IT Governance:
The Safe Way to Effective and Efficient Governance

Ioannis Chalaris[1], Panayiotis P. Lemos[2], and Michail Chalaris.[3]

[1] TEI of Athens, Dept. of Informatik, ixalaris@teiath.gr

[2] Hellenic Naval Training Command, Skaramangas, Greece
lemospan@ieee.org

[3] Integrated Information Systems, Athens, mikehlr80@yahoo.gr

Abstract. Software Quality Management Systems should include all the activities, responsibilities, procedures, resources, measurements and measurement tools that are used to assure that all projects under development would satisfy the pre-agreed quality factors. One of the main issues of the selected quality management plan should be the specific methodology that would be followed for the measurement, analysis and interpretation of the results. This methodology should combine and correlate all factors that affect the final product quality as well should adapt to the specification and peculiarities of each software project under evaluation. In case this required management effort is supported by a dedicated software application there is a major confidence that the total required documentation would be successfully delivered, the co-operation among various stakeholders would be highly efficient and the additional requirements like auditing and certification would be effectively concluded. Various approaches have been suggested (e.g. CobiT, ITIL) for a holistic management of IT-Governance processes, while several tools for their support have been developed.. This paper analyzes all above issues and presents existing technologies for IT-Governance management, as well as operational requirements of a prototype QMS, developed by the Quali-Learn Lab of the Athens Technological Educational Institution (TEI) to be used by software development organizations.

Keywords: Quality Management Systems, QA Standards, IT-Governance,CobiT, ITIL, ADOit

1 Introduction

This work aimed at the development of a web-application for the manipulation of a Quality Management System (QMS) of a software development company. The focus has been given on the QMS, but the basic company operations have been implemented for correctness and completeness. The application satisfies the general frame of an applied system for IT governance, which naturally will coexist or very probably will be included in a more general governance infrastructure. The IT Governance prevails without the ignorance of general governance and of course without any discrepancies difficulties in the application and operation of such system.

2 Background

As it is stated in the Board Briefing on IT Governance of the IT Governance Institute "An increasingly educated and assertive set of stakeholders has raised concerns about the sound management of their interests" [4]. This has led to the emergence of corporate governance regulations and standards for overall enterprise governance. These regulations establish board responsibilities and demand that board directors exercise due diligence in their roles of setting strategy and ensuring management implements it. Enterprise governance is the set of responsibilities and practices exercised by the corporation's management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

The definition of IT governance 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 [4].

Initially, governance was more general and concerned globally the placement of strategic objectives of an organization as well as the determination of methods to achieve them, the assurance of right management of its resources, etc., With the continuously wider use of technology however an IT dependence started appearing, therefore the need of focusing on the IT governance was created.

IT is exceptionally useful and in many cases essential for transactions' management operations, and for storage and management of information and knowledge in all aspects of interest, with economic or social objectives. A lot of organizations are based almost absolutely on IT in order to operate, to remain competitive and to expand. Factors as the spread and predominance of internet, e-commerce, the creation of multinational organizations, the collaboration of organizations of different nations and the globalization of economy, contributed considerably in the establishment of IT governance as a subject of main importance and decisive for the present and the future of an organization.

As it is stated, once again on the Board Briefing on IT Governance of IT Governance Institute, "At the heart of the governance responsibilities of setting strategy, managing risks, delivering value and measuring performance, are the stakeholder1 values, which drive the enterprise and IT strategy. Sustaining the current business and growing into new business models are certainly stakeholder expectations and can be achieved only with adequate governance of the enterprise's IT infrastructure"[4], [6],[7].

2.1 Purpose of IT Governance

The purpose of IT governance is to direct IT endeavours, to ensure that IT's performance meets the following objectives:

- For IT to be aligned with the enterprise and realize the promised benefits
- For IT to enable the enterprise by exploiting opportunities and maximizing benefits
- For IT resources to be used responsibly
- For IT-related risks to be managed appropriately

IT governance usually occurs at different layers, with team leaders reporting to and receiving direction from their managers, with managers reporting up to the executive, and the executive to the board of directors. Reports that indicate deviation from targets usually will already include recommendations for action to be endorsed by the governing layer. Clearly this will not be effective unless strategy and goals have first been cascaded down into the organization. The illustration on the next page presents conceptually the interaction of objectives and IT activities from an IT governance perspective and can be applied among the different layers within the enterprise.

