Professor Pavel NĂSTASE, PhD
Professor Floarea NĂSTASE, PhD
Corina IONESCU, PhD Candidate
The Bucharest Academy of Economic Studies

CHALLENGES GENERATED BY THE IMPLEMENTATION OF THE IT STANDARDS COBIT 4.1, ITIL V3 AND ISO/IEC 27002 IN ENTERPRISES

Abstract. *The main purpose of this paper is to emphasize the importance of the implementation of IT best practices in enterprises and to identify the key challenges managers are facing when creating a standardized IT control framework in order to achieve alignment of best practices to business requirements. First, the authors present the increasing necessity of implementing IT standards in organizations acting in IT environments with focus on the standards COBIT, ITIL and ISO/IEC 27002. Second, the paper develops the analysis of the three standards which is a guidance for organizations wishing to adopt IT best practices on how to integrate the leading global frameworks and other practices and standards in inter-organizational relationships. The last part concentrates on the best methods of implementing in an efficient way the IT standards, which include identifying the use of standards and IT best practices, prioritizing processes according to an action plan and planning the steps of the implementation approach.*

Key words: IT standards, IT best practices, COBIT, ITIL, ISO/IEC 27002.

JEL Classification: L84, M15, M42

INTRODUCTION

In the nowadays society every competitive enterprise acting in an IT environment needs to establish the best usage of IT standards and practices in order to suit its individual requirements. The growing adoption of IT best practices has been driven by a requirement for the IT industry to better manage the quality and reliability of IT in business and respond to a growing number of regulatory and contractual requirements. Considering the current IT environment and the multitude of standards that can be applied to information systems, it is a challenge for each organization to choose the most appropriate set of standards which satisfy their needs. It is not simple for IT to define its goals, position services and the need for constant evolution, therefore, in the

current economy, enterprises worldwide are struggling to achieve growth and governance at an affordable cost without compromising the business, its customers, and the integrity and security of their information systems.
The aim of this paper is to explain to business users and senior management the value of IT best practices and how harmonization, implementation and integration of best practices may be made easier. For this, the authors draw the attention on the challenges enterprises are facing when establishing IT best practices by making a comparison between three IT standards and highlighting their features COBIT 4.1, ITIL V3 and ISO/IEC 27002**.** All three standards/practices covered in this paper can play a very useful role: COBIT and ISO/IEC 27002 in helping to define *what* should be done and ITIL in providing the *how* for service management aspects. There is a danger, however, that implementation of these potentially helpful best practices can be costly and unfocused if they are treated as purely technical guidance.
To be most effective, best practices should be applied within the business context, focusing on where their use would provide the most benefits to the organization. Top management, business management, auditors, compliance officers and IT managers should work together to make sure IT best practices lead to cost-effective and well-controlled IT delivery. IT best practices are very important within organizations because they support not only a better management of IT, which is critical to the success of the enterprise strategy, but also the effective governance of IT activities, ITGI (2008). IT best practices enable also an effective management framework of policies, internal controls and defined practices, as well as many other business benefits, including efficiency gains, less reliance on experts, fewer errors, trust from business partners and respect from regulators.

1. Premises for Implementing IT Best Practices

All IT best practices offer support for managers who strive for business improvement through better usage of IT activities, but this paper focuses only on three specific practices and standards that are becoming widely adopted around the world and which have been updated in order to reflect the latest versions:

- ITIL V3 – published by the UK Government to provide a best practice framework for IT service management;
- COBIT 4.1 – published by ITGI and positioned as a high-level governance and control framework;
- ISO/IEC 27002:2005 – published by the International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) and derived from the UK Government's BS 7799, renamed ISO/IEC 17799:2005, to provide a framework of a standard for information security management.

The implementation of best practices should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used, therefore management and staff must understand what to do, how to do it and why it is important.

At worldwide level, specialized institutes show constant preoccupations in order to assure the convergence of IT standards. An example is the collaboration between the UK's Office of Government Commerce and the IT Governance Institute which organized researches in order to reflect changes in COBIT 4.1 and ITIL V3 (www.itsmfi.org). To achieve alignment of best practice to business requirements, formal processes in support of good IT governance should be used, ITGI (2008). COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by ITGI to generically suit every enterprise. There is also a need for detailed, standardized processes. Specific practices and standards, such as ITIL and ISO/IEC 27002, cover specific areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

Figure 1 shows the position of the three standards depending on two factors: degree of abstraction and relevance of the IT.

