Article **Journal-Urban-Rural and Regional Economy**
June, 2021 Vol.5 No.8 1-6

Control Self-Assessment (CSA) as a technology risk management tool

Control Self-Assessment (CSA) como herramienta de gestión de riesgo tecnológico

LÓPEZ, Alma†

Universidad Iberoamericana, Prolongación Paseo de la Reforma 880, Alvaro Obregon, Lomas De Santa Fe, 01219, Mexico City, Mexico

ID 1st Author: *López, Alma*

DOI: 10.35429/JURRE.2021.8.5.1.6 Received March 11, 2021; Accepted June 30, 2021

Abstract

The aim of this paper is to describe how the methodology of risk assessment Self-Control (CFS for short) can assist organizations as a tool for risk management, both for business processes such as for specific processes, as if they are information.For Technologies above we can conclude that the risk assessment Self-control is a methodology that can support organizations in improving risk management, implementation of controls and continuous improvement, creating value and supporting the achievement of business objectives.

Resumen

El objetivo de este trabajo es describir cómo la metodología de evaluación de riesgos de autocontrol (CFS para abreviar) puede ayudar a las organizaciones como una herramienta para la gestión de riesgos, tanto para los procesos de negocio como para los procesos específicos, como si se trata de información.Para las tecnologías anteriores podemos concluir que la evaluación de riesgos de autocontrol es una metodología que puede apoyar a las organizaciones en la mejora de la gestión de riesgos, la implementación de controles y la mejora continua, la creación de valor y el apoyo a la consecución de los objetivos de negocio.

Citation: LÓPEZ, Alma. Control Self-Assessment (CSA) as a technology risk management tool. Journal-Urban-Rural and Regional Economy. 2021. 5-8: 1-6

† Researcher contributing as first author.

Introduction

Control self-assessment (CSA) (Tovar, 2014) is a process through which the effectiveness of internal control is examined and evaluated with the objective of providing reasonable assurance that all business objectives will be achieved. Such methodology can be used by senior executives, auditors and even stakeholders to assess the reasonableness of risk management processes and controls in an organization.

Organizations that use self-assessment (CSA) will have a formal and documented process that will allow senior management and different work teams, and even stakeholders to participate internally in a structured way in order to:

- Identify risk factors and relevant exposures.
- Evaluate the control processes that mitigate or manage those risks.
- Develop action plans to reduce risks to manageable levels.
- Determine the probability that the business objectives will be achieved. (Tovar, 2014)

Self-assessment (CSA) promotes the evaluation of risks and controls by the staff operating the business processes, which is a significant departure from traditional methods of risk and control assessment, as it is based on the belief that the staff performing the day-to-day activities have intimate knowledge of the process, including the strengths and weaknesses in the risk and control environment. This experience provides unique insight into the implementation of controls, their intrinsic usefulness and necessary adherence. However, few companies in Mexico today have implemented control self-assessment, as it requires a certain maturity in Internal Control, which must permeate throughout the organization through the proper management of the control environment.

Technological risk in organizations

The growing dependence on information and systems has become a critical element for the success and survival of organizations, and poor IT risk management can lead to fraud, information leakage, monetary losses, third party losses, etc.

It risks are intrinsically associated with the absence of opportunities to use technology to improve the efficiency or effectiveness of business processes or as an enabler for new organizational initiatives, that is, the risks of service delivery and IT operations are associated with all aspects of IT performance and system services, which can lead to the destruction or reduction of value for the organization. That is why it is necessary as a first step to establish a statement in every company that IT risks will always exist even if the organization does not detect or recognize them. (ISACA, 2009).

Internal control and technology risk management

In such a globalized world, it is necessary to have control figures that support and provide top management with reasonable assurance for the achievement of objectives. That is why internal control is defined as a process carried out by the organization's Board of Directors designed to provide reasonable assurance in the achievement of objectives, focusing mainly on the following controls:

- Operational controls - Related to the effectiveness and efficiency in the use of the entity's resources.
- Financial reporting controls - Related to the preparation of reliable financial statements.
- Compliance controls - Related to the entity's compliance with applicable laws and regulations (Commission, 2004).

However, each and every one of the aforementioned controls involves Information Technology (IT) as the fundamental basis of the entire operation. Therefore, it is essential to determine which are the responsibilities in terms of control within an organization, in order to know who should take care of IT risk-control issues. Based on best practices in internal control, senior management is responsible for the supervision, establishment, administration and evaluation of risk and control management processes (Moeller, 2013). (Moeller, 2013).

Operational management is responsible for including risk assessment and controls in their business units, since IT risks also belong to the business and are associated with the use, ownership, operation, participation, influence and adoption of IT in organizations.

