# Framework for Evaluation of IT Controls in Auditing

Eugenio Fernández[1], Antonio Moratilla[1], Carlos Mir[2], Alvaro F. Narciso[1]

[1]*(Department of Computer Science / University of Alcalá, Spain)*

[2]*(Department of Economics and Business / University of Alcalá, Spain)*

***ABSTRACT:*** *For a few decades, companies around the world have faced different challenges, among which we have the rapid development of information and communication technologies, as well as the risk and complexity of the management that these entail, especially in terms of which concerns the financial sphere and the transactions carried out in the company, which must be periodically evaluated by the account auditors. External and internal auditing using a good control-based system can reduce the likelihood of risk. An appropriate set of controls should also include appropriately designed IT controls in order to cover those aspects of the organization's IT environment that may have an impact on risk. Thus, an IT audit with appropriate set of controls will allow to determine whether IT controls protect corporate assets, ensure data integrity and are aligned with the business's overall goals. The aim of this paper is to make a review about the aspects that the regulation establishes in this regarding order to propose a framework that determines the specific scope, in terms of processes, levels and elements, that must be taken into account in order to design, implement and evaluate appropriate IT controls.*

***KEYWORDS*** *–Auditing, Frameworks, Processes, IT Controls, IT Governance, IT Management, IT Operations, IT Security, IT Exploitation, Software Development.*

## I. INTRODUCTION

Companies and other organizations around the world spend billions of dollars using, installing, and upgrading their IT (Information Technology) systems, especially in those systems related to the main business processes, named as Business Applications, what are used by business to increase productivity, to measure productivity, and to perform other business functions accurately.

According to the Institute of Internal Auditors (IIA)[1], these Business Applications can be classified as Transactional Business Applications (such as those related to financial transactions) and Support Business Applications (such as those related to mail communications).

Transactional Business Applications, often referred to as Core Business Applications, are those that process transactions and employees within an organization use to upload and manage assets, and often has a wide breadth of functionality, some of which is visible (or not) to those end-users based on their rights. Examples of popular transactional business applications are SAP, PeopleSoft, Oracle Financials, Sales force or Sage. These systems are often referred to as Enterprise Resource Planning (ERP) systems, which process transactions based on programmed logic and, in many cases, in addition to configurable tables that store unique organizational business and processing rules.

On the other hand, Support Applications are specialized software programs that facilitate business activities. Examples include e-mail programs, fax software, document imaging software, and design software. However, these applications generally do not process transactions.

Both transactional and support applications can present risks to the organization, stemming from the inherent nature of technology and how it is configured, managed, and used by managers, employees, and administrators.

With respect to transactional processing systems, risks can have a negative impact on the integrity, completeness, timeliness, and availability of financial or operational data if they are not mitigated appropriately. Furthermore, the business processes themselves will have some element of inherent risk, regardless of the application used to support them. As a result of these application technology and business process risks, many organizations use a mix of automated and manual controls to manage these risks in transactional and support applications.

However, the degree of successful risk management is directly dependent upon [2]:

- The organization's risk appetite, or tolerance.
- The thoroughness of the risk assessment related to the application.
- The affected business processes.
- **The effectiveness of general information technology (IT) controls.**
- The design and ongoing extent of operating effectiveness of the control activities.

## II. BUSINESSRISKAND AUDITING

According to the International Standard on Auditing 315 [4], Business Risk is a risk resulting from significant conditions, events, circumstances, actions or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies. A significant risk is an identified and assessed risk of material misstatement.

In this context, the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, through understanding the entity and its environment, including the entity's internal control, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

The auditor shall perform risk assessment procedures to provide a basis for the identification and assessment of risks of material misstatement at the financial statement and assertion levels. These risk assessment procedures shall include inquiries of management, analytical procedures, and observation and inspection. Further, in order to obtain more persuasive audit evidence, shall design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of relevant controls if [5]:

(a) The auditor's assessment of risks of material misstatement at the assertion level includes an expectation that the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing and extent of substantive procedures); or

(b) Substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level.

