NOVA IMS Information Management School

MGI

Master Degree Program in

Information Management

The impact of PwC Portugal's IT Audit work to improve Client Information Systems

Maria Helena Figueiredo Silva

Project Work

presented as partial requirement for obtaining the Master Degree in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

The impact of PwC Portugal's IT Audit work to improve Client Information Systems

by

Maria Helena Figueiredo Silva

Project Work presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information Systems and Technologies Management

Supervised by

Vítor Duarte dos Santos, PhD, NOVA Information Management School

February, 2024

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledged the Rules of Conduct and Code of Honor from the NOVA Information Management School.

[Lisbon, February 2024]

ACKNOWLEDGEMENTS

Carrying out this project represents the end of an academic journey characterized by ups and downs, many challenges, and constant learning.

First, I would like to thank my grandmother, Natividade, because it would not be possible to achieve my goals without the opportunity she gave me. I also express my gratitude to my parents and my sister for all the support and encouragement they gave me. To Miguel, I thank you for being a constant motivator throughout this journey and for always believing in me.

To Professor Vítor Duarte dos Santos, for all the support, understanding, and knowledge he shared with me. Thank you for all your help, guidance, total availability, and advice, and for always encouraging me. It was tireless.

To everyone who crossed my path throughout my master's degree, I express my deepest thanks!

ABSTRACT

Companies have been constantly concerned about investing in their information systems in recent years. Additionally, companies that provide auditing services look for IT specialists to ensure that the data in financial reports is intact. This gives rise to the role of the Information Technology Auditor, which, in addition to supporting financial audits in obtaining the necessary comfort regarding the integrity of financial information, also plays a crucial role in evaluating and guaranteeing an information systems company's effectiveness, security, and compliance. They help identify potential risks, ensure data integrity, and assess the entire IT infrastructure to safeguard against cyber threats and ensure compliance with regulations and industry standards.

Given the relevance of using these specialists, this project was developed in the RAS department of PwC Portugal, aiming to understand the methodology used in analyzing the information systems of a client in the Industry & Services sector.

By carrying out this project, it was possible to understand that there are risks associated with using information systems that can be overcome by introducing IT controls. Furthermore, executing these controls contributes to the overall stability and trustworthiness of an organization's IT environment.

KEYWORDS

Audit; Information Systems; Risk; Control; IT Specialist

Sustainable Development Goals (SDG):

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

COBIT	Control Objectives for Information and Related Technologies
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CTO	Chief Technology Officer
DS	Security Department
DSI	Information Systems Department
ERP	Enterprise Resource Planning
IAASB	International Auditing and Assurance Standards Board
IS	Information Systems
ISA	International Standards on Auditing
ISACA	Information System Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technologies
ITGC	IT General Controls
RAS	Risk Assurance Services
SA	Sensitive Access
SoD	Segregation of duties

1. INTRODUCTION

1.1. BACKGROUND

At a time when advances in Information Technologies (IT) have completely changed the business environment of many companies in the last two decades, with investments in their information systems becoming more common, we see an increase in concern on the part of companies in executing best auditing practices. Auditing information systems has proved critical in the current context. It should not be seen just as an extension of the traditional audit, given that the latter now needs to consider new technologies (Tarek et al., 2017).

However, adopting Information Technologies brings new risks in several areas that must be considered, such as virus attacks, hackers, fraud, manipulation, or unauthorized access to data relevant to the company. Thus, auditors must know these risks when planning work, collecting evidence, and issuing audit reports. This forces companies to acquire IT-related skills and techniques and incorporate this knowledge into audit work (Tarek et al., 2017).

Therefore, to carry out a quality financial audit, IT specialists should be used, namely information systems auditors, given that business processes are concentrated in IT components, such as ERP systems, internal applications, and databases, where it is necessary to guarantee the correct storage of data so that they cannot be modified or accessed improperly.

This project, equivalent to a master's thesis, is the final work for the conclusion of my master's in information management at Nova Information Management School and aims to describe in detail the activities carried out within the scope of auditing information systems at PwC, namely in the Risk Assurance Services (RAS) department.

Additionally, it intends to apply the knowledge obtained during this master's degree and understand the whole process to be carried out to analyze the information systems (IS) relevant to a financial audit.

1.2. MOTIVATION

With the growing concern of organizations regarding the security and protection of data and the information systems that process and store data, organizations have had more and more requests and contractual needs from their customers to obtain comfort regarding their technological platforms. In this way, PwC is requested by a service provider organization to carry out an audit to bring comfort to the use of its IT systems.

In addition, we also see an increase in the concern of auditing companies to ensure that the information in financial reports is correct.

To this end, financial audits must resort to IT specialists to obtain comfort regarding the completeness and integrity of the financial information analyzed when issuing the legal certification of accounts.

Given the importance of using these specialists for a quality financial audit, the present project was developed, which aims to demonstrate the methodology used in the analysis of the information systems of a client in the Industry & Services branch, as well as to describe detail the management of the service organization's system and the adequacy of the execution of controls.

This project will make it possible to understand that there are risks associated with the use of information systems that can be overcome with the introduction of computer controls and that the collaboration between financial audit teams and IT specialists allows an increase in the quality of audit work.

Considering this, we can conclude that this project will fall within the *"Audit Support"* typology. It aims to support the financial audit team in issuing the Legal Certification of Accounts, Reports and Accounts, and other corporate or tax audits.

1.3. OBJECTIVE

The project was developed in PwC's Risk Assurance Services (RAS) department in the Digital Assurance team. In addition to providing support to the financial audit team, RAS offers more services to its clients by helping to identify and manage the business risks associated with information systems and to improve the use of IT, such as Systems and Technology Audit (IT Security), Internal Audit, Privacy and Data Protection, Data Assurance, Risk Management & Compliance, Third Party Assurance, Enterprise Systems Risk and Controls, and Process Assurance. This scope is illustrated in Figure 1.1.

Figure 1.1 – Risk Assurance Services (PwC Portugal, 2023)

The project was based on monitoring the performance of audit work at companies in the Industry & Services sector, namely auditing General Computer Controls (ITGC). The primary purpose of the ITGC is to assist the financial audit team in issuing financial reports by providing comfort about the application systems and the state of existing IT controls in the audited organization so that the financial audit team can understand whether they are comfortable with the financial statements documents that are generated by the client's IT systems. The financial audit team collaborates with the IT team throughout the audit process. In addition, after the audit process, companies can obtain legal certification of their internal environment, which must align with international standards and frameworks, such as ISO 27001[1] (for Information Security Management), COBIT[2] (for enterprise IT governance), and COSO[3]. The work's objective consisted of carrying out testing and analysis procedures for IT general controls and using other IT audit procedures to support the Financial Audit Team in assessing the risk of material misstatement of the accounts within the scope of the reporting process.

[1] ISO 27001 - International Organization for Standardization 27001 is the international standard and reference for information security management. The standard's general principle is the adoption by the organization of a set of requirements, processes, and controls to mitigate and adequately manage the organization's risk (*ISO 27001*, n.d.).

[2] COBIT - Control Objectives for Information and Related Technologies is a framework of good IT management and governance practices. Through the various resources it encompasses that can serve as a reference model for IT management, and based on the model, the management of information systems is approached from three main dimensions: IT processes, IT resources, and business requirements (Institute, 2007).

[3] COSO - Committee of Sponsoring Organizations of the Treadway Commission is a framework that evaluates the control environment and its effectiveness. It was created to help identify fraudulent financial reports, analyze the factors that can generate fraud in financial reports, and develop recommendations for organizations, auditors, and regulatory bodies (COSO, 2023).