The governance process starts with setting objectives for the enterprise's IT, providing the initial direction. From then on, a continuous loop is established of performance that is measured and compared to objectives, resulting in redirection of activities where necessary and change of objectives where appropriate [3], [7]. While objectives are primarily the responsibility of the board and performance measures that of management, it is evident they should be developed in concert so that the objectives are achievable and the measures represent the objectives correctly.

In this document, “stakeholder” is used to indicate anyone who has either a responsibility for or an expectation from the enterprise’s IT, e.g., shareholders, directors, executives, business and technology management, users, employees, governments, suppliers, customers and the public. Also, “board of directors” and “board” are used to indicate the body that is ultimately accountable to the stakeholders of the enterprise.

In response to the direction received, the IT function needs to focus on realizing benefits by increasing automation and making the enterprise more effective, and by decreasing cost and making the whole enterprise more efficient; and on managing risks (security, reliability and compliance).

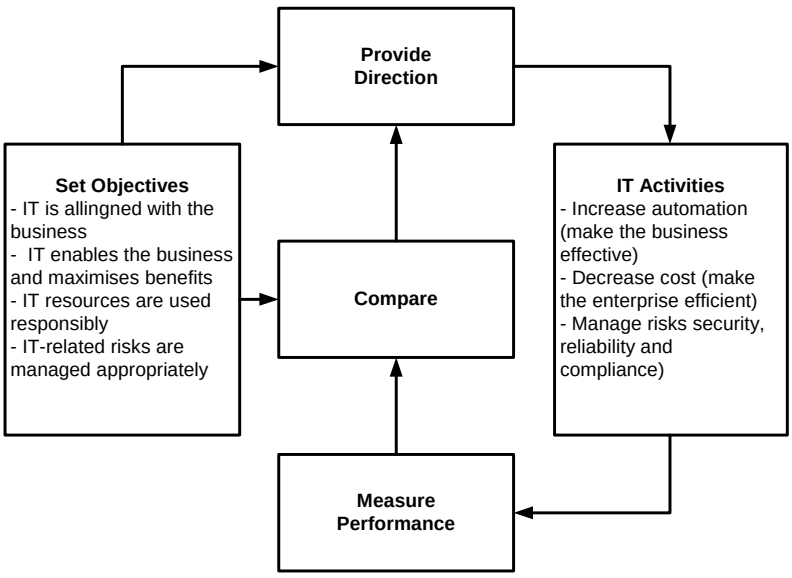


Fig. 1. The IT Governance Framework

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, as shown on Fig.1. 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" [3],[6],[7].

3 Company Description

The company described in this paper, is a typical software production company [2],[3]. The company receives project enquiries from clients and either undertakes or rejects them, or produces software projects that are offered to clients. In both cases, clients quotations are logged. These projects are supported via company's employees' visits to the clients. Software products are getting upgrades and these upgrades are offered to respective customers while all relative offers are logged. A software project, either new or upgraded, can consists of phases that contain specific steps. In order for a project to begin, all relative paperwork has to be produced and approved. In case, this project is an order received from a client, then all necessary data are taken such as specifications, capabilities, etc. as well as the point of contact. Each project is managed by a project team, the members of which undertake one or more of the above referenced tasks. After the implementation of the software project, it is tested usually at the customer's site, and when the testing is finalized again all relative paperwork is produced. All projects usually require and involve procurements at various levels, therefore it is required for the company to co-operate with several sub-contractors. Finally, there is a Human Resources Management database that keeps records of all required data for the company employees, such as previous work experience, skills, competencies, etc.

