almost impossible for many organizations to operate if IT is failing. And when major IT projects are not delivered on time this could result in serious risks of jeopardizing the future or the entire organization.

As a result of these developments, being *in control* of the IT environment has become very important for organizations, but complex at the same time. This is the situation that led to the introduction of IT Service Management. IT Service Management enables the enterprise in controlling the quality of her IT processes, resulting in measurable and controllable performance of IT services, like corporate email, network facilities and desktop environments.

Another important development is IT Portfolio Management. With IT Portfolio Management organizations can manage the overall positive Return on Investment, when managing an enterprise portfolio of IT projects.

However, organizations are being pressed to prove that they are in control of all business processes. And with IT being an integral part of almost all business processes, this forces organizations to get their IT activities more in line with the business goals and the business risks.

Gartner reports that demonstrating the added value of IT and providing IT guidance to the board are two of the top priorities, cited by CIO's.

Recent events regarding Corporate Governance – the Sarbanes Oxley Act

The considerable number of scandals on the stock market (Enron, Worldcom, Xerox, Tyco) has reduced the trust in the American capital market. The United States has responded strongly on these developments by introducing a new law: the Sarbanes Oxley act. The Sarbanes Oxley act puts the responsibilities, regarding governing organizations, in place, especially the responsibilities of the audit committee.

The legislator hopes to recover trust and enlarge transparency by this. The aim is to create a clear division in responsibilities between the supervisory bodies (internal and external) and management, not only in the financial field, but also regarding being in control of the organization. The essence of the act is good Corporate Governance. IT Governance is an integral part of.

Corporate Governance a definition

Many definitions exist for Corporate Governance. A clear definition has been drawn up by the Organization for Economic Co-operation and Development (OECD, 1998). Corporate Governance regards a framework which focuses on the rights, roles and equitable treatment of shareholders; disclosure and transparency; and the responsibilities of the board. The Governance framework should ensure sound strategic guidance of the company, for effective monitoring of management by the board, and for the board to be accountable for the company and to the shareholders. Among the board's responsibilities are reviewing and guiding corporate strategy, setting and monitoring achievement of management's performance objectives, and ensuring the integrity of the organization's systems.

Governance of IT: critical for *good* Corporate Governance

In 1987 the report of the Treadway Commission (National Commission on Fraudulent Financial Reporting) was published in the United States in which it was recommended to develop a common frame of reference of Internal Control. In 1992 the COSO report was published in the United States and in the same year, in the United Kingdom, the Cadbury Commission published 'The Financial Aspects of Corporate Governance' and the supplement 'Code of Best Practice'. This report was followed with the Guidance of Criteria on Control (1994) in Canada, which was inspired by COSO. After this many reports were written in different countries (e.g. Australia, South Africa, France and the Netherlands). Generally most countries have used the ideas of COSO and incorporated them in their own reports.

These developments call for a framework that goes further than IT Service Management and IT Portfolio Management: there is a need for an IT Governance framework.

In this whitepaper we will provide some insight in 'CobiT', the best practice IT Governance framework, and in the type of tools that can be used to implement such a framework.

IT Governance

While governance developments have been driven primarily by the need for transparency on enterprise risks and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT Governance. In the past, boards have seldom been involved in IT issues; most of the time they were only involved when IT problems threatened the viability of the business.

Nowadays IT is critical to the success of most large- and medium-sized organizations around the world, and even a good number of small businesses, unlike 10 years ago when IT played a much less critical role in organizations. IT now is essential for managing transactions, information and knowledge, required to initiate and sustain economic and social activities. These activities increasingly rely on globally cooperating entities to be successful. In many organizations, IT has become an integral part of the business and is fundamental to support, sustain and grow the business.

Figure 1 shows how Corporate Governance relates to IT Governance and what the role of IT is in activities that take place in an organization.

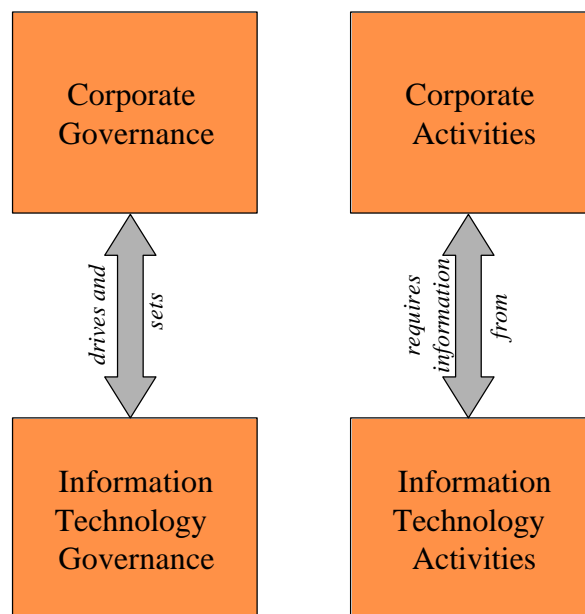


Figure 1. Organization versus IT

Executive management needs to have an appreciation for and a basic understanding of the risks and constraints of IT to provide effective direction and adequate controls. Boards and executive management need to extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies

and objectives. IT Governance is not an isolated discipline. It must become an integral part of overall Enterprise Governance.

From this it is clear that IT Governance, like most other governance activities, intensively engages both board and executive management in a cooperative manner. However, due to complexity and specialization, this governance layer must rely heavily on the lower layers in the enterprise to provide the information needed in its decision-making and evaluation activities. To have effective IT Governance in the enterprise, the lower layers need to apply the same principles of setting objectives, providing and getting direction, and providing and evaluating performance measures. As a result, good practices in IT Governance need to be applied throughout the enterprise.

The CobiT framework: a tool for implementing IT Governance

Currently just one internationally recognized tool exists for implementing IT Governance as a critical element of - not isolated from - Corporate Governance and which adds the component of focus on the alignment between the business and IT strategies. This tool is a framework called CobiT (*Control Objectives for Information and related Technology*). CobiT is developed by the IT Governance Institute and is trademarked by ISACA (Information Systems Audit and Control Association).

CobiT is a proven best practice that has been used by organizations like Philips, the ING Bank, the House of Representatives and ABSA, to ensure that IT resources are aligned with an enterprise's business objectives, and that services and information meet quality, fiduciary and security needs.

The CobiT framework consists of a set of 34 high-level *Control Objectives*. These 34 Control Objectives are grouped into four domains: Planning & Organization, Acquisition & Implementation, Delivery & Support, and Monitoring. By addressing these 34 high-level Control Objectives, the business process owner can ensure that an adequate control system is provided for the entire IT environment.

Figure 2 provides an overview of the CobiT domains and processes. It shows CobiT as a framework tool to realize IT Governance which is in line with business objectives.

Corresponding to each of the 34 high-level Control Objectives is an additional *Audit Guideline*¹, enabling the review of IT processes against CobiT's 318 recommended detailed Control Objectives to provide management assurance and/or advice for improvement.

The *Management Guidelines*, CobiT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT Governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organizational goals, for monitoring performance within each IT process and for benchmarking organizational achievement.

¹ Source: Descriptions taken from the CobiT executive summary. CobiT is developed by the IT Governance Institute and is trademarked and maintained by ISACA. (The Information Systems Audit and Control Association)

