Journal of Modern Accounting and Auditing, October 2015, Vol. 11, No. 10, 487-498
doi: 10.17265/1548-6583/2015.10.001

The Updated COSO Report 2013

Roberta Provasi
Milan-Bicocca University, Milan, Italy
Patrizia Riva
Piemonte Orientale University, Novara, Italy

This paper aims to investigate the issue relating to the internal control system of listed companies, according to the publication of the new framework COSO (Committee of Sponsoring Organization of Treadway Commission) updated in 2013. Since December 15, 2014 came into force the new framework on the procedures to implement and to make use of an efficient system of internal control for listed companies. With the introduction of the new framework, the original framework of 1992 will be considered as the preceding version. The recent 2013 updated framework is considered as an "evolution rather than a revolution". This study will explore the latest changes brought to the 1992 COSO framework and the opportunity arising with the transition to COSO 2013.

Keywords: COSO report, internal control system, corporate governance

Introduction

The internal control system is the instrument through which the management aims to acquire reasonable certainty of the existence of appropriate measures to protect company property and the related accounting records (Messier, 2000). The internal control system should therefore help the company towards its goals and to pursue its mission, minimizing the risks associated with the rapidly changing economic, political, and social context, and to minimize the risks connected to the possible unreliability of the enterprise operating systems that are responsible for the daily strategies and management implementation.

The internal control, according to 1992 COSO (Committee of Sponsoring Organization of Treadway Commission) framework, could be defined as:

> A process effected by an entity's board of directors, management, and other personnel, designed to provide a reasonable assurance regarding the achievement of objectives relating to: (1) operation efficiencies and effectiveness; (2) reliability of the reporting system; (3) compliance with laws and current regulations. (COSO, 1992)

From this definition, it is possible to identify some considerations.

Internal control is a process, which does not depend on occasional events, but it must be systematically set. Control therefore needs to be integrated with all other business processes without overlapping them. This not only improves efficiency, but also reduces significantly the cost and facilitates the control extension to all the new procedures that may take action from time to time. The internal control is achieved not only by procedures and technological support but especially by people.

Roberta Provasi, assistant professor, Department of Business Administration, Finance, Management, and Law, Milan-Bicocca University. Email: roberta.provasi@unimib.it.
Patrizia Riva, assistant professor, Department of Economics and Business Studies, Piemonte Orientale University.

People operate the control and also can make mistakes and incorrect evaluation. At this point, it remains a margin of uncertainty, which in the economic area is a very important element. The uncertainty has already been described by the economist Frank Knight (1921) in his work *Risk, Uncertainty and Profit*, as a separate element from the risk since not measurable. The risk besides being "susceptible to measure" can be limited and contained within certain thresholds that can identify the seriousness.

It should be noted that the concepts of uncertainty and risk are important because they impact on the internal control system. The definition of the internal control system given by COSO is similar to that proposed in the Code of Conduct for the Italian Listed Companies that in Paragraph 7.P.1 states: "The internal control system is the set of processes designed to monitor the efficiency of business operations, the reliability of financial reporting, the compliance with laws and regulations and the protection of the corporate assets" (Comitato per la Corporate Governace, 2014, p. 29). An internal control system can be considered effective if:

(1) It is able to ensure the goals achievement as: strategic effectiveness and operational efficiency defined by top management, information transparency outlined by company policies, the management fairness, and the compliance of laws, rules, and regulations;

(2) It contributes to the protection of the favorable conditions to the value generation, paying attention to the identification and assessment of key risks.

The Evolution of the Framework Supporting the Internal Control System

The internal control activities do not arise in a specific historical context. For a long time, the directors of the single companies have realized the need to introduce a system to monitor the entire corporate structure (D'Onza, 2013). The administration control system and the management system already had a continuous implementation in order to codify the rules supporting the systems; the first by setting hierarchical roles within the company, the second, with the introduction of double entry bookkeeping as a basic rule to record the financial statement items.

