



Revista Científica "Visión de Futuro"  
ISSN: 1669-7634  
ISSN: 1668-8708  
visiondefuturo@fce.unam.edu.ar  
Universidad Nacional de Misiones  
Argentina

## Compliance risk management with a focus on shared values: Application in a case study in Cuba

**Plasencia Soler, Juan Antonio**  
**Bajo Sanjuán, Anna**  
**Marrero Delgado, Fernando**  
**Nicado García, Miriam**

Compliance risk management with a focus on shared values: Application in a case study in Cuba  
Revista Científica "Visión de Futuro", vol. 27, núm. 2, pp. 25-41, 2023  
Universidad Nacional de Misiones

Disponible en: <https://www.redalyc.org/articulo.oa?id=357975013002>

DOI: <https://doi.org/10.36995/j.visiondefuturo.2023.27.02.001.en>



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 2.5 Argentina.

## Compliance risk management with a focus on shared values: Application in a case study in Cuba

*Juan Antonio Plasencia Soler*  
*Universidad de las Ciencias Informáticas, Cuba*  
juanps@uci.cu  
*Anna Bajo Sanjuán*  
*ESIC Business & Marketing School, España*  
anna.bajo@esic.university  
*Fernando Marrero Delgado*  
*Universidad Central de Las Villas, Cuba*  
fmarrero@uclv.edu.cu  
*Miriam Nicado García*  
*Universidad de La Habana, Cuba*  
nicado@rect.uh.cu

DOI: [https://doi.org/10.36995/  
j.visiondefuturo.2023.27.02.001.en](https://doi.org/10.36995/j.visiondefuturo.2023.27.02.001.en)

Recepción: Junio , 13, 2023  
Aprobación: Septiembre , 07, 2023



Acceso abierto diamante

### Abstract

Organizations that aspire to obtain long-term results must correctly manage compliance with laws, regulations, codes, international standards and best practices related to ethics and society's expectations. This research aims to develop a procedure to manage compliance risks with a focus on organizational values. The paper includes the main stages of traditional risk analysis: analysis of the organizational context, identification of obligations, evaluation and assessment of compliance risks and their treatment through action plans. As the main novelty, the authors include a tool that allows the integration of the elements of the context, with the identified obligations, their associated risks and the ethical values shared by the organization, called CORVAL map. The results of the implementation of the procedure in the process of Production of Computer Services in an Cuban entity allow to identify as main risks: illicit contractual relations, lack of knowledge of the code of conduct by the workers, affectations to the prestige of the organization and high rates of electric energy consumption, identifying the shared value Responsibility and its associated behavior, as the most influential principle in the mitigation of the risks of compliance of the process.

**Keywords:** Compliance, Compliance risk, Risk Management, Organizational values.

## INTRODUCTION

In the 1970s and 1980s, governments enacted laws to address a number of social problems related to corrupt financial practices, environmental pollution, health hazards and worker safety, just to mention a few of the most relevant.

Compliance with these laws and regulations has been a challenge for management ever since governments have imposed regulations on organizations. As a result, there has always been some kind of "system" for compliance, where companies develop internal processes capable of ensuring that they comply with the rules and regulations (Coglianese & Nash, 2020).

In more recent decades, organizations have formalized the management of their compliance responsibilities as the complexity of regulations has increased, as well as the complexity of business operations and transactions. Moreover, this management has been integrated into the programs and actions that are executed as part of the organization's culture, bringing both terms, ethics and compliance, to integrate and complement each other.

Ethics and Compliance Management (ECM) has become an important and pervasive issue (Mitra et al., 2020) for organizations to achieve economic, social and environmental sustainability for all stakeholders. The implementation of an ECM is part of a moral reflection and has strategic relevance for organizations (Chan & Ananthram, 2020).

On the other hand, companies nowadays conduct their operations in the presence of multiple stakeholders, divergent values and conflicting beliefs (Bhaumik et al., 2019; Singh & Delios, 2017) so it becomes necessary for the elements of the ECM to combine regulatory compliance with an emphasis on ethical behavior.

According to Kreipl (2020), some of the common elements of ECM are the following: compliance risk management; internal and external information and communication systems; internal control systems; and the development of a compliance culture.

The present research addresses the first of these aspects, compliance risk management. Risk is usually defined as the effect of uncertainty on objectives (International Organization for Standardization, 2018), while compliance risk is associated with the probability of occurrence and consequences of non-compliance with requirements that an organization must mandatorily comply with or chooses to voluntarily comply with (International Organization for Standardization, 2021).