To carry out this audit work, two PwC teams work together, namely, the Financial Audit Team and the Team of Information Systems Specialists (RAS team), so that it is possible to achieve the objectives set for the project.

To achieve the primary goal of the project, namely, the impact of IT audit work for clients, some intermediate steps (milestones) were followed, such as:

1. Training;
2. Participating in the information systems audit process;
3. Assessing the suitability of the information systems used in organizations;
4. Understanding the processes and activities of organizations;
5. Use of techniques for data analysis;
6. Contact with the work team of customers and internal;
7. Understanding of methodologies and internal tools;
8. Planning and time management;
9. Design and characterization of tests and evaluation procedures;
10. Execution of tests;
11. Evaluation procedures and analysis and evaluation of the conclusions.

These milestones provide a path to guide the fulfillment of the primary goal.

2. WORK PLAN

This chapter will focus mainly on defining the Project Work Plan. As such, all project phases and the tools and methodologies supporting its development will be succinctly described. Finally, the project chronogram will be presented, reflecting the phases, activities, milestones, and deliverables, contributing to better organization, planning, and project monitoring.

2.1. PROJECT MANAGEMENT

This project will have three phases: Project Set-up, Project Execution, and Project Evaluation. The first two phases will focus on the project's development and support its primary objective, the execution of an IT audit project for the external client. In the last phase of the project, the results obtained will be evaluated and discussed.

2.1.1. Phase 1: Project Set-up

The first phase consists of the Project Set-up, where the project scope will be defined. Therefore, it is necessary to analyze the company (PwC Portugal) and, more precisely, the department that will be the scope of the impact of the IT audit work for clients. Some intermediate steps (milestones) will be followed to achieve the project's primary goal.

In the second activity of this phase, the methodology that forms the basis for all audits carried out by PwC and the main tools used in this project will be presented.

The third activity of this phase, a collection of literature frameworks, is conducted to support the decision-making process during the project. In this stage, the most relevant subjects of IT Audit are analyzed, and the theoretical background is presented. This stage will be in continuous development in conjunction with the project itself since the outcome of this phase will endorse the decisions made during the project.

The last activity of this phase consists of intensive training on the practices that govern PwC internally, methodologies, and auditing tools. After intense training, another type of training is started, but more geared towards audit work, with integration into the project. It should be noted that training was an ongoing component throughout the project.

2.1.2. Phase 2: Project Execution

The second phase is where the project plan will be put into practice.

At the beginning of the execution phase, all activities that are part of the IT audit process and that precede the testing of Information Technology General Controls (ITGCs) will be covered, namely meetings with the client's Information Systems Department to know the processes, systems, and business activities, as well as the IT environment. Subsequently, the procedures for preparing and presenting requests for information and evidence necessary for the analyses will be described.

In the next activity of the execution phase, the ITGC domains for which the tests were carried out within the scope of the audit carried out for the client will be described.

Finally, the deficiencies found during the IT specialists' analyses will be reassessed, and recommendations from auditors will be presented. Additionally, the mechanism used to issue the final report of the IT audit project will be reported.

2.1.3. Phase 3: Project Evaluation

The last phase of the project will be carried out after all Project Execution stages have been completed to present an evaluation of the project.

To assist this evaluation, a survey will be prepared on the impact of the audit project on the client, and based on its results, it will be possible to discuss them and obtain conclusions.

2.2. METHODOLOGIES AND TOOLS

PwC, as an international network, has adopted a methodology that forms the basis for all audits carried out by PwC. The methodology is based on compliance with ISA[4] (International Standards on Auditing).

The PwC *Audit Guide* explains PwC's methodology and provides a common audit approach for all member firms in the PwC network. This is for each PwC member firm to understand the approach taken by other PwC firms in carrying out another firm's work or project. The PwC *Audit Guide* is designed to be flexible and scalable for all types of engagements.

This built-in guide, along with the additional tools that complement the methodology, provides insight into the development and documentation of each project.

The main tools developed by PwC and used in this project were:

- ***Connect*** - is a workflow tool that optimizes and monitors the flow of requests and information sharing between PwC and its clients during an audit. This tool enhances coordination and automated, real-time job status monitoring (PwC, 2023).
- ***Aura*** – is audit software used for all PwC audit engagements globally. This tool empowers audits to control, review, and report work progress and results (PwC, 2023).

[4] ISA - International Standards on Auditing, are professional standards used in carrying out audits, issued by the International Auditing and Assurance Standards Board (IAASB), to improve and standardize audit work to strengthen the general public's confidence in the work developed by auditing companies (IAASB, 2009b).

2.3. CHRONOGRAM

Figure 2.1 shows the planning of the general work stipulated for the project's development.