Over the years, the need to introduce the codes of conduct and define the rules adopted by companies in order to harmonize their control system springs out. In recent years, the "proper operation" of a control system is not only an internal requirement, but also a guarantee for all those who are interested in the proper business management and in particular for those who do not have administration and organization tools. The internal control system has roots in the last century and developed mainly in the US. Until the 40s, the internal control system has been considered as an important element in the context of the internal auditing. As different companies became more complex, attention to the internal control system has assumed more and more importance.

In the mid-50s, the concept of internal control was much extensive and needed to be defined in a more restricted context. The aim was the approval of the internal clear rules for the big companies, in such a way that companies did not refer to their own self-regulatory codes but also to an "internal control" shared approach. The Statement on Auditing Procedures No. 29, published by the American Institute of Certified Public Accountants (AICPA, 1958), distinguished the concept of administrative controls from the one of accounting controls. The first are framed to support operational efficiency, while the latter concern the corporate assets safeguard and therefore the transparent and correct transcription of financial documents.

In the Statement on Auditing Procedures No. 54 of 1972 (AICPA, 1972), the distinction between the conception of the administrative control and accounting control was better defined. The first kind of control is defined as a support related to decision-making processes, while the accounting control concerns the safeguard of the corporate assets and the reliability of financial records. A first important step towards the recognition of

the internal control importance occurred in the late 70s. The Watergate scandal (1973-1976) emerges the problem of corruption among American companies that operated abroad, and particularly in the third world countries. The discussions and studies that followed led the US government to the belief that the only tool able to contain the phenomenon was a good system of internal control. When in 1977, the Foreign Corrupt Practices Act (FCPA) imposed to listed companies the adoption of an "adequate" internal control system, a strong role of compliance guarantee was recognized to the tool. The notion of accounting control provided by the Statement on Auditing Procedures No. 54 was literally transposed, making the implementation of the system a compulsory requirement for listed companies. However, as until that moment, the internal control systems had been considered a matter for management, nor the practice nor the literature offered a univocal and generally agreed answer to incorporate the contents of the generic prescriptions provided by the FCPA 1977.

In the US, the first who faced the problem were directly the associations involved in financial information management (internal auditors, accountants, accounting academics, business leaders, and experts in industrial accounting). Around the mid-80s in fact, emerged the need to provide for the internal controls inefficiencies also considering bankruptcy procedures often associated with serious illegality components. For this reason, it was established the National Commission on Fraudulent Financial Reporting (known as Treadway Commission) to plan the study of the accounting fraud causes. The work of the Commission was published in 1987. It was named "Report on Fraudulent Financial Reporting" and focused mainly on internal controls as a tool to prevent accounting fraud. The Report on Fraudulent Financial Reporting (known as the Treadway Report), which proposed a solution for the adoption of a risk management policy, seeks to identify areas of the company exposed to a higher risk of fraud in order to mitigate the risks inherent to these areas.

The Treadway Report also stressed the importance of: (1) the control environment; (2) codes of conduct; (3) the competent auditing and operational committees; (4) a dynamic and unbiased internal audit; and (5) the need for reports on the effectiveness of management's internal control system. The organizations behind the Treadway Commission were the five major American professional associations: the American Accounting Association (AAA), the Financial Executives International (FEI), the Institute of Internal Auditors (IIA), the Institute of Management Accountants (IMA, former National Association of Accountants), and the AICPA. These associations then entrusted to a joint committee, the COSO, the definition of a control framework in order to define an innovative reference model useful to the company management as part of the internal control system. Following a long debate, which was attended by all the representatives of the associations involved in the project, the need to publish a single framework arose. In fact, in 1992, the Commission published the COSO Internal Control - Integrated Framework (COSO IC-IF), a four-volume framework on the internal control system that is still the benchmark. The COSO Report was conceived as an operational manual for management and has become in a few years one of the most popular models (Domenico & Salvatore, 2009). This text has also been the reference frame for the predisposition of codes, standards, and other documents on internal controls prepared in numerous countries, including Italy. In order to adapt the content to the Italian context, the work of COSO is resumed and expanded as part of the "Corporate Governance for Italy", promoted and coordinated between 1996 and 1997 by the Italian branch of Coopers & Lybrand. In the context of this initiative, which resulted in the book entitled *The Internal Control System (2001 Publication) - An Integrated Reference Model for Government Business*, was examined the issue of the roles, responsibilities, and processes of interrelation regarding the different parties involved in the internal controls (shareholders, boards of directors, stakeholders, regulators, external review, and the Italian Stock Exchange).