ISSN-On Line: 2524-2083

Since they are composed of events related to technologies, which could potentially affect the organization and the achievement of its strategic goals and objectives. (ISACA, 2009) That is why international regulations such as the Sarbanes Oxley Act (Commission, 2004), and even national regulations such as the Single Circular of the National Banking and Securities Commission, have determined technological risk and the implementation of controls to mitigate it as one of the critical points of any organization. And it is at this point where the reviewing entities (audit and/or comptroller) provide different degrees of assurance of effectiveness in terms of risk management and control processes within the organization. Likewise, it is where the application of the CSA supports the three areas of the technological risk framework, since through the self-assessment of IT processes critical and useful information can be obtained for IT governance, as well as for the identification, assessment, response and management of risk (RISK IT). (ISACA, 2014).

Fundamental aspects for the implementation of Control Self-Assessment (CSA)

The implementation of the self-assessment methodology can be carried out using the following techniques:

- Workshops - where staff and management discuss the control structure, these can be control model workshops or interactive workshops.

- Surveys - where information is obtained from operating personnel regarding certain control topics that have been previously identified.

Also, in accordance with the recommendations of the Risk Management and Security Awareness Program, it is necessary to declare a policy on risk management and a security awareness program that stems from the policies, standards, guidelines and procedures for:

- Securing information assets.
- Awareness of individual duties and responsibilities in the application of their functions.

This will allow us to develop an organizational culture that promotes risk management and effective communication of those risks with stakeholders, all through a clearly documented process and continuous review by senior management. To ensure the success of the implementation of the self-assessment (CSA) the directors, stakeholders, managers and staff at all levels must be aware of and adhere to the concepts of risk and control, for this it is essential that the organization ensures the following:

- That staff understand their role and responsibility related to the organization's mission.
- Knowledge of the organization's policies, procedures and practices.
- Possess adequate knowledge of managerial, operational and technical controls.

The human factor (non-technological or procedural control factor) is key to providing an adequate and appropriate level of risk-control assessment, they are a key factor, but at the same time the weakest link, so a robust awareness program is required.

Frameworks and best practices that can help us in their implementation

The implementation of best practices for IT risk management provide tangible benefits to the business, some of these are:

- Fewer unexpected events and failures.
- Increase in the quality of information.
- Increased stakeholder confidence.
- Reduced regulatory concerns.
- New business initiatives supported by innovative applications.

Some of these best practices can be found in reference frameworks and international standards such as COSO, COBIT, RISK IT, ISO 31000, in the financial sector in the framework of Basel II, among others: COSO, COBIT, RISK IT, ISO 31000, in the financial sector in the Basel II framework, among others. Although the control components are the same in these frameworks and standards, for self-assessment (CSA) and for traditional techniques, the primary difference lies in the methodology implemented to identify, review.

Evaluate and validate the controls, since in traditional techniques it is the auditor or external consultant who issues an opinion on the control framework and performs the analysis and evaluation of risks and controls based on transactions.

However, in the self-assessment process (CSA) all these activities are conducted by business unit personnel and the management in charge of each of them, based on processes, focused on the customer, oriented to risk identification, control effectiveness and process improvement (Graves, Longenecker, Marsh, & Milstead, 2003).

Cost of the implementation of the CSA. The cost of implementing Self-Control can be as low or as high as the organization decides, since it can be executed by means of simple paper surveys, up to the development of computer systems that support the application of such surveys, analysis of results, issuance of reports and notifications to senior management or process owners. In addition to this, awareness and training costs for the personnel that will direct and carry out the practice or process must be considered.

Benefits of the CSA.

In its purest form the Control Self-Assessment (CSA) provides the following benefits:

– Facilitates the gathering and communication of information that leads to improved risk and control management.

– It generates value as it motivates cooperation between the different business units and increases their involvement in the design and maintenance of the risk and control management system, thus promoting a more open and shared culture within the organization.

– Business unit personnel acquire training and experience in risk assessment and risk management through the implementation of controls, improving the opportunity to achieve the organization's objectives.

– Staff are motivated by owning the risk and control management process in their business areas, which means that the corrective actions implemented by these teams are often more effective and timely.

– The entire organization's risk-controls-objectives infrastructure is subject to greater oversight and continuous improvement.

– The organizations' review bodies (audit and/or comptroller) improve their efficiency in obtaining vital and valuable information from the business units' work teams, which allows them to further investigate and perform tests to identify significant control weaknesses and high residual risks.

Premises for the implementation of the CFS

One of the main premises is that if the personnel involved are not sufficiently aware of the importance of this type of practice and do not answer the surveys honestly or do not have the skills to identify risks, this can lead to a lack of certainty in the data provided by the participants. Another important premise is that if top management does not sponsor, encourage and permeate the culture of self-assessment in the organization, it is very difficult, if not impossible, to implement. In other words, a great commitment is required from top management, as well as from the personnel who will be involved in the control self-assessment process.

