JISTEM - Journal of Information Systems and Technology Management
*Revista de Gestão da Tecnologia e Sistemas de Informação*
Vol. 8, No. 3, Sept/Dec. 2011, *pp. 555-580*
ISSN online: 1807-1775
DOI: 10.4301/S1807-17752011000300003

# ALIGNING INFORMATION SECURITY WITH THE IMAGE OF THE ORGANIZATION AND PRIORITIZATION BASED ON FUZZY LOGIC FOR THE INDUSTRIAL AUTOMATION SECTOR

**André Marcelo Knorst**
Coester Automação Ltda - São Leopoldo, RS, Brazil
**Adolfo Alberto Vanti**
UNISINOS - São Leopoldo, RS, Brazil
**Rafael Alejandro Espín Andrade**
Universidade Técnica de Havana, Cuba
**Silvio Luiz Johann**
Fundação Getúlio Vargas Rio de Janeiro, Brazil

## ABSTRACT

This paper develops the strategic alignment of organizational behavior through the organizations´ image, prioritization and information security practices. To this end, information security is studied based on the business requirements of confidentiality, integrity and availability by applying a tool which integrates the strategic, tactical and operational vision through the following framework: Balanced Scorecard - BSC (strategic) x Control Objectives for Information and Related Technology - COBIT (tactical) x International Organization for Standardization - ISO/International Electro Technical Commission - IEC27002 (operational). Another image instrument of the organization is applied in parallel with this analysis to identify and analyze performance involving profiles related to mechanistic, psychic prisons, political systems, instruments of domination, organisms, cybernetics, flux and transformation (MORGAN, 1996). Finally, a model of strategic prioritization, based on compensatory fuzzy logic (ESPIN and VANTI, 2005), is applied. The method was applied to an industrial company located in southern Brazil. The results with the application show two organizational images: "organism" and "flux and transformation ". The strategic priorities indicated a significant search for new business services and international markets. Regarding protection of information, security found the gap between "minimum" and "Reasonable" and in domain 8 (HR) of standard ISO/IEC27002, considered 71% protection as "inappropriate" and "minimal" in the IT Governance context.

*Keywords:* security, information, organizational culture, images, compensatory fuzzy logic

Manuscript first received/*Recebido em* 28/06/2010 Manuscript accepted*/Aprovado em*: 19/07/2011

Address for correspondence / *Endereço para correspondência*

*André Marcelo Knorst*,Gerente de TI -CoesterAutomação Ltda. Mestre em Administração – UNISINOS, Bacharel em Sistemas de Informação – UNISINOS. Rua Jacy Porto, 1157, Bairro Vicentina, São Leopoldo, RS, Brasil. E-mail: amknorst@gmail.com

*Adolfo Alberto Vanti*, Doutor em Direção de Empresas Universidade de DEUSTO – País Vasco – Espanha. Professor Titular do Programa de Doutorado e Mestrado em Administração e do Mestrado em Ciências Contábeis da Unisinos - Av. Unisinos, 950 – CEP 93022-000 – Cristo Rei – São Leopoldo-RS, Brasil – Ciências Econômicas. E-mail: avanti@unisinos.br

*Rafael Alejandro Espín Andrade*, Professor Titular do Centro de Estudos de Tecnologia de Direção da Universidade Técnica de Havana. Matemático e Doutor em Engenharia - Tribunal Nacional Científico de Cuba. Rua 114 número 11900 entre 127 e 119, Marianao, Havana, Cuba. E-mail: espin@ind.cujae.edu.cu

*Silvio Luiz Johann***,** Fundação Getúlio Vargas - Rua Praia de Botafogo, 90 - Rio de Janeiro, RJ Brasil - FGV Management. E-mail: silviojohann@terra.com.br

Published by/ *Publicado por:* TECSI FEA USP – 2011 All rights reserved.

## 1. INTRODUCTION

The culture of a company has a type of collective personality and can be noticed in the form of images that they express. According to Morgan (1996) the proper interpretation and analysis of what is conventionally called the representation of organizational images allows for a proper interpretation of the dominant culture in the company and this reveals some dysfunctional characteristics of each image. These organizational images have certain influence on information technology (IT), specifically on organizational information security.

The relationship between organizational culture and information technology is presented as a complex relationship in which one influences the other in illogical ways. Examples of this illogical influence are the resistance to the implementation of a new technological project or when a modernization project imposes new behavior without respecting the identity of the organization or the way it operates internally. The consequences of behavioral and technological misalignment can generate significant losses for the company, from project delays and failures in implementation to leakage of strategic information.

The examples described above exemplify the theory of complexity, which admits that a small number of simple rules can generate extremely complex results because they make a spontaneous order possible. This can be detrimental to the company and its main projects when it does not respect the factors of flexibility and controllability (ADIZES, 1989).

When organizations are young they are very flexible and are not always controllable, but, as they age, this relationship changes. Normally, over time controllability increases and flexibility decreases, making an older company generally more controllable, but also more inflexible with little propensity for change. This type of situation can be evaluated and analyzed through images (MORGAN, 1996) and instrumented through Johann (2008) developing the images of mechanistic, psychic prisons, political systems, instruments of domination, organisms, cybernetic, and flux and transformation.

Currently, for a company to survive and to be competitive, it is necessary to innovate, constantly changing its profile to a more flexible one. This consequently makes it less controllable and more vulnerable, which can mean problems in information security when behavior emerges and is counter to the organizational culture. So, the problem-question of this study is defined as follows: How to align information security with organizational image in the case of a company in the industrial automation sector studied? To this end an instrument was developed and utilized in the (1) evaluation of analysis of the organizational image in conjunction with an instrument of evaluation and (2) analysis of information security in the company that integrates such models as BSC, COBIT and ISO/IEC27002 (Knorst, 2010).

The combination of the two instruments (technical and behavioral) occurs because the specific security instrument (BSC + COBIT + ISO/IEC27002) can only generate technical characteristics. This form of approach will not solve problems of character vulnerability which are located in the dimension related to personal or behavioral which is represented in organizational culture and counterculture, which is an everyday occurrence in organizations. Finally, a model of strategic prioritization based on compensatory fuzzy logic (LDC) is applied along with the organizational images to identify in which strategic variables it is possible to encounter major vulnerabilities in information security. A company in the industrial automation sector was selected to apply this alignment in practice.

## 2. ORGANIZATIONAL CULTURE AND COUNTERCULTURE THROUGH ORGANIZATIONAL IMAGE

According to Schein (1990) managers often work with new patterns and practices to establish a competitive and stable pattern for the company, but fail to recognize the fundamental corporate culture or "foundation" of the corporate culture. This "foundation" is made up of the values shared by the employees, beliefs and behavior, which emerge from the success of the organization. When a culture becomes counterproductive, executives must work in a new cultural perspective, recovering residual elements of past successes, revitalizing productive habits and managing present conflicts and anomalies so that the organization can recover its essential purpose. In contrast, significant increases in a corporate counterculture or behavior contrary to the expected employee behavior can be compromising, mainly through the leaking of strategic information.

For decades, entrepreneurs and top executives have repeated, ad nauseam, that the greatest assets of the organization are its people. This is a figurative way of enhancing the value of people, since they are only included on the balance sheet as a cost. Often, the reality of the company is that it does not adequately contemplate functional value and the employee can be treated as a simple resource, not a partner, and they could be replaced at any given moment. According to Minarelli (1995) it is a very present reality in organizations and companies are aware of this fact and that its direct consequences can result in the reduction in employee loyalty to the organization. This decrease in loyalty can result in different types of problems including those related to information security, which is the focus of this paper.

