Enterprise Security Governance

A practical guide to implement and control Information Security Governance (ISG)

Gustavo Alberto de Oliveira Alves, Luiz Fernando Rust da Costa Carmo and Ana Cristina Ribeiro Dutra de Almeida
Computer Center (NCE)
Federal University of Rio de Janeiro (UFRJ)
Rio de Janeiro, Brazil
(galberto, rust,anaalmeida)@nce.ufrj.br

Abstract - **Following the advances of Information Technology (IT) Management and Information Security, organizations have felt the need to standardize their activities and, principally, to integrate any technological action with short- and long-term business objectives and administrative strategies. Through the interrelationship of corporative and technological governance, with Information Security Governance (ISG), it becomes possible to reach this alignment, contributing to corporative results. The purpose of this paper is to present a framework for implementing Information Security Governance, which considers the integration between strategical objectives and their indicators - Balanced Scorecard (BSC) - with IT business objectives from CobiT, as well as security best practices from ISO/IEC 17799.**

Keywords: Information Security Governance; Security Dashboard; Security Scorecard

I. INTRODUCTION

The great challenge for managers is to implement information security aligned with business objectives in actual organizations, considering that business globalization has increased considerably, and new regulations and laws have been established. Business globalization has been facilitated by the growth of the commercial use of the Internet.

It is important to point out that the Internet was not created for commercial purposes, but as a simple means for information exchange among researchers in the whole world. Security was not a critical factor at that time. However, with the increasing commercial use of the Internet, its vulnerabilities have been exploited, causing upheavals to some companies which use it for running their businesses. According to the last CSI/FBI report [12], the number of security incidents grows in alarming ratios each year. These statistics indicate that the Information Security area will gain considerable relevance in the next few years. A recent study [13] shows that the number of security professionals in IT can grow at an annual rate of 14% until the year 2008. The study was led by IDC for the International Information Systems Security Certification Consortium – ISC^2. In accordance with the survey, the number of professionals working in the security area will totalize 2.1 million in 2008, 61.5% more than the total verified last November, of 1, 3 million.

Together with this foreseen significant IT enhancement, there is also a recent demand on companies to align internal procedures with best practices, as a prerogative of new regulations and laws. An example of this situation is the actual effort realized by some organizations to be in conformity with Sarbanes-Oxley Act (SOX), which has caused a great impact in financial reports, auditing, internal controls, and in corporate governance. These laws aim to prevent new scandals, such as Enrons, WorldComs and Tycos, from occurring in other companies.

The present work proposes a framework for implementing Information Security Governance (ISG), which considers major aspects such as: (i) maturity level of information security in the organizations; (ii) action plan to reach target goals; (iii) risk evaluation of major processes; (iv) selection of indicators to track Information Security (IS) evolution; (v) identification of main critical factors of success; (vi) integration of operational indicators with strategical indicators and (vii) difficulties in the implementation of an information security governance. The current approach considers the integration between strategical objectives and their indicators (BSC), with IT business objectives from CobiT, as well as security best practices from ISO/IEC 17799. Through the interrelationship between those three elements, it becomes possible to create a framework to support ISG.

This paper is organized as follows: Section II presents some concepts about information security; Section III introduces governance concepts, distinguishing information security from corporate governance; Section IV describes the proposed framework for ISG following an evolutionary approach; Section V suggests a practical guide for implementing ISG based on the proposed framework; Section VI describes the requirements for the success of the framework; Section VII describes some related work and finally, section VIII reports some of the conclusions of this paper.

II. INFORMATION SECURITY BACKGROUND

According to ISO/IEC 17799 [4] (information security best practices), information is an asset, and like any other important corporate asset, has value for the organization, and therefore, must be appropriately protected. Information security protects information assets from many different threats in order to keep business running smoothly, minimize the impact of such threats, and maximize business opportunities/Return of Investment (ROI).