Implementation Case. In Mexico, one of the most important mortgage institutions in the country decided to implement the CSA control self-assessment practice to improve its risk-control management. The implementation method contemplated the design of the CSA control self-assessment process based on the COSO methodology for business processes and COBIT for IT processes, in which the control objectives to be achieved are defined and 8 control assessment objectives are established based on the reference framework and 5 maturity levels for each one of them.

ISSN-On Line: 2524-2083

Figure 1 Control evaluation objectives established in dimensions and 5 maturity levels based on COSO - ERM
Shore: Infonavit

For this purpose, a computer system was designed to support the automation of the questionnaire application, the issuance of results reports and to facilitate the analysis of results. Workshops were also held with business owners, process owners and key personnel who operate these processes, so that they could obtain a broad representation of the perspectives that support or hinder the achievement of institutional objectives. During this phase, the Internal Comptroller's Office staff was in charge of designing and delivering the workshops, as well as managing and administering the control self-assessment process.

In this practice, the participants (both process owners and operators) evaluate the strengths and weaknesses of their processes (risks and controls) and comment on the impact that certain critical activities of the operation have on the achievement of institutional objectives, from a global approach to a very particular one, depending on their involvement and responsibility in the institution.

These evaluations are applied periodically using the same criteria in each exercise to facilitate accumulation and comparisons throughout the organization. Once the evaluations are carried out, a report of results is issued, in which each management receives the evaluation report, which is the basis for the exchange of ideas between management, operating personnel and the internal comptroller's office, including matters of interest for the definition of improvement actions to support institutional risk management.

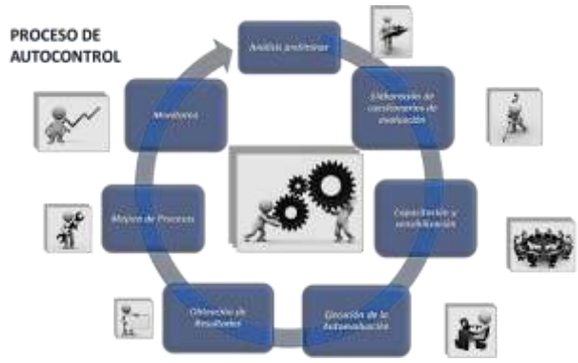

Figure 2 Self-evaluation process
Shore: Infonavit

These reports compare the evaluation of the controls of each component against the maturity level of the entire institution and determine the level of confidence of the results through the validation of evidence that supported the answers of the participants, obtaining valuable information regarding potential controls, due to the specialization of each process.

Figure 3 Comparison of results by business area and processes against institutional results corporate results
Shore: Infonavit

Throughout the 3 years that the control self-assessment has been implemented, the maturity level has been raised, since in its first exercise in 2011 it obtained a maturity level of 3.71, which placed it as a CAPABLE organization in which risk management presented moderate opportunities for improvement, which placed it as a CAPABLE organization in which risk management presented moderate opportunities for improvement and over time through the implementation of improvements derived from the results and feedback from the Self-Assessments it has reached in 2015 a MATURE level with a score of 4. 05.

In which the opportunities for improvement are minimal in the management of risk-control within its processes, generating value in terms of technological risk management and its business processes, since today there are standardized activities in the business processes, with documented risks and controls and operations supported by Institutional Information Systems; reflecting that both the processes and their results are quantitatively understood and controlled.

Conclusions

The implementation of a control self-assessment system requires a certain degree of maturity on the part of the company, since lack of senior management sponsorship usually means failure in the implementation of the CSA. Such implementation facilitates the identification and management of risks in a timely and accurate manner since it is the staff who have a more finely tuned sense, who are intimately related to the operation and who know in detail what the root-causes of these risks might be, who participate in the self-assessment exercise.

The best practices or frameworks generate great value in the implementation of control self-assessment, as they can strengthen the implementation of this to the business areas that require from service delivery (ITIL), risk-control management (COBIT, ISO 31000 & RISK IT), to implications concerning the field of information security (ISO 27000). With a good sponsorship and implementation of the risk-control self-assessment (CSA), top management will have a better understanding of the risks and controls that impact the business and the financial statements; IT staff will have ownership of the control structure because they are involved in the design and evaluation of it. This will generate value in the management of the organization's business and technology risks.

References

Commission, C.-T. C. o. S. O. o. t. T. (2004). Enterprise Risk Management. 2.

Graves, S. M., Longenecker, B., Marsh, T. L., & Milstead, H. (2003). Evaluating Internal Controls. Government Finance Review, 19(3), 40.

ISACA. (2009). The Risk IT Framework.

ISACA. (2014). Relating the COSO Internal Control—Integrated Framework and COBIT.

Moeller, R. R. (2013). Executive's Guide to COSO Internal Controls Understanding and Implementing the New Framework. John Wiley & Sons, Incorporated.

Tovar, F. (2014). Seminario CCSA (Certificación en Autoevaluación del Control). Instituto Mexicano de Auditores Internos A.C.