## III. BUSINESS RISK DERIVED FROM THE USE OF IT

Generally, IT benefits an entity's internal control by enabling an entity to consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data; enhance the timeliness, availability, and accuracy of information; f Facilitate the additional analysis of information; enhance the ability to monitor the performance of the entity's activities and its policies and procedures; reduce the risk that controls will be circumvented; and enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems [4].

Never the less IT also poses specific risks of disruption, deception, theft and fraud to an entity's internal control, such us reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both; unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions, or inaccurate recording of transactions; the possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties; unauthorized changes to data in master files; unauthorized changes to systems or programs; failure to make necessary changes to systems or programs; inappropriate manual intervention; or potential loss of data or inability to access data as required [4].

Thus, the organization's executives should know the right questions about IT to ask and what the answers mean. For example [3]: Why should I understand IT risks and controls?: Two words, assurance and reliability.

- What is to be protected?: Trust should be protected because it ensures business and efficiency.

- Where are IT controls applied?: Everywhere.
- Who is responsible?: Everyone.
- When should IT risks and controls be assessed?: Always.
- How much control is enough?: Management must decide based on risk appetite, tolerance and mandatory regulations.

From the auditing perspective, some IT conditions and events may clearly indicate risks of material misstatement. For example:

- Inconsistencies between the entity's IT strategy and its business strategies.
- Changes in the IT environment.
- Installation of significant new IT systems related to financial reporting.

Therefore, in understanding the entity's control activities, the auditor shall obtain an understanding of the information system, including the related business processes, relevant to financial reporting, and also how the entity has responded to risks arising from IT systems.

The auditor should obtain assurance that IT-related controls are working as intended. This assurance is based on understanding, examining and evaluating the key controls related to the risks they manage and performing sufficient tests to ensure that the controls are properly designed and function effectively and continuously.

In this way the auditor should feel comfortable with general IT concepts and controls so they can talk and exchange risk and control ideas with the Chief Information Officer (CIO) and other people in IT management.

## IV. IT CONTROLS

One of the most cost-effective and efficient approaches organizations use to manage these risks is through the use of controls that are inherent or embedded (e.g., three-way match on account payable invoices) into transactional and support applications as well as controls that are configurable (e.g., accounts payable invoice tolerances).

COSO defines internal control [6, 7, 8, 9, 10, 11, 12, 13, 14, 15] as a process, effected by an entity's board of directors, management, and other personnel. This process is designed to provide reasonable assurance regarding the achievement of objectives in:

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

IT controls encompass those processes that provide assurance for information and information services and help control or mitigate the risks associated with an organization's use of technology. These controls range from written corporate policies to their implementation within coded instructions; from physical access protection to the ability to trace actions and transactions to the individuals who are responsible for them; and from automatic edits to reasonability analyses for large bodies of data.

These IT controls are essential to protect assets, customers, partners, and sensitive information; demonstrate safe, efficient, and ethical behavior; and preserve brand, reputation, and trust. They have two significant elements: the automation of business controls (which support business management and governance) and control of the IT environment and operations (which support the IT applications and infrastructures) [3].

The three main operations that allow managing controls are:

- Implementation: of a control means that the control exists and that the entity is using it. There is little point in assessing the implementation of a control that is not effective, and so the design of a control is considered first. An improperly designed control may represent a significant deficiency in internal control.
- Evaluating: the design of a control involves considering whether the control, individually or in combination with other controls, is capable of effectively preventing, or detecting and correcting, material misstatements.
- Monitoring: of controls is a process to assess the effectiveness of internal control performance over time. It involves assessing the effectiveness of controls on a timely basis and taking necessary remedial actions. Management accomplishes monitoring of controls through ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are often built into the normal recurring activities of an entity and include regular management and supervisory activities. Management's

monitoring activities may include using information from communications from external parties such as customer complaints and regulator comments that may indicate problems or highlight areas in need of improvement.