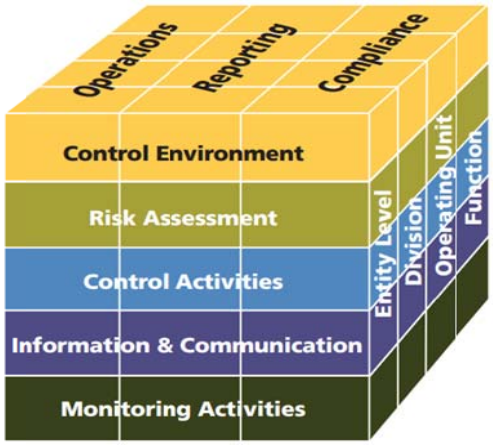

Figure 1. COSO report* (* COSO.org).

The five key elements that represent the control system components are (see Figure 1):

(1) Control environment: environmental controls;

(2) Risk assessment: risk assessment stage;

(3) Control activities: activities and controls that the company implements to achieve its goals;

(4) Information & communication: the exchange of information which must exist for the proper society functioning;

(5) Monitoring activities: the activity of testing whether the controls have been conducted in an operational and correct way.

These components are used to achieve the three classes of targets (the other cube side shown in Figure 1):

(1) Operations: business operations;

(2) Reporting: reliability of the financial reporting system;

(3) Compliance: compliance with applicable regulations.

The last cube side represents the organizational units of the companies' structure: the key elements that should achieve the three targets classes must exist regardless the ways the company is organized. The main goal of the COSO is to establish unique parameters and a common understanding around the three interconnected elements: internal control, enterprise risk management (ERM), and fraud in the financial sector. If for the first element we refer to COSO IC-IF, for the second we take into consideration the COSO ERM, published in 2004, which extends the model IC-IF with elements concerning the risks and business targets.

The 2013 Updated COSO Report

In November 2010, the COSO has announced that it had started a project for the release of a new framework that would represent the update of the 1992 one. The goal of the Committee was to increase the importance and the relief of its structure within an economic environment ever more complex than in the past, representing a valid support for organizations all over the world to conceive, implement, and monitor an internal control system. During the 20 years passed since the first framework was developed, corporate environments and operations radically changed, becoming much more complex, technological, and international. At the same time, stakeholders have become more committed and competent, seeking greater transparency and accountability for the integrity of the SCI. Even the reference standards have evolved rapidly reflecting this process and COSO has considered it necessary to update the reference framework. The

Committee considered that the release of an updated framework can bring several benefits for organizations, for example, provided that such a change can help companies that use it to adapt to the increasing complexity, to mitigate the risks to the goals achievement, and to provide reliable information to support managerial decisions. David L. Landsittel, former chairman of COSO, pointed out that the definition of internal control and its five elements presented in the framework of 1992 are "timeless" and therefore have not been modified and have to be presented in the next updated reports.

Among the goals of the new framework, whose philosophy is the constant promotion of a risk-based approach instead of a "check-the-box approach", there is a cost reduction pursued through the elimination of controls deemed ineffective, inefficient, or unnecessary as adding small value in reducing the failure risk in achieving business goals.