3.1 Short Description of the Company's Quality Management System

- The Quality Management System (QMS) that has been designed, developed and implemented in the company is one that completely covers the above referenced activities in a flexible and smart way. The documentation developed for this reason is shown in titles below:
- List of QMS procedures and guidelines
- List of QMS Documents and Plans
- Internal Audits Plan
- Internal Audit Report Template
- Inquiry for Corrective or Preventive Action
- Personnel Training Plan
- Personnel Training records
- Management Review
- Re-collection Order
- External Documentation List
- Supply Orders' List
- Project Phase Review
- Project Status Report
- Project Assignment

- Final Project Test
- Project Revision Monitoring
- Project File
- Project Time Management Report
- Project Representative Weekly Schedule

3.2 Initial Evaluation of the introduced Quality Management System

The QMS introduced to this software development company is in accordance with the framework of IT Governance and Governance in general. It covers most of the company's requirements regarding the storing and management of all relevant information. It enables supporting activities for the IT Governance and implements relative procedures. It does not raise any problems to the remaining Governance; on the contrary, it works towards a supporting way.
Once again, according to the Board Briefing on IT Governance του IT Governance Institute: "Fundamentally, IT governance is concerned about two things: that IT delivers value to the business and that IT risks are mitigated. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need measurement, for example, by a balanced scorecard. This leads to the four main focus areas for IT governance, all driven by stakeholder value. Two of them are outcomes: value delivery and risk mitigation. Two of them are drivers: strategic alignment and performance measurement."

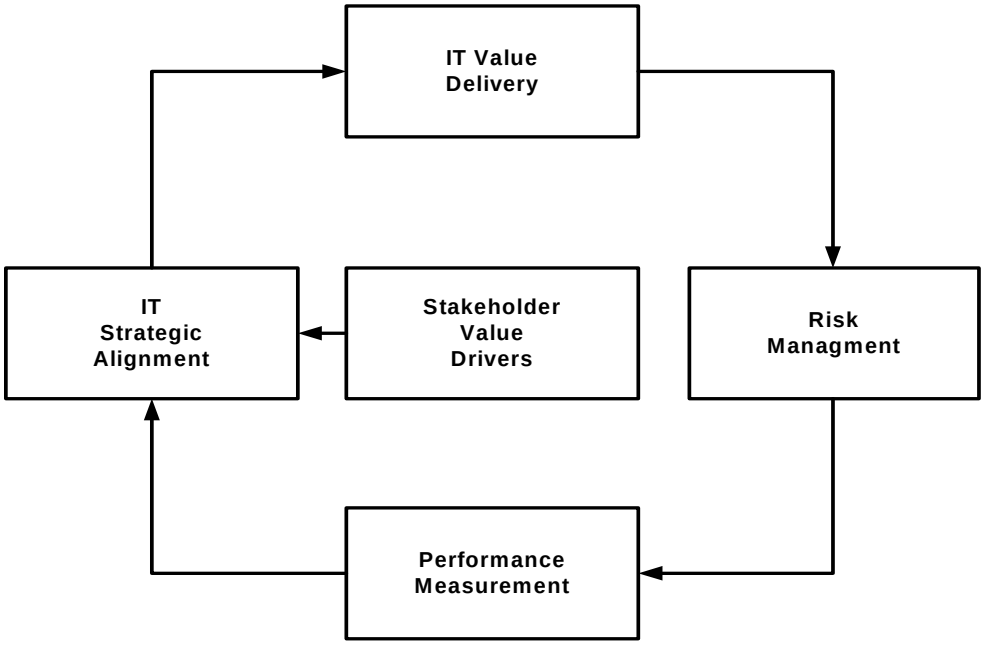


Fig. 2. The IT Governance Implementation Loop

IT governance entails a number of activities for the board and for executive management, such as being informed of the role and impact of IT on the enterprise, assigning responsibilities, defining constraints within which to operate, measuring performance, managing risk and obtaining assurance [1],[5],[8].
For the IT Governance Implementation Loop:

- Strategic Alignment: covers the required harmonization between the company's strategy and the company's IT strategy.

- Value Delivery: covers the quality of the production or the services delivered to the customers.
- Performance Measurement: Covers the effectiveness and efficiency measurements required by the QMS.
- Strategy: has taken on a new urgency as enterprises mobilize intangible and hidden assets to compete in an information-based global economy. Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, measuring those relationships and knowledge-based assets necessary to compete in the information age: *customer* focus, *process* efficiency and the ability to *learn* and grow. At the heart of these scorecards is management information supplied by the IT infrastructure, shown in Fig. 3.