ISO/IEC 17799 argues that information protection is the fundamental concern of information security and can be seen as the discipline to ensure confidentiality, integrity, availability, authentication, non-repudiation, and compliance

(with appropriate law and regulations) of assets. However, it is not always necessary to bring together all those properties to reach an acceptable security level. For example, considering a site with public information, it is necessary to guarantee availability and integrity; however, as information is classified as public, confidentiality is not required.

Different nomenclatures are used to describe a security scenario: (i) *asset* – everything that has value for business (people, technology, physical infrastructure); (ii) *threats* – potential agents for causing a security incident (hackers, crackers, natural agents, etc); (iii) *vulnerabilities* – flaws which can be exploited by threats (e. g. accounts without passwords, buffer overflow, etc); (iv) *risk* – risk evaluation allows the identification of asset threats, vulnerabilities and incident occurrence probabilities, and the impact of exposure for each risk factor.

III. GOVERNANCE

Governance is the act of creation (and maintenance) of an efficient/optimal corporate structure. It is achieved by integrating persons, processes and technology and by creating an appropriate organizational culture for reaching corporate success. Some important governance concepts will now be introduced.

Vision - perception of what the market needs and how the organization will support it.

Mission - is the formalized set of corporate intentions and aspirations to be intentionally spread throughout all departments.

Transparency - the main executive and chief executive officers (CEOs) must provide all pertinent information, beyond the ones required by law or regulation, as soon as it is available, to all interested parties, prevailing substance above over form; the board of directors must supply transparent information, using an accessible format to the target public.

Equity – can be characterized by a fair and equal treatment for minority groups, shareholders, stakeholders, customers, suppliers, creditors and related others; discriminatory approaches, or policies, are totally unacceptable under any circumstances.

Accountability - agents of the corporate governance must always provide reports of their performance, thus being wholly responsible for all their acts.

Corporative Responsibility - council members and executives must look after the durability of their organizations sustainability, taking social and ambiental issues into account; corporative responsibility is an ampler vision of this strategy, including all the relationships with the community where the company is located.

A. Corporate Governance

Corporate governance is directly related to the concepts of vision, mission and organization strategy, i.e., whenever one of these elements is incorrectly planned or defined, the company might veer away from its business objectives. Information security governance will inherit the concepts from corporate governance (figure 1).

Figure 1. Governances

B. Information Security Governance

Information security governance (figure 2) is the act of directing and controlling an organization aligned with the strategy and business objectives, establishing and retaining a culture of information security, optimizing the related processes (based on indicators and learned lessons), and assigning activities to the most competent people to perform the necessary actions. The board of directors must support all those actions.

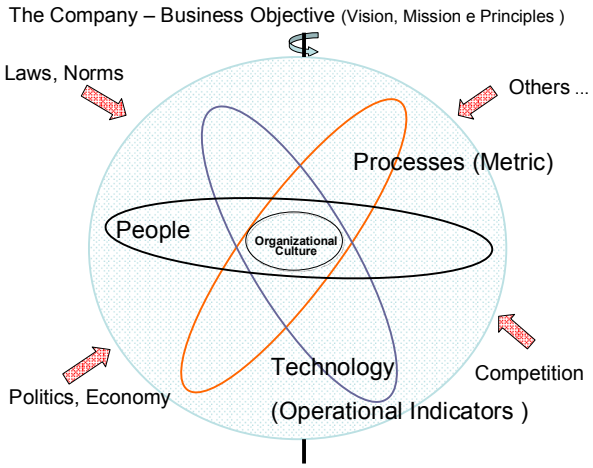

Figure 2. ISG concepts

IV. AN INFORMATION SECURITY GOVERNANCE FRAMEWORK

A. Governance, Processes and Operational

Nowadays, one of the greatest difficulties experienced by IT professionals is to anticipate negative/positive impacts that daily operations can cause in the company. Figure 3 illustrates the relationship between governance, processes and the consequences of inadequate actions taken at the operational level, which can cause decisive impacts on corporate strategy (defined by corporate governance). The use of inadequate control tools and internal practices for risk treatment produces negative impacts in the management process and can compromise strategical objectives (corporate governance).