When an organization has a high level of shared beliefs and values, it has a dense culture which, in the view of Freitas (1991), is based on the existence of few disagreements or ambiguities in the personal attitude and in decision making, as well as the management of information security. On the other hand, when the culture of an organization is not dense, a simultaneous existence of various different sub-cultures within the organization can occur. These sub-cultures can be specific to departments, units, etc., which can have very significant differences in relation to the core of the corporate culture. In some cases, sub-cultures that are too different in relation to the central core of the company can generate potential compromising corporate sustainability (Freitas, 1991).

The counterculture binds groups or subgroups that reject that which the organization represents or it tries to become a covert opposition to the dominant values and/or power structure of the company. This counterculture often arises during times of stress or during major transformations within the company. For Freitas (1991, p. 77), "these forms of resistance and conflict express breaches in the system of formal power, […] that include: negation or hiding of information can arise during times of stress or during significant transformations in the company; the boycott of or resistance to innovations; and failing to cooperate amongst workgroups".

In the central nucleus of Organizational Culture is the “self”, which represents the integration of conscience and unconscious systems. These systems are a set of actions repeated over time, establishing a form, which are the guidelines adopted by the company. To identify the unconscious systems of an organization is, in truth, to recognize their grey areas. Their images can be identified as taboos or prejudices that somehow obscure the central idea of the organization and of information security. This “self” can be represented through organizational images (Morgan, 1996) such as mechanistic, psychic prisons, political system, instruments of domination, organisms, cybernetic and flux and transformation, and then it features a synthesis that develops the understanding of the application of the specific instrument of images (Johann, 2008):

**Mechanistic:** Organizations that impose rigid routines and patterns, hierarchically distributed. Dealings are impersonal and control of the organization is bureaucratic. Because it is very predictable, it is no longer regarded as ideal, even in stable and authoritarian institutions. This style also presents difficulties for innovation.

**Psychic Prisons:** Inflexibility is a characteristic of this image, becoming a prisoner of past events, allied to fundamental attitudes by their idealizers. Some of their traps are false assumptions, rules without questioning and fanaticism around the charisma of the leader.

**Political Systems:** This view is not often in the interest of the group and often favors authoritarian executives. This includes companies with participatory management that is encompassed in political systems because although there is a certain distribution of power, the central objective will be executed by both subordinates and the owners of the capital.

**Instruments of Domination:** In organizations viewed as instruments of domination, the employees and managers need to completely dedicate themselves to the company. They feel insecure about their employment and experience a lot stress on the job.

**Organisms:** The fundamental principal of organisms is that it is based on the employees’ intellectual capital. Motivation is a substantial factor. Because of constant innovation and deadlines, the employees tend to obey a biological clock because there are targets to reach and constantly innovations to develop.

**Cybernetic:** Intellectual capital is highly valued and is constantly being stimulated to improve. Decision-making needs to be done “through formal or temporary processes, producing policies and plans that offer a point of reference or a structure for information processing” (JOHANN, 2008, p.33). The definition of cybernetic is given due to the fact that information technology is permanently present, which ensures better conditions in the review of political norms and procedures, addition to learning how to absorb changes in the environment.

**Flux and Transformation:** Organizations that best mirror flux and transformation are those that modify and evolve to conform to change and evolution in the environment. Their survival depends on their internal and external environments.

The images described above led to the creation and implementation of an identification instrument for these types in different companies. This instrument is presented in the following pages and finalizes the behavioral analysis. It analyzes information security in the context of IT governance, integrating BSC x Cobit x ISO27002. This instrument that analyzed the information security in IT Governance context was very detailed in (Knorst, 2010).

## 3. IT GOVERNANCE

The ITG can be considered the way in which decisions and responsibilities are directed towards a desirable behavior using IT (Weill and Ross, 2006). Another definition states that the ITG is an integral part of corporate governance established by management, organizational structures and processes to ensure the expansion of the strategies and objectives through the practices of IT (ITGI, 2009). ITG can also be considered the organizational capacity exercised by the board and executive management to control the formulation and implementation of IT strategies to ensure the integration between business and IT (Grenbergen and De Haes, 2005). The models of ITG like BSC (Kaplan and Norton, 1996), COBIT (ITGI, 2009) and ISO/IEC27002 (ISO/IEC 2005) assist with more effective management of IT resources.

This work focuses on these models of IT governance, BSC, COBIT and ISO/IEC27002 as a continuation and expansion of the work of Knorst (2010). These were analyzed with a behavioural approach and strategic prioritization for assessing information security.

## 4. INFORMATION SECURITY

Confidentiality, integrity and availability are basic requirements for business information security and provide the maintenance requirements of the business (ITGI, 2009), (Kwok and Longley, 1999), (Fitzgerald, 2007), (Sêmola, 2003), (Dias, 2000), (Moreira, 2001).An organization's dependency on their IT infrastructure combined with the neglecting of security requirements can put the entire information system at risk. A brief description of this being Confidentiality (C): All information must be protected according to the degree of secrecy of their content, aimed at limiting its access and used only by the people for whom they are intended; Integrity (I): All information must be kept in the same condition in which it was released by its owners, in order to protect it from tampering, whether intentional or accidental; Availability (D): All the information generated or acquired by an individual or institution should be available to their users at the time they need them for any purpose.

The ISO/IEC27002 standard emphasizes the fact that information is an important asset of the organization. The three elements described above are essential to preserve the competitiveness of the company. Following is the summary of the goals of the areas of standard, starting at 5 in order to preserve the numbering of the chapters (chapters 1 through 5 are introductory chapters: 0= introduction; 1= scope; 2= terms and definitions; 3= structure of the standard; 4= risk assessment and treatment). Politics of Information Security (PI) is chapter 5 and compliance is chapter 15.

**Politics of Information Security (PI):** Provide guidance and direction for information security in accordance with business requirements and the relevant laws and regulations.

**Organization of Information Security (OI):** Managing information security within the organization as well as maintaining the security of information processing resources that are accessed, processed, communicated or managed by external parties

**Asset Management (GA):** Achieve and maintain appropriate protection of organizational assets. Ensure that information receives an adequate level of protection.

**Human Resources Security (HR):** To ensure that employees, suppliers and third parties understand their responsibilities and are in agreement with their roles, reducing the risk of theft, fraud and misuse of resources. They are aware of the threats and concerns related to information security, their responsibilities and obligations, and are prepared to support the information security policy of the organization during their work, to reduce the risk of human error and so they don't leave the organization or change disorderly their work.

**Physical and Environmental Security (SA):** Prevent unauthorized physical access, damage and interference with the organizations facilities and information. Prevent loss, damage, theft or compromise of assets and interruption of activities of the organization.

**Communications and Operations Management (GO):** Ensure the correct and safe operation of the processing resources of information and minimize the risk of systems failures. Protect the integrity of software and information and maintain the integrity and availability of information and information processing resources, as well as ensuring the protection of information networks and the protection of infrastructure and support. Prevent unauthorized disclosure, modification, removal and destruction of assets and interruption of business activities. Guarantee the security of electronic commerce services and their safe use and detect unauthorized activities of information processing.

**Access Control (CA):** Controlling access to information and ensuring access for authorized user and prevent unauthorized access to information systems. Prevent access by unauthorized users and prevent compromise or theft of information and resources for information processing, prevent unauthorized access to network services, and to preventing unauthorized access to operating systems. Prevent unauthorized access to information contained in application systems ensuring information security when using mobile computing resources and remote work.

**Information systems acquisition, development and maintenance (AQ):** To prevent errors, loss, unauthorized modification or misuse of information in applications. Protect the confidentiality, authenticity or integrity of information by cryptographic means ensuring the security of system files. Maintain the security of application systems and information reducing risks of exploitation of vulnerabilities of known techniques.