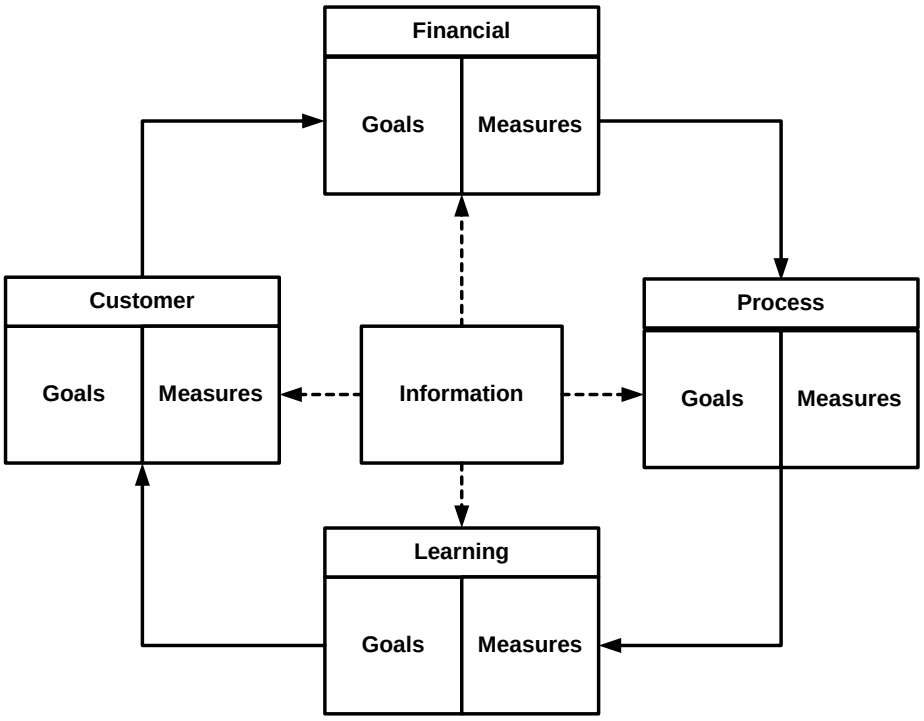


Fig. 3. The IT Infrastructure

But IT does more than provide information to obtain a global picture of where the organization is and where it is going. It also enables and sustains solutions for the actual goals set in the financial (enterprise resource management), customer (customer relationship management), process (intranet and workflow tools) and learning (knowledge management) dimensions of the scorecard. IT not only contributes information to the business scorecards and tools to the different dimensions being measured, but also, because of the criticality of IT itself, needs its own scorecard. Defining clear goals and good measures that unequivocally reflect the business impact of the IT goals is a challenge and needs to be resolved in co-operation among the different governance layers within the enterprise.

Risk Management: The objective of Risk Management / Assessment is the identification of possible risks to which the company's infrastructure and resources are vulnerable to and the probability of their appearance, as well as the documentation of their consequences and the preventive measures for their avoidance or the mitigation of the consequences in case of appearance. Regarding the IT Governance, Risk Management can be expressed using three words: Integrity, Availability and Confidentiality of the Information.

There are several internationally accepted techniques for the analysis and the assessment of hazard that can be applied depending on the system under evaluation. These techniques differentiate from each other with respect of the approaching methodology of the risk assessment and the methodology used for the quantization of the analysis results. The most practical approach is the Preliminary Hazard Analysis (PHA) followed by the Failure Mode, Effects and Criticality Analysis (FMECA).

Preliminary Hazard Analysis is the foundation for effective systems hazard analysis. It should begin with an initial collection of raw data dealing with the design, production, and operation of the system. The purpose of this procedure is to identify any possible hazards inherent in the system. The four main categories of this approach are hazard, cause, main effects, and preventive control. The hazard effects and corrective/preventive measures are only tentative indicators of potential hazards and possible solutions.

While PHA studies hazards in the entire system, FMECA [1],[5] analyzes the components of the system and all of the possible failures which can occur. This form of analysis identifies items whose failures have a potential for hazardous consequences. Following that, these hazards are categorized relatively to their degree of criticality (Criticality Ranking) among Catastrophic (I), Critical (II), Marginal (III) and Negligible (IV) based on their consequences in the activity under investigation. Because the frequency of each potential occurrence is also an important factor, a risk assessment matrix can be used to codify the risk assignment, which in conjunction with the Risk Assessment Table present the total picture of the threats/hazards that the company faces, their consequences as well as their probability of occurrence. The Risk Assessment Matrix is presented in Table 1.

