2. The Analytical Framework Integrated Internal Control and Enterprise Risk Management: An Overview

Fabio Accardi and *Roberto Rosato*

1. General Overview

As previously seen in Chapter 1, the more complex the risks the companies have to manage become, the more important the correct use of a framework is. In this sense, "[e]nterprise risk management enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value" (COSO, 2004: 1).

We can examine COSO (2004) as a framework into three principal dimensions:

- the objectives;
- the components;
- the entity's units.

In particular, as for the objective dimension, the framework identifies the following components, set forth in four categories (COSO, 2004: 3–4):

- **strategic**: These are general aims in line with the corporate mission. They are declined and contextualized according to the other three categories of objectives;
- **operational**: Effective and efficient use of resources;
- **reporting**: Both internal and external reliability of information;
- **compliance**: Compliance with laws and regulations.

The framework additionally comprises eight interrelated components, which "are derived from the way management runs an enterprise and are integrated with the management process" (COSO, 2004: 3). The components of the framework are described in the following paragraphs:

1 – Objective Setting

The definition of objectives is a prerequisite for an effective event identification, risk assessment and risk response. The strategic objectives are the foundation in order to define the operational objectives, reporting, and compliance. In choosing targets, companies must make sure to align themselves to acceptable risk, fixed by the companies themselves, that are determined according to the levels of risk tolerance

2 – Event Identification

Management must identify events that may affect the company. If they compromise the achievement of the objectives, they represent risks that require evaluation and determination of response measures. If they have a positive impact, they represent opportunities worth pursuing in redefining strategies. The events are influenced by internal and external factors, and their identification involves the application of structured techniques.

3 – Risk Assessment

Risk assessment measures the repercussions of a potential event on the achievement of objectives in terms of likelihood and impact, through qualitative and/or quantitative techniques. The evaluation regards the individual event categories of potential events interconnected with the various levels of the company. Risks can be assessed in terms of inherent risk (i.e., independent from the existing control system) and in terms of residual risk, which considers the effects on the probability and/or impact of the activated risk responses.

4 – Risk Response

Based on the risk assessment, management must select the most appropriate responses to the risk (e.g., avoiding the risk, re-

ducing it, sharing it, accepting it). The choice depends on several factors: cost/benefit analysis; desired effects on the probability/impact; capacity to reduce risk within the limits of tolerance. The risk mitigation strategy should allow bringing the overall level of residual risk within the limits of acceptability set by top management.

5 – Control Activities

Control activities are the application of policies and procedures to ensure the implementation of directives to address the risks that may affect the achievement of the objectives. Control activities are implemented at all levels of the organization, and may consist of approvals, authorizations, verifications, reconciliations, review of operational performance, protection of company assets, separation of duties.

6 – Information and Communication

The company should identify, collect, and disseminate relevant information to enable everyone to fulfill their responsibilities. They must take the form of implemented information systems that deal with both internal and external information for the risk management and decision making. Effective communication flow must be ensured through the entire organization: top-down (e.g., communication objectives); bottom-up (significant reports); transversal (i.e., management processes); third parties.

7 – Monitoring

Monitoring fulfils the function of assessing in real time the presence and operation of the components of the control and risk management system. It is carried out through continuous supervision, by the operating management, or through specific testing and evaluation systems. The monitoring scope and frequency depends on the risk assessment and effectiveness of continuous oversight.

8 – Internal Environment

Normally, this component is described as the first of the set. The reason is that it embodies the essential identity of an organization and determines the ways in which the risk is to be tackled.

Therefore, it can be considered as the very foundation of the other components of the Enterprise Risk Management. The internal environment is affected/influenced by factors such as the philosophy of risk management, the level of acceptable risk, the supervision of the Board, the integrity, ethical values, competence, the modalities of the delegation of powers and responsibilities, training staff. We have decided to place this component as the last one of the list because it can be considered as the most relevant in order to analyze the objectives of compliance and the translation of them in a Compliance Program. Focus on compliance will be introduced in the last section of the chapter.

The COSO (2004) was first published in 2004 and it represents an evolution with respect to the framework COSO (1992). Indeed, COSO's (1992) framework was structured in only five components:

1) Control environment;
2) Risk assessment;
3) Control Activities;
4) Information and Communication;
5) Monitoring.