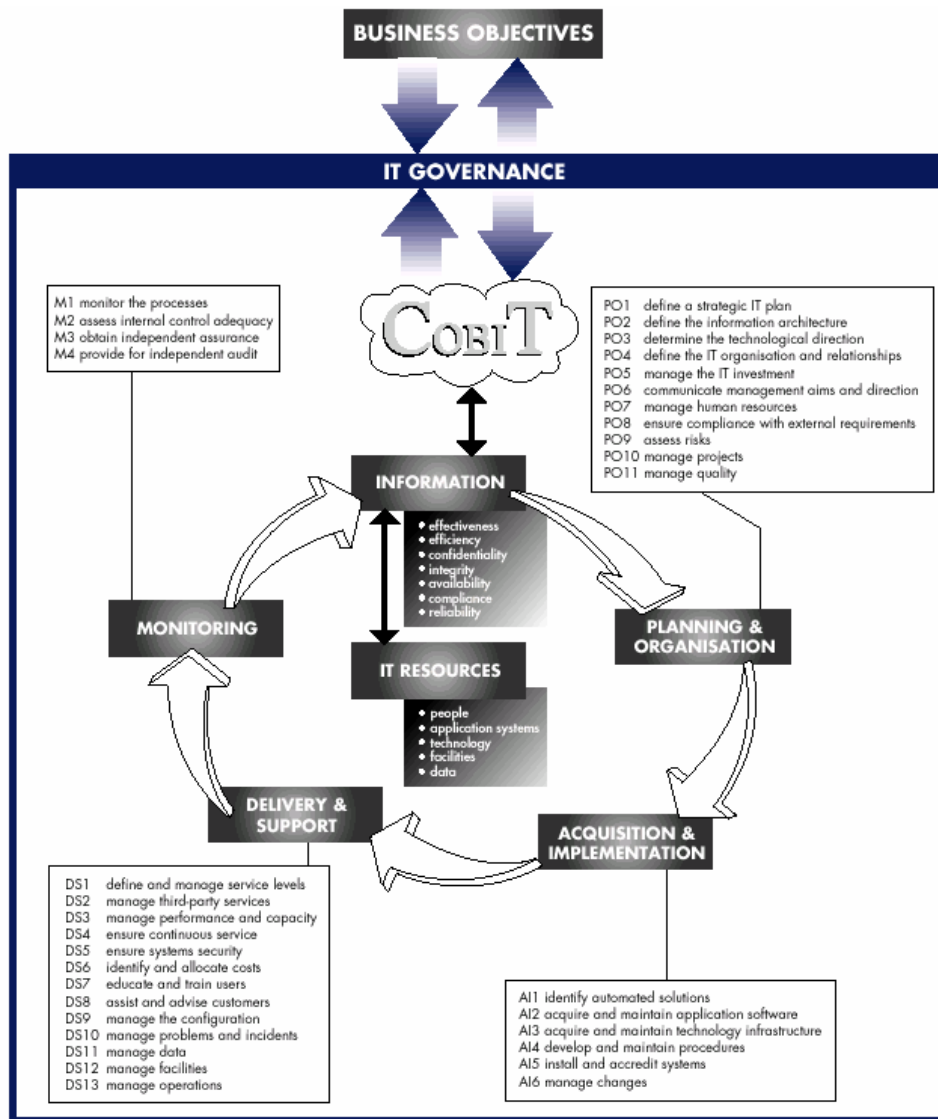


Figure 2. The CobiT framework (source ITGI)

Specifically, CobiT provides:

- **Maturity Models** for control over IT processes, so that management can map where the organization is today, where it stands in relation to the best-in-class in its industry and to international standards, and where the organization wants to be;
- **Critical Success Factors**, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes;
- **Key Goal Indicators**, which define measures that tell management - after the fact - whether an IT process has achieved its business requirements;
- **Key Performance Indicators**, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

CobiT also contains an *Implementation Tool Set* that provides lessons learned from those organizations that quickly and successfully applied CobiT in their professional environments. It has two particularly useful tools - *Management Awareness Diagnostic* and *IT Control Diagnostic* - to assist in analyzing an organization's IT control environment.

Implementing CobiT in the existing organization

Legitimate questions regarding the implementation of CobiT could be:

- “If IT Governance is conditional for having good Corporate Governance and if CobiT is the only internationally recognized framework for IT Governance, than what is the impact on the organization when I want to implement the CobiT framework?”
- “What about processes and tools I already have implemented in my organization?”
- “Do I have to start implementing processes and tools all over again?”

The general answer to these questions is “No”. When CobiT was developed, best practices were incorporated in the framework.

For example: most organizations have been focusing on implementing IT Service Management processes to be in control of IT. Generally they have done this by implementing ITIL and ITIL-like best practices. The good news is that the principles behind the CobiT and ITIL frameworks are consistent. CobiT provides a set of key goal and performance indicators, and critical success factors for each of its processes. These add value to ITIL because they establish the basis for managing the ITIL processes. Many of the CobiT processes - particularly those in the delivery and support domain, such as DS1, DS3, DS4, DS8, DS9 and DS10 - map well onto one or more ITIL processes, such as Service Level, Configuration, Problem, Incident, Release, Capacity, Availability or Financial Management. Similarly, the AI6 Change Management process maps well onto ITIL's Change Management process and other supporting processes, such as Release Management.

In June 2002, Gartner Group published a report with the title: “Combine CobiT and ITIL for Powerful IT Governance”. In this report the authors state: “CobiT is a complementary framework to ITIL. Enterprises that wish to put their ITIL program into the context of a wider control and governance framework should use CobiT.”

CobiT is an umbrella framework and the same situation applies not only to ITIL, but also to other best practice frameworks, such as the Software Engineering Institute's Capability Maturity Model and ISO 9000.

This also answers the last part of the question: “What does it mean for the tools I am using?” The answer is that these tools probably fit into the CobiT framework. To help make this fit, this white paper contains some examples of how such tools typically can also support CobiT domains and processes.

Software tools supporting CobiT processes

Since CobiT can be seen as a umbrella framework that provides guidelines to manage all activities and since CobiT is built on best practice standards such as ITIL, BS7799, the Balanced ScoreCard and many more, it is logical that organizations should look at leveraging there existing investments in supporting software tools before implementing new tools.