Table 1. The Risk Assessment Matrix

ency of Occu	Hazard Category			
	I Catastrophic	II Critical	III Marginal	IV Negligible
	1	3	7	13
	2	5	9	16
al	4	6	11	18
	8	10	14	19
ble	12	15	17	20

while the categorization of the combined consequences/probability assessment is shown in Table 2.

Table 2. Combination of Consequences-Probability Assessment

Risk Index	Risk Acceptance Category
1-5	Unacceptable
6-9	Undesirable
10-17	Acceptable with review
18-20	Acceptable without review

4 Audit Process

4.1 General

Elevating IT from a pure managing level to the governance level has been the natural fallout of the recognition of the pervasive influence of IT on all aspects of business. With significant increases in investments in IT by the business, it has become very important and necessary to ensure that tangible benefits for the business are derived from these investments. Accordingly, IT governance is concerned with objectives that focus on such areas as:

- Alignment of IT with business
- Value and benefits of IT to the business
- Management of the risks associated with IT
- Performance measures for IT services to the business.

Companies depend on IT to stay competitive, so it's no surprise there is a big push to provide the same level of oversight to IT that is traditionally reserved for areas such as finance and accounting. However, governing IT is more involved due to its technical nature, and poses unique challenges for board members and management. Some of the areas management must take into account are: understanding the impact IT has within the company, providing boundaries for IT professionals to do their jobs, establishing performance measurement, and reassuring shareholders that the IT investment is performing according to preset goals.

To help the management of a company (board) get its IT governance program moving in the right direction, you need a plan that suits the company's particular needs. To begin, the board must take the lead in developing an IT governance agenda for management to follow. IT governance must have complete board member buy-in and even the non-technical members must be made aware of its importance. The following steps should help with this process [4],[8]:

- Create an IT strategy committee for better communications between the board and management.
- Each board meeting includes IT as an agenda item.
- The board should align IT projects with business goals.
- Measurements should be established by the board regarding IT performance.
- The board should challenge management on IT initiatives by benchmarking measurable results [1],[4],[5].

After the board has established the direction for an IT governance program, it is up to management to put it into action. To help management decide where to begin, the following steps are suggested:

- Create an outline that will move IT governance forward with clear responsibilities for all IT professionals.
- Management should promote responsibility among the IT staff for the success of IT projects.
- Establish a scoring technique to measure current performance results. Monitor these key points: organizational support for the implementation, risk management responsibilities within the organization, the need for interdepartmental sharing of business information, and project communication.
- Drill down and define the process areas in IT that are critical to managing high risk areas.
- Manage expectations among IT staff by making it clear this is not an overnight process.

- Understand the risks associated with IT investment. Consider the company's previous patterns of performance, current IT staff qualifications, complexity of IT environment, and the type of new IT initiatives being considered.
- Analyze current capability and identify gaps. Find out where improvements are needed most.
- The program should consist of a series of continuous improvement phases rather than a one- or two-step process.
- Decide which improvement strategies are the highest priority projects. This decision should be based on the most potential benefit and ease of implementation of an IT project.
- Align IT strategy with business goals by asking tough questions such as: where does IT fit in the overall strategy for the company, what is management's risk tolerance level with IT investments, and what are the major IT issues facing the organization at the moment.

4.1 Operational Characteristics of the developed Application

The application covers all QMS processes as well as the major part of data relative to the operation of the company. There are 3 main categories of processes, namely:

- Data, including all organizational and operational company's data (employees, customers, departments, etc.)
- Project, including all necessary information for the conclusion of a project, and
- System, covering all necessary QMS documentation.

There are also three access levels for the manipulation of these data (read, write, modify) as expected to most management information systems, but with totally independent assignment. For this application it is not unacceptable for a user to have right to enter or modify data but not to be able to read it. The access level assignment is a responsibility of the QMS supervisor.

System documentation on the other hand is divided into two major subgroups. One subgroup deals with data entry, while the second subgroup deals with the automated preparation of all required documentation. This approach makes the application very user friendly as each user (from novice to expert) recognizes the correct form/interface for his interaction with the application.