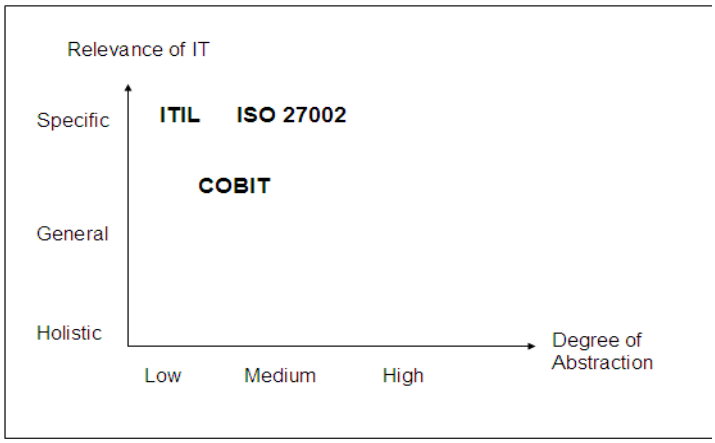

Figure 1. Model of IT Standards

(Source: Popa & Ionescu, 2005)

As mentioned before, COBIT provides a general control framework for IT processes and has an almost medium abstraction degree according to this model. But, since it

focuses only on IT processes and controls it locates itself between the general and the specific area closer, though to the general part. On the other hand ITIL and ISO 27002 have a very specific content, ITIL being characterized by a low degree of abstraction and ISO 27002 by a medium one.

2. The Need of IT Best Practices in Today's Society

IT best practices have become significant to managers because of the increasingly competitive environment. First, one of the key concerns of business managers and boards is to demand better returns from IT investments, which implies the assurance that IT delivers what the business needs in order to enhance stakeholder value. Therefore, the management shows constant preoccupation over the generally increasing level of IT expenditure and over the increasingly complex IT-related risks, such as network security, Selig (2008). Second, in all sectors of the economy there is the need to meet regulatory requirements for IT controls which implies that managers should drive IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities in order to increase business value and reduce business risk. Third, managers always seek to optimize costs, in this case by driving standardized approaches. And the last reason for implementing IT best practices is the fact that organizations need to assess how they are performing against generally accepted standards.

All the above factors contribute to the continuous growth in the use of standards and best practices but at the same time they create new challenges and demands for implementation guidance. For senior managers it is important to find answers to following questions: Are IT and the business strategy in alignment? Is the enterprise achieving optimum use of its internal and external resources? Does everyone in the enterprise understand the IT objectives? Is the impact of IT on enterprise risk understood and is the responsibility for IT risk management established?

Due to their technical nature, IT standards and best practices are known mostly to the experts (IT professionals, managers and advisors) who may adopt and use them with good intent but potentially without a business focus or the customer's involvement and support. Even in organizations where practices such as COBIT and ITIL have been implemented, some business managers understand little about their real purpose and are unable to influence their use. To realize the full business value of best practices, the customers of IT services need to be involved, as the effective use of IT should be a collaborative experience between the customer and service providers (internal and external), with the customer setting the requirements. Other interested stakeholders, such as the board, senior executives and auditors, also have a great interest in either

receiving or in providing assurance that the IT investment is protected properly and delivering value. Increasingly, the use of standards and best practices, such as ITIL, COBIT and ISO/IEC 27002, is being driven by business requirements for improved performance, value transparency and increased control over IT activities (IIA Research Foundation).

The UK Government recognized very early on the significance of IT best practices to Government and, for many years, has developed best practices to guide the use of IT in Government departments. These practices have now become common standards around the world in private and public sectors. ITIL was developed more than 15 years ago to document best practice for IT service management, with that best practice being determined through the involvement of industry experts, consultants and practitioners.

ISACA recognized in the early 1990s that auditors, who had their own checklists for assessing IT controls and effectiveness, were speaking a different language to business managers and IT practitioners. In response to this communication gap, COBIT was created as an IT control framework for business managers, IT managers and auditors based on a generic set of IT processes meaningful to IT people and, increasingly to business managers. The best practices in COBIT are a common approach to good IT controls, implemented by business and IT managers, and assessed on the same basis by auditors. Over the years, COBIT has been developed as an open standard and is now increasingly being adopted globally as the control model for implementing and demonstrating effective IT governance. In 1998, ISACA created an affiliated body, the IT Governance Institute, to oversee further development of COBIT and to better communicate IT governance-related messages to business managers and, in particular, the boardroom.