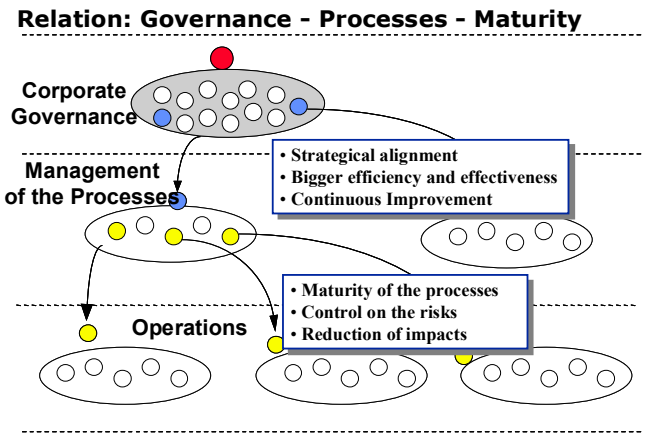

Figure 3. Governance, Processes and Operational

B. Organization and Environment

The company strategies involves: (i) identification of opportunities and recognition of environmental modifications in its working area, (ii) evaluation of organization strengths and weaknesses, and (iii) capacity for anticipating market demands and for facing competitors under risk conditions. Therefore, corporative strategies must combine social, political and economical forces with the organizational capacity for adding value to the business.

Figure 4 shows that Corporate Governance needs technological assistance to support the various business requirements, guaranteeing transparency in transactions amidst internal agents to the company (direction boards, employees) and external ones (investors, customers, suppliers, partners, government and society in general). In this context, ISG acts as a strategical assistant, creating structured processes aligned to business objectives (continually monitored).

Tools like PEST analyses (Politics Economy Society Technology) and SWOT analyses (Strengths, Weaknesses, Opportunities, and Threats) are already used by corporate governance and can also be used to support the ISG.

C. Organizational maturity

An adequate information security governance has a clear and objective process governance, whereas a process can be defined as a set of interconnected and ordered activities, controlled by a central vision, with clear objectives, exceeding specific areas, consuming resources and using information. Any organizational operation is always supported by one or more registered (or not) processes. Therefore, processes have a decisive role in a governance model of information security. Processes are defined through "process models", considering different related dimensions, i.e., business-oriented goals, metrics, organizational culture, abilities, data flow, etc.

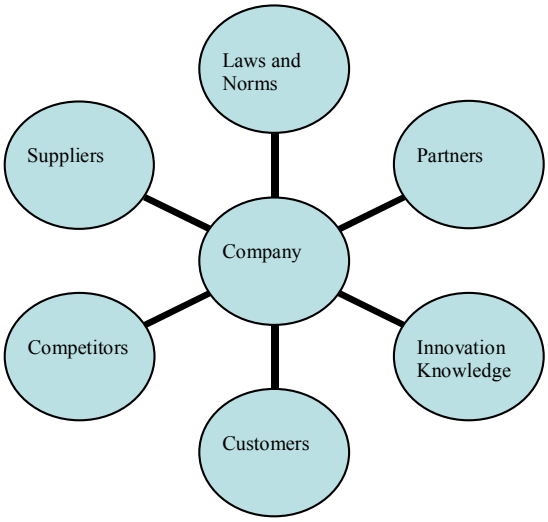

Figure 4. External powers

Some of the major advantages in adopting process-oriented approaches are:

- measurable quality improvements;
- measurable IT management services;
- consistent and standardized way to work;
- continuous improvement of communication processes;
- better definition of responsibilities and related duties;
- better costumer satisfaction;
- prevention of redundant procedures /activities;
- assistance in achieving ISO 9000 certification.

