After the corporate scandals from the beginning of the 21st century, there was a general lack of confidence in the quality of the financial reporting. The Sarbanes-Oxley Act came to address this issue, by imposing rules that would prevent such scandals in the future. In order to help companies with the compliance, control frameworks have been issued. The framework of the Committee of Sponsoring Organisations of the Treadway Commission offers guidance in matters of internal controls, whereas the Control Objectives for Information and related Technology focus on IT controls. The present paper intends to critically address the changes in the COSO and COBIT framework, that took place during 2012 and 2013.

Key words: Internal control, Committee of Sponsoring Organisations of the Treadway Commission (COSO), Control Objectives for Information and related Technology (COBIT), framework

JEL code: G34, M41, M48

1. Introduction

A general lack of confidence characterised the public opinion in the aftermath of the corporate scandals from the beginning of the 21st century. The scandals of Enron, WorldCom, Ahold, Group Société Generale, ABN AMRO are just some examples of control bloopers. The Sarbanes-Oxley Act came in 2002 just in time to fix this lack of confidence in the financial statements and in the control mechanisms that led to this situation. Some argue that this was the fastest written law in history, whereas others claim that in reality the law was written before, but the authors waited for the right moment to publish it. Regardless of that, the act came to enforce new ways of control, to improve the management’s behaviour and to restore the confidence in the “gatekeeper function”\(^{39}\) of the auditing profession.

An important element of this act is SOX 404 “Reporting on Internal Controls over Financial Reporting”. This part regards the internal control undertaken by the companies. The companies have to define their control procedures and perform checks of the enforcement of these controls every 3 months. When implementing this article, ING defined 12,000 controls, which implied 48,000 checks per year, taking into account that the controls had to be checked 4 times a year.

In order to come in the help of the companies, the COSO (Committee of Sponsoring Organisations of the Treadway Commission) framework have been approved as being SOX-compliant. The framework had been issued since 1992, but it gained wider acceptance after the financial control failures in the beginning of 2000s.

The IT control has also been an issue after the introduction of automated operations. The COBIT (Control Objectives for Information and related Technology) framework has also been issued in the 1990s, but its visibility increased when it gained the SOX-compliance status.

This paper intends to present the evolution of these two control frameworks, from their first version in the 1990s to their current state, after the improvements brought in 2012 and 2013.

2. The COSO framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was the common initiative of five private sector organizations: American Accounting Association (AAA), American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), Institute of Management Accountants (IMA) and The Institute of Internal Auditors (IIA). Their purpose is to provide guidance “through the development of frameworks on enterprise risk management, internal control and fraud deterrence”.\(^{40}\)

\(^{39}\) Speech by resigning SEC Commissioner Glassman with recommendations on SOX 404, 2006

\(^{40}\) COSO Internal Control – Integrated framework, exposure draft from December 2011
Its history dates back to the 1992, when the first version of the framework was issued, to serve the purpose of improving the internal controls in the companies. The framework was intended to be of use for all sizes of companies and types of organizations: public companies, privately held companies, not-for-profits and governmental entities.

In COSO's vision, internal control is “a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of reporting;
- Compliance with applicable laws and regulations.”

In order to address these aspects, the first version of COSO presented 5 elements of internal control: the control environment, risk assessment, control activities, information and communication and monitoring.

Figure 1. COSO Cube

The COSO cube presents the 5 elements of internal control and the 3 levels on which they apply: operations, financial reporting and compliance. The COSO cube "represents a depiction of the COSO Internal Control – Integrated Framework.”41 This cube resisted the test of time and even in the third version of COSO, issued in 2013, we find unaltered the core definition of internal control and the five elements of internal control.

The first element of the framework, the control environment, represents the company's internal environment and is the sum of the “hard” and “soft” controls. The hard controls are represented by the segregation of duties and various procedures, whereas the soft controls are represented by the company’s culture. The most important element to represent the company’s culture is considered to be the “tone at the top”. Thus, if the management creates an environment based on ethical values, the tone from the top will be transmitted to all levels of the company. For example, in IKEA, a company specialised in cost-cutting, the top management does not fly in business class because it is considered a waste of money. Consequently, neither the other employees will fly business class, because if economy class is enough for the top management, it will also be enough for the lower-level employees. Other elements that define the company’s culture are the management’s philosophy, the commitment to excellence and the pressure to perform. With a strong pressure to perform, like in Enron, when an employee performs worse, his peer’s performance will look better. This pressure creates a competitive atmosphere, whose ethical values can be questioned in some cases, particularly in Enron’s case.