From the auditing perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process, and include effective General IT Controls and Application IT Controls, which must be considered in three essential IT processes:

- Information Security.
- Systems Operation and Exploitation: maintenance, operation and support.
- Software Development.

A good and accepted classification of the controls is as follows (Fig. 1 and 2) [3]:

In what follows, we will make a description of the different types of controls, based on the approach made by GTAG (Global Technology Audit Guide) [1, 2, 3].

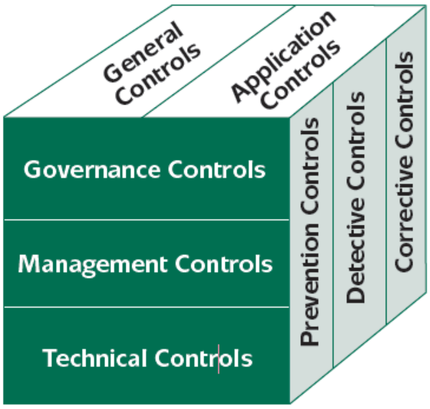


**Figure 1**. IT Controls Classification. Source: [3]

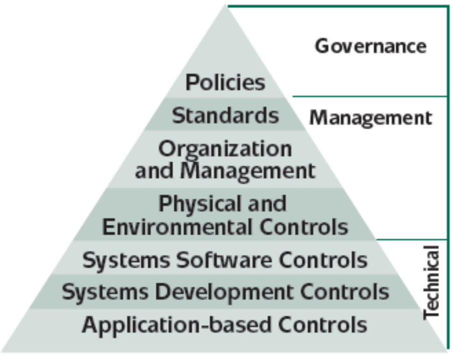

Governance
Policies
Standards
Management
Organization and Management
Physical and Environmental Controls
Systems Software Controls
Systems Development Controls
Application-based Controls
Technical

**Figure 2**. Hierarchy of IT Controls. Source: [3]

## GENERAL IT CONTROLS.

General IT Controls apply to all systems components, processes, and data for a given organization or systems environment. They are policies and procedures that relate to many applications and support the effective functioning of application controls maintaining the integrity of information and security of data.

General controls include [3], but are not limited to, IT governance, risk management, resource management, IT operations, application development and maintenance, user management, logical security, physical security, change management, backup and recovery, and business continuity. Some general controls are business-related (e.g., segregation of duties or governance arrangements), whereas others are very technical (e.g., system software controls and network software controls) and relate to the underlying infrastructure.

## APPLICATION IT CONTROLS.

Application controls [24] pertain to the scope of individual business processes or application systems and include controls within an application around input, processing, and output.

They are manual or automated procedures that typically operate at a business process level and apply to the processing of transactions by individual applications. Application controls can be preventive or detective in nature and are designed to ensure the integrity of the accounting records.

Accordingly, application controls relate to procedures used to initiate, record, process and report transactions or other financial data. These controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed. Examples include edit checks of input data, and numerical sequence checks with manual follow-up of exception reports or correction at the point of data entry.

## PREVENTIVE CONTROLS

Preventive Controls [3] prevent errors, omissions, or security incidents from occurring. Examples include simple data entry edits that block alphabetic characters from being entered into numeric fields; access controls that protect sensitive data or system resources from unauthorized people; and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.

## DETECTIVE CONTROLS

Detective Controls [3] detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective Controls also can include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or that the sender cannot be authenticated.

## CORRECTIVE CONTROLS

Corrective Controls [3] correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data entry errors to identifying and removing unauthorized users or software from systems or networks to recovery from incidents, disruptions, or disasters.

## GOVERNANCE CONTROLS.

The primary responsibility for internal control oversight resides with the Board in its role as keeper of the governance framework. IT control at the governance level [3] involves overseeing effective information management, principles, policies, and processes and ensuring that they are in place and performing correctly. These controls are linked with the concepts of governance, which are driven both by organizational goals and strategies and by outside bodies, such as regulators.