Efficiently modeled processes can reach a high level of maturity much faster, contributing directly to adequate corporate governance (figure 3). The act of developing process maturity can be objectively defined as the way to:

- obtain advanced knowledge about business procedures;
- follow best practices of the market, aiming at more effective results;
- use policies that enable adjustments (in organization, people, process) to support governance requirements;
- use IT as a facilitator for process automation, guaranteeing quality and efficiency in corporative activities;
- define risk processes;
- integrate different risks (financial, security, etc.);
- continually monitor processes, looking for problems and possible improvements;
- realign processes to the business objectives.

D. Identifying current maturity

Before any action is taken, a company must identify its current organizational situation and its business status. It is fundamental to start planning based on real premises, prioritizing activities in order of relevance according to corporative strategy. Considering the current situation, the organization can develop an action plan to support business requirements, including the design of any process that is essential for the success of ISG. As defined by CobiT, maturity can be evaluated through a quantitative approach (figure 5), with six different levels:

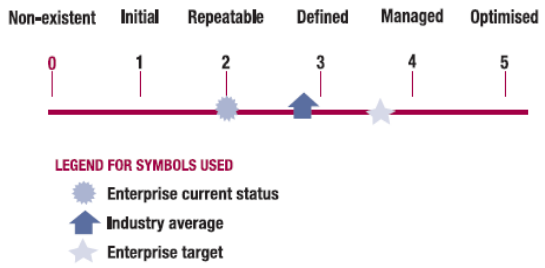

Figure 5. CobiT's Maturity Model

- level 0 : non-existent
  - awareness of the need for IS governance is inexistent
- level 1 : initial
  - awareness of the need for IS governance exists
  - structures are disorganized; inexistence of standards
  - support groups and IT are not linked
  - tools and services are not linked
  - services are provided as mere reaction to incidents
- level 2 : repeatable
  - spread of the awareness of the need for IS governance
  - some initiatives of governance activities (and indicators)
  - residual level of organization, without standardization
  - some quality efforts, without refined methodology (incident repetition)
  - no change control
- level 3 : defined
  - higher level of governance awareness
  - standardized, implemented and documented processes
  - change control
  - consistent indicators
- level 4 : managed
  - dissemination of governance awareness at each level of the corporation
  - implementation of SLA's (Service Level Agreements) and services catalogues
  - non-existence of financial management
  - IT is not seen as profitable for business
  - beginning of the process for continuous improvement
- Level 5 : optimised
  - general governance awareness
  - financial management (ROI application)
  - best practices adopted and managed
  - IT continuous improvements
  - processes continually optimized

E. Measuring Quality costs

A difficult question for managers is how to establish the target level of process maturity. The answer is not simple, since for each company the same process can have a different importance. It is necessary to carry out a careful evaluation, taking into account critical issues for applications and business objectives. However, there exists a technique to help this identification procedure, taking into account the relation between *cost* and *perception* for customers. Figure 6 illustrates this concept: managers can find a critical point, ideal for the related process. To determine this point, a manager makes use of a well-known technique, called *Quality Cost* [14].

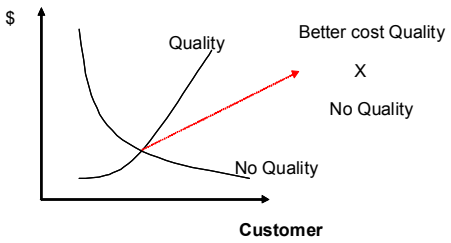

Figure 6. cost x quality relationship

F. Metrics/Indicators to control ISG (Security Scorecard)

It is fundamental for any manager to measure the contribution of their department (and respective resources) in the business results and to have a better control of the current

situation of their department/area at any time. Any decision taken by a manager must be based on real data.