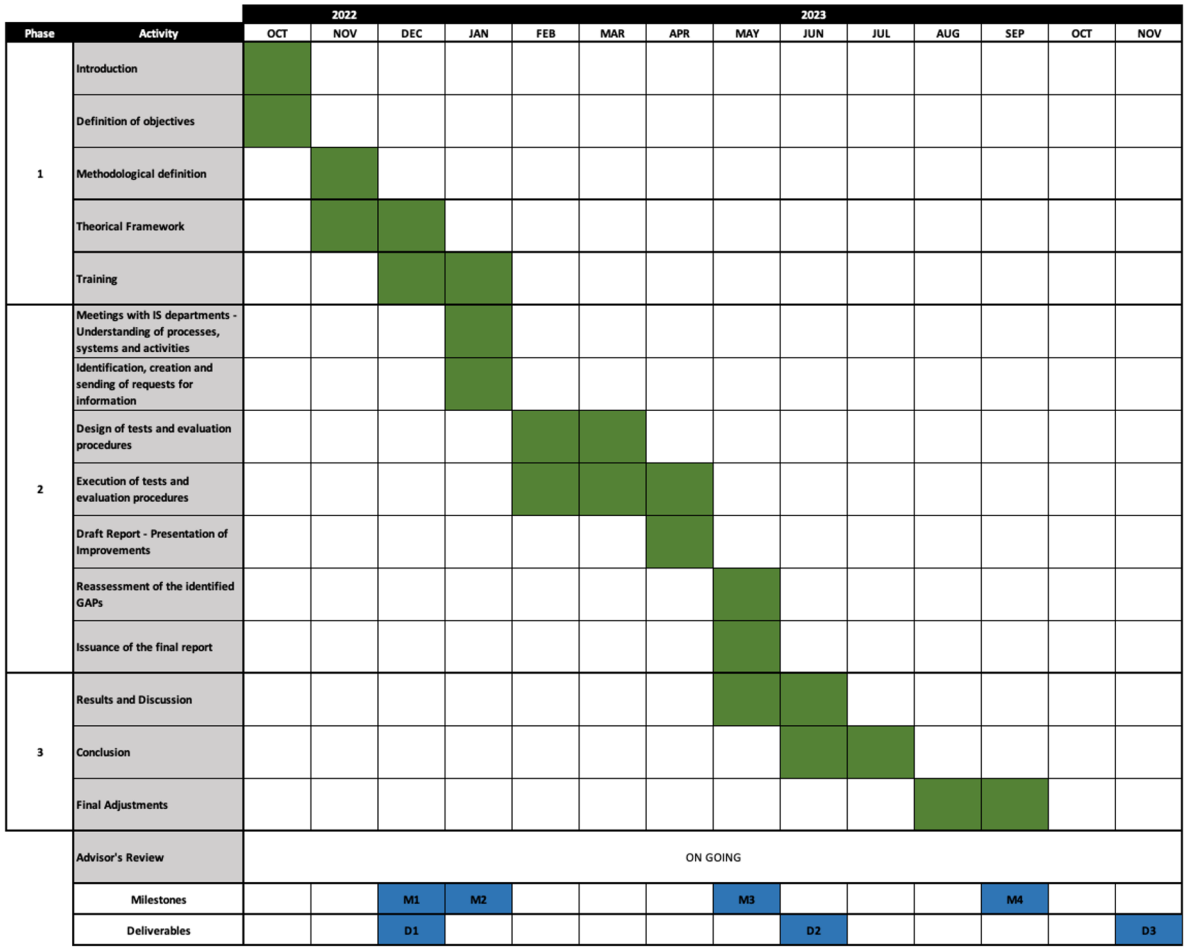

Figure 2.1 – Project Chronogram

Source: Prepared by the author

3. LITERATURE REVIEW

3.1. THE AUDIT PROCESS

Nowadays, information plays a fundamental role for companies, being considered one of their most important and strategic assets. Information is present in almost everything you do, and effectively managing the data from it is crucial in increasing competitiveness and growth in modern organizations. Companies need to understand the benefits associated with information management when making decisions that enable the delivery of products and services to customers (Evans & Price, 2016). However, it is essential to consider the risks associated with it, from reception, storage, use, consultation, and sharing. These risks can lead to sharing confidential information, server failures, or technical problems that prevent consultation or destroy relevant information (Ayinde & Omotayo, 2019).

Since information is an increasingly essential resource, it is natural for companies to invest in improving or acquiring new business applications, which allow them to differentiate themselves and improve their performance index, aiming to obtain a competitive advantage over companies competing in the market.

The former CTO of @WalmartLabs, Jeremy King (n.d.), once said, *"There used to be a big distinction between tech companies: those that develop enterprise technology for businesses and the global companies that depend on those products. But that distinction is now diminishing for this simple reason: every global company is becoming a tech company .... we're seeing technology as a critical component for business success."* (Pearlson et al., 2016). Companies increasingly use IS to manage their daily activities, and they are integrated with almost all aspects of the business. Some examples are real-time accounting systems, e-commerce platforms where financial information is disclosed, and accounting software that allows accounting processes to be carried out. Walmart is a technological company that used IS to build platforms that improved the worldwide e-commerce experience. Through the IS, it was possible to simplify organizational activities and processes, such as moving goods and stocking shelves, through devices that provide employees with real-time access to the store's inventories. In addition, IS enables the development of new search engines that improve the customer's online experience (Pearlson et al., 2016).

Allied to the use of technologies, there is a threat to information security in companies. The information results in data present in various systems, such as hardware, software, installations and physical security, users, access, authentication, and web communications, and with technological evolution, the security and reliability of data can be called into question. According to Dai & Vasarhelyi (2016), digital crimes affect companies' cybersecurity and data privacy, given the use of technology to steal large amounts of information without leaving evident traces. Therefore, corporations that benefit from technological advances reflected in the use of systems must be aware of the significant threats to the security and privacy of the information they represent (Alao & Gbolagade, 2019), given that the business

or even the survival of the company can be seriously conditioned the more significant the is dependence on the use of information systems.

All the risks associated with information systems can lead to adulteration of the information present in the financial reports of companies, which is why audits must be carried out that can provide confidence to the capital market participants so that the market works smoothly and efficiently (Kilgore et al., 2011).

The audit process can be defined as a formal inspection of an organization, verifying whether guidelines are applied and complied with their accurate records and whether the proposed efficiency and effectiveness goals are achieved (ISACA, 2015). Therefore, the main objective of performing an audit is to verify that the financial statements are free of distortion, which may arise due to fraud or errors, and that they are prepared following an adequate reporting structure (IAASB, 2009f).

Several steps must be fulfilled to do a correct audit job, and the International Standard on Auditing (ISA) must be considered (IAASB, 2009a). ISAs are professional standards used in carrying out financial audits issued by the International Auditing and Assurance Standards Board (IAASB) to improve and strengthen public confidence in the work carried out by auditing companies.

The first step is the planning phase, where it is necessary to establish the strategy that will be adopted in the audit process, define the scope, time, and objectives of the audit, as well as consider the results of previous audit work that may be relevant to consider when preparing the work. The planning phase is an iterative and ongoing process that often starts right after completing previous audit engagements and runs through to the end of the current audit engagement. However, certain activities must be carried out at the beginning of the work, such as risk assessment, understanding of legal issues, determining materiality, and the involvement of specialists (IAASB, 2009c).

The main benefits of this phase of the audit work are the help it gives the auditor to dedicate his focus to the most critical areas, properly organize the work to be carried out so that it is carried out effectively and efficiently, assist in the selection of members of most appropriate teams, as well as in determining the need for the use of specialists (IAASB, 2009c).

Both this stage and all the others must follow specific requirements demanded of the auditor, including ethical requirements that guarantee integrity, objectivity, professional competence, confidentiality, and professional behavior. It is also necessary to ensure that the auditor plans and performs the audit work with professional skepticism, consistently exercises professional judgment, and obtains appropriate and sufficient evidence to allow the auditor to draw reasonable conclusions to issue an opinion (IAASB, 2009a).

When obtaining evidence, it is necessary to pay attention to whether they are relevant and reliable for the audit, consider whether they meet the accuracy and completeness criteria,

and confirm whether they are accurate enough to be used in work. It is also necessary to select the items to be tested, with three means available to choose the number of items to be tested. If it is a small population or there is a high risk that cannot be mitigated with other evidence, it may make sense to look at the entire population (IAASB, 2009d). According to ISA 530, the population is the data set to be considered when selecting a sample that allows the auditor to draw conclusions (IAASB, 2009e).

However, there may be more effective methods than this form of testing, and therefore, the possibility of testing only specific items or a population sample is available (IAASB, 2009d). For any of the chosen forms of testing, one must evaluate which procedure(s) to carry out to analyze the evidence, which includes inspection, observation, confirmation, reperformance, recalculation, and carrying out analytical procedures. Another procedure is the questionnaire (inquiry), which should not be used in isolation but rather as a complement to other procedures (IAASB, 2009e).

After obtaining evidence, determining the items to be tested and the test procedure to be carried out, it is necessary to properly document the audit work carried out so that it is sufficient to allow an auditor who has not had contact with the work performed to understand the nature, period, scope and extent of the work performed, the evidence and results obtained and issues that have arisen during the work, as well as the professional judgments made to arrive at the conclusions of the work and the respective findings. It is also essential to document the characteristics of the tested items or subjects, who performed the work, the date on which they were completed, who reviewed the work, and when the review took place. The discussions held with management or other persons in charge of the audited entity on the significant points found during the work must also be documented (IAASB, 2009b).

3.2. INFORMATION SYSTEMS AUDIT

With all the technological advances, the auditing process has naturally been changing, as access to data is increasingly faster and more complex, causing significant modifications to the information recording procedure. Thus, the financial audit process requires auditors specializing in other areas. According to ISA 620, an expert auditor is an individual or organization with experience in areas other than accounting or auditing and whose work is used to obtain appropriate and sufficient evidence (IAASB, 2009a).