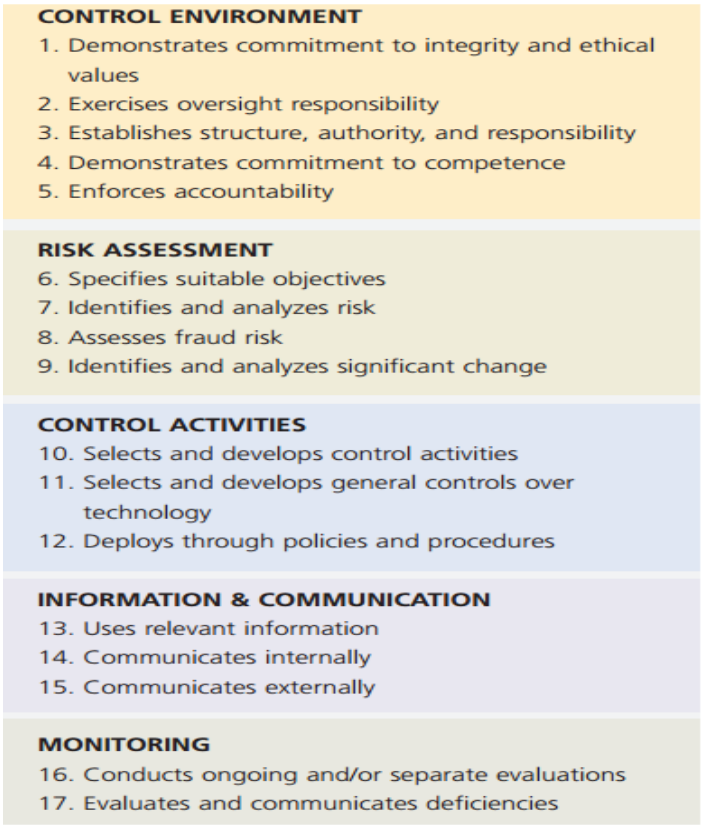

Figure 2. COSO report 2013* (* Coso.org).

On May 14, 2013, the Commission has finally released an updated version of the COSO IC-IF to be adopted by those who still used COSO 1992 by December 15, 2014. From this date, the previous framework has been considered outdated. The 2013 framework is the result of a significant multi-year project to review, update, and modernize the original one taking into consideration business models significant changes occurred in different businesses from 1992 such as the use of evolving technologies, which has become increasingly important to improve performance, processes, and decision. Finally, regulatory authorities and other stakeholders have higher expectations regarding the supervision of governance, risk management, and the prevention and detection of fraud. The updated framework (see Figure 2) develops principles and focus within each of the five key components of the internal control: risk assessment, environment control, information

flows within the company, control activities, and monitoring activities. In particular, according to the updated framework, these components must not be considered in an atomistic way, but as a system of variables, which contribute together as pillars for the overall internal control system.

Control Environment

The control environment represents the set of general controls that are the basis of the organization and that outline the procedures and policies reflecting the attitude of the economic entity. Through the provision on one hand of self-regulatory codes and on the other hand of internal codes and regulations regarding ethical values, management should try to convey the organization climate necessary for the pursuit of vast and complex business goals. This is achieved with the implementation of procedures that include high standards of ethical conduct. In general terms, an effective control environment is characterized by an organizational climate in which, competent people, aware of their responsibilities and their authority limits, show motivation and commitment to comply with the policies and organizational procedures for the pursuit of business goals. The framework of the component "control environment" can be described as follows.

Demonstrate commitment to respect ethical values and integrity. Codes of conduct are the starting point for evaluating adherence to ethical values and integrity both inside and outside. The COSO suggests, for example, informing employees about the codes of self-conduct from the time of their employment and during the training courses. The COSO also focuses on the importance of practices such as environmental sustainability and green economy which should be transparent and visible especially outside.

Exercise oversight (monitoring). For a proper operation of the organization, it is important to respect the hierarchy of roles. It is up to the board of directors the responsibility for overseeing the management and the various managers to implement similar systems for process control of the individual business units. To monitor and evaluate the implementation of correct procedures, qualified, experienced, and independent managers must be placed.

Establish structure, permissions, and responsibilities. Managers with more experience should establish the organizational structure of the company so as to contribute to the improvement of information flow inside.

Demonstrate commitment regarding competence. Each business unit or product line has to be associated with the relative risks, therefore, engage staff with the appropriate skills and qualities needed to cope with them.

