



NAVUS - Revista de Gestão e Tecnologia

E-ISSN: 2237-4558

navus@sc.senac.br

Serviço Nacional de Aprendizagem

Comercial

Brasil

Gehrmann, Maico

COMBINING ITIL, COBIT AND ISO/IEC 27002 FOR STRUCTURING COMPREHENSIVE  
INFORMATION TECHNOLOGY FOR MANAGEMENT IN ORGANIZATIONS

NAVUS - Revista de Gestão e Tecnologia, vol. 2, núm. 2, julio-diciembre, 2012, pp. 66-77

Serviço Nacional de Aprendizagem Comercial

Santa Catarina, Brasil

Available in: <http://www.redalyc.org/articulo.oa?id=350450810007>

- How to cite
- Complete issue
- More information about this article
- Journal's homepage in redalyc.org



Scientific Information System

Network of Scientific Journals from Latin America, the Caribbean, Spain and Portugal

Non-profit academic project, developed under the open access initiative

# Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations

Maico Gehrman<sup>1</sup>

## ABSTRACT

Several methodologies, tools and standards have been designed to help IT management within organizations. Companies seek, with the use of these mechanisms, the placement of IT management and organizational strategies, mainly to ensure that IT helps with the objectives of the business and the results of the organization. Despite the vast amount of options for tools, methodologies and standards available, when they are used independently, these are not sufficiently wide-ranging to meet all the needs of IT management. This document analyzes ITIL, COBIT and ISO/IEC 27002 methodologies through literature review, highlighting their similarities and differences through the comparison between them. From this analysis, an overall structure is proposed which uses a combination of ITIL, COBIT and ISO/IEC 27002 that can be used by any organization as a more comprehensive solution for the handling and servicing of IT management. As any process, there are positive and negative points. Some negative points of a methodology may be strengthened by the positive ones of other methodologies. This creates more efficient processes.

Keywords: ITIL. COBIT. ISO/IEC 27002. Information Technology for Management

## 1 INTRODUCTION

The management of Information Technology (IT) proposes to guide and control a group of resource with the aim of achieving a particular goal in. This management encompasses several dimensions within an organization, among which may cite human resources, financial resources and technological resources as the key dimensions related to IT Management.

IT management in organizations is recent, some companies have already used widespread IT management methodologies, others have used their own methodologies and many organizations still do not have structured the management of their information technology.

There are several methodologies, standards, tools, frameworks and good practices for managing

<sup>1</sup> Mestrado em Engenharia de Produção pela Universidade Tecnológica Federal do Paraná - maicog@gmail.com

information technology. The most applicable and used today are ISO/IEC 27002, COBIT and ITIL. Each has its positive aspects and its limitations. As a result, this paper aims to combine the positive points of ISO / IEC 27002, COBIT ITIL in a comprehensive manner and propose an IT management structure that covers broader aspects and supports all the needs of the organizations for more efficient IT management.

The efficient use of IT by organizations is a goal to be achieved and has been sought after by many companies. Some of these companies have already achieved the level of complexity required by the use of these technologies, acquiring a competitive edge in the marketplace where they belong. This level can be achieved through the management of IT, however the management of IT has a much broader focus and is extremely complex. It contains much more comprehensive actions than the administration of information technology, for the users of these technologies and processes.

An area of IT management today must be composed of the combination of two sets of guidelines, the information technology itself and consequently, the business management. The main reason of this article is to address the use of combined methodologies ISO / IEC 27002, COBIT and ITIL as a tool for IT management, considering that there are several difficulties, deficiencies and needs that are not met by using only one methodology. That is because IT can take on different aspects within the organization, depending on the existing perspective. This can take on aspects of IT applications and infrastructure that are part of the processes and services of the company whose responsibility and technical support are provided by suppliers. In other aspects, the organization can have its own set of skills and resources to support the application and IT infrastructure. There are cases that can be categorized as services used by companies, and the total responsibility lies on the service provider. Considering all aspects, it is clear the importance of defining, implementing and applying an IT management.