Here begins the role of the information systems auditor, or in other words, the IT specialist, who, in collaboration with the financial auditors, forms a team that aims to achieve the initially identified objectives. Since audited organizations use IT in financial and accounting practices, financial auditors should consider technology-based controls and their contribution to supporting internal financial controls (Stoel et al., 2012).

In the digital era, dependence on IT is increasing, and therefore, organizations are investing more and more in information security to ensure that information is appropriately protected.

Information security refers to managing access, safeguarding information from unauthorized access, or verifying the identity of those claiming authority to access information.

In addition, using IS allows the reduction of human errors and the improvement of business processes. However, it introduces risks to companies that must be overcome by implementing controls that protect information relevant to financial reporting. In this way, it is increasingly necessary for IT specialists to carry out tests on the technological environments of companies to guarantee that financial data are protected and that the vulnerabilities present in the systems cannot be exploited for the practice of fraud (Barta, 2018).

According to Sayana (2002), information systems auditing is a process of gathering and evaluating evidence to determine whether an IS safeguards assets and maintains data integrity. It enables the organization to achieve its objectives effectively and efficiently (Sayana & CISA, 2002).

To resume, a strong team between auditors and IT specialists brings benefits to audit work, as greater cooperation and information sharing increase the quality of the audit (Estep, 2021) to guarantee the availability, consistency, confidentiality, and integrity of the information. In addition, internal controls must be effective in providing comfort regarding the correct operation of business processes and controls that depend on IT, such as automatic controls, reports generated by a system, calculations performed by a system, security/segregation of functions and interfaces between systems, to mitigate the risk associate.

3.3. THE ROLE OF IT SPECIALIST IN FINANCIAL AUDIT

Carrying out a correct audit of relevant information systems from the perspective of financial auditing requires obtaining a good understanding of the company's IT environment, realizing which applications, IT infrastructure (network, operating systems, and databases), IT processes, and employees involved in these processes that the organization has available to support the business operation. In addition to this, it is also necessary to identify the main controls that the organization has implemented (IAASB, 2019).

This understanding is vital since there are risks associated with the use of information technologies that can lead to the processing of data inaccurately due to improper access, which can destroy data, obtaining inappropriate privileges, undue alterations of master data, occurrence of failures in changes or updates of applications and loss of data (IAASB, 2019).

To mitigate these risks, companies implement IT controls in their business processes. As risks are identified, it is up to the company to decide whether to assume the risk and not take any action or determine if it is justifiable to implement and develop specific controls to mitigate these risks. As such, it is necessary to ensure the effectiveness of the implemented controls, namely the general IT controls (ITGC).

We can define ITGCs as general IT controls that are applied to the IT processes of organizations, aiming to ensure that services, applications, operating systems, databases, and IT infrastructure provide adequate support to business processes. Implementing these controls is required by regulators for most companies and helps mitigate the risk of data theft or fraud (IAASB, 2019).

According to the IT Governance Institute, general IT controls are divided into four categories, which are Access to programs and data (1), Program changes (2), Computer operations (3), and Program development (4)(Institute, 2006).

As an organization's connectivity expands both internally and externally, the importance of controlling access to programs and data (1) grows ever more critical. The heightened risk of cyberattacks, malicious software, and unauthorized access attempts by current or former employees poses a significant threat to the integrity of both data and programs.

The controls incorporated within the program changes (2) category ensure the appropriate management of applications. As such, it becomes imperative to handle the continuous alterations required and implement new system versions effectively. This necessitates a strategic approach to managing the changes while ensuring that all updates are seamlessly integrated and the system functions optimally.

The computer operations (3) category controls are critical to ensure the smooth functioning of daily operations and the timely delivery of information services. To achieve this objective, it is necessary to define the operations that must be carried out, which include the acquisition, installations, configurations, integration, and maintenance of the IT infrastructure.

Lastly, in the program development category (4), the organization undertakes a comprehensive assessment to identify automated solutions that can be implemented. Additionally, the organization prepares requirements, tests, approvals, supervision, and risk assessments for any project related to acquiring or implementing new applications. These measures are essential in ensuring the smooth integration of new applications while mitigating any potential risks associated with the project.

Therefore, the main objectives of ITGCs are to ensure the integrity of the data and processes that the systems support. According to ISA 315, the most prominent ITGCs within companies are the following:

- **Backup and recovery controls:** ensure that financial reporting data is backed up as planned and that data can be recovered when needed;
- **Authentication controls:** ensures that a user accessing an application or other IT system does not use another user's login credentials;

- **Authorization controls:** allows the existence of segregation of functions, as it allows users to access only the information necessary to perform their tasks at work and nothing else;
- **Privileged access controls:** allow monitoring of accesses made by administrative users or with privileged powers;
- **Physical access controls:** validate/monitor physical access to the Data Center and hardware.

Suppose the ITGCs are not correctly implemented or are not operating effectively. In that case, the organization cannot have confidence in the controls to manage the risks inherent to its operation (Bellino et al., n.d.).

After analyzing the organization's controls and the IT environment, it is necessary to report the main conclusions of the audit work, validate the problems encountered with the customer, and develop action plans for their correction.

According to Otero (2018), conclusions are audit opinions based on factual evidence obtained and documented by the auditor as a result of the audit activity. Conclusions are documented in audit engagement documents and should support audit procedures performed during the auditable period. All evidence collected is essential to support the findings, conclusions, and recommendations indicated in the audit report.

Additionally, the recommendations are described as "*formal statements that describe a course of actions that should be implemented by the company's management to restore or provide accuracy, efficiency, or adequate control of audit subjects. A recommendation should be provided by the auditor for each audit finding for the report to be useful to management.*" (Otero, 2018).

4. PROJECT

The project was based on monitoring the performance of audit work at a company in the Industry & Services sector. It monitored all audit processes from their beginning to their conclusion. For security and data protection, the company's identification will remain anonymous.

The assignment's goal was to conduct comprehensive testing and analysis of IT general controls and utilize other IT audit procedures to assist the financial audit team in evaluating the potential for material misstatements of the accounts concerning the entity's financial reporting process.

To carry out this client's audit project, the IS audit was carried out following several activities, which constitute the three phases previously presented in the schedule:

- Carrying out intensive training, which precedes the start of the project;
- Identified IT dependencies and definition of the application scope, and testing strategy in order to test IT dependencies;
- Execution of design and operability tests of the planned controls;
- The evaluation and execution of additional audit procedures to validate whether the risk inherent to the identified controls was mitigated and
- Reporting and job completion.

The IT team for the project comprises a manager, a senior member, and an associate. The manager oversees the planning and coordination, while the senior member oversees the distribution and accessibility of tasks for development among the team members, including the associate. They consider the expertise of each team member to ensure that tasks are allocated optimally. Most of the time, work priorities are defined in agreement with the client so that both sides are in tune.

As we saw earlier, this project comprises three significant phases described in depth in this chapter. An organizational context will be introduced before focusing on a project by itself.

4.1. PROJECT SET-UP

4.1.1. Organization Context

PwC, a multinational consulting and auditing firm, was formed in London in 1998 through the merger of Price Waterhouse and Coopers & Lybrand. In 2010, the PwC brand was officially established, though its legal name remains PricewaterhouseCoopers. With a presence in 152 countries and over 328,000 employees, PwC offers financial auditing, information systems auditing, financial and IT consulting, and taxation services (PwC, 2023).

PwC has been operating in Portugal for over 60 years, and its structure includes firms in Cape Verde and Angola. The group of companies currently has 58 partners and more than 2,000 employees across offices in Lisbon, Porto, Coimbra, Funchal, Luanda, and Cidade da Praia. PricewaterhouseCoopers Digital Technology Consulting, lda, which provides information technology consultancy services, is also part of the PwC network and operates in Portugal (PwC, 2023).