Impose responsibilities. To empower employees, it is necessary to recognize their efforts and results achieved through the mechanism of incentives.

Risk Assessment

This component consists in risk assessment inherent to company goals achievement. Prerequisite to obtain a reliable and satisfactory corporate performance is to set goals both short and medium-long term. Each of these may involve risks which must be sufficiently clear, with regard to both their nature and the probability that they will occur.

It is a step prior to the actual control which provides the basis for further checks to be implemented in order to safeguard the company. Risks are future events and uncertainties that may affect the achievement of strategic, operational, and financial goals of an institution. In the past, attention was focused only on the negative side of risks. The best scenario was then considered the one without any adverse effect. Today, on the contrary, risks, as uncertain and unpredictable events, start being considered not just a threat but also a possible source of opportunity. The framework of the component "risk assessment" can be described as follows.

Specify relevant (suitable) targets. Prior to identify risks, it is necessary to clearly identify management goals. Goals can be associated with different risks depending on their nature.

Identify and analyze the risks. Once the targets have been identified, related risks must be considered and mechanisms by which they can be mitigated have to be identified. COSO ERM Framework (ERM 2004) had already extensively examined the principle. COSO IC-IF 2013 quoted ERM 2004.

Assess the risk of fraud. Fraud is an intentional act that leads to an error, in order to achieve an unfair or illegal advantage. An error, in fact, may be intentional or unintentional. When it is intentional, we deal with premeditated crimes and we need to say that the risk of fraud is high.

Identify and evaluate significant changes. The internal control system must be updated from time to time regarding the significant changes that may affect the economic performance of a company. In order to tackle this issue, the COSO has suggested a list of different circumstances that should be monitored with special attention.

Control Activities

Management implements controls to mitigate the major risks identified during the above described process of goals definition and risks evaluation. Control activities can be preventive or detective. Activities are carried out to prevent risks. Investigative activities, however, are carried out also after events have already occurred, trying to identify the causes, to reveal the impact, and to implement corrective measures for the future. The framework of the component "control activities" can be described as follows.

Select and develop control activities. Select means to match those elements that are identified in the previous phase of the risk assessment. Develop means to implement them in an appropriate way responding to the individual risk and processing it in order to detect the impact of all risks.

Select and develop general controls on the technologies used. The update of the COSO 2013 has pointed out the impact of new technologies for both implementation and control of the informative system. There is a remarkable relationship between technology level and the internal control system efficacy.

Implement controls through policies and procedures. Checks should reflect the corporate policies and should be corrected if not complying with them, in order to pursue business goals. Policies and the corporate philosophy, in fact, must be known by the entire organization as each employee is asked to be aware of his/her own tasks and responsibilities. The effectiveness of the policies must be then reviewed periodically by the management in relation to the decisions they intend to pursue.

Information & Communication

Effective internal control systems are characterized by the implementation of effective information tools. In this context, it is necessary to refer to both the information and communication. The framework of the component "information & communication" can be described as follows.

Use relevant information. In order to achieve the aim of disclosing relevant information internally or externally, it is necessary to process a series of data in order to reduce the considerable amount of knowledge available selecting material and useful information.

Spread the internal communication. Communicating internally allows to spread the company's values and to clear the important role played by each employee to reach the goals set from time to time.

Communicate externally. Companies must continuously and clearly communicate to stakeholders and third parties so that values as well as codes of conduct get to be well known. Having external confirmations, facilitating unbiased inputs, and developing mechanisms to get feedbacks from stakeholders help the firm to get trusted.

Monitoring

The system of internal control requires specific and constant monitoring over time. This is because that the companies' constant external and internal changes imply a periodic critical evaluation of all components of the framework. So monitoring, more than representing the fifth component, acts as a basic principle to control and, in the event, correct the pillars of the control system, namely, the four other components. The framework of the component "monitoring" can be described as follows.

Conduct ongoing or periodic assessment processes. These processes relate mainly to the effectiveness of the internal controls project and the effective operation of the same in order to ensure that they operate according to the goals formulated.