We do expect new enterprise software tool vendors to enter the market with messages on CobiT compliancy and we expect new software vendors to enter the market with specialized management solutions for IT risk, IT goals, performance and IT scorecards. We believe that these new vendors should be evaluated and that new point solutions can provide great benefits for organizations that are actively looking for software solutions to implement best practices. Business Activity Management, Business Intelligence and Business Process Management vendors could play a major role in providing new solutions.

We also expect independent software vendors who operate in the IT Service Management or IT Project Portfolio Management markets to claim that a one stop shop for implementing IT Governance practices exists. However we would like to advise organizations to be wary for these kinds of propositions. Since IT Governance and CobiT are umbrella concepts and frameworks, it is unlikely that any single software tool would fit all the IT Governance requirements of your organization: IT Governance is not just a dashboard that sits on top of IT Portfolio Management or IT Service Management software suites. Al-

though this could be a great starting point for an organization, it should not be the finish line.

Let's examine a couple of the CobiT processes and look at them a bit more in detail.

If we examine the AI6 Control objective of CobiT, "Managing Changes", we can immediately see that this is related to the ITIL process Change Management. The Key Performance Indicators, described in the CobiT framework for this process, are:

- Number of different versions installed at the same time
- Number of software release and distribution methods per platform.
- Number of deviations from the standard configuration.
- Number of emergency fixes for which the normal change management process was not applied retroactively.
- Time lag between the availability of the fix and its implementation.
- Ratio of accepted to refused change implementation requests.

In order to collect these KPI's on a regular basis we have to combine information that most likely resides in multiple databases such as an ITIL based Change Management database, a Helpdesk Management database, in Project Management databases, in Software Distribution Tools and in Configuration Management databases.

Another example: CobiT's control objective DS6 "Identify and Allocate Costs". The Key Performance Indicators here are:

- Percentage of variance between budgets, forecasts and actual costs.
- Percentage reduction in information service rates.
- Percentage increase in optimization of user service requests.
- Percentage increase in optimization of IT resources usage.
- Number of cost optimization initiatives.

Again we can immediately see that this high-level Control Objective is related to the ITIL process Financial Management. (Formerly known as Cost Management)

In order to track the KPI's for this Control Objective, an organization will most likely have to combine information from for instance: the ERP financials application, Helpdesk, Change, Configuration and Cost Management applications, and System and Network Management systems.

By performing such an exercise for all CobiT's high-level and detailed Control Objectives, organizations can build a map of which existing applications hold what governance data.

When implementing CobiT in the IT Operational environment, organizations should examine which KPI's are easily available on a regular basis by running reports on operational databases.

Figure 3 can be used as an example for building such a map.

The next step for organizations would be to support this process of KPI collection and KPI representation so that an historic database of governance practices can be built, and the results can be analyzed and interpreted and followed by improvement actions.

Although spreadsheet programs are a good starting point, we do not believe that spreadsheets are the right tools for this type of analysis. An integral part of governance is becoming transparent to all stakeholders involved. It is important that management communicates aims and directions concerning IT activities and that the IT organization itself can benefit from the IT Governance practices. Technologies such as Data warehouses, Risk Management solutions, Enterprise Dashboards, Management Scorecard applications and Business Activity Monitoring applications are well suited in order to reach these goals and objectives. We believe these kind of enterprise software applications will play a major role in formalizing Enterprise Governance structures.

	AI1	AI2	AI3	AI4	AI5	AI6
Application Management		X				
Asset Management			X			
Billing				X		X
Business Process Management (BPM)						X
Change Management	X	X			X	X
Desktop Management		X				
Project Management	X	X			X	X
Release Management					X	
Service Management	X	X	X	X	X	X
Service Desk	X	X			X	X
Enterprise Application Integration	X	X	X			
Risk Management						X
Application Development	X	X		X		

Figure 3. Example of mapping enterprise applications to the Acquisition and Implementation Domain of CobiT

Conclusion

In this white paper we have seen that IT Governance is an important topic in today's business environment.

Currently, only one real open standard framework is available for IT Governance: CobiT. The CobiT framework is compatible with best practice IT Management frameworks such as ITIL, CMM, Prince2, DS7799 and others. This is good news for organizations, since it means that they can leverage their existing investments in these supporting frameworks. This also means that the enterprise software applications that support these frameworks are most likely tools that can also support organizations when it comes to implementing CobiT as an operational IT Governance structure.

Organizations should look at their existing tools as data sources for CobiT's control objectives.

Organizations should look at new tools for pulling all these data sources together and to analyze and interpret the results, allowing organizations to take action and better manage IT risks and IT quality.