**Information security incident management (GI):** Ensure that the vulnerabilities and security event information associated with information systems are disclosed, allowing corrective actions to be taken in time. Ensure that a consistent and effective approach is applied to the management of information security incidents;

**Business Continuity Management (GC):** Do not allow the interruption of business activities and protect critical processes from the effects of significant failures or disasters and ensure their timely resumption.

**Compliance (CF):** Avoid violation of any criminal or civil statutes, regulations or contractual obligations and any requirements for information security. Guarantee that systems comply with organizational policies and standards of information security maximizing efficiencies and minimizing interferences in the process of auditing of information systems.

With the objective of verifying compliance with the standard areas, Eloff and Eloff (2003) proposed a framework for the governance of information security´s four levels of protection against security practices. This allows organizations to take a holistic view and verify the current stage of development of each business area. The stages are as follows:

**Inadequate protection:** There is no organizational effort to implement any of the controls recommended for their specific needs. Certified products and equipment have no influence on the classification of the sections at this level.

**Minimal protection:** The organization demonstrates minimal effort in adopting some of the recommended controls. Certified products and equipment have no influence on the classification of the sections at this level.

**Reasonable protection:** Most controls are implemented and must meet the requirements based on written procedures and processes running on a reasonable level. Certified products and equipment are preferred for use.

**Adequate protection:** Implement all controls recommended for the area. Wherever possible, it is obligatory to use certified products and equipment.

These evaluation metrics, in conjunction with the recommendations of the standard, permit the formulation of an instrument to assess the security of information, identifying the stage where they are safe practices.

## 5. MODEL INTEGRATION AND CREATION OF A RESEARCH INSTRUMENT TO EVALUATE INFORMATION SECURITY

Strategically, it is possible to establish a strategic relationship using the criteria of security and integrating them through the BSC model, COBIT and ISO/IEC27002, as depicted in Figure 1. These models facilitate the mapping of generic objectives for the IT business from the perspectives of the BSC with the overall goals of IT for business, those suggested by ITGI (2009). Following in (Knorst, 2010) it is possible to map the generic IT goals for business with COBIT processes involving the requirements of confidentiality, integrity and availability. Finally, to reach a technical and operational level, this alignment also included the mapping of COBIT processes with the practices of ISO/IEC27002.

Here the mapping process results in a framework involving the following steps:

1) Identification of business objectives in the perspectives of the BSC;
2) Identification of IT objectives;
3) Mapping of IT goals with business goals;
4) Mapping of IT goals with COBIT processes with respect to safety requirements Confidentiality, Integrity and Availability;
5) Mapping of COBIT processes with safety practices proposed by ISO/IEC27002.

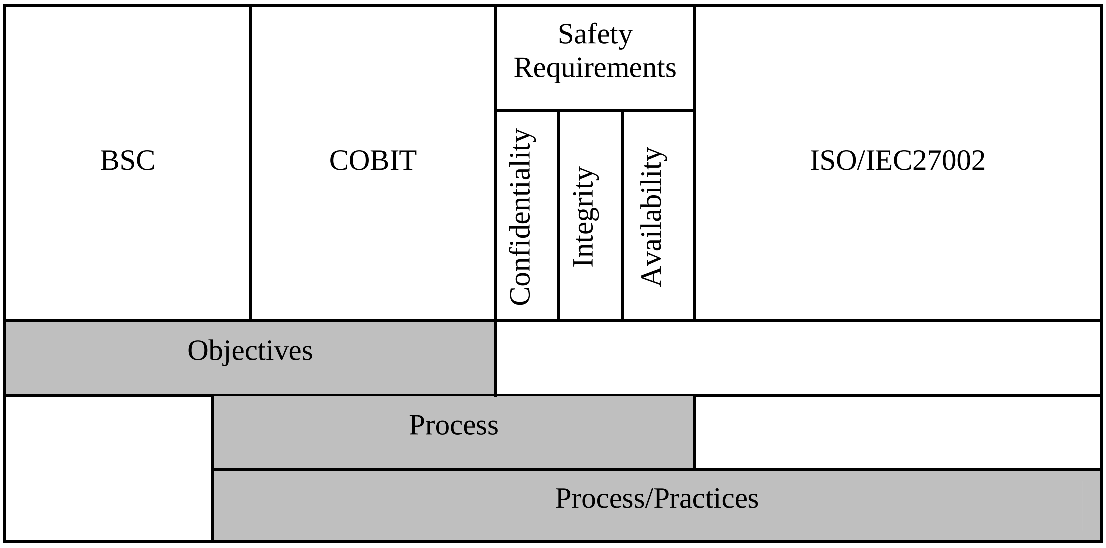

**Figure 1: Integrating the BSC model, COBIT and ISO/IEC27002**

**Source: KNORST (2010, p.49)**

In Knorst (2010) it is possible, in details, to identify the BSC x COBIT x ISO27002 mapping in relation to the generic IT requirements that impact security requirements, Confidentiality, Integrity and Availability. This confirms the first model and instrument in information security.

## 5.1. Model Compensatory Fuzzy Logic (CFL) to Prioritization

To define strategic prioritization, the study elaborated the strategic map based on Compensatory Fuzzy Logic (CFL) and it is necessary to cross various sets of data in order to form the guiding actions of the organization. These sets of data include such items as strengths, weaknesses, opportunities, threats, objectives and actions. In the following, the principal points within the items mentioned above are presented. This is also a way to define which information is strategic for the control of internal security aspects.

This is a logical model of the qualitative and quantitative type, based on CFL in which it is first defined as strategic variables related to SWOT analysis, with the addition of Strategic Objectives and Actions (SWOT-OA) (Vanti et al, 2006) . This model is defined with the structuring of matrices, and the relation between the variables is based on compensatory fuzzy logic validated by the manager of the company.

CFL, according to Espin and Vanti (2005), aims to compensate Boolean logic, which uses only the extremes of decision, 0 or 1 {0,1} and works with the principle of gradualism within the interval [0,1] in order to measure the truthfulness of its predicates, considering 0 or 1 as the extremes of truthfulness (completely true) or falsity (completely false). This analysis (0.5) represents complete uncertainty or maximum vagueness. This representation is shown in the table of truthfulness found in Table 1.

| Truth Value | Category |
|---|---|
| 0 | False |
| 0.1 | Almost false |
| 0.2 | Slightly false |
| 0.3 | Somewhat false |
| 0.4 | Falser than true |
| 0.5 | As true as false |
| 0.6 | Truer than false |
| 0.7 | Somewhat true |
| 0.8 | Slightly true |
| 0.9 | Almost true |
| 1 | True |

**Table 1: Scale of Truth**

**Source: The Authors**

The values of truthfulness found in Table 1 are obtained to be included as data input into the matrices and also to calculate the results of these predicates that are sensitive to the changes of basic predicate truth values, or to the verbal meaning of the truth values, calculated as shown below. This proposal uses the geometric mean as a conjunction operator, negation as the classical function n(x)=1-x and the dual of geometric mean as a disjunction operator. Universal and existential quantifiers are introduced in the following way:

$$\forall_{x\in U} p(x) = \bigwedge_{x\in U} p(x) = \sqrt[n]{\prod_{x\in U} p(x)} =$$

$$= \begin{cases} \exp\left(\frac{1}{n}\sum_{x\in U} \ln(p(x))\right) & if \quad x\ p(x) \neq 0 \quad (1) \\ 0 & \text{other case} \end{cases}$$

$$\exists_{x\in U} p(x) = \bigvee_{x\in U} p(x) = 1 - \sqrt[n]{\prod_{x\in U} (1 - p(x))} =$$

$$= \begin{cases} 1 - \exp\left(\frac{1}{n}\sum_{x\in U} \ln(1 - p(x))\right) & \text{if} \quad x\ p(x) \neq 0 \quad (2) \\ 0 & \text{other case} \end{cases}$$

$$v(p_1 \wedge p_2 \wedge \ldots \wedge p_n) = (v(p_1).v(p_2)\ldots v(p_n))^{1/n}$$

$$v(p_1 \vee p_2 \vee \ldots \vee p_n) = 1 - ((1 - v(p_1)).(1 - v(p_2))\ldots(1 - v(p_n)))^{1/n}$$

This formulation transfers the classical linguistic knowledge of SWOT to calculate strategic priorities, looking to compensate for the lack of associative properties from conjunction and disjunction operators. It also amplifies its framework to join strategic objectives and actions in order to turn the SWOT analysis into an alignment, ranging from threats and opportunities to objectives and actions that the employees should perform.