Ferrell et al. (2015) express that organizations transform an initially more rule-oriented culture, i.e. focused on compliance, into a more value-based one. And that is that compliance management must be approached with a well-defined set of shared values (Bussmann & Niemeczek, 2019) and a management that is seen to implement and respect these values. The integration of the values approach to compliance risk management in an organization involve the fundamental contribution made by this article.

The purpose of this research is to develop a procedure for compliance risk management with a focus on shared values, taking a Cuban organization as a case study. In the first section, a theoretical foundation is provided on compliance risk management and the organizational values approach. In a second section, the steps and methods used in the research are presented. Then, the main results of the application of the procedure in a Cuban organization, selected as a case study, are highlighted. Finally, the conclusions of the study are stated.

### Conceptual framework

In this section a brief conceptual framework is developed where the main definitions associated with compliance risk management and the steps to carry it out are discussed, as well as the organizational values and their main concepts.

### Compliance risk management

Risk management is defined as the set of coordinated activities to direct and control the organization in relation to risk (International Organization for Standardization, 2018) by reducing or mitigating its negative effects (Society of Corporate Compliance and Ethics, 2022). The most common stages of risk management are context determination, risk assessment and risk treatment (Dvorsky et al., 2021; Sanchez et al., 2022).

On the other hand, regulatory compliance refers to adherence to laws and regulations approved by official regulatory bodies, as well as to the general principles of an organization's ethical conduct (Society of Corporate Compliance and Ethics, 2022). Compliance is sustained by integrating it into the culture of an organization, as well as in the behavior and attitude of employees.

Compliance risk management does not differ in its implementation from the management of other risks (Puteri Nur Farah Naadia & Khairuddin, 2021), it is necessary to take into account the strategic and operational objectives of the organization (Brondolo et al., 2022), its internal and external context, as well as the use of techniques for its evaluation and treatment (Krepysheva et al., 2020).

The authors Ferreira de Araújo Lima et al. (2020) enunciate four types of risks: financial, security, operational and strategic risks, including in these aspects related to the fulfillment of organizations' obligations. Ramakrishna (2015) proposes a classification for compliance risks: integrity risk, commercial risk, reputational risk, regulatory risk; interpretation risk; legal risk; litigation risk; and risk of financial loss; however, Krepysheva et al. (2020) consider that this type of divisions is loosely structured, because the same compliance risk could be categorized in several of the above classifications.

Compliance risks cover a wide spectrum and may be associated with privacy and data protection, information security, use of social networks, or cybersecurity. In governance issues, risks related to conflicts of interest with third parties or corruption must be taken into account, aspects that are sought to be mitigated through the code of ethics and conduct.

At the operational level, other risks to consider are intellectual property infringement, occupational health and safety, consumer protection, product safety, or trade. All this, in addition to a long list of others, including environmental risks.

Once the regulatory risks have been identified, they must be assessed to determine how likely they are to occur and what impact they may have on the company and its stakeholders. According to a study by Weber and Wasieleski (2013), organizations use compliance risk assessment primarily for four purposes: to identify areas of concern before they become problems, to detect fraud, to comply with legal requirements, and to evaluate the effectiveness of their information systems.

Risk is often expressed in terms of risk sources, an element that has the potential to generate risk; potential events, a particular set of circumstances; its consequences, the outcome of an event that affects objectives or obligations; and its probabilities, the possibility of something happening (International Organization for Standardization, 2018), but the authors consider that an underexplored category, and one that should be taken into account in the risk management process, is its relationship to an organization's shared values.

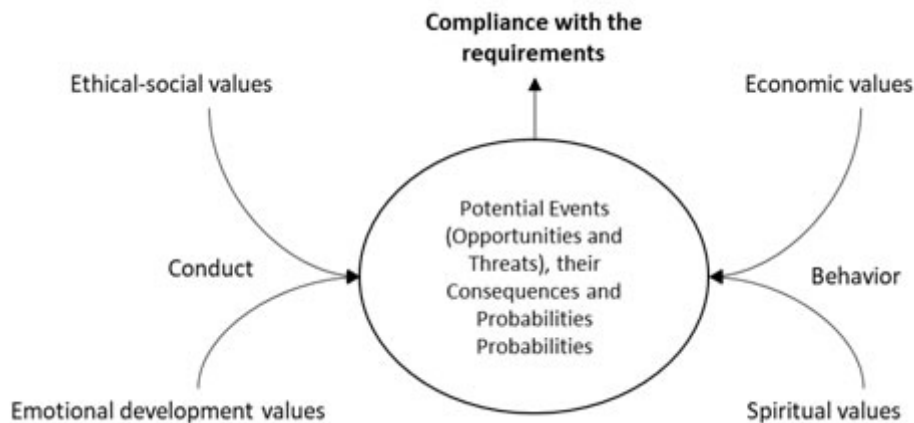
## Organizational values

Organizations commonly define from their strategic planning a set of organizational values, in order to establish a guide for the decision-making process to achieve strategic objectives (Gabel-Shemueli et al., 2013), constitute a source of motivation (Gaete Quezada and Gaete Quezada, 2020) and improve the behavior of workers in their work performance (Montañez-García, 2017).