Figure 4.1 describes the values that characterize PwC Portugal.

Figure 4.1 – PwC Values (PwC Portugal, 2023)

4.1.2. Training

At PwC, whenever a new employee is hired to join a project, a series of training sessions are carried out prior to the start of the project. The training period is a continuous process and consists of three phases.

During the initial phase, we focused on topics about good behavioral, ethical, and moral practices. We covered various topics such as professional skepticism, which refers to the questioning attitude and critical assessment of evidence; independence, which is the ability to maintain impartiality and objectivity; confidentiality, which stresses the importance of privacy and keeping sensitive information secure; and ethics, which encompasses the principles and values that govern decision-making and behavior.

In the intermediate phase of the training program, the company opted for online training, also referred to as *e-learning*, to provide a comprehensive understanding of auditing-related topics. The trainers provided extensive explanations of the company's methodology and tools used in auditing. This phase aimed to complement the earlier training phase and equip trainees with the skills and knowledge required to conduct successful audits.

In the last training program phase, the focus shifted toward the RAS department. The training sessions were designed to provide a comprehensive understanding of the methodology used in audit projects where RAS elements are involved as IT specialists. In addition, the training covered some fundamental topics that are crucial for the successful realization of projects.

As a supplement to their initial training, PwC provides a valuable resource for their auditors called the *Audit Guide*. This platform serves as a guide for their audit work, offering a wealth of information on the methodology used by the company.

4.2. PROJECT EXECUTION

4.2.1. On-The-Job-Training

Following the initial theoretical training, the practical phase commences with the On-The-Job Training, where the team is gradually immersed in the information systems audit project. During this phase, the team is briefed on the client's background and the work completed by the preceding team, including the insights gained and tasks accomplished.

After gathering all relevant client information, the RAS and financial audit teams conducted internal meetings to plan the audit project's activities. This planning phase involved outlining the action plans, determining the scope of applications, identifying ITGC domains to test, and pinpointing IT dependencies that required control testing.

Subsequent to this, preliminary meetings were held with the customer's Information Systems Department (DSI) and Security Department (DS) to establish a common understanding of the project goals, including deadlines. After the discussion, concise meeting minutes were created to guarantee that no critical details were overlooked.

After aligning the work and discussing the relevant dates, the preparation and submission of requests for information and necessary evidence followed. To this end, a survey was carried out of the information needed to obtain a good understanding of the client's IT environment and the evidence necessary to respond to the analyses of controls to be carried out in the various domains within the scope of the work.

Based on this information, a list of requests was created that can be divided into the following categories:

- **General requests**, such as lists of collaborators, the organization's organization chart, and contracts entered into with suppliers;
- **Access management** is used to obtain information regarding granting, removing, and reviewing access and security issues such as password settings and privileged access.
- **Change management**, in order to obtain information regarding the changes made to applications, databases, and operating systems in scope;

- **Operations management**, in order to obtain information regarding the operations carried out on the systems, such as evidence of the performance and monitoring of backups and system jobs, as well as procedures and policies for managing incidents and business continuity;

This order list was later inserted into the *Connect* platform and shared with the customer's interlocutors to make the exchange of information more accessible.

Between sending requests for information and collecting evidence from the client, the assistant associate was responsible for preparing the *Aura* database to document the project work.

4.2.2. Execution of tests to controls

After receiving the requested evidence and information, it was necessary to select the items to be tested, deciding for each test whether to analyze the entire population or just a sample.

To define the sample, it was first necessary to determine the population to be tested. The population is defined by a set of data from which we select our sample and about which we wish to draw conclusions.

Factors to consider when determining populations for testing include:

- The frequency of exercise of control by the entity during the period;
- The period during the audit period that the auditor is confident in the operational effectiveness of the control;
- The relevance and reliability of the audit evidence to be obtained on the operational effectiveness of control at the assertion level and
- Each item needs to have an opportunity to be selected.

After ensuring that the population we will use for sample selection is complete and the most appropriate, it is possible to select the sample.

The sample selection method can be carried out in the following ways:

- **Haphazard:** selecting a judiciously representative sample without relying on a truly random process. It does not mean without thought or effort. Instead, it means that sample items must be selected without any conscious bias (that is, without any particular reason for including or omitting items from the sample);
- **Random:** method that guarantees that all items in the population have the same chance of being selected. To select randomly, we can use tables of random

numbers, random numbers generated in software such as *Microsoft Excel*, or random selection offered by sampling software or *Microsoft Excel*; or

- **Systematic:** method of selecting a sample using every nth item. A sampling interval is established based on the number of items without reference to the size or monetary value of the item. Systematic selection is only appropriate when the characteristics of interest are randomly distributed throughout the population.

In the case of the project presented, it followed a *Haphazard* sample selection method.

The company's IT infrastructure data has been meticulously documented in the Aura database. This comprehensive database encompasses crucial information, including the customer's IT department, IT management policies, vendor management, internal control functions, key attributes of the systems scope, access management, change management, and business continuity.

Subsequently, tests were carried out on the controls for the ITGC domains of *Program Changes*, *Access to Programs* and *Data,* and *Computer Operations*.

4.2.2.1. Program Changes

The objective of this domain is to ensure that changes to programs and related infrastructure components are requested, authorized, executed, tested, and implemented to achieve application management control objectives.

In this domain, the following tests were carried out:

- Test if the changes made to applications, databases, network, and configurations were correctly tested and approved before moving to the production environment;
- Test the existing control regarding changes processed in the systems during the year 2023 and are periodically monitored for adequacy;
- Test if there is a correct segregation of environments (development, testing, and production);
- Test existing control over access to the production environment and whether it is restricted to authorized IT people and
- Test whether direct changes to data or database structure are avoided.

Carrying out these tests made it possible to verify whether the change management procedure and associated controls are operational to mitigate the risk of undue changes to the applications in scope.

Documents relating to the change management process were requested to perform these tests and analyze the control design. A sample of changes made to the client's systems was then selected to validate whether the process was being followed, namely whether there was formalized approval for the development of changes, tests in a test environment, and approvals to carry out the transfer to production.

In cases where non-compliance with the process defined by the company was found, understanding meetings were held with the client's information systems department, and the deficiencies found were subsequently documented.

4.2.2.2. Access to Program and Data

The purpose of this domain is to ensure that only authorized access is granted to programs and data upon authentication of a user's identity. Controls over access to programs and data include the processes used by the entity to add, delete, and change users (both business users and IT personnel) and their related access rights following the control objectives established in the audit design (i.e., to achieve the entity's objectives for appropriately restricted access and segregation of duties).

In this domain, the following tests were carried out:

- Test existing controls regarding the granting of access that makes it possible to verify that requests for access to applications, databases, and operating systems are duly analyzed and authorized by the administration;
- Test existing controls regarding the removal of access that makes it possible to verify that the access rights of the closed application, database, and operating system user are removed promptly;
- Test existing controls regarding access review that allow checking whether access rights to applications, databases, and operating systems are periodically monitored for adequacy;
- Test existing controls on monitoring activities carried out by users with privileged access to the covered systems;
- Test the existence of Sensitive Access (SA)/Segregation of Duties (SoD); and
- Test whether password settings for applications, databases, and operating systems align with the customer-defined password policy and best practices.