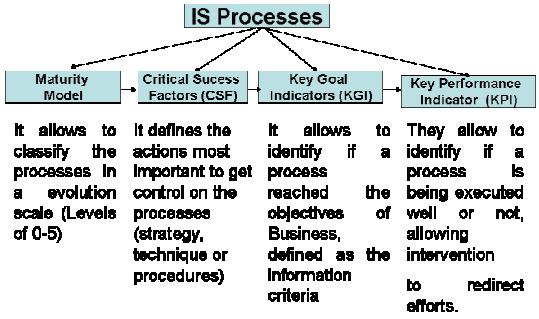

Figure 7. Indicators relationship

To measure performance and effectiveness of goal accomplishment, some indicator concepts are currently being adopted by organizations. These indicators enable the evaluation of process alignment with business strategy. The control panel for metrics called Security Dashboard allows a manager to reach the development of their own area, assisting them in any decision handling. The Security Dashboard is composed of seven domains, which support the Security Governance (figure 7) as listed below:

- dissemination of IS knowledge;
- measurement of process maturity level;
- performance of critical processes;
- information for stakeholders;
- conformance level (internal and external norms);
- surveillance of processes gap;
- alarming functionalities.

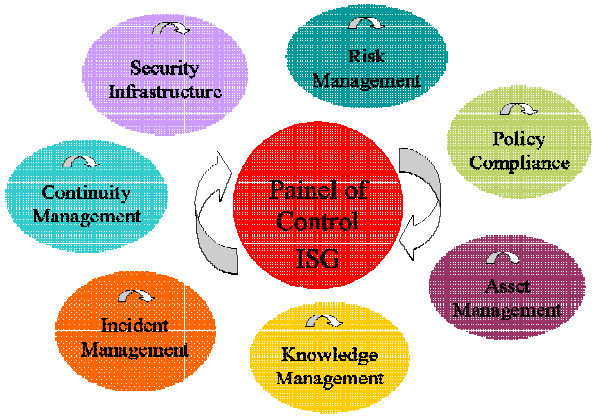

Figure 8. Security Dashboard

A point must be strongly stressed, though: each organization can adopt its own Security Dashboard customizing metrics and indicators in accordance with its necessities, using, or not, the seven domains mentioned. The CobiT [3] can be used as support for each area of the panel, a mapping of the processes used by CobiT being necessary for each domain. In the next paragraph some generic metrics are listed that can be used together with the pre-defined ones of the CobiT Management Guidelines.

Risk Management:

This domain makes it possible to evaluate excellent criteria for evaluation and risk management control.

- risk indicators (risk analysis)
- exposition (analysis of vulnerabilities)
- % of system without security controls
- % of system analyzed
- risk tolerance level
- % of physical environment analyzed

Policy Compliance:

This domain makes it possible to evaluate and control the compliance level, normative, internal policies and laws which the company is subject to.

- % of non-compliance with norms and laws
- % of non-compliance with the security policy
- maturity level of IS processes
- % of internal controls not implemented
- % of control system audits
- total of auditing realized
- total of updates of the security policy
- % of system/services monitored by intrusion detection system
- total of norms/procedures registered
- % of systems that treat integrity, availability and confidentiality

Asset Management:

This domain makes it possible to control and classify the corporative assets with greater clarity.

- total of assets inventoried
- % of assets classified
- % of asset with value defined
- % of owners defined
- % of assets labeled

Knowledge Management:

This domain makes it possible to measure the degree of knowledge and learning of the collaborators of the organization.

- % of users trained in IS
- % of managers/technicians trained in IS
- % of knowledge acquired in IS
- % of departments covered by the awareness program
- total time invested in security awareness
- % of information garbage reduction
- % of weak passwords
- % of password modifications

Incident Management:

This domain gives a general view of incidents and their impacts on the organization.