Organizational values can be defined as the idealization of the collective experience of success in the use of a certain skill and the emotional transfiguration of previous beliefs (Gagliardi, 1986), hierarchically organized (Alves and Carvalho, 2021) that guide human behavior and are concretized in actions and behaviors of people (Rokeach, 1973) in the work environment (Díaz Chica et al., 2019). The concept of value gathers five essential characteristics: they are perceptions or beliefs; they relate desired actions and the

final state of behavior; they transcend to specific situations; they guide the choice or evaluation of behaviors; and they can be ordered according to their relative importance (Bolzan-de-Campos, 2018).

According to Dolan and Altman (2012) organizations should consider four types of values, ethical-social (way in which people behave and relate in an environment), economic (ensure organizational survival in a competitive environment), emotional development (related to the intrinsic motivation of people) and spiritual (able to align the other instrumental values). On the other hand, values make it possible to adapt the rules and controls established by individuals (Barrios-Pineda, 2018) so it is possible through their definition, communication, and integration, to reduce the effect of uncertainty on the requirements that an organization must comply with mandatorily or voluntarily (see Fig. N° 1).



**Figure 1**  
The influence of organizational values on compliance risks  
Own elaboration

From what has been analyzed in this section, the authors of the research consider that ethical values play a fundamental role in the mitigation of compliance risks in an organization, and this is an aspect that has been little addressed in the scientific literature consulted, so the following section presents a procedure that integrates the shared values approach to traditional regulatory risk management.

## DEVELOPMENT

This section describes the methodology used for the case study; the procedure for risk management with a shared values approach, taking into account the aspects and considerations studied in the previous section and the proposals of international instruments, such as the International Standard ISO 37301:2021 on Compliance Management Systems and the International Standard ISO 31000: 2018 on Risk Management. Then, the main results of the application of the procedure in the process of Production of Computer Services in a Cuban entity are shown.

### Methodology

The research is a case study, having a descriptive approach, due to the fact that it reflects the compliance risk assessments. The authors first selected an Information and Communication Technologies organization in Cuba. Then they decide to apply a procedure for compliance risk management. For the development of the procedure, qualitative methods such as the analysis of primary and secondary sources and the expert method are used. In addition, quantitative methods are used to evaluate risks through a criticality index. The main results of the use of the methods are shown below and finally the proposals for improvements are summarized.

### Procedure for risk management with a shared value approach

The procedure considers the focus on the organization's shared values, from its integration to compliance risk management, through the preparation of the CORVAL map (acronym associated to the words: Context, Obligations, Risks, Values) to contribute to the mitigation of the risks identified in the processes. The sequence of stages is shown in Fig. N° 2.

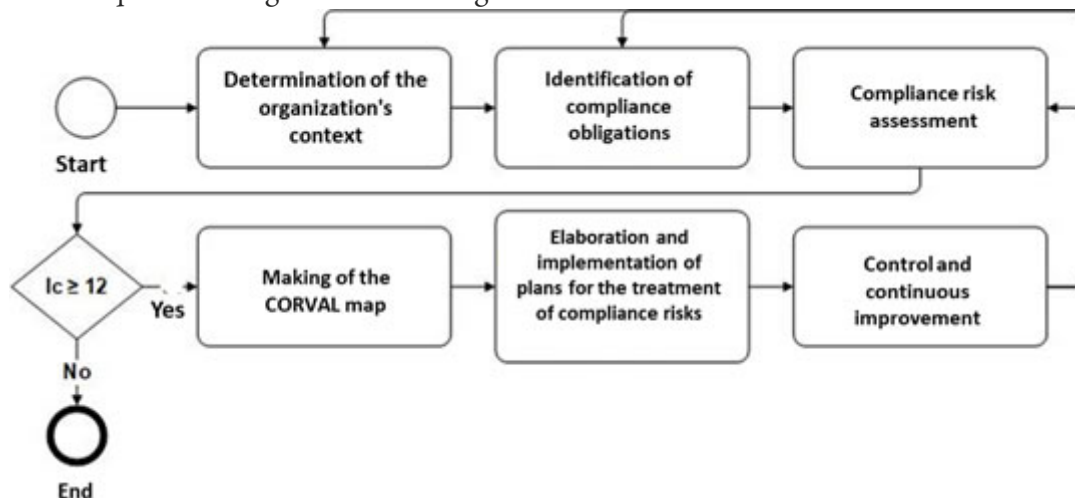


Figure 2

Procedure for compliance risk management with a focus on organizational values  
Own elaboration.