Before testing these controls, it is essential to consider the risks associated with them to understand the impact of testing the controls, namely:

- The possibility of end users of the application, database, and operating system ignoring the authorization imposed by the systems and segregation of duties controls;
- The possibility of superusers ignoring the authorization imposed by the systems and segregation of duties controls, and
- Weak authentication controls or security configurations allow access rights to be bypassed.

By conducting these tests, it was possible to ascertain the efficacy of the implemented controls in this area. We sought to determine whether there was any potential for unauthorized access to the systems within scope, which could lead to the processing of inaccurate and invalid information. Furthermore, we assessed the presence of privileged accesses and ensured that they were solely granted to key users for the necessary performance of their assigned functions. We also confirmed whether the management of generic accounts was being carried out correctly, checking the existence of a generic inventory where it was possible to identify the function of the profile accessed and the person responsible for each account to validate adequate segregation of functions.

To conduct the required tests, we thoroughly reviewed the company's information security policy and other policies related to account naming conventions, access authorization, access review, password policies, and removal of access. Once these documents were analyzed, we provided a detailed evaluation of the control design and proceeded to perform tests based on the evidence we gathered. This evidence included a list of system users, which allowed us to verify access grant and removal dates and profile associations to determine the proper assignment of privileged access and segregation of duties. Additionally, we examined the list of employee departures for 2023 to ensure that no former employees maintained active access.

As the final step, we thoroughly analyzed the password configurations across various systems. The primary objective of this analysis was to validate the alignment of the configured parameters with the parameters outlined in the password policy and industry best practices.

4.2.2.3. Computer Operations

The objective of this domain is to ensure that systems process information completely and accurately and that processing problems are identified and resolved entirely and accurately to maintain the integrity of financial data.

In this domain, the following tests were carried out:

- Test whether access to creating or changing routines is restricted to those responsible;

- Test whether there is a data backup policy and processes and whether there is any consistent data recovery process or activity;
- Test whether the execution of routines in the environment and corresponding status are registered and monitored periodically;
- Ensure that the creation/change of access to the data center and restricted areas is granted after approval to guarantee physical security conditions in backup storage locations and
- Test whether the review of access to restricted areas is carried out.

Before testing these controls, it is essential to consider the risks associated with them to understand the impact of testing the controls, namely:

- The possibility of incorrectly changed routines due to unauthorized access to create or change routines;
- The possibility that information may be lost (for example, due to system failure) and the data may not be recoverable or may be corrupted in the recovery process, and
- The existence of unauthorized or improper access to the data center and restricted areas.

These tests have helped us verify how customers respond to incidents or disasters that could disrupt business operations. It is essential to ensure that the company adheres to the implemented regulations, follows the established international standards, and tests the ability to recover data when needed.

To conduct these tests, the information systems department was tasked with supplying the protocols for scheduling, executing, and monitoring processes that ensure the uninterrupted operation of the company's systems. Upon examining these protocols, an evaluation was provided regarding their efficacy. Subsequently, tests were conducted to scrutinize the defined backup schedule, confirming that they were executed without errors on the expected dates and accurately stored.

In addition, the evidence for backup monitoring was examined, and the detection and correction of any backup errors were requested to ensure maximum safety and security of the company's information systems.

4.2.2.4. Reassessment of the identified gaps

During the entire IT audit project, it was necessary to hold several meetings with the client to improve the understanding of the company's IT environment or to clarify doubts or deficiencies identified by the team during the execution of the tests.

As a rule, whenever analyses of control tests are completed, and inconsistencies are identified between what was being practiced and correct practice, mitigating procedures are carried out to check whether the risk has been mitigated. Therefore, after completing the execution of the defined controls, a draft report was prepared by the IT audit team with identified gaps, where the results obtained in the audit were shared for subsequent remediation by the client. In this process, it was agreed with the client that whenever each identified gap was reassessed and corrected, evidence would be sent to the audit team with documentary support through the *Connect* platform. To this end, the client was asked for various justifications, and additional analyses were carried out to better understand the existing risk and its impact on the financial reporting items.

Some deficiencies identified during the IT audit project were low-risk regarding the various systems' information security policy and password security configurations.

Regarding the information security policy document, the description of password parameterization needed to be identified, and it was found that the document was last reviewed in the three years preceding the audit. The lack of standardization of IT processes constitutes a risk, so its impact may involve incorrect management and increased exposure to more risks.

Regarding password configuration, it was found that the applications in scope did not have a complete and defined password parameterization, with the minimum character limit being just six. This constitutes a risk, as it contributes to undue access and alterations to sensitive or confidential information.

On the other hand, more impactful deficiencies with greater aggregate risk were also identified. The first deficiency identified was related to the review of accesses, where the implementation of a procedure for reviewing accesses and network profiles, applications in scope, and production database still needed to be identified. Several impacts are associated with this deficiency, such as undue access, changes to sensitive or confidential information, and profiles not being approved and reviewed.

Another deficiency identified was related to the revocation of access to a system in scope, where after carrying out a comparison analysis between the list of outputs and the list of active users in the same fiscal year, nine employees were identified with active access after the date of your exit. One of the impacts of this deficiency is related to improper access, changes, or transactions to sensitive or confidential information.

The last deficiency identified concerns about profiles with extended access in one of the systems in scope. After analyzing users with extended access profiles in the system, it was found that they were known to the client management and were authorized correctly. However, access to profiles assigned to external consultants in the production system was identified, and the client did not monitor their activities, which could expose the company to a high risk. The impact of this deficiency will be related to the lack of control or insufficient

segregation of duties, as well as undue access and alterations to sensitive or confidential information.

Most of the deficiencies identified are still being remedied. For all deficiencies the RAS team could not mitigate, the financial audit team was informed about the issue and conducted additional analyses of the company's accounts.

4.2.3. The work completion meetings

After completing all the design and operational effectiveness tests of the controls implemented by the client, keeping all the documentation that supported the tests, and analyzing all the evidence provided by the client, meetings were held between the members of the risk assurance team to discuss the results and conclusions obtained from the project. Subsequently, the results and deficiencies in the identified controls were communicated to the financial audit team so that they could analyze the need to carry out additional procedures.

A draft report was then prepared with the deficiencies found in the execution phase, which was shared with the client. After sharing this report with the client, meetings were held to clarify doubts about the deficiencies so that they were clear to the client so that they could develop corrective measures to respond to the deficiencies found.

Finally, a final report was prepared and issued for the audited fiscal year. This report included the changes that resulted from the meetings and corrective measures designed by the client, as well as a presentation of the client's IT environment, the objectives of the IT audit project for the client, the organization chart of the Information Systems department, the descriptive of all processes that constituted the audit work and all controls adopted to protect the service provided to the client, including the auditor's testing procedures and the results of each control.

Additionally, the final report reflected all the deficiencies identified during the execution of the tests that did not undergo immediate corrective measures, and the impact and associated risk of each identified deficiency were described, as well as recommendations suggested by IT specialists.

4.2.4. IT Specialist Recommendations

Considering the deficiencies raised, recommendations were suggested by IT auditors so that the risks associated with them are mitigated and do not arise in the next year of the audit project.