This way, the formula continuously tests the matrices, applying geometric means which operate with conjunctions to subsequently carry out disjunctions, until they reach the limit multiplication of the objective x objective matrix (minimal error in Matlab function) and final calculation of the sum of the variables. Such a model was programmed in the Delphi language and it is used in research and academic exercises in business administration and accounting courses for strategic prioritization definitions.

For the data input, the manager of the company followed a sequence of questions to define the quantification of each crossing amongst the variables. These questions are:

- How certain is it that each characteristic of the company is recommendable to propose each objective?
- How certain is it that each characteristic of the environment is recommendable to propose each objective?
- How certain is it that each characteristic of the company together with each characteristic of the environment must be considered to choose the strategies that lead to the company's vision?
- How certain is it that each characteristic is a characteristic of the company? It represents the evaluation of the presence of characteristic.
- How certain is it that each characteristic is a characteristic of the environment? It represents the evaluation of the presence of each characteristic of the environment.
- How certain is it that the fulfillment of each objective has influence on (or great importance to) the fulfillment of each of the other two objectives?
- How certain is it that the performance of each action has influence on (or great importance to) the fulfillment of each of the other two objectives?

After the generation of the matrices, it was possible to process them along with the equations structured through computer systems. Thus, the relative importance of each variable was generated between 0 and 1, the same Scale of Truth (table 1).

To identify data, a questionnaire was used with the technical team to check the safety practices involving information systems. The practices identified were based on the ISO/IEC27002. Figure 1 is mapped through the integration of BSC x COBIT x ISO/IEC27002 models considering the security requirements Confidentiality, Integrity and Availability (Eloff and Eloff, 2003). They proposed a classification of protection practices with the following criteria: "Inadequate", "Minimal", "Reasonable" and "Adequate", but after the pre-test with the information technician, it was suggested to include a category called "Not applicable". This proved to be appropriate because the rule suggests that some practices in the context of the business do not apply. Due to space savings in the present study this instrument is shown already filled with the results of the case study, the Coester Automação Industrial Company.

## 5.2. Model of Images of the Organization

The instruments of identification of images of the organization were developed based on Morgan (1996) and Johann (2008). This instrument performs linear summaries to identify which image or images are the most predominantly in each organization to which it is applied. To this end, this is accomplished with a criterion of evaluation (1 through 4) which is presented in following:

*1 = Practically nonexistent in my organization.*

*2 = Low incidence in my organization.*

*3 = Reasonable occurrence in my organization.*

*4 = Strong presence in my organization.*

The questions developed to identify the images are the 35 that are presented next and, at the end, the same is presented in a summary table with an evaluation section for each question. The 35 questions are related to the different images of the organization, which are Mechanistic (M), Psychic Prisons (PP), Political Systems (PS), Instruments of Domination (ID), Organisms (O), Cybernetic (C), and Flux and Transformation (FT).

**Questions:**

1) Procedures, operations and processes are standardized.

2) Changes in the organization are normally a reaction to changes that already occurred in the macro business environment.

3) Administrators frequently talk about authority, power and superior-subordinate relationships.

4) Flexible and creative action.

5) Working in inadequate circumstances and conditions is considered a proof of loyalty to the organization.

6) The organization sees itself as a part of a larger system where there is an interdependence that involves the community, suppliers and the competition.

7) People and groups tend to display infantile behavior.

8) Past achievements are constantly cited as references and as examples on how to deal with present situations and how to face future adversities.

9) The organization evolves in harmony and balance with its macro environment.

10) People act under constant stress and pressure.

11) There is constant questioning and redirection of actions.

12) Power serves to provide discipline and achieve order in conflicts of interest.

13) The organization considers the motivations and needs of people.

14) There are rigid patterns and uniformity in people’s behavior.

15) The company has and utilizes a great number of rules, norms and regulations about operational aspects of the business.

17) The delegation of power to operational levels tends to be very restricted.

18) Negative feedback is encouraged to correct the organizational direction.

19) The organization expects complete devotion and dedication from its employees.

20) The company benefits more from external events (environmental, etc.) than from strict planning.

21) There are many taboos and prejudices in the organization.

22) The relationships between superiors and subordinates tend to contain elements of love and hate.

23) Long term achievements will be achieved in partnership with the forces acting with the macro-environment and not against it.

24) To dismiss people and streamline activities are part of the game.

25) Most people think about and influence on the destiny of the company.

26) Interpersonal gossip consumes energy and diverts attention from productivity.

27) Organizational objectives and people's needs can be met simultaneously.

28) The organization is a realm of bureaucracy.

29) The organization is expected to operate in a routine, efficient, reliable and predictable manner.

30) Employees are seen as valuable resources who can offer rich and varied contributions to the organizations activities, provided that the organization attends to their needs and motivations.

31) Rumors and gossip are frequent.

32) The organization tends to offer quick answers to changes in their macro-environment.

33) The organization values executives who appear framed and faithful to the mode of being of the company

34) In strategic decision making the company normally abandons the simple view and prefers to take into account the complexity of the situation.

35) People are dedicated to the organization because they feel they belong to something greater, which transcends their existence and individual limitations.

The questionnaire used for data collection was developed, taking as its basic premise the concept that organizations send some images which can, in principle, be perceived by the people who work in them, especially their employees. In constructing the questionnaire, the theoretical approach of Morgan (1996) was used as a reference by eight types of metaphors - or images - that characterize the culture of each organization. Thus, this theoretical approach was applied to the field of organizational practice considering how people, who work in the same organization, perceive the characteristics of their business's organizational metaphors - or images - described by the author.

In constructing the questionnaire it was also found that the organizational images are not uniformly present in the company and that they vary in intensity or presence according to the company under review. That is, some images are more present in a particular organization, while others are more intense. MORGAN (1996) outlined eight possible types of images (metaphors), and in the search - and consequently in the construction of the questionnaire - "organizations as culture" was not included in the metaphor, because in reality all of the other seven images can comprise features of the culture of a company.

Johann (2008) notes that a company's culture is a kind of collective personality and the images of Morgan may serve to characterize the self organization of a collective personality. The self organization, even within the definition of Johann, is the central complex and the nucleus of culture and is repeated in the interaction between people and the consolidation of a set of attitudes that act within the consciousness and unconsciousness (zone shadows), reflect the organizational values and the rules of the game.

In Morgan's approach, it is emphasized that the organization sends multifaceted images – they can, therefore, be regarded as images of self organization - which are perceived by employees. These images take on different facets according to the nature of the culture of their company. So, we worked with the ability to check people's perceptions about the following images of Morgan - or organizational "self" - in the construction of the questionnaire:

M - organizations are perceived as machines;
O - organizations are perceived as Organisms;
PS – organizations are perceived as Political Systems;
C - organizations are perceived as Brains (cybernetic);
ID – organizations are perceived as Instruments of Domination;
FT - organizations are perceived as Flux and Transformation;
PP - organizations are perceived as Psychic Prisons.