In Cuban entities, risk management is the responsibility of senior management, through the company's Prevention and Control Committee, which represents an advisory body and is chaired by the highest authority of the organization. However, there are usually departments or working groups for Internal Control, which guide this activity methodologically. For the purposes of research and possible generalization of this procedure, we will refer to the group, department or management in charge of risk management in the organization as the working team. The steps that make up the procedure are described below.

### Step 1. Determination of the organization's context

The work team must determine the issues that are relevant to achieving its purposes and that affect its ability to achieve the intended results and bring them to the approval of the organization's Prevention and Control Committee. The determination of the context can be divided into the analysis of external factors -cultural, political, economic, social, technological, ecological and legal- and internal factors -procedures, policies, processes and resources-. In this activity, stakeholders and their requirements should also be identified through the preparation of a materiality map.

In determining the internal context, it is important to identify the organization's main processes, which will then allow the regulatory compliance obligations and risks to be associated with these processes, commonly classified into strategic, key and support processes.

To determine the external context, it is suggested to use the PESTEL analysis; while for the internal context it is recommended to use methods to obtain information, such as interviews, analysis of balance sheet reports or results of previous periods and consultation of documents.

The data obtained in this step provide information on the legal and regulatory context, the economic, social and cultural situation, the internal structure and processes, as well as aspects of the strategy and nature of the business under study, which is necessary to determine compliance obligations.

### Step 2. Identifying compliance obligations

Based on the analysis of the organization's context carried out in the previous step, the work team is responsible for identifying the obligations and submitting them to the Prevention and Control Committee for approval.

These obligations come from norms and resolutions relevant to the organization and the sector to which it belongs; rules or guidelines issued by regulatory agencies; treaties, agreements and protocols; agreements with community groups; environmental commitments; laws and decrees, among others. On the other hand, from an internal point of view, the policies, codes, standards and other obligations that govern the organization's behavior are analyzed.

In this step it is very important to identify the organizational values. It is common for organizations to have identified a group of beliefs or organizational values, so the work team will take these to continue with the analysis, but if they are not defined, or if it is in the interest of top management to redefine them, this is done through the following activities.

First, the basic beliefs of the members of the organization must be diagnosed, which is usually done through a questionnaire. Then, an order or importance of the selected values must be established, for example by using a group of experts to prioritize the identified values; it is important, in this step, to have the approval of the entity's top management. Finally, each of the values must be operationalized for a better understanding among employees.

It is necessary to have communication channels that identify new developments and changes in the obligations to ensure that they are updated for the organization. The participation and organization of events, presence in social networks, relations with the media, subscription to magazines and gazettes of regulatory agencies in the territory, participation or implementation of compliance observatories, as well as the application of questionnaires, may be some of the communication channels to be used by the entity.

### Step 3. Compliance risk assessment

Risk assessment includes the activities of risk identification, analysis and evaluation, which are described below.

First, the compliance risks arising from the organization's obligations are identified by assessing the negative effects of non-compliance with regulations. Although the regulations often detail the penalties that non-compliance entails, it is necessary to make an assessment that goes beyond this, considering the effects that could also occur in terms of a drop in sales, a drop in positions in the reputation indexes, a worsening of the brand image, loss of support from prescribers. As previously indicated for the obligations, the risks will also be associated with the processes.

The second activity corresponds to risk assessment. This can be studied through the possible consequences, the probability of occurrence and the difficulty of detection (Sanchez et al., 2021). The authors propose using an ordinal scale, as shown in Table N° 1.

**Table 1**  
Risk assessment scale

Value	Consequences ( $C_i$ )	Occurrence ( $O_i$ )	Detection ( $D_i$ )
5	Catastrophic	Almost Certain	Almost impossible
4	Major	Likely	Difficult
3	Moderate	Possible	Likely
2	Minor	Unlikely	Very likely
1	Insignificant	Rare	Certain

Own elaboration

Finally, the risk is evaluated by means of a risk criticality index as shown in equation 1:

$$Ic_i = O_i * C_i * D_i$$

Where:

$O_i$ : Probability of compliance risk occurrence (i).