- total of reported Incidents
- total of Incident responses
- average time taken by incident responses
- % of business incident impacts analyzed
- % of learning from incidents
- % of skilled people to deal with incidents
- % of tests of emergency plans

Continuity Management:

This domain informs the level of assets and process availabilities of the organizations.

- network performance level
- system performance level
- % of critical assets enclosed in recovery plans
- % of business processes analyzed
- system / network out of service period due to incidents
- time to recover assets after incident
- using level of disaster recovery plans
- % of disasters solved
- % of skilled people to implement the disaster recovery plan
- frequency of continuity tests

Security Infrastructure:

This domain allows an overview of the basic infrastructure requirements to guarantee the security of information.

- amount of meetings/workshops promoted by the Security Committee
- % of participation of stakeholders in meetings/workshops
- % of planning actions implemented
- % of management processes documented
- % of outsourcing services
- total of security indicators
- % of IT budget allocated for IS
- % projects involving the IS department

G. Integrated Governance: BSC, CobiT and ISO/IEC 17799

A great challenge for the information security governance is the integration of best practices already in use with business objectives.

The model of figure 9 proposes a way to integrate business vision with information security.

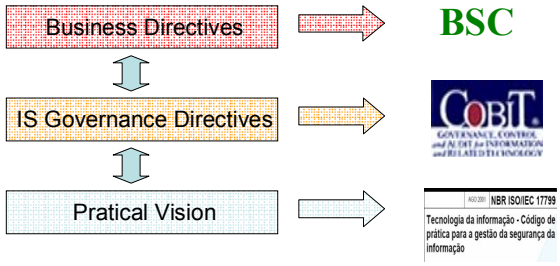

Figure 9. Business integration with security information

The BSC works as an interpreter for the business goals, meeting vision requirements, mission and strategical planning (lined up with the board of directors) in four different perspectives (financial, customer, internal processes and innovation/learning). CobiT works as a bridge for business processes, considering business objectives and being controlled by the BSC. This link makes the interpretation of IS processes easier considering business requirements.

The proposed framework correlates the CobiT standard with ISO/IEC 17799, mapping business objectives into security practices. This correlation aids the ISG implementation, as well as the establishment of the Security Dashboard, assisting in decision handling. Tables II, III an IV describe some examples of correlation between the CobiT and ISO/IEC 17799. A complete list can be found in reference [1].

V. PRACTICAL GUIDE TO IMPLEMENT ISG

Table I describes a practical guide for implementing Information Security Governance, composed of five different stages.