Each of the components must exist and operate in an integrated way in the different levels of the organization so as to achieve the objectives (including compliance). The principal aspects in which we can summarize the transition from COSO (1992) to COSO (2004) are:

- COSO (2004) does not replace COSO (1992), which remains as a stand-alone internal control framework;
- COSO (2004) incorporates the IC framework, acknowledging that a strong system of internal control is essential to effective enterprise risk management;
- COSO (2004) expands and elaborates on elements of internal control as set out in COSO (1992) by:
  - bringing together risk culture and control culture;
  - strengthening the link between internal control, risks, and achievement of objectives through: i. pertinence and legiti-

macy of internal control considering its added value to an effective risk control; ii. relevance of the controls implemented to the previous identification and assessment of risks.

We must also point out that both frameworks are described as **Processes**. However, while COSO (1992) is particularly focused on Internal Control, the emphasis of COSO (2004) is on risks. Therefore, COSO (2004) could be described as a process set up by the Board of Directors, the Management, and other operators of the corporate structure used for the formulation of strategies across the organization, designed to identify potential events that may affect the company, **to manage the risk within the limits of acceptable risk, and to provide reasonable assurance regarding the achievement of corporate objectives.**

In order to better understand how the process works and analyze the relations between objectives and components, we can focus our attention on Table 2.1. This table introduces the third dimension of the framework, **the entity units**.

Table 2.1 Entity units of the COSO's (2004) framework of analysis.

	Small contractor	**Building contractor**	**Specialist Contractor**	**Main Contractor**
Approach to the employer (type of contract)	Sale of specialist work (working on behalf of)	Building a project (designed by an engineer or an employer)	Design and execution of building or engineering works	Provide a fully equipped facility ready for operation ('at the turn of the keys')
Pricing model	Redemption costs	Price for building	Price for design & building	Turnkey price
Production models	Decentralization of non-specific work	Decentralization of activities peaks (induced occasional)	Decentralization of routine (induced qualified)	Decentralization of specialist activities (star model)

	Small contractor	Building contractor	Specialist Contractor	Main Contractor
Success factors	Saturation and performance of human resources	Focus of offers and development of expertise	Development of exclusive technologies and standardization projects	Links with other companies and capacity of government of proj. compl.
Organizational models	Functional structure	Functional structure project	Project	Project-matrix structure
Emphasis on objectives ERM	Operational	Operational / Compliance	Operational / Compliance / Financial	Operational / Compliance / Financial / Strategic
Emphasis on ICS	Processes	Processes / Risk areas	Processes / Risk areas	Top risks

Table 2.1 could be interpreted as the different types or the different stages of evolution of companies that compete and operate in the construction sectors.

The first type of company (i.e., **small contractor**) is the simpler in terms of production model and organization structure. We may assume that the owner of the company (sometimes, a single engineer) is in charge of the entire production process. The owner can manage a team of workers and try to optimize the saturation and the performance of the human resources. In this sense, the objective of the ERM and ICS systems must be respectively oriented towards operations and processes. Therefore, the objectives of ICS may be focused on the **effective and efficient use of resources**.

In the case of a **building contractor**, we may assume that the company must have a more structured organization and information system than the one in the case of a small contractor. In

terms of organization, there must be a basic **separation of duties** between different commercial, administrative, and production functions. The control systems have to account for different projects in order to evaluate performances for different construction areas, which may probably be supervised by different constructions managers. Basic internal rules, policies and procedures have to be defined. Thus, the emphasis of ERM and ICS should not be limited to operational objectives, but it must be placed also on **compliance objectives**, defined in terms of processes and risk areas.

When examining the third type of company, **specialist contractor**, the first consideration is that a relevant portion of risk is transferred from employers to contractors, due to design and engineering activities. Therefore, the deployment of proper contract management and project management techniques become key success factors in order to optimally allocate risks among projects contractual frameworks and to mitigate ensuing uncertainty. In the case of a specialist contractor, the company must be geographically structured, with its center providing special and qualified services for the projects. In terms of organization, there must be a complete separation of duties, enhanced by a large use of information systems. The control systems should be clearly defined and embedded into the management systems, in order to ensure consistency of practices among projects. The ERM emphasis should encompass operational, compliance, and financial objectives, while the assurance on internal control may focus on processes (i.e., bottom-up approach) or risks (i.e., top-down approach).