$C_i$ : Consequences on compliance risk obligations (i).

$D_i$ : Compliance risk detection capability (i).

Finally, compliance risks can be evaluated taking into account the ordinal scale proposed in Table N° 2.

The authors establish the classification of trivial risks, based on previous research, consultation with experts, and analysis of the results of previous applications of the procedure.

**Table 2**

Risk assessment scale according to their criticality index

Range of $Ic_i$	Evaluation of $Ic_i$
$64 \leq Ic_i \leq 125$	Extreme
$30 \leq Ic_i < 64$	Critical
$20 \leq Ic_i < 30$	Moderate
$12 \leq Ic_i < 20$	Marginal
$1 \leq Ic_i < 12$	Trivial

Adapted from Joshi y Singh (2017) y Laszcz-Davis (2019).

In the case of compliance risks assessed as trivial, taking as a reference a limit of  $Ic_i < 12$ , no intervention by management is necessary, unless the improvement can be introduced in a simple manner and would favor the improvement of quality aspects of the process (Hernández-Oro, 2015).

Risks with evaluations above the limite ( $Ic_i < 12$ ) should be assigned control actions and behaviors associated with organizational values, until the criticality index is lower than the defined limit.

#### Step 4. Preparation of the CORVAL map

The aim of this stage is to integrate all the elements defined in the previous stages into a single tool, which will make it possible to link compliance risk mitigation actions with the behaviors associated with the defined organizational values. This technique, designed by the authors, is the main novelty of the procedure proposed in this article, and should be applied prior to the development of risk treatment programs.

The CORVAL map makes it possible to relate the context of the organization (C) to the organization's obligations (O), to these commitments its risks (R) and to the possible shared values that can mitigate or reduce them (VAL). Fig. N° 3 shows the scheme for the design of this type of instrument.



**Figure 3**  
Scheme designed for the elaboration of the CORVAL map  
Own elaboration.

### Step 5. Implementation of plans for the treatment of compliance risks

Risks with evaluations above the limit should be assigned control actions and intentional behaviors associated with organizational values, until the criticality index ( $Ic_i$ ) is lower than the defined limit.

The top management of the organization must promote at all levels of the organization, decision making based on organizational values, intentional behaviors, defined in the operationalization of the value, which allow at the same time to mitigate compliance risks.

Based on the CORVAL map, the authors propose the elaboration of action programs for the treatment of risks from the identified organizational values, which allows to integrate in a single program, the proposed actions and behaviors, together with other elements of this type of plans, such as: the necessary resources, the deadlines foreseen for the realization of the actions and the people responsible for both the approval and their implementation.

### Step 6. Control and continuous improvement

As plans for the treatment of compliance risks are implemented, for each process the new values of occurrence, consequences and detection of risks should be reevaluated.

The authors propose to calculate the residual criticality index of the compliance risk ( $Icr_i$ ), substituting in the second equation, the residual values of the probability of occurrence, the consequences and the possibility of detection of the risks. This allows evaluating the impact of the actions and behaviors proposed to mitigate them. The improvement actions are then plotted according to the results of the residual criticality indexes of the compliance risks. The continuous improvement process must take into account changes in the context and, therefore, in the organization's obligations.

### Application of the procedure in a case study in Cuba

This section shows the main results of the application of the procedure for compliance risk management with a focus on organizational values, taking as a case study an Information and Communication Technologies organization in Cuba.

In the determination of the context, the processes of the organization are identified, being a key process: Production of Informatics Services. The authors of the research select this process to show in this research the main results of the application of the procedure.

Next, the organization's compliance obligations and organizational values are identified. In the specific case of the organization under study, it has identified the organizational values, their conceptualization and their modes of action, which are used by the work team for this research (see Table N° 3).

**Table 3**  
Organizational values and their conceptualization

Organizational values	Brief conceptualization
Creativity	We possess original, innovative, objective and scientific thinking that manifests itself in the generation of new ideas and concepts aimed at solving problems.
Responsibility	We satisfactorily fulfill our duties and commitments to ourselves, family, work, society and the environment.
Honesty	We act with transparency and express ourselves with critical judgment, being able to recognize mistakes in order to contribute to social, collective and personal well-being. Achieve correspondence between thought, speech and action, not allowing immoral or indecent positions in our environments, or positions that attempt to overshadow the achievements of the organization.
Humanism	We place the human being at the center of all processes, we defend ethical positions with their sense of social justice, respect for rights, democracy and solidarity.

Own elaboration

The obligations resulting from the analysis of the context and compliance risks identified in the IT Services Production process are shown in Table N° 4.