## MANAGEMENT CONTROLS.

Management responsibility for internal controls typically involves reaching into all areas of the organization with special attention to critical assets, sensitive information, and operational functions [3]. Management must make sure the IT controls needed to achieve the organization's established objectives are applied and ensure reliable and continuous processing. These controls are deployed as a result of deliberate actions by management in response to risks to the organization, its processes, and assets.

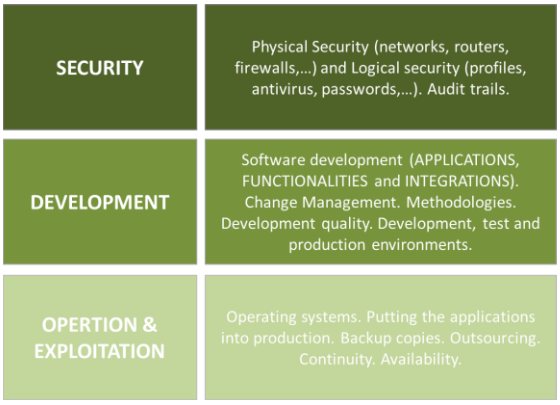
## TECHNICAL CONTROLS

Technical controls [3] often form the backbone of management's control framework. Therefore, if the technical controls are weak, the impact affects the entire control framework. For example, by protecting against unauthorized access and intrusion, technical controls provide the basis for reliance on the integrity of information, including evidence of all changes and their authenticity. These controls are specific to the technologies in use within the organization's IT infrastructures. Examples of technical controls are operating system controls, database controls, encryption, and logging.

## V. IT FRAMEWORK

Considering everything previously related, it is necessary to define a framework so that the auditor can implement an adequate methodology for the design, implementation and adequate evaluation of the controls in the audit process.

To form this framework, we first define the three IT processes that the ISAs establish [4, 5] on which the auditor should focus attention (Fig 3):



| | |
|---|---|
| SECURITY | Physical Security (networks, routers, firewalls,...) and Logical security (profiles, antivirus, passwords,...). Audit trails. |
| DEVELOPMENT | Software development (APPLICATIONS, FUNCTIONALITIES and INTEGRATIONS). Change Management. Methodologies. Development quality. Development, test and production environments. |
| OPERTION & EXPLOITATION | Operating systems. Putting the applications into production. Backup copies. Outsourcing. Continuity. Availability. |

**Figure 3**. Main IT Processes.

Next, we define the set of levels on which the different controls will be applied (Fig. 4).These levels correspond to a definition of IT in the organization that goes from a more general level (Context) to a more operational level (Operations), to finally have the level of specific

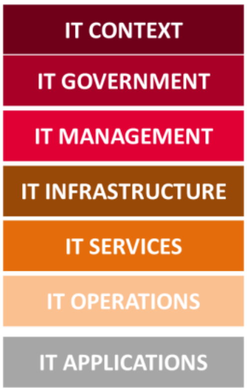


**Figure 4**. Levels.

applications subject to audit. At the IT Infrastructure level, the following elements are considered (Fig. 5)

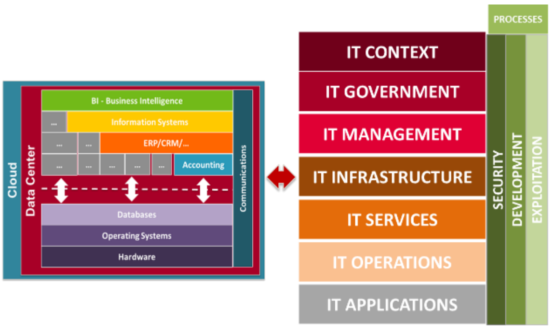


**Figure 5**. IT Infrastructure.

This level includes both low-level technological elements (hardware and operating systems), as well as those related to applications, from monolithic software as accounting software to those related to BI processes, passing through intermediate layers of software such as databases. Additionally, it includes the elements referring to communications, the data enter itself, and aspects related to the context of the cloud.