## 2 CONCEPTUAL FOUNDATIONS

### 2.1 Information Technology

Information Technology (IT) can be regarded, generally, as a collection of information resources of an organization, its users and its management, including the IT infrastructure, and all other information systems of an organization (POTTER; RAINER JR.; TURBAN, 2005). In this context, IT is defined as the macro environment where the information systems are embedded, comprising of IT tools (hardware, software and networks), people, services and IT management (GTI), which aims to support the business organization at all organizational levels. The main methodologies of GTI are based on the study of this article, which aims to assess how GTI can reconcile COBIT, ITIL and ISO / IEC 27002.

Embedded within the IT context, there are information systems (IS) that are considered by O'Brien (2004) as a group of interrelated components working toward a common goal, receiving inputs and producing results in an organized transformation process. In the areas of IT, there is a data entry process, the processing of this data, and an output of information. Through this process, one of the main objectives is the cost-efficient process of data to generate information and knowledge (POTTER; RAINER JR.; TURBAN, 2005). Data processed by information systems has no value for the organization if it cannot be turned into information and knowledge. It will only be generating an expense in storage without being able to offer any benefit or competitive advantage.

### 2.2 IT Management

IT Management (GTI) is essential for the managing of the operations, information and knowledge of the organization, thus helping the company to maintain or expand its economic and social activities. These guidelines should be aligned to the strategies and objectives of the organization. According to the Board Briefing on IT Governance (ITGTI, 2008), GTI is the responsibility of the corporate directors and executive management. It is an integral part of corporate governance and consists of leadership, organizational structures and processes that ensure that the IT of the organization sustains and expand the strategies and objectives of the organization. In order to improve the competitive dimensions of the company and maximize its results, the IT departments assess ways of structuring their governance models, in order to fully adapt to the

trends and strategic demands of the business, reviewing roles, responsibilities, processes and procedures, as well as the portfolio of products and services so that they have complete adherence to the requirements of the competitiveness required in the markets where they operate (OLIVEIRA, 2007).

GTI can offer many benefits to an organization, but it is difficult to assess these benefits, since the results generated by GTI can be tangible or intangible. To evaluate these benefits, several methodologies can be used to measure the actual benefits of GTI. Besides the benefits, the use of IT offers great risks to the organization, it is up to GTI to assess and manage these risks. There are several ways for GTI to assess the benefits and risks of the use of IT in organizations; the purpose of this paper is not to discuss the methodologies used by companies to measure the benefits of GTI, but to evaluate the benefits that GTI brings to the organization, regardless of the methodology used.

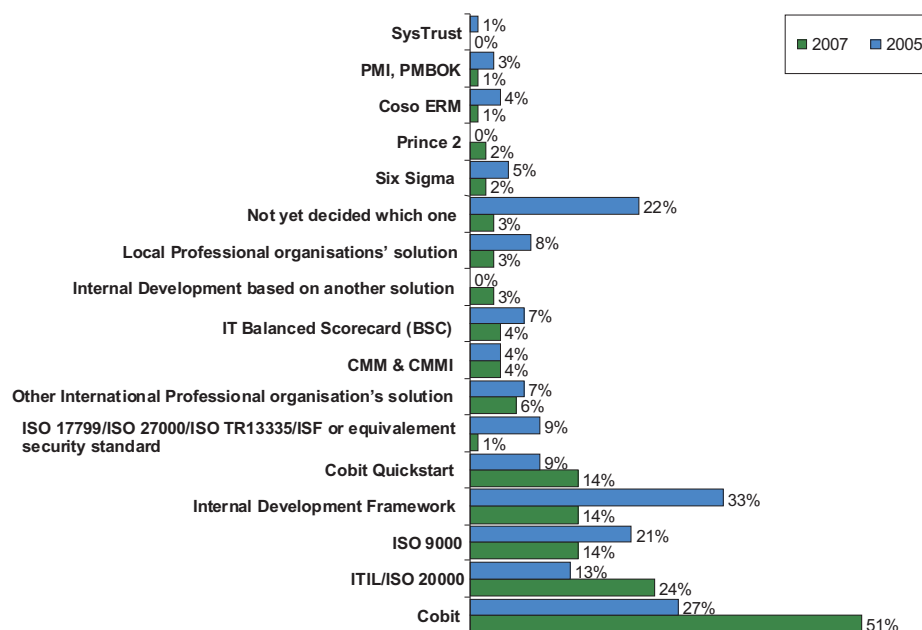
A methodology used by some companies to manage its information technology is Cobit (Control Objectives for Information and Related Technology) that was developed by ISAC (Information Systems Audit and Control Association); this model assumes the use of good practices and indicators for GTI (OLIVEIRA, 2007). Another way that GTI is widely used is the ITIL (Information Technology Infrastructure Library) which was developed by the British Government and has an efficient structure and it has been adopted by various organizations being recognized worldwide as a standard for service management. The ISO / IEC 20000 and ISO / IEC 9000 series are also widely used to standardize security IT in organizations.