**Table 4**  
Obligations and compliance risks of the IT Services Production process

Obligations	Compliance risks	Code
Produce IT applications and services	Delays in the execution of contracted projects	R301
	Non-compliance with consumer rights	R302
	Ignorance of the code of conduct by employees	R303
	Unlawful contractual relationships	R304
Guarantee working conditions for employees	Impact on the organization's prestige	R305
	Occupational accidents or diseases	R306
Protecting information related to products and services	Loss of source code of products and services	R307
	Improper access to work premises	R308
	Use of networks and technological resources to generate individual revenues	R309
Saving energy, financial and material resources	High rates of electricity consumption	R310
	Violations in the life cycle of technological equipment.	R311

Own elaboration

The risks are then evaluated. Fig. N° 4 shows a preliminary analysis according to the expert evaluation of the consequences and probability of occurrence of the risks identified in the process.

This technique makes it possible to classify seven of the risks identified as extreme, with non-compliance with consumer rights being the risk with the highest weighting.

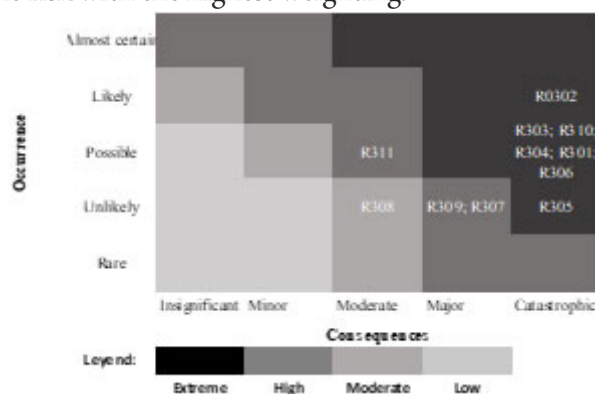


Figure 4

Consequence and occurrence matrix in the IT Services Production process  
Own Elaboration

The values issued by the experts on the occurrence, consequences and detectability of the risks, allow prioritizing and evaluating the identified risks through the criticality index. Eight of the risks identified are classified as critical for the process, one as moderate and two as marginal. Of all of them, the most relevant compliance risks are: illicit contractual relations and lack of knowledge of the code of conduct by employees (Table N° 5).

Both the consequence and probability matrix and the  $Ic_i$  indicate that all 11 risks should be addressed.

Table 5

Regulatory compliance risks of the IT Services Production process

Code	Compliance risk	O	C	D	$Ic_i$	Ranking
R304	Unlawful contractual relationships	3	5	4	60	Critical
R303	Ignorance of the code of conduct on the part of employees	3	5	4	60	Critical
R310	High rates of electricity consumption	3	5	3	45	Critical
R302	Non-compliance with consumer rights	4	5	2	40	Critical
R305	Impact on the organization's prestige	2	5	4	40	Critical
R309	Use of networks and technological resources to generate individual income.	2	4	4	32	Critical
R301	Delays in the execution of contracted projects	3	5	2	30	Critical
R306	Accidents or occupational diseases	3	5	2	30	Critical
R307	Loss of the source code of products and services	2	4	3	24	Moderate
R308	Improper access to work premises	2	3	3	18	Marginal
R311	Violations in the life cycle of technological equipment	3	3	2	18	Marginal

Own elaboration

Previously to the elaboration of the actions for the treatment of risks, the CORVAL map is drawn up, taking into account the context analyzed, the obligations and risks identified, and the shared values of the organization under study (see Fig. N° 5).

From the external point of view, it is possible to observe a variety in the rules and resolutions that govern the IT Services Production process. On the other hand, of the five organizational values that affect or can mitigate risks, in this process specifically, the Responsibility value has greater relevance, due to its influence on all the defined risks of the process. This means that if workers comply with their individual and social obligations, being consistent with their actions, it contributes significantly to mitigate the risks of the process.