The questionnaire was developed comprising a set of 35 questions in total. Each of the seven images above was addressed in the questionnaire through five issues for the consideration of respondents. The issues contained in the questionnaire were distributed throughout this instrument to collect data, looking for its dispersal is aiming to become less obvious the logic of the questionnaire from the perspective of the respondents.

## 5.3. Application of Instrument to identify Images of the Organization

The automation of industrial processes involves an extensive chain of activities that start in scientific research and end when put into operation in a productive unit. Technological evolution in the industry is constant, the plants are not alike and thus its automation is unlikely to be normalized.

Legacy systems (pre-existing) are different and always require adjustments to make new equipment, infrastructure and communications applications compatible with existing ones. This causes the activities, related to the automation of industrial processes, to demand highly qualified manpower and investments in research and development.

According to the company's quality manual, Coester was founded in 1963 and was originally dedicated to communication equipment for businesses and offices. In the mid-60s, beginning with the 1st Brazilian Naval Construction the company directed its activities to design and manufacture of control systems for ships. The company's current focus has become industrial automation.

From an interview with the directors, it was possible to identify the images of the organization as Table 2. The instrument finds totals for each one of the images, which are composed in 35 questions and are presented in Table 2

.

| Test Results | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **M** | | **O** | | **SP** | | **C** | | **ID** | | **FT** | | **PP** | |
| **01:** | 3 | **02:** | 4 | **03:** | 1 | **04:** | 3 | **05:** | 2 | **06:** | 3 | **07:** | 1 |
| **14:** | 2 | **13:** | 3 | **12:** | 3 | **11:** | 2 | **10:** | 2 | **09:** | 3 | **08:** | 4 |
| **15:** | 3 | **16:** | 3 | **17:** | 2 | **18:** | 2 | **19:** | 3 | **20:** | 4 | **21:** | 2 |
| **28:** | 2 | **27:** | 3 | **26:** | 1 | **25:** | 2 | **24:** | 2 | **23:** | 4 | **22:** | 1 |
| **29:** | 2 | **30:** | 3 | **31:** | 2 | **32:** | 2 | **33:** | 3 | **34:** | 3 | **35:** | 2 |
| **12** | | **16** | | **9** | | **11** | | **12** | | **17** | | **10** | |

**Table 2: Results from the Application of the Organizational Image Instrument**

**Source: The Authors**

## 5.4. Analysis of the Models Used (Images and Information Security)

The analyses resulting from the implementation of the organizational image instrument generated a distribution image of "flux and transformation" (17) and the image of "organisms" (16). Flux and transformation are the organizations that best change and evolve according to a changing and evolving environment, their survival depends on its internal and external environment. Organisms, on the other hand, are based principally on the basis of its employees who form the intellectual capital; motivation being a substantial indicator, since it tends to follow a biological clock because there are deadlines to be met and the constant innovations.

So we can say that the company is “dynamic”. It follows the innovations of the external environment and as a part of these same changes allies itself to a significant investment in the functional area. This latter aspect allows us to understand that the workforce can be easily aligned to a dense organizational culture or principal with little existence of a counterculture.

## 5.5. Application of Compensatory Fuzzy Logic (CFL) for Prioritization

First, to identify the strategic priorities the variables of the SWOT analysis (WRIGHT et al, 1998) were defined with the board of directors. Later these variables were expanded to include the Objectives and Actions and with the SWOT a more realistic sense of the business process. Thus, it will generate the mathematical model and computational SWOT-OA sustained by Compensatory fuzzy logic (CFL) which gives the intersection of all the variables together and the processes to generate the final prioritization or differentiated level of importance.

In continuation, all the strategic variables, the filling of the matrixes and finally the result of the processing to direct the funds to be invested in information security are described.

*Primary Strengths within the company:*

a) Proprietary technology;

b) Local engineering;

c) New product line;

d) Lean structure;

e) Flexibility;

f) Structure of local service;

g) Employee qualifications;

h) Financial balance.

*Primary weaknesses within the company:*

a) Structure of deficient services;

b) Very diversified produce;

c) Small scale production;

d) Lack of incentives or appreciation for employees;

e) Communication failures between sectors.

*Opportunities for the company:*

a) Currency appreciation;

b) Economic growth;

c) Increased competition amongst competitors;

d) Predatory competition;

e) Specialists;

f) Turn Key Solutions.

*Threats to the company:*

a) Economic Expansion;

b) Service Market;

c) Prospective international vendors;

*Objectives listed:*

a) Develop skills for services management;

b) Rearrange structure and commercial operations;

c) Enhance the development of overseas business;

d) Intensify the dissemination of new product line;

e) Make communication effective;

f) Develop internal marketing actions;

g) Alignment and cooperation amongst areas;

h) Migrate management controls to SAP.

*Actions:*

a) Establish a methodology for project management;

b) Hire an HR consulting company;

c) Design a program for jobs and wages;

d) Hire a commercial manager;

e) Consolidate the network of sales representatives in the country;

f) Develop commercial representatives for Mexico and the USA;

g) Design advertising material;

h) Restructure the company's website;

i) Communication training for leaders;

j) Create a process map;

k) Hire a certified SAP consultant.

The matrix shows the continuation of the SWOT (Strengths and Weaknesses Opportunities and Threats x) in which the Column and Row "Presence" is equal to how true it is that each of the variables actually exist in the organization or the environment. The geometric mean of each row is multiplied by the Presence. Subsequently, all united matrices are processed by the Matlab function in SWOT-OA system. The total equations were presented in Espin and Vanti (2005). See Table 3: SWOT Matrix

| **STRENGHT/WEAKNESS**<br>**OPPORTUNITY/THREAT** | CurrencyApreciation | EconomicBubble | IncreasedCompetitionAm ongsCompetitors | PreditroyCompetition | Specialists | Turn Key Solutions | Economic Expansion | Service Market | Prospective International Vendors | **Presence Question 4** |
|---|---|---|---|---|---|---|---|---|---|---|
| Proprietary Technology | 0.7 | 0.6 | 0.7 | 0.9 | 0.8 | 0.8 | 0.9 | 0.9 | 0.3 | **0.8** |
| Local Engineering | 0.6 | 0.5 | 0.6 | 0.8 | 0.7 | 0.7 | 0.8 | 0.8 | 0.7 | **1** |
| New Product Lines | 0.7 | 0.6 | 0.7 | 0.9 | 0.8 | 0.8 | 0.9 | 0.9 | 0.6 | **1** |
| Lean Structure | 0.6 | 0.5 | 0.6 | 0.8 | 0.7 | 0.7 | 0.8 | 0.8 | 0.7 | **0.7** |
| Flexibility | 0.7 | 0.6 | 0.7 | 0.9 | 0.8 | 0.8 | 0.9 | 0.9 | 0.6 | **0.7** |
| Local Service Structure | 0.7 | 0.6 | 0.7 | 0.9 | 0.8 | 0.8 | 0.9 | 0.9 | 0.7 | **0.7** |
| Employee Qualifications | 0.8 | 0.7 | 0.8 | 1 | 0.9 | 0.9 | 1 | 1 | 0.7 | **0.8** |
| Financial Equilibrium | 0.6 | 0.5 | 0.6 | 0.8 | 0.7 | 0.7 | 0.8 | 0.8 | 0.8 | **0.8** |
| Structure of Deficient Services | 0.7 | 0.6 | 0.7 | 0.9 | 0.8 | 0.8 | 0.9 | 0.9 | 0.6 | **0.9** |
| Very Diversified Product | 0.5 | 0.4 | 0.5 | 0.7 | 0.6 | 0.6 | 0.7 | 0.7 | 0.7 | **1** |
| Small Scale Production | 0.5 | 0.4 | 0.5 | 0.7 | 0.6 | 0.6 | 0.7 | 0.7 | 0.5 | **1** |
| Lack of Incentives or Appreciation for Employees | 0.8 | 0.7 | 0.8 | 1 | 0.9 | 0.9 | 1 | 1 | 0.5 | **0.7** |
| Communication Failures Between Sectors | 0.6 | 0.5 | 0.6 | 0.8 | 0.7 | 0.7 | 0.8 | 0.8 | 0.8 | **0.7** |
| **Presence Question 5** | **1** | **0.7** | **0.8** | **0.7** | **1** | **1** | **1** | **0.8** | **0.8** | XXX |

**Table 3: SWOT Matrix**

**Source: The Authors**

The subsequent matrix compares Strengths and Weaknesses x Strategic Objectives.