Today, as every organization tries to deliver value from IT while managing an increasingly complex range of IT-related risks, the effective use of best practices can help to avoid reinventing their own policies and procedures, optimize the use of the IT resources and reduce the occurrence of major IT risks, such as: project failures, wasted investments, security breaches, system crashes and failures by service providers to understand and meet customer requirements, Nastase & Ionescu (2008).

3. Adoption of IT Best Practices

Organizations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful business outcomes when using IT to support the enterprise's strategy.

Strong framework tools are essential for ensuring that IT resources are aligned with an enterprise's business objectives, and that services and information meet quality and security needs. COBIT and ITIL are not mutually exclusive and can be combined to provide a powerful IT governance, control and best-practice framework in IT service management, ITGI (2008).

However, users need more guidance on how to integrate the leading global frameworks and other practices and standards. In response to this need, ongoing research has been undertaken into the mapping of COBIT to a wide range of other practices. COBIT is based on established frameworks, however, COBIT does not include process steps and tasks because, although it is oriented towards IT processes, it is a control and management framework rather than a process framework. COBIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is senior business management, senior IT management and auditors. Due to its high level and broad coverage and because it is based on many existing practices, COBIT is often referred to as the 'integrator', bringing disparate practices under one umbrella and, just as important, helping to link these various IT practices to business requirements.

ITIL is based on defining best practice processes for IT service management and support, rather than on defining a broad-based control framework. It focuses on the method and defines a more comprehensive set of processes. Additionally, ITIL provides a business and strategic context for IT decision making and for the first time describes continual service improvement as the key activity which drives maintenance of value delivery to customers.

Now that these standards and best practices are increasingly being used in real-world situations, experiences are maturing and organizations are moving from ad hoc and chaotic approaches to IT, to defined and managed processes. As IT governance gains acceptance, IT best practices will increasingly be aligned to business and governance requirements, rather than technical requirements. COBIT 4.0 introduced key activities for all IT processes to help guide roles and responsibilities for effective IT governance.

In a climate of increasing regulation and concern about IT-related risks, best practices will help not only enterprises to realize value from IT investments and IT services but also to minimize compliance issues and the concerns of auditors by: making compliance and the application of internal controls 'normal business practice', demonstrating adherence to accepted and proven industry good practices, improving trust and confidence from management and partners and creating respect from regulators and other external reviewers.

4. COBIT, ITIL and ISO/IEC 27002 – Overview of the Standards

As the subject of this paper consists of the analysis of the three standards: COBIT, ITIL and ISO27002, the next part of the article focuses not only on the comparison of these standards but also on offering a best practice guide on how to use these standards most efficiently in organizations acting in IT environments.

The first approach of the standards' overview is presented in the following figure which enables the understanding of the key similarities and differences between the three standards:

Table 1

Overview of COBIT, ITIL and ISO/IEC 27002

STAND / AREA	COBIT	ITIL	ISO27002
Function	Mapping IT Process	Mapping IT Service Level Management	Information Security Framework
Area	34 Processes and 4 Domains	9 Processes	10 Domains
Issuer	ISACA	OGC	ISO Board
Implementation	Information System Audit	Manage Service Level	Compliance with security standards
Consultant	Accounting Company, IT Consulting Company	IT Consulting Company	IT Consulting Company, Security Company, Network Consultant

(Source: Priandoyo, 2008)

A first difference of the three standards is the fact that they are issued by different organizations with different areas of activities and objectives. The general function of the standards is also slighlty different. COBIT provides best practices and tools for monitoring and mapping IT processes while ITIL aims to map IT service level management and ISO 27002 provides guidelines for implementing a standardized information security framework. COBIT consists of 4 domains and 34 processes which are required for the implementation of the information system audit. ITIL's best practice framework covers a total of 9 processes and enables the implementation of IT service level management with focus on achieving business effectiveness and efficiency in IT service management.

When choosing the right standard, managers should also consider the type of vendor that can offer them the desired solution of implementing the IT standards. All three standards can be provided in general by an IT consulting company, but COBIT is exclusively provided by an accounting company and ISO 27002 by a security or network consultant company.