Risk assessment is the second element of the framework. It regards the identification of the risks and their evaluation, in order for control activities to be defined in relation to them. This element of the framework has been given more attention in the second version of the framework, issued in 2004.

The control activities are the activities established by the company for the risks identified at the previous step. These activities include direct controls such as direct supervision and surveillance cameras and indirect controls, represented by segregation of duties, controls in the IT systems and top level reviews.

41 http://blog.aicpa.org/2012/01/internal-control-integrated-framework-20-years-later.html#sthash.sflf98r4.dpbo
The "Information and Communication" element regards the reduction of the information asymmetry and adverse selection between top management and lower-level employees. This information gathering regards both oral and written communication and focuses on availability and quality of the information provided.

"Monitoring" is the fifth element of the framework and can be considered the final step in the control process. After defining the internal environment, assessing the risks, defining control activities and disseminating information, the next step is the monitoring of the proceeds and the quality of the internal control systems. This can be done through direct supervision, internal and external audits and also through the reception of various signals from the market, such as the complaints received from the customers.

In 2004, a new version of the COSO framework has been issued. This version gave more attention to the risk component. According to "Risk assessment in practice", a research commissioned by COSO in October 2012, the process of risk evaluation comprises 6 steps:

Step 1. Identify the risk
Step 2. Develop criteria
Step 3. Assess risk
Step 4. Assess risk interactions
Step 5. Prioritise risks
Step 6. Respond to risk

First, the identification and categorisation of the risk incurs. Then the actual assessment of the risk is made, and comprises steps 2, 3 and 4: the development of the assessment criteria (usually probability and impact), the actual assessment based on qualitative and quantitative techniques and the evaluation of risk interactions. This assessment leads to the drawing of a "heat map" and the placing of a certain risk at the intersection of its corresponding impact and probability. Based on the assessment, the risks are prioritised and a risk response is defined: accept, avoid, shared or mitigate. The company will accept the risks that are perceived as inherent to the business and cannot be reduced by controls. The risks that can be avoided (e.g. not choosing to move the headquarter in a building that is prone to demolition) should be taken into consideration and eliminated from the list of eventual uncertainties, through avoidance. There are also risks that can be shared through insurances so that the company would split the risk with the insurance company to whom the insurance fee is paid. If a company decides to mitigate the risk, then it will define control activities in order to reduce the inherent risk to the value of residual risk.

Then control activities are established by the company only for the risks that want to be mitigated by the company.

The 2013 edition of the COSO framework came with some additional updates: it made explicit 17 principles connected to the 5 elements of internal control, that can be used in the development and evaluation of the effectiveness of the internal controls. Also, the objective of the framework has been extended and now also comprises the compliance objective and the supporting of the non-financial reporting.

"The COSO Board believes these updates will result in a more flexible, reliable and cost-effective approach to the design and evaluation of internal control systems for organizations looking to achieve operational, compliance and reporting objectives." (Kayla Briggs, Certified Public Accountant, Senior Technical Manager – Business, Industry & Government, AICPA - 2012)

The first 5 new principles issued regard the control environment:

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. The management establishes, with board oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

These principles emphasize a clear organisational structure, the role of internal audit in the control environment and also outlines the necessity of the enforcement of a code of conduct that would comprise attitudes and responses to deviations of behaviour, consistent at all management levels.

The "risk assessment" element is now guided by 4 principles:

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the systems of internal control.

Thus, the company should define its risk tolerance and risk appetite, being known that these two concepts are different. In “Risk appetite and tolerance guidance paper”, issued in 2011 by the Institute of Risk Management, Richard Anderson defines the difference between risk universe, risk tolerance and risk appetite. The risk universe encompasses all the risks that an organisation might face. The risk tolerance is the maximum risk the organisation can bear and the risk appetite is the risk that the organisation wants to bear. As can be inferred, the risk universe is wider than the risk tolerance, which is wider than the risk appetite.

At this point, is is necessary to underline that in the process of risk assessment, fraud should not be confused with mistake, as fraud also has an ethical component. In defining fraud, the fraud triangle is an useful notion to be mentioned.