Regardless of methodology or form of assessment used, the goal of GTI is to help the organization and to improve its competitive advantage compared to its competitors. Chase, Jacobs and Aquilano (2006) comment that the competitive advantage occurs from the time that organizations design efficient and effective operations. Efficiency means doing something at the lowest possible cost and effectiveness means doing the right thing to create the greatest value to the company.

Given this perspective, to identify the contribution of GTI and the use of IT in organizations is a more plausible to measure this contribution through the creation of IT indicators that should be aligned with strategic indicators that govern the organization.

This will create a direct relationship between the company's results and the GTI results, and therefore the organization can improve its competitive results. It will also improve its efficiency and effectiveness. GTI will be helping this result and this evidence can be shown by the results of the indicators that were created.

Figure 1 – GTI Solutions Used



Source: Adapted from the IT Governance Global (2008)

The growing quest for methodologies and standards for GTI by organizations comes from the U.S. Sarbanes-Oxley law. The law was created in June 2002 after several scandals in organizations that were manipulating their financial results. As IT is the main tool used by organizations to generate data, the reliability of the company's financial information is heavily dependent on IT tools, and organizations are adopting these methodologies and standards to highlight safety to the financial market about the GTI that has been adopted. In addition to COBIT, ITIL and the ISO / IEC standards there are other methodologies which are used by many organizations to standardize processes within the GTI. It is up to these organizations to assess whether these methods adhere to standards and methodologies commented on by this article. As seen in Figure 1, COBIT methodologies are the most disclosed and widely used by organizations, as claimed by the IT Governance (2008).

### 3 METHODOLOGY

The research methodology used in this article has some basic features, qualitative and exploratory, because it aims to provide greater familiarity with the problem in order to make it explicit or construct hypotheses. It generally takes the forms of literature searches (SILVA, 2009).

Procedures using bibliographic research were adopted, which aim to study different methods of IT management, adding the strengths of these tools in a compound methodology. The compound methodology that is shown seeks to structure IT management more comprehensively in organizations, providing a better control of processes and IT services and therefore better competitiveness, results and benefits for the organization.

The bibliographic research is based on international publications because these IT management methodologies began to be used in Brazil a few years ago, but are widespread references in the international context and also because there are few researches and publications about these subjects in the national context. This research was drawn from previously published material, consisting mainly of books, articles from periodicals and material currently available on the Internet (SILVA, 2009).

### 4 PROPOSED COMBINATION BETWEEN ITIL, COBIT AND ISO/IEC 27002

#### 4.1 ITIL

ITIL or Information Technology Infrastructure Library is a library of good practices related to the services of Information Technology (IT). ITIL was developed in England in the late 1980's by the Central Computer and Telecommunications Agency (CCTA), which is currently recognized as the Office of Government Commerce (OGC). ITIL provides a framework for good practices to guide the management of IT services; the acceptance of this methodology is growing and becoming a widely accepted approach to managing IT services throughout the world (ZHANG et al., 2009).

Many worldwide organizations are adopting these good practices to improve the control of IT services that are outsourced by companies. The increase on outsourcing these services is against the ITIL philosophy. Its acceptance within organizations is growing because with its use companies are achieving improvements in the outcome of these processes. OGC defines service as a means of providing a value to a client, making it easier to achieve the same results without the costs of ownership and the specific risks.