Assessing and reporting deficiencies. Assessments can also represent opportunities to improve the effectiveness of controls.

Criticality and New Relevant Update of COSO Report 2013

With the update of the framework in 2013, four frames of reference were released:

(1) IC-IF Executive Summary, which consists in a summary that recaps the most important aspects of COSO 2013. It is intended to provide advices to CEOs and other senior executives, managers, and regulators;

(2) Internal Control, Integrated Framework, and Annexes. It defines the framework in detail, gives the definition of internal control, and describes the internal control components and principles. In addition, it provides the direction for all management levels in the planning and implementation of internal control and assesses its effectiveness;

(3) Internal Control, Integrated Framework Illustrative Tools for Assessing Effectiveness of the System of Internal Control. This text contains illustrative tools to evaluate the effectiveness of an internal control system;

(4) External Internal Control Over Financial Reporting: A Compendium of Approaches and Examples. The compendium provides practical approaches and examples that illustrate how the components of the principles set out in the framework can be applied in drawing up balance sheets.

Adopting the framework of 2013 is not a mandatory process: there are no penalties for those who do not comply. The framework is a procedural support that provides precise rules to facilitate the mechanisms of the internal control system. Therefore, the company itself has the possibility to choose whether or not to comply, aware that:

(1) It is the result of a 20-years updating process;

(2) It was made by selected professionals at the international level;

(3) It provides guidelines very simple to follow depending on the business complexity;

(4) The implication of the 17 "key principles" has been developed in sets of more analytic documents.

To implement the COSO Report 2013, a few significant steps should be taken (McNally, 2013). The first step in the transition to COSO 2013 is to build awareness on the framework itself, that is, to know in order to be masters of the change made. The following concepts are declared to be relevant by the Committee itself:

(1) Timeless concepts. The 2013 framework continues to predict the three categories of targets-operations, and is still made up of the five integrated components such as the internal control environment, risk assessment, control activities, information & communication, and monitoring. It emphasizes, then, that some concepts in relation to internal control are timeless;

(2) Expanded reporting category. The category embraces now more explicitly and clearly, both financial reporting (financial statements and other files reporting) and the non-financial, and management objectives inside and outside;

(3) Codified principles. The framework of 1992 introduced the five components of internal control. As these are essential, present and functioning, these concepts have been explicitly articulated in 17 principles. The Committee believes that each principle adds value, is suitable for all entities, and thus is presumably relevant;

(4) Requirements for effective internal control. To conclude that a system of internal control is effective, all five components of internal control and all relevant principles must be present and functioning. Being "present" means that a given or a principle exists in the planning and implementation of the company's internal control system. "Functional" means that the component or the principle continues to exist in the configuration of the control system. The effectiveness of the internal control also requires that all five components work together in an integrated way;

(5) Internal control deficiencies. According to the 2013 framework, a major deficiency in controls greatly reduces the likelihood that an entity will achieve its goals. Although the 2013 COSO defines the term deficiency and severe deficiency, management should use relevant criteria as established by the regulators and other relevant third parties for defining the severity of evaluating and reporting the deficiencies of the internal control;

(6) Points of focus. COSO's updated framework describes the points of focus to help management in designing, implementing, and maintaining an internal control and in assessing whether the 17 principles are present and functioning. Points of focus represent important principles features. As analyzed, every principle has in it sub-principles that are focal considered relevant to understand its principles. Management is required to ensure that these components have been carried out because they help the enforcement of the principles; but their lack does not mean an ineffective control system.

Once developed awareness and expertise, it is necessary a second step to evaluate how its implementation can have an impact on compliance with rules and regulations in relation to the particular sector of society. To conduct a preliminary assessment of the impact, it is necessary to map the existing system of internal control against the updated COSO. This is important to determine the degree of work required to complete the transition.

Step three involves the organization as a whole to build awareness and to test the preliminary impact assessment conducted in step two. Depending on the nature and complexity of the organization, there may be multiple layers of assessment. For example, each business unit or any location may prepare its own local assessment in relation to their role. The impact of 2013 COSO framework on the whole system should also be discussed with the company's auditors.