Further than a typical project management capability, the developed application offers the user a kind of "expert" matching of possible solutions to an existing problem, thus shortening the procedure for the decision making. This matching is based on the core of the QMS application that is built on a cause – relative solution concept.

Further to the above referenced specific capabilities, the application offers most of the typical QMS software, i.e. hard copy creation, selected space for signatures, even though not yet digital. The application is very strict on the creation of documentation by the users, as it is considered that all required documentation is prepared by the application. This is a major control point of the efficiency and the effectiveness of the application. A basic TMR (Time Management Report) module is encapsulated in the application contributing to the already referenced project management capabilities.

No documentation exchange capability has been designed for this application since it is considered that all paper work is performed with usual conventional methods, including email. Of major importance to efficiency of the application os the capability to create documentation "on the fly", i.e. based on stored data avoiding to consume valuable space for the storage of electronic documentation. Hard copy filing system covers this rational requirement.

The application is compatible with all operating systems and with the browsers I.E., N.N (version 4 and newer) and Mozilla 1.1a (according to official statements of corresponding developers regarding compatibility). The tools EasyPHP v 1.6.0.0 and phpMyAdmin v 2.4.0-rc2 were used for the development of the application.
The appendix of the present paper presents the system's general functional requirements illustrated in the form of a 1st level DFD as well as an E_R model, which point out the extent and complexity of the OMS-System developed.

5 ADO*it*® - The IT Management Tool in Conformity with ITIL® and CobiT®

One of the main challenges for today's IT managers is the strict alignment of information technology (IT) with the company's business objectives. Thus, opening more opportunities for cooperation with corporate management and supporting the business processes using IT gains more and more importance. As a result, extended requirements on quality, availability and costs of IT must be met. These are accomplished by an effective IT Architecture and Service Management.

The IT Management Framework
ADOit supports IT management by integrating the ITIL and CobiT Best Practices into a comprehensive IT management framework. Due to the integral view from the strategic level down to the ICT infrastructure, IT services are effectively and efficiently orientated towards the customers' requirements and integrated into a scaleable and standardised IT architecture.

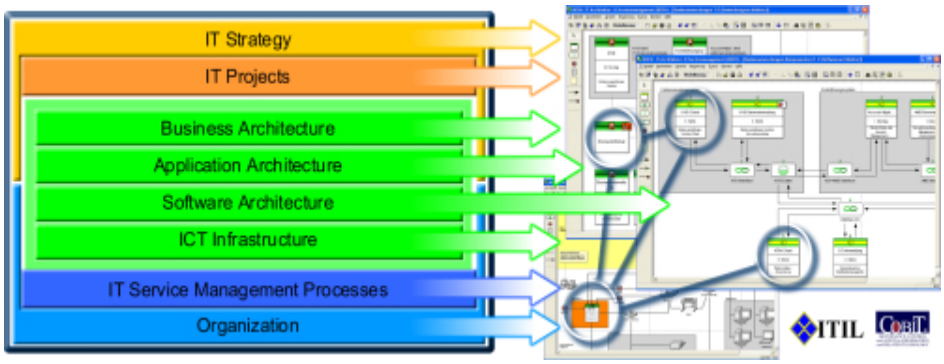


Fig. 4 IT Architecture Management with ITIL®

Dynamic processes, short innovation cycles, as well as mergers and acquisitions, are just some of the reasons that call for a permanent adaption and consolidation of the IT architecture. In this context the focus lies on optimisation and orientation of the current IT towards an architecture with optimal resource allocation and minimal costs.

IT Service Management with ADOit®
An integral and process-based view on IT services considering the IT strategy and the requirements of the business processes represents the key to successful IT Service Management (ITSM). The IT Infrastructure Library (ITIL) offers a process-based and scaleable approach to improve planning, implementation and support of your IT services.
The ITIL® Best Practices Library
The best practices described in ITIL are at one's disposal as a hierarchical ADOit reference process library. It includes a comprehensive, model-based documentation of the ITSM

processes described in the IT Infrastructure Library. The areas "Service Delivery" and "Service Support" are documented in more than fifty reference models.