**See Table 4: Quantification: Strategic Objectives x Weaknesses and Strengths**

The subsequent Matrix compares Opportunities and Threats x Strategic Objectives.

| MATRIX 2<br>Question 2 | Strategic Objectives | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Develop Skills for Services Management | Rearrange Structure and Commercial Operations | Intensify the Development of Overseas Business | Intensify the Dissemination of the New Product Line | Make Communication Effective | Develop Internal Marketing Actions | Alignment and Cooperation Amongst the Areas | Migrate Management Controls to SAP |
| **STRENGHT/WEAKNESSES** | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx |
| Proprietary technology | 0 | 0.6 | 0 | 0.5 | 0.2 | 0.7 | 0.2 | 0 |
| Local Engineering | 0.7 | 0.7 | 0.8 | 0.8 | 0.7 | 0 | 0.2 | 0 |
| New Product Line | 0.7 | 0.9 | 0.9 | 0.9 | 0.9 | 0.8 | 0.9 | 0.9 |
| Lean Structure | 0 | 0.9 | 0.8 | 0.3 | 0.9 | 0 | 0.8 | 0.8 |
| Flexibility | 0.8 | 0.8 | 0.8 | 0 | 0.8 | 0 | 0.8 | 0.3 |
| Local Service Structure | 1 | 0.9 | 0.9 | 0.5 | 0.3 | 0 | 0.7 | 0.3 |
| Employee Qualifications | 1 | 0.8 | 1 | 1 | 0.8 | 0.8 | 0.8 | 0.9 |
| Financial Balance | 0.8 | 0.5 | 0.8 | 0.8 | 0 | 0 | 0.7 | 0.6 |
| Structure of Deficient Services | 1 | 0.9 | 0.9 | 0.5 | 0.3 | 0.7 | 0.8 | 0.7 |
| Very Diversified Product | 0.2 | 0.2 | 0 | 0.5 | 0 | 0 | 0.8 | 0.8 |
| Small Scale Production | 0.2 | 0.2 | 0 | 0 | 0 | 0 | 0.9 | 0.8 |
| Lack of Incentives or Appreciation for Employees | 0.8 | 0.8 | 0.8 | 0.7 | 0.3 | 0.8 | 0.7 | 0.8 |
| Communication Falure Between Sectors | 0.2 | 0.2 | 0 | 0.8 | 1 | 1 | 1 | 1 |

**Table 4: Quantification: Strategic Objectives x Strengths and Weaknesses**

**Source: The Authors**

**See Table 5: Quantification: Strategic Objectives x Opportunities and Threats**

The subsequent Matrix compares Strategic Objectives x Strategic Objectives.

| MATRIX 3<br>Question 3 | Strategic Objectives | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Develop Skills for Services Management | Rearrange Structure and Commercial Operations | Intensify the Development of Overseas Business | Intensify the Dissemination of the New Product Line | Make Communication Effective | Develop Internal Marketing Actions | Alignment and Cooperation Amongst the Areas | Migrate Management Controls to SAP |
| **THREATS/<br>OPPORTUNITIES** | xxxx | xxxx | xxxx | xxxx | xxxx | xxxxx | xxxx | xxxx |
| Currency Valuation | 0 | 0.6 | 1 | 0.8 | 0.1 | 0 | 0 | 0 |
| Economic Bubble | 0 | 0.4 | 0.8 | 0.2 | 0 | 0 | 0 | 0 |
| Increased Competition Amongst Competitors | 0.9 | 0.8 | 0.8 | 0.8 | 0.2 | 0 | 0.1 | 0.6 |
| Predatory Competition | 0.8 | 0.8 | 0.8 | 0.1 | 0 | 0 | 0.1 | 0 |
| Specialists | 1 | 0.8 | 0.9 | 0.1 | 0 | 0 | 0.8 | 0 |
| Turn Key Solutions | 1 | 0.8 | 0.9 | 0.2 | 0 | 0 | 0.8 | 0 |
| Economic Expansion | 1 | 0.9 | 0.9 | 0.9 | 0.6 | 0 | 0.3 | 0 |
| Services Market | 1 | 1 | 0.8 | 0.2 | 0.8 | 0 | 0.9 | 0.8 |
| Prospective International Vendors | 0.2 | 0 | 1 | 0.2 | 0.2 | 0.3 | 0.8 | 0.8 |

**Table 5: Quantification: Strategic Objectives x Opportunities and Threatens**

**Source: The Authors**

## See Table 6: Quantification: Strategic Objectives x Strategic Objectives

The subsequent Matrix compares Actions x Strategic Objectives.

| Strategic Objectives | Develop Skills for Services Management | Rearrange Structure and Commercial Operations | Intensify the Development of Overseas Business | Intensify the Dissemination of the New Product Line | Make Communication Effective | Develop Internal Marketing Actions | Alignment and Cooperation Amongst the Areas | Migrate Management Controls to SAP |
|---|---|---|---|---|---|---|---|---|
| Develop Skills for Services Management | 1 | 0.8 | 0.9 | 0.6 | 0.8 | 0.5 | 0.8 | 0.9 |
| Rearrange Structure and Commercial Operations | 0.8 | 1 | 0.8 | 0.3 | 0.3 | 0.7 | 0.8 | 0.8 |
| Intensify the Development of Overseas Business | 0.9 | 0.8 | 1 | 0.8 | 0.8 | 0.8 | 0.9 | 0.6 |
| Intensify the Dissemination of the New Product Line | 0.7 | 0.8 | 0.8 | 1 | 0.8 | 0.9 | 0.9 | 0.2 |
| Make Communication Effective | 0.8 | 0.8 | 0.7 | 0.7 | 1 | 0.9 | 0.8 | 0.9 |
| Develop Internal Marketing Actions | 0.9 | 0.7 | 0.7 | 0.8 | 0.9 | 1 | 0.9 | 0.8 |
| Alignment and Cooperation Amongst the Areas | 0.9 | 0.9 | 0.9 | 0.5 | 1 | 0.8 | 1 | 0.9 |
| Migrate Management Controls to SAO | 0.8 | 0.6 | 0.7 | 0.2 | 0.8 | 0.8 | 0.8 | 1 |

**Table 6: Quantification: Strategic Objectives x Strategic Objectives**

**Source: The Authors**

## See Table 7: Quantification: Strategic Objectives x Actions

Each of the matrices was filled by the IT Manager for each one to be subsequently inserted into the computer system for calculating importance, which defines ranking or strategic priorities. The result of this processing is represented in table 8.