When a comprehensive impact assessment has been completed, it is time to develop and execute the plan. As with any well-run project, the planning phase is usually the most important. During this phase, the governance project and decision rights must be defined, a detailed project plan with key milestones must be defined, and resources must be identified and allocated.

The transition plan will pass through three phases:

(1) Documentation and evaluation: During this phase, it may be necessary to update the format and/or the flow of the basic documentation, aligning it with the new mapping created during phase two. In particular, management must be able to conclude that its internal control system is effective and that all five components of internal control are present and functioning. This step also involves the evaluation of the planning control and improvement according to the needs;

(2) Valuation testing and gap remediation: It is necessary to perform tests to ensure that the controls have been implemented and are operating as expected. If deficiencies are identified as a result of this test, it is required that there are ways to mitigate them;

(3) External review and testing: At some point, it becomes crucial the role of the external auditor who shall evaluate the program, in accordance with the rules and regulations, analyzing the supporting documentation.

When the transition to the new framework is complete, it is important to adopt an attitude aimed at a continuous improvement as a result of different practices. It is first required to make sure that the "tone-at-the-top" is appropriate to communicate the clear commitment of the company to integrity and ethical values, the importance of maintaining effective the internal control and the expectation that all employees fulfill their duties. It is then necessary to embed the responsibility of a proper internal control in the company's culture in its business processes and procedures. One way to achieve this is to implement a control self-assessment program as part of the ongoing company evaluation within its monitoring activities component. Technology solutions need to be used to compare the details of transactions against thresholds, monitor models, and evaluate automated performance indicators. Control report and communication must be improved, considering the processes development, activities, or controls alerting users for potential anomalies or failures. And last, it is important to enhance ERM. Integrating the ERM process with the IC framework will improve the company's ability to achieve its strategic, operational, reporting, and compliance objectives.

Conclusions

The framework of 1992 had two main limitations:

(1) It was related only to financial reports and not to all kinds of reports;

(2) Monitoring of efficiency and effectiveness was described as an operative matter.

These limitations have been overcome both with the introduction of the 17 principles and with the publication of the COSO ERM in 2004 which better deepened the company risks in case of a control lack to achieve its goals. The updated COSO Report of 2013 aims both to overcome these limitations and to implement new approaches to achieve a better structuring of the internal control system. The updated framework reflects how the business environment has changed and provides guidance to assess risk and keep related current controls (see Table 1). In particular, additional three goals areas are very relevant:

(1) Operations: It includes the operational and financial performance goals and is no longer limited to "effective and efficient use of entity's resources";

(2) Reporting: It refers not only to financial but also non-financial reporting to various internal and external stakeholders. In the framework of 1992, the aimed purpose was much strict related to a reliable financial statement;

(3) Compliance: Considers increased demands in laws, regulations, and accounting standards.

Specific significant enhancements to the 1992 framework that may pose relevant challenges to management are the following:

(1) More detailed emphasis on risk assessment concepts, including those related to inherent risk, risk tolerance, how risks may be managed, and linkage between risk assessment and control activities;

(2) Increased role of technology, two of the new principles require careful consideration related using IT to assist in continuous monitoring and for ensuring quality of information (data integrity);

(3) New approach to minimize and identify fraud: Previously, fraud risk was typically considered an integrated part of control activities and embedded in the overall assessment of financial reporting risk. The 2013 framework suggests the need for a broader fraud risk assessment that can also address operational business objectives (Protiviti, 2014).