The last case is the most challenging. Here a main contractor has to deal not only with the employer or grantor and its subcontractors and vendors, but also with various other stakeholders, including its shareholders, financial institutions, the policy makers, trade unions, local communities, and the financial market. Each stakeholder has specific interests in the organization

that should be protected. Then, the complexity and dimension of each single project cannot be managed with a centralized silos approach. In this situation, risk is everywhere and could be operational, compliance, financial and, at the very least, also strategic. Therefore, the company should define a sound, balanced and formalized governance, risk management and internal control system, in order to protect and create sustainable value. In terms of organization, a matrix structure should be adopted, in order to ensure both decentralization of specialist activities and integration of practices and standards. ERM area is the widest possible, encompassing as well strategic risks, strategy setting, and risk appetite definition. Accordingly, ICS should comprise all the elements of the previous cases, but it must also focus on top risks, that is, those events that could damage the organization value.

As shown in Table 2.1, the difference between entities can outline different priorities and place emphasis on the objectives of ERM, and this can influence the way the framework operates in terms of components (COSO, 2004: 7):

> *The eight components will not function identically in every entity. Application in small and mid-size entities, for example, may be less formal and less structured. Nonetheless, small entities still can have effective enterprise risk management, as long as each of the components is present and functioning properly.*

The question is what the role of internal auditing can be in different contexts concerning the risk management, and what the criteria are that can guide the definition of its mission and activity. That is what we will try to define in the next section.

2. The roles of internal audit in risk management

Risk management is a continuous and pervasive process, which includes activities carried out within the organization, in

order to assess, manage, and report events in terms of risks or opportunities, which may affect the achievement of business objectives. It should allow management to obtain timely relevant information for strategic decisions making, to manage uncertainty within the limits of risk tolerance, to provide reasonable assurance on the achievement of objectives.

Within Risk Management, Internal Audit can play a fundamental role, assisting:

1) the Board, which defines the strategies and has the ultimate oversight duty to protect the interests of all the stakeholders;
2) the management, who are responsible for carrying out and monitoring processes, by identifying and mitigating risks.

Therefore, Internal Audit should address different expectations and needs. On the one hand, Internal Auditors must provide independent and objective assurance on risk management processes, for Board and senior management; on the other, Internal Audit plays a key role in providing management with methodologies for the identification, assessment, and reduction of risk in the organization.

According to the IIA Professional Standard (Institute of Internal Auditors, 2012: 11–12), there should be flexibility and discretion on the role of the Internal Auditors, considering both the assurance and consulting roles. The position of Internal Audit actually depends on the specific internal environment (objectives, complexity and size of the organization), the existence of other internal or external assurance providers, the maturity of risk management processes into the organization.

This approach is more clearly exemplified by the Institute of Internal Auditors (2009). This paper includes recommendations on possible roles of Internal Audit in ERM, which do not question its objectivity and independence, as shown in Figure 2.2.

The legitimate activities, which have a consulting nature, indeed, have greater weight when risk management system is less mature. For this reason, Interpretative Guidance 2120-1 (Institute