4.1. COBIT

Executives need confidence that they can rely on information systems and the information produced by those systems and get a positive return from IT investments. COBIT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. COBIT provides the tools to direct and oversee all IT-related activities. COBIT is a globally accepted framework for IT governance based on industry standards and best practices. Once implemented, executives can ensure IT is aligned effectively with business goals and better direct the use of IT for business advantage. COBIT provides a common language for business executives to communicate goals, objectives and results with audit, IT and other professionals, ITGI (2007).

COBIT provides best practices and tools for monitoring and managing IT activities. The use of IT is a significant investment that needs to be managed. COBIT helps executives understand and manage IT investments throughout their life cycle and provides a method to assess whether IT services and new initiatives are meeting business requirements and are likely to deliver the benefits expected. The COBIT framework, in versions 4.0 and higher, focuses its activity on 5 areas which enable the IT governance: framework, process descriptions, control objectives, management guidelines and maturity models.

The difference between enterprises that manage IT well and those that do not, or cannot, is tremendous. COBIT enables clear policy development and good practice for IT management. The framework helps increase the value attained from IT. It also helps organizations manage IT-related risks and ensure compliance, continuity, security and privacy. Because COBIT is a set of proven and internationally accepted tools and techniques, implementation of COBIT is a sign of a well-run organization. It helps IT professionals and enterprise users demonstrate professional competence to senior management. As with many generic business processes, there are specific IT industry standards and good practices that enterprises should follow when using IT. COBIT captures these and provides a framework for implementing and managing them. Once the key COBIT principles relevant to an enterprise are identified and implemented, executives gain confidence that the use of IT can be managed effectively.

4.2 ITIL

Nowadays, organizations are dependent on IT to satisfy their corporate aims, meet their business needs and deliver value to customers. For this to happen in a manageable, accountable and repeatable way, the business must ensure that high-quality IT services are provided. These should be matched to business needs and user requirements, be compliant with legislation, be effectively and efficiently sourced and delivered and be continually reviewed and improved.

IT service management is concerned with planning, sourcing, designing, implementing, operating, supporting and improving IT services that are appropriate to business needs. ITIL provides a comprehensive, consistent and coherent best practice framework for IT service management and related processes, promoting a high-quality approach for achieving business effectiveness and efficiency in IT service management, ITGI (2008). ITIL is intended to underpin but not dictate the business processes of an organization. The role of the ITIL framework is to describe approaches, functions, roles and processes, upon which organizations may base their own practices and to give guidance at the lowest level that is applicable generally. Below that level, and to implement ITIL in an organization, specific knowledge of its business processes is required to drive ITIL for optimum effectiveness.

In ITIL V3, the most significant development has been the move from a process-based framework to a more comprehensive structure reflecting the life cycle of IT services. In this new context, the key processes have been updated, but more significantly, ITIL now describes IT service management functions, activities and organizational structure; strategic and sourcing concerns; and integration with the business, ITIL V3 (2008).

4.3. ISO/IEC 27002

The international standard of IT security controls, ISO/IEC 27002:2005 was published by ISO and the IEC, which established a joint technical committee, ISO/IEC JTC 1, ISO 27000 Directory (2005). Its goal is to provide information to parties responsible for implementing information security within an organization. It can be seen as a best practice for developing and maintaining security standards and management practices within an organization to improve reliability on information security in inter-organizational relationships. It defines 133 security controls strategies under 11 major headings. The standard emphasizes the importance of risk management and makes it clear that it is not necessary to implement every stated guideline, only those that are relevant.

The guiding principles in ISO/IEC 27002:2005 are the starting points for implementing information security. They rely on either legal requirements or generally accepted best practices. Measures based on legal requirements include: protection and non-disclosure of personal data, protection of internal information and protection of intellectual property rights. Best practices mentioned in the standard include: information security policy, assignment of responsibility for information security, problem escalation and business continuity management, Calder (2006).

4.4. Interconnecting the standards COBIT, ITIL and ISO/IEC 27002

It may be useful to think of the three standards as an interconnected system network which aims to support the service management structure by offering a set of compliance rules of these standards inside every organization. Attempting to mix the three management specifications (COBIT, ITIL, and ISO 27002) is a very complex process which has been already the subject of many researches at worldwide level with the goal of obtaining a harmony between them in order to simplify the mapping of IT standards in organizations, Greenfield (2007). The interconnection of the three standards can be reflected in the following model:

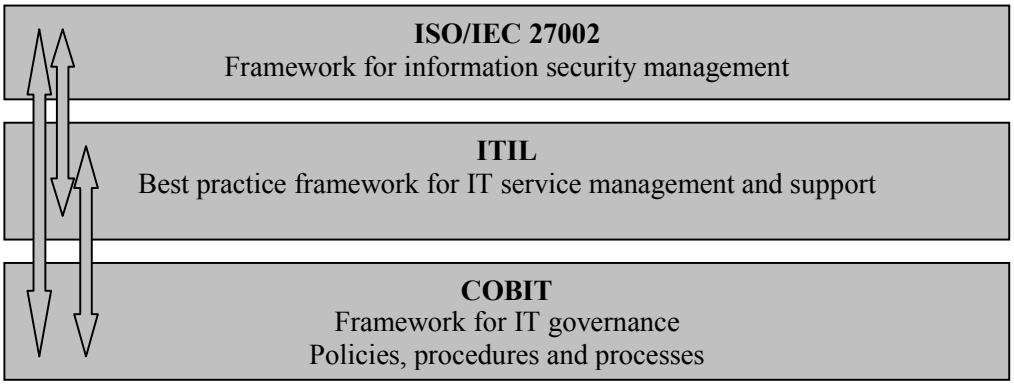

Figure 2. Interconnecting the standards

The international standard ISO/IEC 27002 represents a formal specification and organizations may seek accreditation to demonstrate compliance with the standard. It represents a framework for information security management which lays out a process for securing IT services and addressing legal requirements. The standard specifies best practices for security in 12 areas and offers guidance on such topics as protecting personal data, internal information and intellectual property. ISO/IEC 27002 is much

more different from COBIT and ITIL, because ISO27002 is a security standard, which has a smaller but at the same time deeper domain compared to COBIT and ITIL.

Next to ISO/IEC 27002 is the ITIL best practice guidance, which helps to ensure and demonstrate that the provisions of the standard are being met. ITIL was developed by the U.K. government and it describes how to go about implementing the processes in order to deliver IT services. It provides best practice guidance for IT service management and support which helps to ensure and demonstrate that the provisions of the standard are being met. As part of the presented network, ITIL processes may be used to achieve and demonstrate compliance with COBIT control objectives.

Although ITIL is quite similar with COBIT in many ways, there is a basic difference between the two of them. On one hand, COBIT sets the standards by focusing on the process based system and on the risks generated by the utilization of IT, and on the other hand ITIL sets the standards from the basic IT service.

COBIT is positioned as a high-level governance and control framework for IT processes which provide to management assurance and advice for improvement of IT processes. In other words, COBIT tells what to monitor and to control. COBIT's goal is to help IT understand the needs of the business and to put practices in place to meet them as efficiently as possible. The COBIT main function is to help the company, mapping their IT process to ISACA best practices standard. COBIT is usually chosen by a company which is performing information system audit, whether related to financial audit or to the general IT audit.

5. Guidance for Implementing COBIT, ITIL and ISO/IEC 27002

Specialists have concluded that the effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities which strives for standardization. Adoption of standards and best practices enables quick implementation of good procedures and avoids lengthy delays in creating and agreeing on new approaches of processes. However, the best practices adopted have to be consistent within a risk management and a control framework, appropriate for the organization, and integrated with other methods and practices that are being used. Standards and best practices don’t guarantee 100% success to a company which seeks to implement IT standards and controls. Their effectiveness depends on how well they have been implemented and kept up to date, Van Grembergen & De Haes (2008). It is the role of the management to include the standards and IT best practices into the continuous improvement project of their company, because the IT environment is

changeable and managers must be aware of all the changes and how they affect the IT processes.

5.1. Choosing the Best Standard

Before starting to implement the standards and objectives, one should be able to ensure that policies and procedures will be effectively utilized, which requires that management and staff personnel must understand what to do, how to do it and why it is important. Therefore, for best practices to be effective, the use of a common language and a standardized approach oriented towards real business requirements is a key factor, as it ensures that everyone follows the same set of objectives, issues and priorities.

Managers should focus first on where it is easier to make changes and deliver improvements, and build from there one step at a time. They also have to manage expectations because in most enterprises, achieving successful oversight of IT takes time and is a continuous improvement process, Nastase (2007).