The following recommendations in the final report are made:

- Regarding the information security policy, it was recommended that the definitions of password requirements to be adopted in applications, databases,

and networks be included in a formal document and periodically reviewed, as well as their disclosure;

- When configuring the password, it was suggested to standardize the security policies established by the company, which should be implemented in all systems considered critical. The following recommendations were suggested for password security: a minimum length of 12 characters, a maximum expiration period of 42 days, disallowance of reusing the last five passwords, implementation of password complexity controls (such as the use of alphabetic and numeric characters), and blocking of profiles after three unsuccessful attempts;
- Regarding access review, it was recommended to implement periodic control to review network access and profiles, applications, and respective databases. In this review, key users from the business area must be considered to evaluate functions, and the segregation of functions within the application itself must be evaluated. Additionally, during the execution of the control, it was recommended that information extraction procedures be formalized (e.g., screenshots of the filters in the reports or queries used) and that, after the review is completed, its results be formalized;
- Regarding the revocation of accesses, it was suggested that the accesses be removed and, additionally, the need to implement compensatory control be assessed to ensure that all accesses are properly deleted and
- Regarding extended access, it was suggested that access be granted according to the employee's role and responsibility. In case of exceptions, it was recommended to implement a compensatory control to review the activities carried out by the employee while having extended profiles.

5. PROJECT EVALUATION: RESULTS AND DISCUSSION

To evaluate the impact of the IT audit project on the external client, a survey was carried out among four people, three of whom had different positions within the Information Systems Department.

The "The impact of IT Audit work" questionnaire had five questions, four of which were mandatory answers, with different types of answers (multiple choice, single choice, and open response).

Of the total number of questions that made up the survey, three of them were designed to understand the feedback from individuals on the impact of the IT audit on their team, and one of them was created for the team that carried out the IT audit project to receive suggestions from the client for improvement in their work, and the remaining question was designed to identify the function of the individual who responded to the survey (see Appendix A).

5.1. SURVEY: PERSONAL CATEGORIZATION ANALYSIS

The questionnaire was answered by four people belonging to three different teams from the external client's Information Systems department, namely:

- Information Systems Directorate;
- Control and Management Systems Core;
- Enterprise Application Service.

As we can see in Figure 5.1, the number of responses obtained allows us to identify the team to which each participant who responded to the survey belongs, with one response from the IS Department (corresponding to 25%), one response from the Control and Management Systems Core (corresponds to 25%) and two responses from the Enterprise Application Service team (corresponds to 50%).

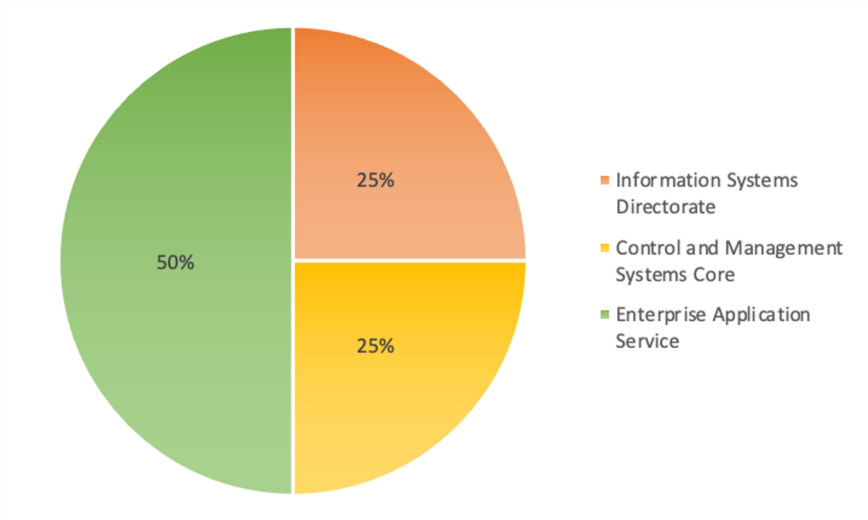

Figure 5.1 – Responses per team

Source: Prepared by the author

The number of responses per team can be explained by each team's impact and interaction with IT analysts during the audit project.

The Enterprise Application Services team represents the largest group of responses, as it is responsible for all application management, namely four applications audited during the project, through which it is possible to test general IT controls (ITGCs) and subsequently identify deficiencies in control.

In the case of the Control and Management Systems Core, we only obtained one response, as the interaction with audit work is more focused on IT environment issues rather than precisely testing ITGCs. These are complementary analyses carried out by the team of IT analysts on: access management policies; information security policies; password parameterization policies; validation of information about IT infrastructure (applications, interfaces...); the tools used to monitor networks, control internal and external traffic, and due and improper access; the IS department organizational chart; and the tools used to protect against viruses. In this team, only two people were directly involved in the project, and only one was selected to answer the survey.

The last level of response is consistent with the importance of IT audit work because the input of the manager of the Information System Department is vital to ensure that IT audits are appropriately integrated into a project, addressing IT-related risks and contributing to its success.

Regarding the roles performed by the individuals who responded to the questionnaire, it is possible to see in Figure 5.2 the distribution of roles by team.

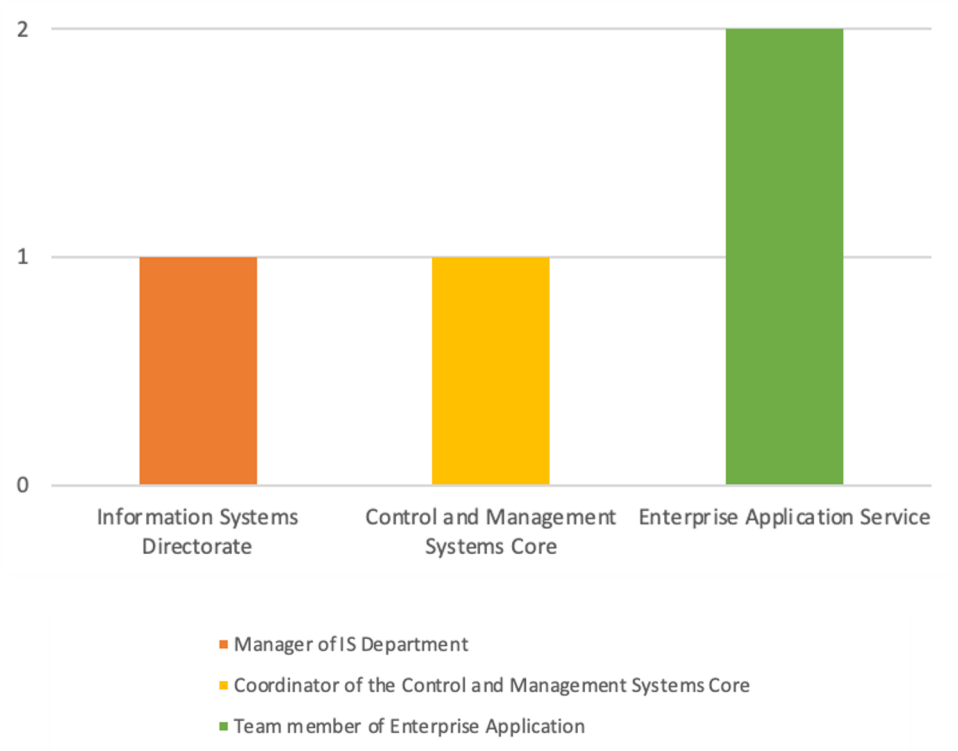

Figure 5.2 – Distribution of roles per team

Source: Prepared by the author

Through Figure 5.2, it is possible to understand that within each team involved in the IT audit project, there is a person responsible for a different position - Manager, Coordinator, and Team Member - represented in the survey. With this type of feedback, it is possible to understand the IT audit work's impact from the management to the execution level.