##### 4.1.1 SERVICE STRATEGIES

The service strategy provides guidance for the design of the scope, development and implementation of service management based on the capacity and organizational strategy perspective. These guidelines empower the organization in relation to the principles that should underpin the management practices of the services. The ITIL management service represents the development activities of internal and external suppliers, control of services and implementation of control strategies through their life cycle. These principles are extremely useful to develop policies to manage and control the lifecycle of ITIL services. The service

strategies of ITIL. The service strategy should include actions in the following processes:

- Financial Management.
- Service Portfolio Management.
- Demand Management

#### 4.1.2 SERVICE PROJECTS

The process of projects service includes the guidelines for design and development of services and processes related to IT management. These actions include the conversion process of strategic objectives which has already been defined in a portfolio of services. Through this process, necessary changes and improvements are adopted in order to enlarge and maintain the value of IT to its users during the life cycle of the services related to them. The continuity of these services, the assessment of service levels and the correlation with the rules and regulations governing information security are some of the responsibilities of their service project, which also include the following processes:

- Service Managing Catalogs
- Service Levels Management
- Availability Management
- IT Services Continuity Management
- Capacity Management
- Information Security Management Suppliers
- Data and Information Management Business

#### 4.1.3 TRANSITION SERVICES

This library offers guidance with the development and improvement of transition capacities from current processes for new services, transforming these processes into operations. The transition of services lists the requirements of service strategy, analyzes the services project and effectuates this context into service operations, controlling the risks of failure and providing guidance about the requirements of the Service Strategy encoded in Service Design which are effectively carried out in the service operation, controlling the risks of a failure. This part of the ITIL framework combines practices in the management of the version, program management and risk management and places them in the context of the management services practice.

- Change Management.
- Service asset and Configuration Management.
- Release and Deployment Management.
- Transition Planning.
- Stakeholders Management.
- Knowledge Management.
- Support and Service Evaluation.

#### 4.1.4 SERVICE OPERATION

The Operation of Service incorporates the practices of servicing objectives in order to achieve effectiveness and efficiency in the delivery and support services to ensure a value for the customer and the service provider. The management processes of the services operation are:

- Event Management
- Incident Management
- Orders Requesting Service Management
- Problem Management
- Access Management

- Technical Management
- IT Operations Application Management

#### 4.1.5 CONTINUOUS IMPROVEMENT OF SERVICES

Many organizations have been applying continuous improvement in their management processes, production, among others. Following this trend, the organizations have realized that the incremental improvement has had a large effect on service quality, operational efficiency and the continuity of services. This library guides the creation and maintenance of values for customers through a better conception, implementation and operation of the services. Understanding and combining the principles, practices and methods of quality management, change management and capacity management. These processes include:

- Services Measurement.
- Reporting Services.
- Process Improvement in 7 Steps.

#### 4.2 COBIT

COBIT (Control Objectives for Information and related Technology) was created by ISACA (Information Systems Audit and Control Association) through the ITGI (IT Governance Institute); its objective is to provide good practice through a structured international standardization process of IT. The implementation of the GTI through the COBIT standards helps to relate the IT strategy to the business requirements, to organize the activities of IT accepted process and standardized models; to identify the key IT capabilities and the leveraging of the results and the defining of control objectives to be considered by the GTI. The mission of COBIT includes research, development, dissemination and promotion of authority, update and the international acceptance of GTI control accepted by organizations, which is increasingly used by the management in their businesses, IT professionals and professional guarantee - COBIT 4.1 (ITGI, 2007). COBIT guarantees GTI through a structure that aligns IT to the business strategy, enabling IT to the business and maximizing its benefits, ensure the responsible use of the IT resources and appropriate management of IT risks. Ridley, Young and Carroll (2004) argue, the proper alignment between the use of IT and the business objective of the organization is fundamentally an efficient and effective GTI.

This structure is based on the following 5 areas of focus of COBIT as can be seen in Figure 3. While a range of standard structures and documents emphasize the need for the control of IT, the primary focus of COBIT is aligning the use of IT to achieve the goal of the organization (RIDLEY; YOUNG; CARROLL, 2004). The strategic alignment links the business plan the company to the GTI, aligning IT with the company's operations. The value of the service ensures the delivery of the targets optimizing costs and proving the value of IT in the strategic outcome. Resource management aims to optimize the IT tools (applications, information, infrastructure and people), managing critical resources, improving investment and knowledge about these resources. Risk management provides a clear vision of the significant risks to the company, incorporating the responsibilities of risk management to the organization. Performance measurement monitors the implementation of strategies, project completion, and use of resource, performance of provided services, balancing and translating strategies into action to achieve the goals.