![The Fraud Triangle](image)

Figure 2. Fraud triangle

According to the criminologist Donald Cressey, in order for an ordinary person to commit fraud, three element have to be present: the pressure to commit fraud, the opportunity to commit fraud and the rationalisation of fraud. For a person to be tempted to commit fraud, must be a pressure for it, determined either by inside factors (e.g. some needs that require to be satisfied) or by exterior factors (e.g. pressure to perform better than the peers). Then, the opportunity to commit fraud will provide the person the method by which to commit the crime. Regarding the rationalisation of fraud, it is considered that 4% of the people have no conscience at all, 4% act morally in every situation and therefore the rest of 92% is tempted to perform fraud. When these three elements are present, a person is prone to committing fraud.

The control activities are now under the governing of 3 principles:
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

The control activities defined by the company are put in place in order to reduce the inherent risk, that is automatically related to a certain product or action, to the level of residual risk, that is the one that remains after applying internal controls.

The 3 principles regarding the information and communication are:
13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

The company should therefore define its information requirements, taking into consideration both the benefits and the costs associated to the process. The communication should be directed also towards the outside of the organisation, namely to shareholders and other stakeholders. But this information function should also consider the information gathered from whistleblowers. Whistleblowers are the
persons that discloses misconduct or illegal activities undertaken in the company. According to SOX 806, whistleblowers are protected and should not be fired because of the disclosure of illegal activities.

The last 2 principles introduced by the new version of COSO regard the monitoring function.

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

These principles give an increased attention to the internal audit function, whose role is to provide an additional assurance of the state of internal control within the company. The internal audit should report directly to the board of directors, in order to keep its independence and not be influenced by the managers who are the subjects of the controls.

Another new element brought by COSO 2013 is the “Lines of defence” model. The four lines of defence present in a company are:

Line 1: The business management
Line 2: The staff
Line 3: The internal audit
Line 4: The external audit and external authorities

The four lines of defence are the areas for managing risk within a company. The model assumes that risk is everyone's business. Each employee takes on a slightly different function, depending on his or her specific location within the organization.

The first line of defence is represented by the business management. The second line of defence is comprised of the departments that help the managers by performing specific tasks for them, namely risk department, compliance department, human resources department, IT, financial department. The third line of defence, the internal control, checks some processes and gives an opinion over the internal controls. The second and third line of defence cannot be combined and should be totally separated. The forth line of defence is represented by external parties (external auditing, Central Bank) that take a more objective look over risk management.

But although COSO is trying to improve and keep the pace with the evolution of society, it has not been avoided by critics. For example, in 2005, Ali Samad-Khan published an article entitled “Why COSO is flawed”, arguing that “COSO not only fails to help a firm assess its risks, it actually obfuscates the risk assessment process.” In order to support this statement, he stated that COSO offers too much attention to false-positive risks and no attention to false-negative risks.

1. COSO vs reality: COSO produces false positives and false negatives

The false positive risks are the ones that according to COSO represent a moderate risk, when actually there is a big risk. The false-negative risks are the ones that presumably are very important but in reality they do not exist. This is the case of “phantom risks”, that have high probability and high impact, fact that can be understood that there are risks that appear very frequently and every time they occur they cause the company severe losses. If these risks really existed, they might take the company out of the market because of their high likelihood and high impact.

Figure 3. Risk assessment: reality versus COSO (source: "Why COSO is flawed", 2005)
Also, the author considers that it is wrong to represent a risk as a point on a graph, as long as its likelihood and impact are distributed and therefore a line would be more representative. He gives the example of the risk of damage in a car accident: there are 40% chances of a small damage, 30% chances of medium damage, 29% chances of large damage and 1% chances of extreme damage.

3. The COBIT framework

The information technology (IT) control is a part of the internal control. The COBIT (Control Objectives for Information and related Technology) framework was elaborated by the Information Systems Audit and Control Association (ISACA) as an IT control framework, designated for information technology management and IT governance.

The IT controls are also important for SOX implementation. As stated by PCAOB Auditing standard number 5 “An Audit of Internal Control Over Financial Reporting that is Integrated with an Audit of Financial Statements”\(^\text{42}\), “IT general controls over program development, program changes, computer operations and access to programs and data […] have a pervasive effect on achieving many overall objectives of the control criterion.” and also mentions that other controls are dependent on the information technology general controls.\(^\text{43}\)

The first version of COBIT framework was released in 1996. The current version is COBIT 5 and has been issued in 2012.

Just like the COSO framework, COBIT is intended to be of use for all sizes of companies and types of organizations: public companies, privately held companies, not-for-profits and governmental entities.


According to its producer, ISACA, “COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.”\(^\text{44}\) The current version of the framework holds that the IT can be managed in a holistic manner, for the entire company.