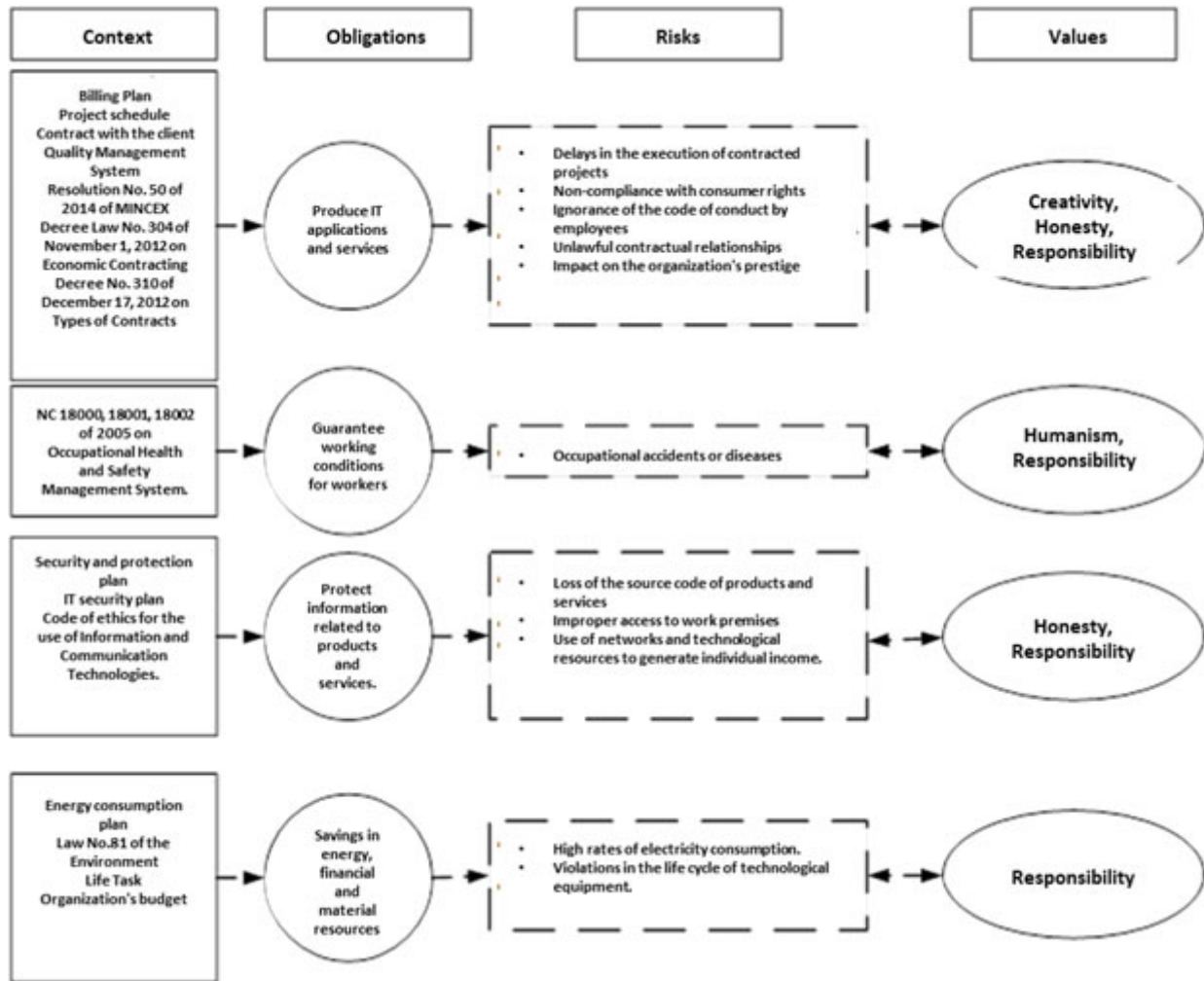


Figure 5  
CORVAL map for the IT Services Production Process  
Own Elaboration

Taking into account the map that relates the context, obligations, risks and organizational values, a program is defined for the process, which includes, among other aspects, an action plan to treat and mitigate the risks previously evaluated. Table N° 6 shows a sample of the compliance risks and the control actions for their treatment belonging to one of the programs associated with the shared value Responsibility in the process under study.

During implementation, the plans for the treatment of compliance risks are monitored and controlled. To assess the impact of the actions and behaviors proposed to mitigate the risks, the compliance risk residual criticality index ( $Icr_i$ ) is calculated. Fig. N° 6 shows the variation of the criticality index of the regulatory compliance risk in the IT Services Production process.

The analysis of this index shows a decrease in the criticality levels of the 11 compliance risks addressed. However, seven risks must continue to be addressed by the organization's senior management, including:

illicit contractual relations, lack of knowledge of the code of conduct by employees, and damage to the organization's prestige.