The GTI shouldn't be considered only as a support for the organization, but as a primary tool for maintenance of administrative management and strategy of the company. The main objective is to build and maintain the support of IT tools as defined by Potter et al. The analysis of this process must ensure and guide the company in deciding about new projects, purchases of new IT tools and the efficient use of existing tools, following the technological evolution which occurs quickly and often radically nowadays.

The structure of COBIT is organized in some areas that are interrelated in order to reflect a model for the processes related to IT. These areas have their own process characteristics and exact activities. As seen in Figure 3, which represents the overall structure of COBIT, the areas include Planning and Organization, Acquisition and Implementation, Delivery and Support and Monitoring and Evaluation.



#### 4.2.1 ORGANIZATION AND PLANNING

The process of planning and organizing COBIT deals with strategies and tactics. It also focuses on identifying the way IT can best contribute to the achievement of the business objectives. To achieve a strategic vision planning, discussions and management of different perspectives of evaluation are necessary. The organization that has an IT infrastructure can deploy this model, which usually deals with the following design issues according to Nabiollahi and Sahibuddin (2008):

- Define a Strategic IT Plan.
- Define Information Architecture.
- Determine technological management.
- Define IT processes, the Organization and Relationships.
- Manage IT investments.
- Communicate Management and Board Goals.
- Manage HR in IT.
- Manage Quality.
- Identify and Manage Risks.
- Manage Projects.

#### 4.2.2 ACQUISITION AND IMPLEMENTATION

Acquisition and Implementation relate to the IT strategy. The solutions need to be identified, developed or acquired, implemented and integrated within the business process. Improvements to the maintenance of existing IT are responsible for that domain, ensuring that these solutions continue to meet business objectives and normally deal with the following questions for acquisition and implementation (BRENNER, 2009).

- Identify automated solutions.
- Acquire and Maintain Software Applications.
- Acquire and Maintain Technology Infrastructure.
- Enable operation and utilization.
- Look For IT resources.
- Manage Change.
- Install and Approve Solution and Change.

#### 4.2.3 DELIVERY AND SUPPORT

Delivery and support are concerned with the delivery of required services, including distribution services, security management and continuous service support to users. This area is also responsible for managing data and operational facilitating, which normally deals with the following questions of delivery and support (NABIOLLAHI; SAHIBUDDIN, 2008):

- Define and Manage Service Levels.
- Manage Third Party Services.
- Manage Performance and Capacity.
- Guarantee Continuous Service.
- Ensure System Security.
- Identify and Allocate Costs.
- Educate and train users.
- Manage Services and Incidents.
- Manage the configuration.
- Manage problems.
- Manage Data.
- Manage the Physical Environment.
- Manage Operations.



#### 4.2.4 MONITORING AND EVALUATION

All IT processes need to be regularly assessed in order to measure their quality and compliance with operational requirements. It includes activity performance management and monitoring of internal controls, which usually deals with the following issues of monitoring and evaluation (BRENNER, 2009).

- Monitor and evaluate IT performance.
- Monitor and evaluate internal control.
- Ensure Compliance with external requirements
- Provide IT Management.

Based on the four areas that COBIT is structured, the methodology GTI 34 defines control objectives that should be used for the continuing evolution of this process. These goals are listed in their respective fields, which represent how the GTI is benefited by the use of this structure. The organizational data are generated and modified by IT resources, this information is necessary for the field of planning and organization and its goals. The output requirements of the planning and organization area are information requirement inputs for the Acquisition and Implementation domain and goals that define the entry requirements for domain Delivery and Support, and then define the entry requirements Domain for Monitoring and Evaluation.

#### 4.3 ISO/IEC 27002

It corresponds to a series of guidelines and principles that serve to initiate, implement, maintain and improve the management of IT in organizations. This norm has as its focus, the management of HISMSH information security, an internationally recognized standard because of its good practice for the security of information. This regulation lists a number of specific security controls to be followed and a number of specific security controls that are suggested to be implemented.