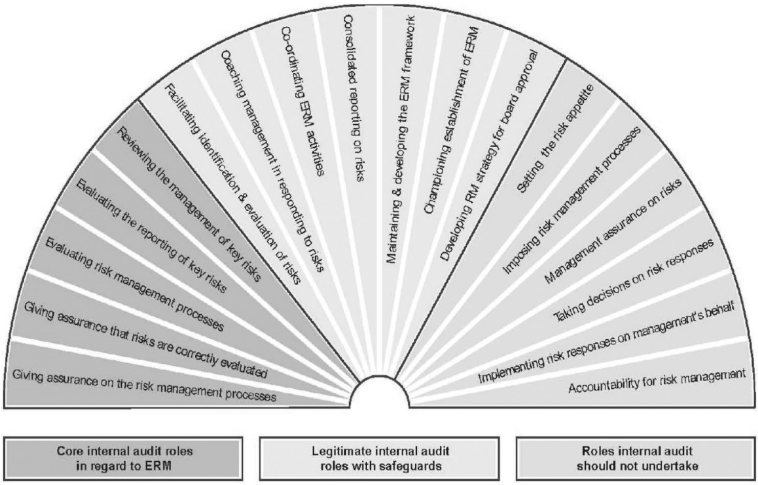

Figure 2.2 The role of Internal Auditing in enterprise-wide risk management (Institute of Internal Auditors, 2009: 4).

of Internal Auditors, 2012: 11) states that the Chief Audit Executive (CAE) firstly should determine whether formal processes of risk management are operating into the organization and are embedded into governance, businesses, and support processes. If they are not, it is CAE's responsibility to recommend their implementation, promoting the adoption of a standard framework, assisting management in developing commitment, participation, awareness, and consistent practices.

At the early stages, when the company decides to formalize its organizational governance, risk management, and internal control processes, Internal Audit Activity can contribute in exploiting skills and methodologies for the benefit of the organization. A useful means for this purpose is coordinating Control & Risk Self-Assessment projects. In carrying out this kind of engagements, one of the most important contributions by the Internal Audit comprises sharing and inspiring risk assessment techniques, such as:

- development of risk catalogs and registers, which are worthwhile for the identification of possible events that could hinder the achievement of strategic, business, reporting and compliance objectives;
- arrangement of common criteria for the measurement of likelihood and impact, in order to assess the relevance of identified risks;
- statement of method in order to evaluate residual risk, based on the adequacy of existing internal controls, which should ensure that risk response strategies are properly implemented.

Such approach allows progress through sharing, improvement of methodological patterns and the creation of a common language and understanding of risks. This represents a crucial prerequisite for the implementation of a truly integrated risk management system. Moreover, it helps the organization in managing information flows and reporting on the main risks, which Internal Audit should catalyze and address to senior management.

The higher the maturity of the risk management is, the greater could be the contribution internal auditors can provide by focusing on their assurance roles. In such a complex process of risk management, the main objective of an independent assurance is to evaluate whether individual components of the framework operate effectively, efficiently, and consistently, and whether the overall system fits the organization's needs.

According to the International Standard 2120 (Institute of Internal Auditors, 2012: 11), this judgment depends on how internal audit answers to these four questions:

1) Do organizational objectives support and align with the organization's mission, taking into account the acceptable risk level?
2) Have significant risks been identified and assessed?
3) Have appropriate risk responses been selected in order to align risks with the organization's risk appetite?

4) Has relevant risk information been captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities?

Internal Audit can play different and strategic roles in enterprise risk management, depending on the maturity of the process. Among the various options, the choice should be made considering a slight trade-off: on one side, the need for internal audit activities to be always independent and objective, avoiding to carry on management responsibilities; on the other, the opportunity to sponsor the improvement of risk management and controls systems, thus increasing its authority and reliability and adding more value to the organization.

3. Focus on compliance: How ethics and sustainability can create value and competitive advantage to the role of internal auditing?

As we stated in Chapter 1, management of compliant must be considered a priority in each context the internal audit operates. The focal point is that the adoption of a code of conduct, ethical principles, and objectives of sustainability must undeniably be considered as the very foundations of ERM and ICS. Many of the negative events occurred during the last decades (scandals, bankruptcies, collapses in financial markets) can be attributed to a poor management of compliance. As long as compliance is considered as a form of bureaucratic procedure and the attention is placed only on the costs the company has to sustain and not on benefits, any compliance objective is destined to fail.

Globally, law enforcement and regulations on corporate irregularities and crimes are becoming stricter in order to protect the various stakeholders. Therefore, companies must necessarily estimate into their strategic plans the cost of being compliant, meaning the costs of adopting rigorous compliance programs,

on one side, and the cost of saving on controls, considering the likelihood of negative consequences, on the other side.