Table 1

Comparison of Principles in the 2013 Framework With the Related Sections in the 1992 Framework

Principle in 2013 framework	Related sector in 1992 framework		Summary of enhanced concepts in 2013 framework
	Chapter	Section	
1. The organization demonstrates a commitment to integrity and ethical values	Control environment	1. Integrity and ethical value; 2. Human resources policies and procedures	1. Integrity as a prerequisite to ethical behavior and an effective system of internal controls; 2. Need to consider impacts of control environment across the structure; 3. Importance of: (a) Tone at the top as a set by the board of directors and management; (b) Establishing standards of conduct for employees and outsourced service providers (OSPs); (c) Evaluating adherence to expected standards and addressing any deviations in a timely manner.
2. The board of directors demonstrates independence from management and oversight development and performance of internal control	Control environment	Board of directors or audit committee	1. Expanded discussion of governance concepts including the need to establish oversight responsibilities for the board and its committees; 2. Matters related to board independence, skills, and expertise; 3. Includes a detailed table illustrating board oversight responsibilities for each of the five components of internal control.
	Roles and responsibilities	Management board of directors	
3. Management establishes with board oversight structures reporting lines and appropriate authorities and responsibilities in the pursuit of objectives	Control environment	1. Management's philosophy and operating style 2. Organizational structure 3. Authority and responsibility assignment	Defining, assigning, and limiting authority and responsibility at different organizational levels and among the various reporting lines (e.g., considering product or services lines, legal entity structures, geographic markets and arrangements with OSPs)
	Roles and responsibilities	Management, board of directors, internal auditors, other entity staff	

Note. Source: Burns and Simer (2013).

The limitations concerning the 2013 framework were estimated by the board:

(1) Lack of suitability between the goals established and the internal control system;

(2) The human judgment in making decisions can be wrong and subject to bias;

(3) Possibility of events' collapse due to human mistakes;

(4) Management disregarding the internal controls;

(5) Management and other staff ability to bypass internal controls through collusion;

(6) External events beyond the organization control.

As can be seen, most of the limitations arise from the fact that the control system is monitored by human beings. This is a problem that can never be considered overcome as long as the decisions will be made by the companies and humans. Whether the error was made intentionally or not, there is a risk that the consequences can be disastrous.

These limitations can be only bypassed, as well as in trying to implement an effective system of control, posing a constant focus on people: management and their staff have to implement more thorough and aware controls. Implementing a policy of this kind could certainly minimize these limitations.

As far as 2013 COSO has dealt with the framework restriction, the real limitations can be recognized only when the new framework will be fully implemented by the companies.

The objective of this contribution was to highlight the main innovation introduced by COSO Report updated in 2013 for a later empirical investigation of the benefits from the new rules of operation for the internal control system.

References

American Institute of Certified Public Accountants [AICPA]. (1958). *Statement on Auditing Procedure No. 29: Scope of the independent auditor's review of internal control*. Committee on Auditing Procedure.

American Institute of Certified Public Accountants [AICPA]. (1972). *Statement on Auditing Procedure No. 54: The auditor's study and evolution of internal control*. Committee on Auditing Procedure.

Burns, J., & Simer, B. (2013). COSO enhances its internal control — Integrated framework. *Heads Up*, Volume 20, Issue 17. Deloitte.

Comitato per la Corporate Governace. (2014). *Codice Autodisciplina*. Borsa Italiana.

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (1992). *Internal control - Integrated framework.*

Committee of Sponsoring Organizations of the Treadway Commission [COSO]. (2013). *Internal control - Integrated framework.*

D'Onza, G. (2013). *Internal auditing. Profili organizzativi, dinamica di funzionamento e creazione del valore*. Torino: Giappicchelli Editore.

Domenico, M. G., & Salvatore, L. (2009). Lo scudo e la lancia nella guerra dei "subprimes": Ipertrofia e perforabilità del sistema dei controlli. *Analisi Giuridica dell'Economia, 1*, 89-104.

Knight, F. H. (1921). *Risk, uncertainty and profit*. Boston, MA: Hart, Schaggner & Marx; Houghton Mifflin Co..

McNally, J. S. (2013). *The 2013 COSO framework & SOX compliance: One approach to an effective transition*. Strategic Finance, COSO.

Messier, W. F. (2000). *Auditing*. Milano: McGraw-Hill.

Protiviti. (2014). *The updated COSO internal control framework: Frequently asked questions* (2nd ed.). Retrieved from http://www.protiviti.com/en-US/Pages/default.aspx