The standards of ISO/IEC are internationally recognized and they are disclosed and accepted by organizations. This shows the relevance and importance of these established standards that include the best security practices for companies in any sector of the economy, regardless the branch operations because they need to protect their information. This normalization is sub-divided into 11 sections (SAINT-GERMANY, 2005):

- Information; Security Policy.
- Organizing Information Security.
- Asset Management.
- Safety of Human Resources.
- Physical Security and the Environment.
- Operations and Communications Management.
- Access Control.
- Acquisition, Development and Maintenance of Information Systems.
- Information Security Incidents Management.
- Business Continuity Management.
- Compliance.

#### 4.4 ITIL compared to COBIT

The difference within the ITIL methodology is the way the processes are described and treated with different activities and flowcharts that guide organizations to use IT efficiently and effectively. If there is an excellent cost-benefit ratio, it deals with the issues of implementing new technologies and guidance for the analysis of critical success factors. However, the critical success factors are better described and addressed by COBIT.

COBIT is better structured to address issues related to IT auditing, being widely used and appropriate for this purpose. With striking features when it comes to issues related to management, COBIT references the Critical Success Factors along with Performance Indicators and maturity models of capacity. Simonsson and Johnson (2008) argue that ITIL does not support the strategic interests of IT. For this purpose COBIT is

recognized to have better governance structures.

Comparing ITIL with COBIT, it can be seen that they are very similar and both models are structured with high similarity of IT management, especially COBIT that uses the ITIL methodology for grounding its structure in its latest version.

Many problems addressed by these methodologies have slightly different connotations as it can be seen in Frame 1 but they treat the same problems and issues.

Frame 1 – Similarity between the ITIL and COBIT processes

ITIL	COBIT
Incident Management	Administrate the problems and incidents
Problem Management	Administrate the problems and incidents
Configuration Management	Administrate and Configure
Change Management	Administrate Change
Version Management	Administrate Change and Configuration
Service Level Management	Define and Manage Service Levels
IT Services Financial Management	Identify and carry out Appropriation Costs
Capacity Management	Administrate Performance and Capacity
Continuity of Service Management	Ensure Continuity of Services
Availability Management	Administrate Performance and Capacity

Fonte: The autor

The ITIL methodology has a difference in its structure, this deals with incident management with a specific approach in its structure, which has no equivalent section within the COBIT framework. This, however, does not mean that despite not having an equivalent section, the COBIT methodology does not address the approach to this problem in other parts of its structure or with a different approach. ITIL handles this in a very detailed way and the levels of maintenance of service (SLA) and level of operating agreements (OLA) (SIMONSSON; JOHNSON, 2008).

#### 4.5 ITIL and COBIT related to ISO/IEC 27002

The ISO/IEC 27002 standard is widely used to address issues related to information security and not only the problems related to IT management. With these general objectives, it is clear that the ISO/IEC 27002 standard does not correspond to an equivalent to the ITIL methodology as we can compare the ITIL methodology and the COBIT methodology. Saint-Germainy (2005) highlights that the implementation of security and control of ISO/IEC 27002 standards combined with ITIL or COBIT diminish the critical threats that may interfere with the results of the project.

ISO/IEC 27002 has its main structure to be applied based on an organization and guarantees the overall safety at all levels of information security of an organization. The problem of administration and management addressed by ITIL and COBIT methodologies does not have an equivalent structure addressed in the ISO/IEC 27002 standard.

The management of configurations has a major impact on the IT environments, which should be handled safely. The ISO/IEC 27002 has features to preserve the confidentiality, integrity and availability of the information in organizations. This availability of information is handled within the ITIL and COBIT with aspects of quality, reliability and maintenance of IT. Simonsson and Johnson (2008) emphasize that the ISO/IEC 27002 together with the ITIL can help the creation of processes related to the delivery and support of IT.

Another point that may be compared with these methodologies is related to financial issues, as the ISO/IEC 27002 does not address this issue comprehensively. It only deals with risk management, leaving it up to the executor to control and reduce the risk to avoid increasing costs. This approach which is treated differently by ITIL and COBIT, provides an effective risk management and financial aspects of IT-related costs

In Frame 2, the characteristics related should be used in each methodology to compose a more

comprehensive, efficient and effective methodology.