Properly combining the elements previously shown, we obtain the framework on which to design, implement and evaluate IT controls (Fig. 6).

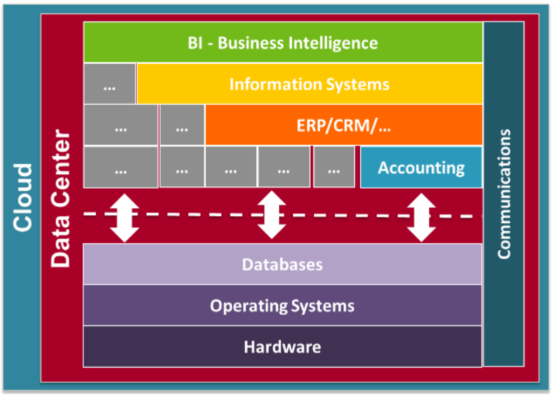


**Figure 6**. Framework for Evaluation.

## VI. Conclusion

Organizations must define an appropriate framework in the field of IT to strengthen the internal control structure, optimize the effectiveness of their IT control environments, and improve the efficiency of their IT compliance, governance, management, infrastructure, services, operations and applications, regardless of the size of the organization. On the other hand, assessing IT risks and controls represents one of the first steps in gaining an understanding of the IT environment and its significance in business risk management. This requires a thoughtful and organized plan. Chief auditing executives and internal auditors should plan sufficient time and skilled resources to do a professional job and create a sustainable process for ongoing analysis. This work presents a working framework that defines and justifies the processes and levels at which controls must be defined in order to ensure a correct risk assessment of the organization in the audit process.

## References

[1] *Coates, S., et al., (2013). Global Technology Audit Guide (GTAG): Management of IT Auditing, 2nd Edition (2013). The Institute of Internal Auditors. https://na.theiia.org/*

[2] *Bellino, C., Wells, J., & Hunt, S., (2007). Global Technology Audit Guide (GTAG): Auditing Application Controls. The Institute of Internal Auditors. https://na.theiia.org/*

[3] *Mar, S., et al., (2012). Global Technology Audit Guide (GTAG): Information Technology Risk and Controls. The Institute of Internal Auditors. https://na.theiia.org/.*

[4] *INTERNATIONAL STANDARD ON AUDITING 315. https://www.iaasb.org/*

[5] *INTERNATIONAL STANDARD ON AUDITING 330. https://www.iaasb.org/*

[6] *www.coso.org*

[7] *https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework.*

[8] *Schandl, A.amd Foster P.L. (2019): COSO INTERNAL CONTROL INTEGRATED FRAMEWORK: An Implementation Guide for the Healthcare Provider Industry. www.coso.org.*

[9] *"COSO Issues Updated 'Internal Control – Integrated Framework' and Related Illustrative Documents," COSO news release, May 14, 2013, coso.org/Documents/COSO-Framework-Release-05142013.pdf.*

[10] *COSO, "Internal Control – Integrated Framework," Executive Summary, p. 3.*

[11] *Mary E. Galligan and Kelly Rau, "COSO in the Cyber Age," January 2015, p. 1, coso.org/documents/ COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf*

[12] *"Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934," SEC Interpretation, June 20, 2007, https://www.sec.gov/rules/interp/2007/33-8810.pdf.*

[13] *COSO, "Internal Control Over External Financial Reporting (ICEFR): A Compendium of Approaches and Examples," p. 70.*

[14] *COSO, "Illustrative Tools for Assessing Effectiveness of a System of Internal Control," pp. 1-8.*

[15] *"COSO – Internal Control – Integrated Framework, Framework and Appendices," p. 5.*

[16] *PCI Security Standards Council LLC, Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 2.0., Oct. 2010.*