| **Strategic Objectives** | Develop Skills for Services Management | Rearrange Structure and Commercial Operations | Intensify the Development of Overseas Business | Intensify the Dissemination of the New Product Line | Make Communication Effective | Develop Internal Marketing Actions | Alignment and Cooperation Amongst the Areas | Migrate Management Controls to SAP |
|---|---|---|---|---|---|---|---|---|
| **Actions** | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx | xxxx |
| Establish a methodology for project management | 0.9 | 0.7 | 0.6 | 0.6 | 0.6 | 0.8 | 0.7 | 0.8 |
| Hire an HR consulting company | 0.9 | 0.9 | 0.8 | 0.7 | 0.8 | 0.8 | 0.8 | 0.7 |
| Design a program for jobs and wages | 0.7 | 0.8 | 0.6 | 0 | 0.6 | 0.7 | 0.3 | 0 |
| Hire a commercial manager | 0.7 | 1 | 0.9 | 0.7 | 0.5 | 0.7 | 0.3 | 0.7 |
| Consolidate the network of sales representatives in the country | 0.5 | 1 | 0.5 | 0.8 | 0 | 0.6 | 0.3 | 0 |
| Developed commercial representatives for Mexico and the USA | 0.5 | 0.9 | 1 | 0.8 | 0 | 0.8 | 0 | 0 |
| Design advertising material | 0 | 0.4 | 1 | 1 | 0.5 | 0.5 | 0 | 0 |
| Restructure the company's website | 0.5 | 0.7 | 0.8 | 0.8 | 0.8 | 0.7 | 0.6 | 0.8 |
| Communication training for leaders | 0.3 | 0.8 | 0.8 | 0.5 | 1 | 0.9 | 0.9 | 0.8 |
| Create a process map | 0.5 | 0.8 | 0.3 | 0 | 0.8 | 0.5 | 0.9 | 0.9 |
| Hire a certified SAP consultant | 0.3 | 0.8 | 0.3 | 0 | 0.6 | 0 | 0.8 | 1 |

**Table 7: Quantification: Strategic Objectives x Actions**

**Source: The Authors**

## See Table 8: Prioritization based in Compensatory Fuzzy Logic (CFL)

The results highlighted in red are those that should receive more attention from the security management in a more strategic way, that is, involving not only internal variables of the organization, but also external variables such as Opportunities and Threats. The strategic priorities indicate a significant search for new business in services and international markets and that means the hiring of manpower to meet this demand.

| | | |
|---|---|---|
| Organizational Characteristics | | |
| st7 | Employee Qualifications | 1 |
| st6 | Local Service Structure | 0.84096875 |
| st3 | New Line of Products | 0.83740745 |
| st5 | Flexibility | 0.83740745 |
| st1 | Proprietary Technology | 0.82798177 |
| st8 | Financial Balance | 0.79322776 |
| st2 | Local Engineering | 0.78434395 |
| st4 | Lean Structure | 0.78434395 |
| we4 | Lack of Incentives or Appreciation for Employees | 1 |
| we1 | Structure of Deficient Services | 0.83206217 |
| we5 | Communication Failures Between Sectors | 0.78978055 |
| we3 | Small Scale Production | 0.73074916 |
| we2 | Very Diversified Product | 0.72858576 |
| Environmental Characteristics | | |
| op2 | Local Engineering | 0.84948461 |
| op3 | Services Market | 0.84948461 |
| op1 | Economic Expansion | 0.73077657 |
| th3 | Increased Competition Amongst Competitors | 0.84948461 |
| th1 | Currency Valuation | 0.79417651 |
| th2 | Economic Bubble | 0.79417651 |
| th4 | Predatory Competition | 0.73738553 |
| th6 | Turn Key Solutions | 0.73738553 |
| th5 | Specialists | 0.68366691 |
| Strategic Objectives | | |
| ob1 | Develop Skills for Services Management | 1 |
| ob3 | Intensify the Development of Overseas Business | 1 |
| ob4 | Intensify the Dissemination of New Product Line | 1 |
| ob7 | Alignment and Cooperation Between Areas | 0.77453586 |
| ob6 | Develop Internal Marketing Actions | 0.75263601 |
| ob5 | Make Communication Effective | 0.74630662 |
| ob2 | Rearrange Structure and Commercial Operations | 0.73503024 |
| ob8 | Migrate Management Controls to SAP | 0.72180293 |

| Actions | | |
|---|---|---|
| ac6 | Develop a commercial representative for the U.S. and Mexico | 1 |
| ac7 | Design advertising material | 1 |
| ac2 | Hire an HR consultancy | 0.83621855 |
| ac9 | Communication training for leaders | 0.79504613 |
| ac4 | Hire a commercial manager | 0.79498275 |
| ac1 | Implant a project management methodology | 0.79233469 |
| ac8 | Restructure the company website | 0.78601955 |
| ac10 | Conduct process mapping | 0.68926213 |
| ac5 | Consolidate the network of sales representatives in the country | 0.65111586 |
| ac3 | Design a program of jobs and wages | 0.623552 |
| ac11 | Hire a SAP certified consultant | 0.61280733 |

**Table8: Prioritization based in fuzzy logic**

## 5.6 Application of Information Security Model

The instrument that generated the integration of BSC (strategic) x COBIT (tactical) x ISO/IEC27002 (operational) model, in the case studied, allowed us to observe that in the "Minimal to Reasonable" technical level information security it is treated through isolated actions based on technical knowledge. It is confirm the theoretical reference points as a constraint on model for IT management in organizations, there is no executive view on aspects surrounding the security of information.

Posthumus and Solms (2004) confirm that information security should be incorporated into corporate governance and cared for at the highest management levels. For information security to be effective, it has to be incorporated into the culture of the organization through techniques such as the establishing of policies, training, awareness and application of disciplinary practices (Solms and Solms, 2004).

The implementation of the protection of the norm instrument, domain 8 (HR) concentrated 71% of “inadequate” protection to “minimum” protection and this demonstrated a potential risk. This is possible because a knowledgeable, but unsatisfied employee can harm the company through theft, fraud and improper use of resources related to information.

The same argument can be extended to domain 9 (physical and environmental security), 77% of inadequate protection, with the possibility of damage and interference with the facilities and organization information causing loss, damage, theft or compromise of assets and disruption of activities of the organization.

**See Table 9: Results from the protection with qualitative of information security**

| Protection | | | | Areas of standard |
|---|---|---|---|---|
| 1 - Inadequate | 2 - Minimal | 3 - Reactive | 4 - Adequate | |
| 0.00% | 50.00% | 50.00% | 0.00% | 5 - (PL) – Information Security Policy |
| 15.79% | 47.37% | 36.84% | 0.00% | 6 - (OI) – Organizing Information Security |
| 0.00% | 62.50% | 25.00% | 12.50% | 7 - (GA) – Asset Management |
| 14.29% | 57.14% | 14.29% | 14.29% | 8 - (RH) – Human Resources Security |
| 4.17% | 70.83% | 16.67% | 8.33% | 9 - (SA) – Physical and Environmental Security |
| 16.07% | 32.14% | 42.86% | 8.93% | 10 - (GO) – Operations and Communications Management |
| 18.60% | 27.91% | 39.53% | 13.95% | 11 - (CA) – Access Control |
| 15.63% | 56.25% | 28.13% | 0.00% | 12 - (AQ) – Acquisition, Development and Maintenance of Information Systems |
| 63.64% | 18.18% | 18.18% | 0.00% | 13 - (GI) – Information Security Incident Management |
| 0.00% | 50.00% | 50.00% | 0.00% | 14 - (GC) – Business Continuity Management |
| 31.58% | 26.32% | 42.11% | 0.00% | 15 - (CF) – Compliance |

**Table 9: Results from the protection with qualitative Fuzzy Results (norm control)**

**Source: The Authors**

## 6. CONCLUSION

IT Governance enables the expansion of compliance and Corporate Governance through the use of different models such as the audit of IT processes and information security. This provides more robust systems and internal control; however, limitations have been identified for achieving strategic alignment between IT and Business.