The Advantages on a Glance
Cost-cutting through extensive IT management - from the strategy down to the production architecture, Measurable quality improvement via ITIL-compliant IT service and process management, Standardisation for both the ITSM processes and IT architecture by using standards like ITIL, CobiT, eTom, or British Standard (BS) 15000, Time and cost savings when using the ITIL Best Practices as ADOit reference models, Enhancement of the planning reliability and prevention of architecture breaks with numerous analysis and simulation mechanisms, More efficient communication - both inside the company and with the customers

6 Conclusion, Recommendation and Perspectives

Putting an IT governance program in place is no small task and may seem like overkill when IT makes up only a small portion of the company's overall budget. However, with today's budget constraints and tight margins, coupled with IT's increasing role in running and growing an enterprise, the work involved in establishing an IT governance program can provide dividends by enabling a more responsive and cost-effective organization. By using these tips to implement your governance program, you should have a clearer picture of your IT organization's strengths and weaknesses.

The application constitutes an operation and management tool of the Quality Management System of the company as well as of the main operating part of it. It agrees with and follows the frames and main principles of IT governance and governance in general. It supports, as long as its nature and objectives allow, the IT governance in all basic aspects. Finally, it assists the governance and does not conflict or contradicts with governance principles. The application, given its size, the crowd of the information processed and the operations executed, the complexity, the connection and harmonization with IT governance and governance in general, has a huge big potential of growth and in particular to many directions. With regard to the information, it can be supplemented with still more and respective procedural controls to be added, as well as controls of correctness of data and integrity of database. From the side of operations it is obvious that the additions can be many. For example and for the near future, a system of digital signatures and certificates for the signature of documents (eg with use ssl) could be incorporated and a system of distribution of documents, between the users (eg with exploitation of likely local network or mail server) could be implemented.

More generally small or bigger additions and improvements are limited only by the current technological capabilities, the economic means of company and imagination of the builders. Of course, all aforementioned will take place according to the wishes and the vision of the company and/or its Quality Management System. From an IT governance point of view, as it appeared also from the relative analysis above, it remains specialized tools of management and special operations depending on the precise system that will select the company to be added. Finally, concerning governance, it is considered better the application to be separated from its special operations, as it is by far more general and far away from IT and the relation among the nature of the company, the application itself, and the IT governance. Thus, it is much more convenient to work with its own set of tools rather than incorporates the tools of governance to this application.

Finally, it is worth pointing out that the use of suitable tools such as ADOit has proven to be a great aid in the management of quality establishment procedures fulfilling national

standards and, furthermore, in combination with the OMS-System of the Quali-Learn Lab of the Athens Technological Educational Institution (TEI), they offer an overall technology for the management that covers from the modeling up to the installation and exploitation of an OMS-System.