TABLE I. PRACTICAL GUIDE TO IMPLEMENT ISG

Steps	Activity	Actions	Responsible
Initialization	*Convincing board of directors*	*Use of strategical planning tools (PEST and SWOT) to convince Board of directors about the importance of Security Governance as a complement to Corporate Governance*	*IS Director*
	Deciding to implement	*Declare and formalize the decision of launching an implantation process, granting resources to support a continuous process of security management*	*Board direction*
	Creating an executive committee of IS	*Create an executive committee to define directives, support tactical decisions about IS and establish responsibilities*	*IS Director*
	Promoting an executive seminar	*Homogenize the understanding of the model of Security management necessary to reach business goals between Executive Committee of IS and the Board of directors*	*IS Director*
	Identifying global strategies	*Identify the mission and objectives of IS inside the strategical planning for reaching medium and long-term business goals*	*IS Committee*
	Defining an execution team	*Establish the organizational structure necessary to implement CobiT for IS Governance. This structure will rely on a leader in charge of shaping the new model of management, diagnosis, planning and implementation of CobiT inside the organization*	*IS Director*
	Preparing team	*Disseminate information about concepts, models and methods of CobiT for the execution team*	*Execution team leader*
Current scenario Diagnosis	*Evaluating risks*	*Find out major business risks in the organization to settle on which processes are really critical, and to support indicator selection (KPI's, KGI's and FCS's).*	*Auditing team*
	Evaluating maturity levels of processes	*Evaluate the maturity level of each one of the 34 CobiT processes in accordance with the CobiT's management guide.*	*Execution team*
	Evaluating criticality levels of processes	*According to the IS objectives (in accordance with the business objectives), establish the critical level of each CobiT process for IS governance*	*Execution team*
	Defining IS profile	*Elaborate graphical analysis of previous evaluations revealing the maturity degree of the processes.*	*Execution team*
	Assessing profile	*Compare maturity degree of the IS processes with related market (companies from the same segment, size and others of specific interest).*	*Execution team*
	Profile divulgation	*Present to the IS committee the results from the maturity and benchmark analyses in order to justify a customized solution to reach IS objectives and defined goals*	*Execution team*
Execution Strategy	*Selecting processes and objectives*	*Set processes context and establish respective maturity targets*	*Execution team*
	Analyzing gaps	*Define existing gaps between each process and respective target and define main actions to be implemented.*	*Execution team*
	Conceiving solutions	*In accordance with IS requirements for the business, critical degree of the processes and best practices, choose a product from CobiT family that better matches the requirements of IS Governance*	*Execution team*
	Approving solutions	*Approve the implementation model and the selected product to implement IS governance.*	*IS committee*
Planning	*Identifying requirements*	*Define the critical factors of success for each one of the processes of the improvement context, and select general and specific indicators of goal and performance, according to company needs*	*IS committee*
	Developing an execution project	*Establish premises, activities, teams, resources, delays, costs and risks of the project of implementation of the CobiT framework to support governance strategies and requirements and to reduce diagnosed gaps.*	*Execution leader*
Execution	*Implementing solutions*	*Implement policies, procedures and recommended practices in the information resources (systems, asset of TI, etc.) to support the requirements defined for quality, security and confidentiality (and also to create a continuous management for preserving reached levels)*	*Execution team*
	Adjusting Execution	*Validate the implementation of controls according to established strategy and requirements*	*Auditing team*

TABLE II. RISK MANAGEMENT

NBR ISO/IEC 17799:2000	CobiT V.3
Security risks evaluation	PO9.1 Business Risk Assessment PO9.2 Risk Assessment Approach PO9.3 Risk Identification PO9.4 Risk Measurement PO9.5 Risk Action Plan PO9.6 Risk Acceptance
Control selection	PO9.7 Safeguard Selection
Critical Success Factors	PO9.8 Risk Assessment Commitment
3.1.Information Security Policy	PO4 Define the IT Organisation and Relationships PO6 Communicate Management Aims and Direction

TABLE III. BUSINESS CONTINUITY MANAGEMENT

11. Business Continuity Management	
11.1. Aspects of Business Continuity Management	PO3 Determine Technological Direction
	PO7 Manage Human Resources
	DS2 Manage Third-Party Services
	DS4 Ensure Continuous Service
	DS12 Manage Facilities
	DS13 Manage Operations

TABLE IV. COMPLIANCE MANAGEMENT

12. Compliance	
12.1 Compliance with legal Requirements	PO6 Communicate Management Aims and Direction
	PO8 Ensure Compliance with External Requirements
	DS11 Manage Data
	M1 Monitor the Processes
	M3 Obtain Independent Assurance
12.2 Reviews of Security Policy and Technical Compliance	PO6 Communicate Management Aims and Direction
	PO11 Manage Quality
	AI2 Assess Internal Control Adequacy
12.3 System Audit Considerations	AI1 Identify Automated Solutions

VI. REQUIREMENTS FOR THE SUCCESS OF THE FRAMEWORK

It is important to make sure that the organization has some essential factors for the success in the implementation of the framework being considered, as for example: a directed organizational culture for aspects of information security, commitment of the senior-level, good communication among organizational departments, commitment of the staff, and budget to invest in human and technological resources.