Managers involved in the process of implementing IT standards and controls have always asked the question: which standard should be implemented first? Unfortunately, no one can give an exact solution to this problem, because it depends on the company's IT processes and procedures and on their requirements. It is true that most companies start to implement COBIT first because these standards cover in general all information systems. And after that, if needed, they usually choose between ITIL and ISO27002. The budget of the company should also be taken into consideration because COBIT's implementation usually runs from an internal audit budget while ITIL and ISO27002 are usually performed using an IT department budget, Priandoyo (2008). Taking into account that the budget is one of the most important elements in every project or in every activity of every organization, the last consideration is often used in order to decide what kind of standard should be implemented first, depending on the management policy. From the implementation point of view, ITIL is the easiest standard to be implemented, because ITIL can be implemented partially without any impact on the company's performance. For example, if the IT department lacks of budget its management can choose to implement only the IT Service Delivery layer, and the next year they he will try to implement IT Release Management or IT Problem Management. On the other hand both COBIT and ISO27002 are quite difficult to be implemented partially because they need to have an overview of all the processes first and only then can be implemented.

Not only budget is important to the management but also choosing the right provider of the required IT standard, because as specialists state, there is no single solution applying to all standards. On one hand, the COBIT provider usually comes from an Accounting Company which has an IT Audit department and on the other hand, the standards ITIL and ISO27002 usually come from a General IT Consulting Company, (IBM, HP, Accenture) or an IT networking company.

5.2. Identifying the Uses of Standards and IT Best Practices

Irrespective of the standard each company chooses for its IT processes and controls, the management needs to identify and establish the usage area and the roles of standards and practices to suit its individual requirements. All three IT standards can play a very useful part, COBIT and ISO/IEC 27002 helping to define *what* should be done and ITIL providing the *how* for service management aspects. Typical uses for these standards and practices aim to enable IT support governance such as providing a management policy and control framework, to align IT objectives with business objectives and to ensure an efficient IT resource allocation in order to realize the execution of the company's IT strategy.

Identifying the uses of standards and IT best practices contribute also to define requirements in service and project definitions to create a framework for audit/assessment or to facilitate continuous improvement by: maturity assessments, gap analysis, benchmarking, improvement planning and avoidance of re-inventing already proven good approaches.

5.3. Prioritizing

Because in every management decision process the budget represents a key factor, managers should avoid costly and unfocused implementations of standards and best practices by prioritizing where and how to use standards and practices. The enterprise needs to have an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction that management should follow. The management should be guided by helping align IT initiatives with real business needs and ensure that management appreciates the potential impact on the business of IT-related risks. The board should also insist that IT performance be measured and reported to the board and should establish an IT governing council with responsibility for communicating IT issues between the board and management. And last but not least the board should insist on the usage of a management framework for IT governance based on a common

approach such as COBIT and of a best practice framework for IT service management and security based on a global standard such as ITIL and ISO/IEC 27002.

5.4. Planning the Implementation of the Standards

After fulfilling the above steps, management can initiate and put into action an implementation approach of IT standards and best practices according to the suggestions and rules of the company which is responsible for the IT services support and framework. To help management decide where to begin and to ensure that the implementation process delivers positive results where they are needed most, the following steps are suggested, based on ITGI's *IT Governance Implementation Guide* (2007):

1. Set up an organizational framework (ideally as part of an overall IT governance initiative) with clear responsibilities and objectives and participation from all interested parties who will take implementation forward and own it.
2. Align IT strategy with business goals. This involves analyzing the current business objectives in which IT has a significant contribution and obtaining a good understanding of the business environment, risks and business strategy related to IT. COBIT's management guidelines (specifically the goals and metrics) help define IT objectives.
3. Understand and define the IT related risks which result from the enterprise's business objectives. COBIT contains a process for risk management which enables risks to be identified and owned. As an addition to COBIT, ITIL clarifies operational risks and ISO/IEC 27002 clarifies security risks.
4. Define target areas and identify the process areas in IT that are critical to delivering value and managing these risk areas. The COBIT process framework can be used in this situation as the basis, being completed by ITIL's definition of key service delivery processes and by ISO/IEC 27002's security objectives, Tarantino (2008).
5. Perform a maturity capability assessment and a gap identification to find out where improvements are needed most. The COBIT maturity models provide a general support to managers who may also decide to go more in detail using ITIL and ISO/IEC 27002 best practices.
6. Develop improvement strategies (such as continuous improvement initiatives) and set the highest priority projects that will help improve the management and IT governance. As in the step above, the COBIT control objectives offer the basis while ITIL and ISO/IEC 27002 support this process by more detailed guidance.