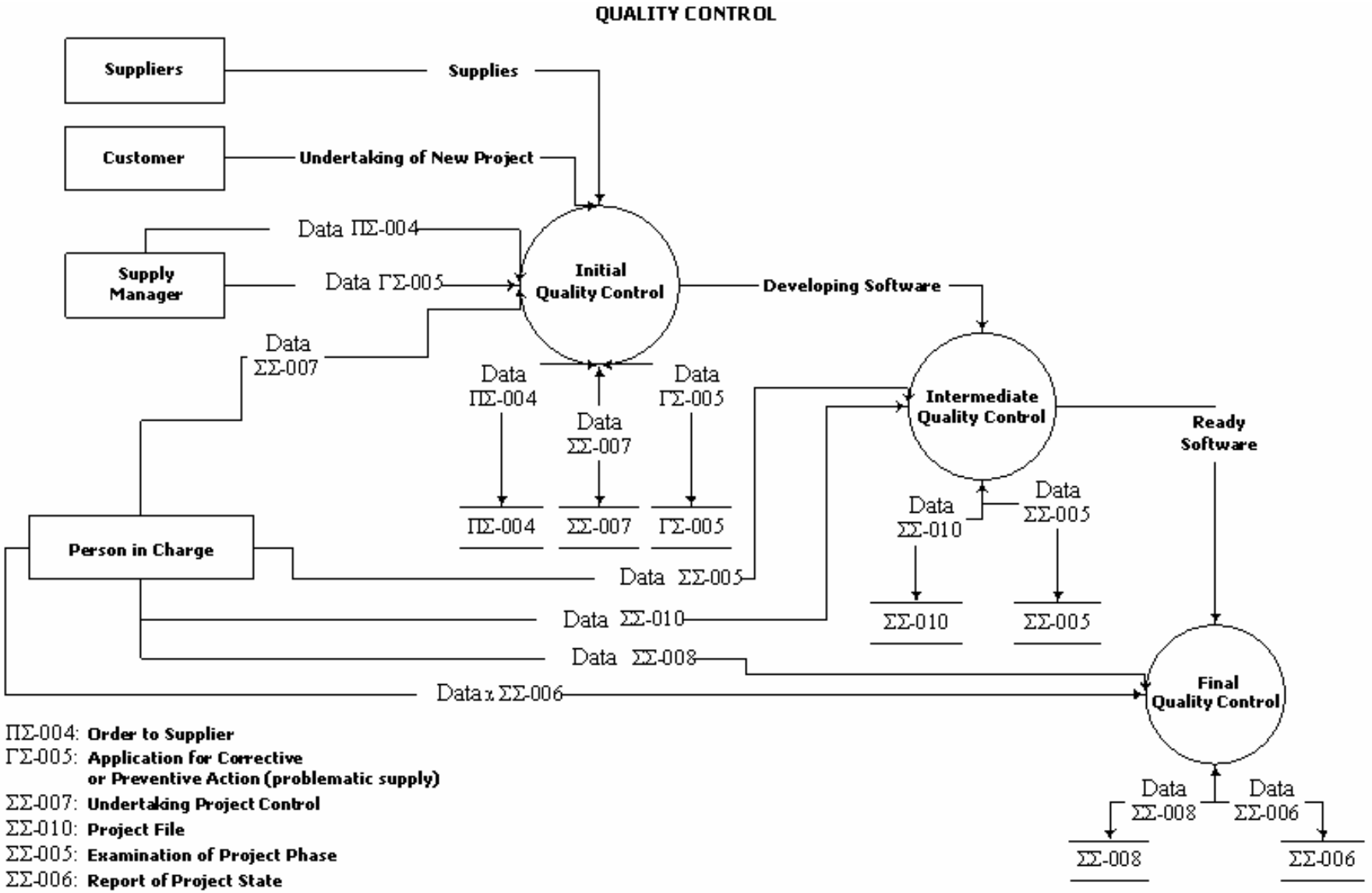
Acknowledgements: The present essay was co-funded at a percentage of 75% by the European Union and at a percentage of 25% by the Greek Public in the framework of the Operational Program of Education and Initial Professional Training (EPEAEK II) – Research Action '**Archimides**' – Project 031.

References

1. Kavanian, H. R. and Wentz, C.A., 1990. *Occupational and Environmental Safety Engineering and Management.* Van Norstrand Reinhold, New York.
2. Frangos, S.A., *Implementing a Quality Management System using an Incremental Approach*, sqm 95 Proceedings, April 1995.
3. J. Halaris, S. Fragkos *An effective way of establishing Quality Management Systems,* Proceedings of 7th Hellenic Conference on Informatics, Ioannina, August 1999, pp VI.2 – VI.10
4. Information Systems Audit and Control Association, Standards Booklet "Index IS Auditing Procedures") July 2002 http://www.isaca.org/standards
5. Information Systems Audit and Control Association, S Risk Assessment, effective 1 July 2002 *(Standards Booklet pages 61-73,* http://www.isosecurity solutions.com/accelerator1.html
6. Helmut Barzelt, "Software Management und Qualitaetssicherung – Unternehmensmodelierung" Spectrum Akademischer Verlag,1997.
7. Roger Pressman, "Software Engineering – A practitioner' s Approach" – European Adaptation, 5th edition 2000.
8. Watt S.Humphrey, "A disciplin for software Engineering", Carnegie Mellon University, 1995 Addison – Wesley Publishing Company.

Web sites

http://www.itil-itsm-world.com/
www.boc-eu.com
http://www.ogc.gov.uk/prince/
www.ktpae.gr



ΠΣ-004: **Order to Supplier**
ΓΣ-005: **Application for Corrective or Preventive Action (problematic supply)**
ΣΣ-007: **Undertaking Project Control**
ΣΣ-010: **Project File**
ΣΣ-005: **Examination of Project Phase**
ΣΣ-006: **Report of Project State**
ΣΣ-008: **Final Project Test**

Q.A.S. Entity Relationship Model