Here, the idea we want to outline is that, in estimating the total cost of compliance according to the risk/opportunities patterns, not only the cost to implement it should be included, but also the higher (mostly hidden) costs resulting from ineffective implementation of internal control systems and risk management, which can result in non-compliance with law, contract or procedure. Investing in compliance is far more convenient than saving these costs.

Compliance is a strategic factor that companies must include in budgets: it is linked to all the activities at all organizational levels and responsibilities. However, costs for arranging and implementing processes, skills, and technologies need to ensure appropriate and significant levels of compliance. Companies need to establish a systematic, holistic and proactive approach, in order to:

- be aware of and monitor main legal, contractual and procedural requirements, defining consistent compliance programs;
- provide the management and the board with the information they need;
- anticipate regulatory changes.

Compliance and Internal Audit Activity should play a key role in breaking down the total cost of compliance, in avoiding expensive duplication, and in encouraging the integration of assurance services.

Compliance Departments, where formally established, have a primary duty of monitoring proactively compliance risk, through identification, assessment, monitoring and reporting on compliance with laws, regulations, and procedures. Its scope mainly encompasses: advising and assisting management in decision making, to ensure oversight and compliance; developing policies, procedures, contractual standards with regard to reg-

ulatory requirements; establishing programs to identify, assess and monitor the compliance risks; promoting and disseminating culture of legality.

Internal Audit Activity, instead, must always regard compliance risk in the Audit Plan and evaluate compliance function independently on a regular basis. Moreover, Internal Audit, given its organizational position with a direct reporting line to top management and board, can: i. capture the reporting flow from assurance services; ii. facilitate the coordination of activities, by identifying any area of overlap; iii. make the system more efficient with integrated compliance and assurance. This role has been confirmed by the Corporate Governance Code of the Italian Stock Exchange (Comitato per la Corporate Governance 2015). This Code has identified the Internal Audit as a key player in ensuring to a large extent a more organic, efficient and effective system of risk management and internal control.

From a long-term perspective, the implementation of integrated assurance is not only an organizational solution that helps lower the total cost of compliance, but it also plays a critical success factor in the development of business and it creates value by pursuing new opportunities and gaining entry into new markets. When estimating opportunity costs of non-compliance, missed benefits that would result should also be considered. These benefits may entail organizational and reputation improvement, greater ability to achieve business goals, and mitigating risks.

More concretely, international programs, such as the Global Compact, which is supported by the United Nations for the promotion of human rights, labor standards, environment and anti-corruption principles, demonstrate that ethics and social responsibility have an economic and strategic value: the chance to meet stakeholders' expectations, to develop partnerships, to enhance trust, and to optimize business opportunities.

Similarly, in Italy, for the infrastructure sector, a specific requirement in order to participate in both public and private

initiatives is the adoption of codes of ethic and organizational frameworks, such as the Organizational Model pursuant to Legislative Decree no. 231/2001. Likewise, when selecting vendors, companies must assess not only technical and economic reliability, but also integrity. For instance, for public procurement, since 2013, specific lists have been established by public authority in order to certify that a single economic entity is not corrupted by criminal infiltration.

Management of compliance risk is not an obstacle but a defense for business, since: i. it optimizes the costs of bureaucracy; ii. it facilitates decision-making processes, considering compliance constraints indecision making and allowing to focus on strategic objectives; iii. it produces market opportunities, improving the reputation of the company.

Law and mandatory regulations represent an exogenous variable that is over the controls of the organizations and that entails high costs in terms of compliance or non-compliance costs. As Voltaire wrote, in the best of all possible worlds, if everything went the right way, the costs of non-compliance would be zero. More realistically, it must be clear that cutting controls definitely causes more damages and very few benefits. This is due to the fact that companies are becoming increasingly more aware of the economic impact of rules and regulations, both in terms of costs to adapt and consequences of non-compliance.

Can law makers promote virtuous behavior? Of course, they can by simplifying law requirements. Excessive regulations greatly increase the compliance costs, thus, making efficiency and legality unsustainable. Moreover, the higher the legal tangle is, the less the probability is that violations and crimes are really discovered, prosecuted, and sanctioned. This finally increases the possibility of irregularities and market distortions. Simplification in regulations is moral suasion for organization and a must for the competitiveness of a country and its capacity to attract new investors.