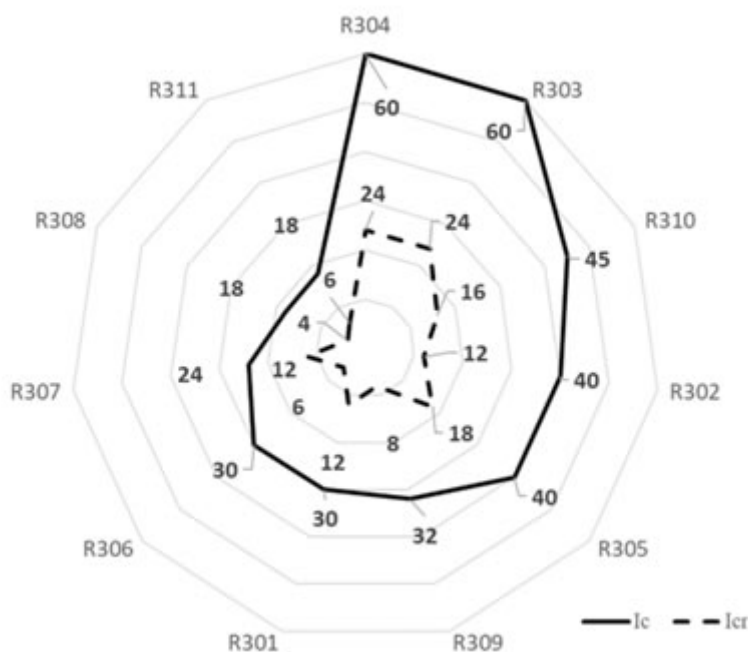
**Table 6**

Regulatory compliance risks associated with the value Responsibility of the IT Services Production process

Risks	Actions
R0304	<p>Verification of the legal documentation of clients and suppliers of the organization.</p> <p>The legal management of the organization provides legal opinions on all contracts.</p> <p>Creation and regular operation of a Contracting Committee in the organization.</p>
R0303	<p>Dissemination and communication through different channels (intranet, newsletters, infographics) of the organization's Code of Conduct.</p> <p>Promote the participation of all employees in the formulation, implementation and improvement of the organization's Code of Conduct.</p> <p>Verify compliance with energy saving measures for electricity consumption.</p>
R0310	<p>Promote a culture of energy saving in production.</p> <p>Promote sustainable information technology and systems practices in IT projects.</p> <p>Develop with discipline, efficiency and quality the tasks that correspond to him/her from the deep and conscious knowledge of his/her functions, duties and rights depending on the context in question.</p>
Modes of action	<p>To be demanding and rigorous in the fulfillment of laws, norms and rights.</p> <p>Contribute to change, objectively and with respect for the development of our society.</p> <p>Conscious participation in decision making in terms of the sustainability of the organization.</p>

Own Elaboration

The process improvement action plan should not only include these seven risks with criticality index greater than or equal to the minimum value proposed in the procedure, but also incorporate in the analysis new risks determined from the analysis of the context and the new obligations identified. This action plan, as well as the implementation of the procedure in other processes and organizations are results that will be shown by the authors in future research.



**Figure 6**  
Variation of the criticality index of compliance risk  
Own Elaboration

## CONCLUSIONS

Instrumental or shared values are part of the strategic projects of organizations, are defined and put into practice through the behavior, first and foremost, of the entity's top management, and should guide decision-making processes at all levels. Risks can be considered threats or opportunities for the fulfillment of the company's objectives or obligations, so that a certain behavior or mode of action can influence not only the fulfillment of an objective, but also the mitigation or not of the risk detected.

Compliance risk management with a focus on values proposes to mitigate risks, not only through control actions, as is currently done, but also by incorporating shared values, taking into account the modes of action of workers in the processes, and this is the main contribution of the research presented here. The authors propose a tool called CORVAL map - designed ad hoc for this research - which allows to integrate the obligations to the context of the organization and then to associate them with risks and shared values.

The results of the implementation of the procedure in the process of Production of Computer Services in an Information and Communication Technologies entity allow to identify as main risks: illicit contractual relations, lack of knowledge of the code of conduct by the workers, affectations to the prestige of the organization and high rates of electric energy consumption. On the other hand, the shared value Responsibility and its associated behavior is identified as the most influential principle in the mitigation of compliance risks of the process. To the extent that workers comply with their individual and social obligations in a timely and efficient manner, they will contribute to mitigate the risks identified in the process.

Future work could be aimed at implementing the procedure in other entities of the technology and communications sector, as well as entities of other strategic sectors of the country, allowing the generalization of the methods proposed in this research. On the other hand, it would be convenient to introduce the value approach in the management of other types of risks, such as strategic and operational risks, and then compare the results with the present research.

## REFERENCES

Please refer to articles in Spanish Bibliography.

## BIBLIOGRAPHICAL ABSTRACT

Please refer to articles Spanish Biographical abstract.