7. Establish a balanced scorecard mechanism using COBIT's goals and metrics and ITIL's seven-stage continual improvement approach for measuring current performance and monitoring the results of new improvements.

6. Recommendations - Aligning Best Practices

Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 is of particular value for enterprises that are undergoing change or restructure. As Robert Stroud, international VP of ITGI confirmed in a written statement, "the mappings of COBIT to other frameworks and standards, including ITIL and ISO/IEC 27002, are especially helpful in merger and acquisition situations". If the other organization involved uses a different standard or guidance, the mapping clarifies how processes from both organizations fit together.

The effective use of IT is critical to the success of an enterprise strategy, because it has the potential of being the major driver of economic wealth in the 21st century. Therefore, IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. COBIT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organization in general. Specific practices and standards such as ITIL and ISO/IEC 27002 cover discrete areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials.

REFERENCES

[1] **Andreica Ma.**, **Dobre I.**, **Andreica M.**, **Nitu M.**, **Andreica R.** (**2008**), ***A New Approach of the Risk Project from Managerial Perspective***, Journal of Economic Computation and Economic Cybernetics Studies and Research, issue 1-2, ASE Publishing House, Bucharest;

[2]**Calder, A. (2006),** ***Implementing Information Security Based on ISO 27001/ISO1779,*** Zaltbommel, Van Haren Publishing;

[3] **Greenfield, D. (2007),** ***ITIL, COBIT, and ISO 17799 Provide a Blueprint for Managing IT Services***, available on-line at:http://www.informationweek.com/news/management/showArticle.jhtml?articleID=204701897&pgno=1&queryText=&isPrev=

[4] **ISO 27000 Directory (2005),*****Introduction To ISO 27002 (ISO27002),*** http://www.27000.org/iso-27002.htm;

[5] **ISO/IEC (2005),** ***ISO/IEC 27002:2005 Information Technology -- Security Techniques -- Code of Practice for Information Security Management***, available on-line at: http://www.iso27001security.com/html/27002.html;

[6] **ITGI (2007*), COBIT 4.1 Executive Summary and Framework***, available on-line at: http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/Content Management/ContentDisplay.cfm&ContentID=34172
[7] **ITGI (2008), *COBIT Mapping: Mapping of ITIL V3 with COBIT 4.1***, Illinois, USA;
[8] **ITGI (2008), *Enterprise Value: Governance of IT Investments. The Val IT Framework 2.0 Extract***, available on-line at: http://www.isaca.org/Template.cfm? Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID =18925;
[9] **ITGI (2007) , *IT Governance Implementation Guide. Using COBIT and VAL IT,*** Illinois, USA;
[10] **Nastase P.**, **Gheorghe M.**, **Boldeanu D.**, **Aleca O.** (**2008**), ***Advanced Techniques in Financial Audit***, Journal of Economic Computation and Economic Cybernetics Studies and Research, issue 3-4, ASE Publishing House, Bucharest;
[11] **Nastase, P. & Ionescu, C.** (**2008**), ***Comparative Analysis Between the Audit Tools in IT Environments,*** 3rd International Conference – Accounting and Management Information Systems (AMIS 2008);
[12] **Nastase, P., Stanciu, V., Ali, E.** (**2007**), ***Auditul şi controlul sistemelor informaționale,*** Bucharest, Economica Publishing House;
[13] **Popa, S. & Ionescu, C. (2005), *Audit în medii informatizate***, Bucharest, Expert Publishing House;
[14] **Priandoyo, A. (2008), *Comparison between COBIT, ITIL and ISO 27001,*** available on-line at http://www.securityprocedure.com/comparison-between-COBIT-itil-and-iso-27001;
[15] **Sallé, M. & Rosenthal, S. (2005), *Formulating and Implementing an HP IT Program Strategy Using COBIT and HP ITSM,*** the 38th Hawaii International Conference on System Sciences;
[16] **Selig, G.J. (2008), *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management***, Zaltbommel, Van Haren Publishing;
[17**] Tarantino, A. (2008) ,*Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices,*** New Jersey, John Wiley & Sons Inc.;
[18*/ Van Grembergen, W. & De Haes. S. (2008), Implementing Information Technology Governance: Models, Practices and Cases***,** London, IGI Publishing;
[19] www.iso.org/iso/home.htm
[20] www.itil-officialsite.com/home/home.asp
[21] www.itsmfi.org
[22] www.ogc.gov.uk/sdtoolkit