Frame 2 – Combination of the Proposed Methodology

ITIL	COBIT	ISO/IEC 27002
Concepts / Processes	Critical Success Factors	Information Security
Activity	(CSF, KPI) Metrics	
Cost / Benefits	Good Practices (CMM)	
Planning for deployment	Auditing	

Fonte: The autor

Based on the characteristics of each of these methodologies, the strengths and weaknesses of their structures was evaluated. It can be concluded that the combined use of ITIL, COBIT and ISO/IEC 27002 methodologies should be implemented as shown in Frame 2.

Frame 2 was established by comparing similar control objectives between the ITIL, COBIT and ISO / IEC 27002 methodologies. The identification of good practices (Frame 2) between the methods was listed by the handling of the approaches dealt with by each objective. The Critical Success Factors of the Cobit methodology address a larger number of aspects in comparison to the ITIL and ISO/IEC 27002 methodologies.

As a result of this work the proposed suggestion is that ITIL methodology should be used to define the strategies, concepts and processes related to IT management. COBIT should be used to evaluate the critical success factors, metrics, indicators and audits. In addition, the ISO/IEC 27002 standard should guide the management of IT in relation to issues of IT security.

## 5 CONCLUSION

The efficient use of IT by organizations is a goal to be achieved and has been sought after by many companies. Some of them have already achieved this level of complexity required by the use of these technologies, acquiring as a result, a competitive edge in the marketplace where it operates. This level can be achieved through the GTI, however the GTI has a much broader focus and it is extremely complex.

There are many more comprehensive actions than the administration of information technology, for users of these technologies and processes that they operate.

There are several developed and distributed methodologies in organizations to manage information technology. Regardless the methodology used, the objective of GTI is to help the organization improving their competitive advantage compared to its competitors. Chase, Jacobs and Aquilano (2006) argue that the competitive advantage occurs from the time that organizations conceive efficient and effective operations. Efficiency means doing something at the lowest possible cost and effectiveness means doing the right thing to create the greatest value for the company. In this context, IT operations must be carried out efficiently, minimizing security risks and in accordance with legal requirements.

These goals are difficult to achieve, even as the methodologies of IT management are more effective and comprehensive in some aspects and contrariwise. In order to achieve better results and meet all the needs of IT management, the article proposes an organization to use a combination of ITIL, COBIT and ISO/IEC 27002 to achieve the organizational goals.

As is proposed throughout this work (items 4 to 4.5), the combination between the management methodologies of ITIL, COBIT and ISO/IEC 27002 will provide a more comprehensive and efficient approach, enabling features that were not previously considered by the use of a single method begin to be addressed and controlled by the organization.

The relationship between these methodologies suggests several aspects in common as can be seen in Frame 1, after the analysis of the interaction and the good practices of the methodologies was possible to propose a model of interaction between these models that can be seen in Frame 2.

## COMBINANDO ITIL, COBIT E ISO / IEC 27002 PARA A ESTRUTURAÇÃO DA TECNOLOGIA DA INFORMAÇÃO ABRANGENTE NA GESTÃO DAS ORGANIZAÇÕES

### RESUMO

Várias metodologias, ferramentas e padrões foram concebidos para ajudar a gestão em TI dentro das organizações. As empresas procuram com o uso desses mecanismos, a colocação do gerenciamento de TI e estratégias organizacionais, principalmente para garantir que a TI contribui com os objetivos do negócio e os resultados da organização. Apesar da grande quantidade de opções disponíveis de ferramentas, metodologias e padrões estes não são suficientemente abrangentes para atender todas as necessidades de gestão de TI, quando usados de forma independente. Este documento analisa ITIL, COBIT e ISO / IEC 27002 metodologias através de revisão bibliográfica, destacando suas semelhanças e diferenças através da comparação entre os citados. A partir desta análise, uma estrutura geral é proposta, cuja esta, usa uma combinação de ITIL, COBIT e ISO / IEC 27002 que pode ser utilizada por qualquer organização como uma solução mais abrangente para o manuseio e assistência da gestão de TI. Como qualquer processo, há pontos positivos e negativos. Alguns pontos negativos de uma metodologia pode ser reforçada pelos positivos de outras metodologias. Isso cria processos mais eficientes.

Palavras-chave: ITIL. COBIT. ISO / IEC 27002. Tecnologia da Informação para Gestão.