VII. RELATED WORK

In [8] Posthumus reconfirms the need for integrating information security into corporate governance through the development of an information security governance (ISG) framework and proposes guidelines to aid an organization in its ISG efforts. Basically, some structural directives are proposed, but not a practical framework for implementing ISG.

There are still those who claim that information security has now become such a crucial component of good Corporate Governance that it should rather be called Business Security instead of Information Security [5].

However, most of the proposals found in the literature do not regard security governance as a complete framework, but some of them discuss important issues that must be integrated in such a framework. Von Solms [2] argues that for good Information Security Governance and good Corporate Governance, Information Security Operational Management and Information Security Compliance Management should be totally separated, and housed in separated departments.

Andersen [11] proposes the use of an information security governance maturity model to establish rankings for security in an organization. Our proposal also makes use of a maturity approach, but in an integrated manner with operational indicators to enable a more realistic notion of the current scenario.

VIII. CONCLUSION

Although the concepts of corporate governance are well known, its integration with the concepts of Information Security governance is still a great challenge for the IT professionals, which aim to align the best practices from one to the other, in order to reach an ideal model of information security governance (ISG).

This paper proposed an innovative framework combining best practices from corporative management and best practices from information security. Therefore, the integrated use of BSC (administrative indicators) and Security Dashboard (operational indicators) allow the clear visualization of the strategical alignment between information security and business objectives

Another important contribution offered in this paper is the conception of a practical guide to implement information security governance, using best practices from both administrative (e. g. PEST and SWOT) and technological (CobiT and ISO/IEC 17799) areas.

The proposed framework can be tailored in accordance with organizational profile to support the existing structure, resources and culture with best profit. Professionals can also adapt the stages of the proposed guide to already used methodologies, contributing to enhancing the efficiency and efficacy of an ISG implementation.

REFERENCES

[1] Gustavo Alberto de Oliveira Alves, "Information Security, An original vision of Mangement", Ed. Ciência Moderna, 2005 (in portuguese).

[2] Basie von Solms, "Information Security Governance e Compliance management vs operational Management", Computers & Security, 24, Elsevier, pp. 443-447, 2005.

[3] IT Governance Institute, "Control objectives for information and related technologies (CobiT)",3rd ed., USA, 2000.

[4] ISO, "Information technology - Code of practice for information security management", ISO/IEC 17799, Switzerland, 2000.

[5] Basie von Solms, Rossouw von Solms, "From information security to business security?", Computers & Security 24, Elsevier, pp. 271-273, 2005.

[6] IT Governance Institute, "Information Security Governance: Guidance for Boards of Directors and Executive Management", ISBN 1-893209-28-8, USA, availble from: <www.itgovernance.org>.

[7] National Cyber Security Summit Task Force, "Information Security Governance - a call to action", available from <http://www.technet.org/resources/InfoSecGov4_04.pdf>.

[8] Shaun Posthumus, Rossouw von Solms, "A framework for the governance of information security", Computers & Security, 23, Elsevier, pp. 638-646, 2004.

[9] Entrust, "Information Security Governance (ISG): An essential element of corporate governance", Available from: http://itresearch.forbes.com/detail/RES/1082396487_702.html, 2004.

[10] Ken Lindup, "The Role of Information Security in Corporate Governance", Computers & Security, vol.15, n. 6, Elsevier, pp.477-485, 1996.

[11] Andersen Paul Williams, "Information Security Governance", Information Security Technical Report, Vol 6, No. 3, pp. 60-70, 2001.

[12] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson, "2005 CSI/FBI Computer Crime and Security Survey", Computer Security Institute, Available from: <http://www.GoCSI.com>, 2005.

[13] IDC, "2005 Global Information Security Workforce Study", International Information Systems Security Certification Consortium - $(ISC)^2$, available from: https://www.isc2.org/cgi-bin/content.cgi?page=929, 2005.

[14] Feigenbaum, A.V. "Quality Costs" [Chapter 7] Total Quality Control. New York: McGraw- Hill, 1991.