The limitations of strategic alignment between IT and Business may be related to aspects of organizational behaviour and strategic prioritization, covered in this work. These limitations create vulnerabilities in the information that is, reducing the security of information, especially for business requirements.

This paper develops the strategic alignment of organizational behavior through the organizations image, prioritization and information security practices. To this end, information security is studied based on the requirements of confidentiality, integrity and availability by applying a tool which integrates the strategic, tactical and operational vision through the following framework; Balanced Scorecard - BSC (strategic) x Control Objectives for Information and Related Technology - COBIT (tactical) x International Organization for Standardization - ISO/International Electro

Technical Commission - IEC27002 (operational).In Knorst (2010) the mapping of this alignment is presented.

Another image instrument of the organization is applied in parallel with this analysis to identify and analyze performance involving profiles related to mechanistic, psychic prisons, political systems, instruments of domination, organisms, cybernetics, flux and transformation (MORGAN, 1996) and (JOHANN, 2008). Finally, a model of strategic prioritization CFL based on fuzzy logic is applied (ESPIN and VANTI, 2005). The method was applied to an industrial company located in southern Brazil.

Many of the problems related to information security are related to behavior that is not suitable to the culture of the organization. This behavior can be characterized as a counterculture that brings together small groups in companies that do not accept the dominant culture.

The consequence of maintaining these small groups may be directly related to the denial of information boycotts of information relating to business innovation and the delivery of information to third parties through the release of passwords or even by sending it out of the organization via scanned files.

A common business response to this type of problem is to implement a greater number of IT solutions. This work, however, presented a solution that aligns the technical answers (IT models/IT governance) aligned with models of behavior and business culture through the study of their images. This indicates that depending on the results evaluated by the applied instruments, you can find good solutions and invest resources correctly for information security with a major investment in staff training, their awareness, and adherence to the dominant culture in the company.

In the case studied, security requirements were aligned with the images of “organism” and “flux and transformation”. Thus, by definition these two images have a significant functional recovery and dynamism with the movement of the market, meaning that it can significantly facilitate the consistency of the work between the technical area and the behavioral area.

For information security, it was concluded that the technical perspective is from “Minimal” to “Reasonable”; this dimension based significantly on isolated actions based on technical knowledge. Thus, it was possible to analyze the Confidentiality, Integrity and Availability applying an instrument that integrates the strategic, tactical and operational vision through the BSC (strategic) x COBIT (tactical) x ISO/IEC27002 (operational)Models.

The organizational profile revealed that images of “organisms” and “flux and transformation” and the area of Human Resources Security (RH) are suggested as minimal and actions are suggested with a base in security policies and training so that employees, suppliers and third parties understand their responsibilities and are aware of the threats and concerns about information security.

The controllability of the company studied diagnosed by the technology instrument also allows certain flexibility for the image of “flux and transformation” aligned to “organisms”. Thus, the company adapts to the external environment and has a high level of control of strategic information, while innovating with adaptations to environmental changes, which are typical of the industry it serves. Finally, it has presented the application in a real case and, in order to preserve the integrity of the company’s private information, some results were analyzed in a more synthetic way.

With the LDC model, it was also possible to find the information security variables that were related to the SWOT and consequently the external environment. This means that the company has the strategic positioning on information security that considers the company's internal environment (strengths and weaknesses), but also considers the external environment (opportunities and threats), which contain the variables of "competitors," "government regulations" and "technological trends" which possess relations of great vulnerabilities.

## REFERENCES

Adizes, I. *Corporate Lifecycles: How and Why Corporations Grow and Die and What to Do About It.*NJ: Paramus, 1989, ISSBN 0-13-174400-3.

Dias, C. *Segurança e Auditoria da Tecnologia da Informação.* Rio de Janeiro: Axel Books, 2000.

Eloff, J.; Eloff, M. Information Security Management: A New Paradigm. *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on enablement through technology*. Republic of South Africa p.130-136, 2003.

Espín, R.; Vanti, A.A. Administración Lógica: Un estudio de caso en empresa de comercio exterior. *Revista BASE.* São Leopoldo, RS- Brasil, ago, 1(3), 2005, pp.4-22.

Fitzgerald, T, Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other. Information Systems Security, Volume 16, Issue 5, Pages 257-263, 2007.

Freitas, M. E de. *Cultura organizacional: formação, tipologias e impactos*. São Paulo: Makron, McGraw-Hill, 1991.

Grenberger, W.; De Haes, S.; Measuring and improving information technology governance through the Balanced Scorecard. *Information Systems Control Journal.*Vol. 2, 2005, ITGI.

ITGI: Information Technology Governance Institute. CobiT 4.1: *Framework, Control Objectives, Management Guidelines, Maturity Models*. Available in: http:// www.isaca.org/, accessed in Feb, 24, 2009.

ISO/IEC 27002:2005. *Information technology e code of practice for information security management.* Switzerland: International Organization for Standardization (ISO), 2005.

Johann, S. L. *Gestão da cultura corporativa: como as organizações de alto desempenho gerenciam sua cultura organizacional*. Porto Alegre: Saraiva, 2008, 2a.edition.

______. Gestão da cultura organizacional. *Working in paper - SIGA* - Sistema de Informação e Gestão), Rio de Janeiro: Acadêmica, da Fundação Getúlio Vargas (FGV), 2008.

Kaplan, R. S.; Norton, D. P.*The Balanced Scorecard: Translating Strategy into Action*. Mass: Harvard Business School Press, 1996.

Knorst, A. M. *Strategic alignment between business goals and information security in the IT governance context: a study in the automation industry*. Thesis Master's degree. Unisinos. São Leopoldo, 2010.

Kwok, l.; Longley, D. *Information security management and modeling, Information Management & Computer Security,* Volume 7, Issue 1, Pág.30 – 40, 1999.

Minarelli, J.A. *Empregabilidade – o caminho das pedras.* São Paulo: Ed. Gente, 1995.

Moreira, N. S. *Segurança Mínima – Uma Visão Corporativa da Segurança de Informações*. Rio de Janeiro: Axcel Books, 2001.

Morgan, G. *Images of organization*. London: SAGE Publications, 1996.

Posthumus, S.; Solms, R.. A framework for the governance of information security.*Computers & Security*, Amsterdam, no. 23, págs. 638-646, 2004.

Schein, E. H. Organizational Culture. *American Psychologist*. San Francisco, v.45, n.2, fev. 1990, 109-119.

Sêmola, M.. *Gestão da Segurança da informação: Visão executiva da Segurança da Informação*. Rio de Janeiro: Campus, 2003.

Solms, R.; Solms, B.. From policies to culture, *Computers & Security*, Volume 23, Issue 4, 2004, Pages 275-279.

Vanti, A.A.; Espin, R.; Goyer, D., Schripsema, A. The importance of objectives and strategic lagging and leading indicators definition in the chain import and export process in the light of strategic planning through the use of Fuzzy Logic*System.ACM SIGMIS Conference Personnel Resource (CPR),* April, Claremont, 2006.

Vanti, A.A.; Espin, R. Metodologia Multivalente para Priorização Estratégica em Construção de Balanced Scorecard (BSC). *Revista CCEI*, vol. 11, no. 20. Ago. 2007, pages 54-67.

Weill, P.; Ross, J. *Governança de Tecnologia da Informação***.** São Paulo, M. Books do Brasil Editora Ltda.

Wright, P.; Kroll, M.; Parnell, J. *Strategic Management: concepts*. New Jersey: Prentice Hall, 1998.