Resembling the 2013 version of COSO, COBIT also comes with new principles, but besides that, it defines 7 enablers.

COBIT 5 is based on five principles for governance of enterprise IT. The purpose of these principles is to build an effective IT governance and management framework, as COBIT 5 emphasises the separation between IT governance and IT management.

The five principles are the following:

![Figure 4. COBIT 5 - principles (source: COBIT® 5, figure 12. © 2012 ISACA®)](http://www.isaca.org/COBIT/Pages/default.aspx?cid=1003566&Appeal=PR)

1. Meeting stakeholder needs – COBIT 5 holds that companies exist in order to create value for their stakeholders. But being given the numerous and different categories of stakeholders, governance system should consider 3 facts when taking a decision: who receives the benefit, who bears the risk and what

\(^\text{42}\) The Public Company Accounting Oversight Board (PCAOB) was created by the Sarbanes-Oxley Act in order to oversee the auditors of U.S. listed companies.

\(^\text{43}\) “Information technology general controls on which other controls are dependent”

resources are needed. The present framework addresses only the IT-related goals that are set in order to achieve the needs of the stakeholders.

2. **Covering the enterprise end-to-end** – the framework intends to regard IT management and governance from an enterprise-wide perspective. For this purpose, it integrates the governance of enterprise IT in the enterprise governance, because the framework is in line with the latest views and changes of regulations in the corporate governance field.

3. **Applying a single, integrated framework** – in this regards, COBIT intends to be considered a management framework integrator, its purpose being to align the enterprise frameworks (COSO, ISO 9000 on Quality Management, ISO 31000 on Risk Management) with IT-related frameworks (ISO 38500 on Corporate Governance of Information Technology, ISO 27000 on Information technology – Security Techniques, Information Technology Infrastructure Library).

4. **Enabling a holistic approach** – this principle deals with the 7 enablers newly defined by the framework and their interconnectedness. These 7 enablers will be dealt with in more detail subsequently.

5. **Separating governance from management** – the COBIT framework makes a clear distinction between governance and management, because these two functions serve different purposes, require different organisational structures and encompass different activities.

   The role of the governance is to evaluate, direct and monitor: it evaluates the stakeholders needs and establishes the objectives accordingly. Through the decisions taken, it provides direction for the course of action and in the end, it monitors the performance.

   The management’s role comprises planning, building, running and monitoring the activities that have to be in line with the objectives and directions set by the governance.

   The framework also defines 7 categories of enablers, also mentioned by the forth principle:

   ![Diagram of COBIT 5 enablers](source: COBIT® 5, figure 12. © 2012 ISACA®)

1. **Principles, policies and frameworks** - are used to translate the objectives and directions into day to day management of actions.
2. **Processes** – are the translation of principles, policies and frameworks into daily activities, undertaken in line with the company’s objectives.
3. **Organizational structures** comprise the hierarchy levels in a company, endowed with decision-making rights.
4. **Culture, ethics and behaviour** deal with the “soft” control of the company and are considered a critical success factor in the governance and management of a company.
5. **Information** is the key product of the organisation, as it is required for keeping the organization running.
6. **Services, infrastructure and applications** define the IT processing necessities of a company.
7. **People, skills and competencies** – because people are the most important asset of a company, they are considered an enabler of uttermost importance because their skills and competencies are used for decision-making (at a high level) and also for implementing the decisions (at a lower level).

### 4. Conclusions

Having in mind the recent scandals that troubled the market, the investors are still demanding continuous performance growth but now they also focus their attention on the enterprise’s risk management. A study undertaken by Ernst&Young in 2008 on institutional investors revealed that these
investors penalise a company when finding that it is not committed to efficient risk management. 61% of the respondents said that they avoided investing in such companies and 48% de-invested when noticing the lack of commitment to risk management. Also, 82% agreed that a company that pays attention to its risk management deserves a premium on its share price.

This demand of the investors emphasize the importance of risk management and internal control frameworks, used for identifying and addressing the risks on time, before causing prejudices and harming the investors’ interests. Therefore, it can be concluded that a company that invests in its internal control and risk management will benefit from the investors’ attention, fact that can be translated as a competitive advantage.

References
2. COSO Internal Control – Integrated framework, exposure draft from December 2011
6. “Risk assessment in practice”, a research commissioned by COSO in October 2012
10. www.coso.org/
11. www.isaca.org/cobit