### REFERENCES

BRENNER, Michael et al. **Towards an Information Model for ITIL and ISO/IEC 20000 processes**. IEEE Computer Society and Information Engineering. [2009]. Available at: <<http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D5188795%26isnumber%3D5188779&authDecision=-203>>. Accessed: July, 3., 2009.

CHASE, Richard B.; JACOBS, F. Robert; AQUILANO, Nicholas. **Administração da Produção para a Vantagem Competitiva**. 10. ed. Porto Alegre: Bookman, 2006.

NABIOLLAHI, Akbar; SAHIBUDDIN, Shamsul Bin. **Considering Service Strategy in ITIL V3 as a Framework for IT Governance**. [2008]. Available at: <[http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?isnumber=4631524&arnumber=4631631&count=113&index=106](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?isnumber=4631524&arnumber=4631631&count=113&index=106)> . Accessed: July, 3., 2009.

IT GOVERNANCE. **Global Status Report**. [2008]. Available at: <<http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=50272&TEMPLATE=/ContentManagement/ContentDisplay.cfm>>. Accessed: May, 30., 2009.

ITGTI - IT GOVERNANCE INSTITUTE. **CobiT 4.1**. Illinois: IT Governance Institute, 2007.

ITGTI - IT GOVERNANCE INSTITUTE. **Board Briefing On It Governance**. 2. ed. 2008. Available at: <[http://www.itgi.org/AMTemplate.cfm?Section=Board\\_Briefing\\_on\\_IT\\_Governance&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39649](http://www.itgi.org/AMTemplate.cfm?Section=Board_Briefing_on_IT_Governance&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39649)>. Acesso em: April, 18., 2009.

O'BRIEN, James A. **Sistemas de Informação: e as decisões Gerenciais na Era da Internet**. São Paulo: Saraiva, 2004.

OLIVEIRA, Fátima Bayma de (Org.). **Tecnologia da informação e da Comunicação: a busca de uma visão ampla e estruturada**. São Paulo: Pearson Prentice Hall, 2007.

POTTER, Richard E.; RAINER Jr, R. Kelly; TURBAN, Efrain. **Administração de Tecnologia da Informação: Teoria e Prática**. Rio de Janeiro: Elsevier, 2005.

RIDLEY, Gail; YOUNG, Judy; CARROLL, Peter. **COBIT and its Utilization: A framework from the literature**. IEEE Transactions on Systems, Man and Cybernetics. Part B, Cybernetics, United States, Jan. [2004]. Available at: <  
<http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D1265566%26isnumber%3D28293&authDecision=-203>>. Accessed: May, 25., 2009.

SAINT-GERMAIN, Rene. Information Security Management Best Practice Based on ISO/IEC 17799. **The Information Management Journal**, v.25, n.1, Jul./Aug. 2005. Available at:  
<[http://www.sis.pitt.edu/~dtipper/2825/ISO\\_Article.pdf](http://www.sis.pitt.edu/~dtipper/2825/ISO_Article.pdf)>. Accessed: July, 3., 2009.

SILVA, Cassandra Ribeiro de O. **Metodologia e Organização do projeto de Pesquisa: Guia Prático**, 2009. Available at:  
<[http://www.cefetce.br/Pesquisa/dippg/metodologia/Metodologia%20e%20Organiza%E7%E3o%20de%20Pesquisa\\_apostila.pdf](http://www.cefetce.br/Pesquisa/dippg/metodologia/Metodologia%20e%20Organiza%E7%E3o%20de%20Pesquisa_apostila.pdf)>. Accessed: April, 19., 2009.

SIMONSSON, Marten; JOHNSON, Pontus. **The IT organization modeling and assessment tool: Correlating IT governance maturity with the effect of IT**. IEEE Transactions on Systems, Man and Cybernetics. Part B, Cybernetics, United States. [2008]. Available at:  
<<http://www2.computer.org/portal/web/cSDL/doi/10.1109/HICSS.2008.447>>. Accessed: August, 25., 2009.

ZHANG, Shaohua et al. **ITIL Process Integration in the Context of Organization Environment**. IEEE Computer Society and Information Engineering, United States. [2009]. Available at: <  
<http://www2.computer.org/portal/web/cSDL/doi/10.1109/CSIE.2009.691>> . Accessed: July, 3., 2009.