5.2. Survey: Analysis of IT Audit Work Impact

To determine the impact that the work of an IT audit has on the audited client, namely the information systems team, the following questions were prepared:

1. *How important and useful do you believe IT Audit works are for your team?*
2. *What are the benefits of IT Audit work?*
3. *Do you consider that the work carried on fulfilled its main purpose? (Identify risks, vulnerabilities, and opportunities for improvement, helping to maintain the integrity of the IT environment, safeguard data, and meet regulatory requirements,...)*

Regarding the first question, presented in Figure 5.3, the answers were unanimous, as all individuals who responded to the questionnaire considered that carrying out an IT audit

project was very important for their teams, so with these answers, it is possible to conclude that the audit work was useful.

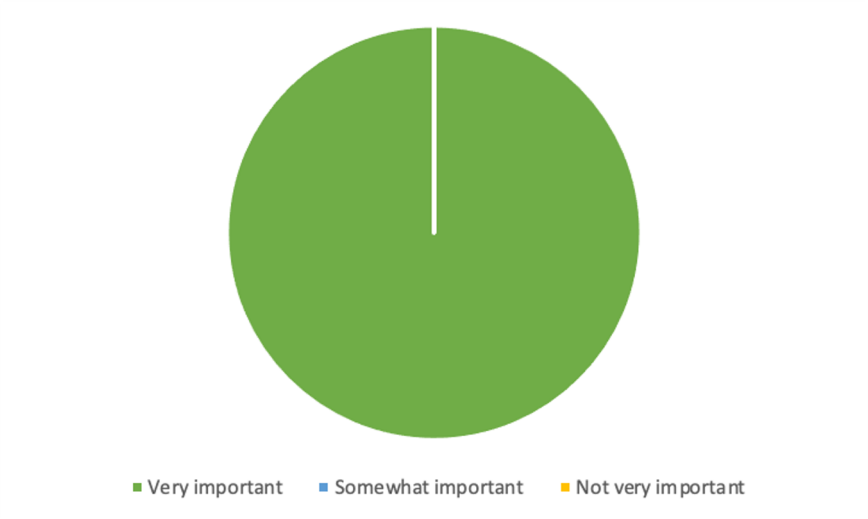

Figure 5.3 – Distribution of Q1 answer

Source: Prepared by the author

Given the results obtained in the first question, it was helpful to understand how the IT audit work was beneficial for everyone involved in the survey.

Figure 5.4 shows the results obtained for the second question, and it is possible to conclude that the answers were also unanimous, as all participants considered the improvement of security, risk mitigation, and compliance assurance as benefits of the audit work. Furthermore, three individuals considered data integrity a benefit of IT analysis projects; one thought of cost savings as another benefit, and one assumed that audit work is advantageous as it contributes to increasing your customers' trust.

Figure 5.4 – Distribution of Q2 answer

Source: Prepared by the author

It is also essential to analyze the answers to this question by role, as it will allow us to understand the benefits of IT audit work both at a management and operational level and to have a general perception of the project's relevance for the participants' teams.

With Figure 5.5, it is possible to check the answers given by each function and draw conclusions regarding the IT audit project's impact on their teams.

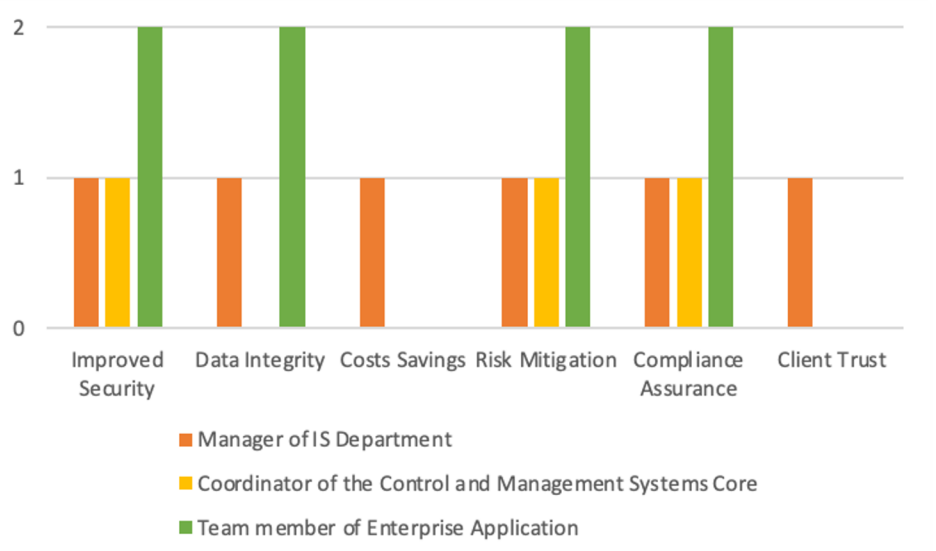

Figure 5.5 – Distribution of Q2 answer per role

Source: Prepared by the author

In this analysis, it is possible to analyze the choices of benefits of IT audit work by role: Manager of the IS Department, Coordinator of the Control and Management Systems Core, and Team member of Enterprise Application. This way, it is possible to compare different perspectives on the project's impact developed for each of those involved in the survey, given that each represents a different position within the IS department.

As previously presented, all participants considered that the IT audit project contributes to adopting a security posture toward protecting their systems and data, so it is possible to conclude that there is unanimity between the three positions on this matter. Risk mitigation and compliance assurance were also recognized as unanimous benefits, as participants recognize that IT auditing can identify risks that lead to potential disasters or monetary losses and ensure compliance with regulations and legislation to avoid possible penalties.

Data integrity was recognized as a benefit for the members of the Enterprise Application team and the IS Department Manager, compared to the Control and Management Systems Core coordinator, who did not consider data integrity to benefit the IT audit. Considering that the audit projects were deemed beneficial to improving security and mitigating risk, the integrity of the data must, therefore, be implicit, as risk may be associated if the data is unreliable. This discrepancy in responses may be because the analyses carried out on the IT environment, in which the Control and Management Systems Core team is involved, focus not on the theme of data integrity but on legislation and security policies.

Another significant discrepancy between the three roles was regarding the benefits of cost saving and client trust, as only the IS department manager considered that these benefits were achieved with the IT audit project. This inconsistency may be related to the fact that these are topics more related to management rather than precisely to execution. For a manager, these topics are crucial and therefore, consider audit work to be impactful, as it contributes to the use of IT resources more efficiently, which allows IT expenses to be reduced, as well as contributing to increasing trust from your customers if they know that the company goes through audit processes.

In conclusion, although the majority of benefits were considered relevant by survey participants, the importance of some benefits differs depending on the impact and usefulness of each position.

Finally, the third question aimed to understand whether individuals considered that the IT audit work fulfilled its primary objectives, such as identifying risks, vulnerabilities, and opportunities for improvement, helping to maintain the integrity of the IT environment, safeguarding data, meeting regulatory requirements or others mentioned throughout the project. In Figure 5.6, it is possible to conclude that all participants considered that the purpose was achieved. Therefore, the audit project had the expected impact.

Figure 5.6 – Distribution of Q3 answer

Source: Prepared by the author

5.3. SURVEY: SUGGESTED IMPROVEMENTS FOR THE IT AUDIT PROJECT

With the aim of the IT audit team having more detailed feedback on suggestions for improvement in their project, an open and non-obligatory question was prepared for the survey on this topic, entitled *"What improvements or enhancements would you like to see in the process of IT Audit project?"*.

Of the four participants involved in the survey, only two responded to the open-ended question, one belonging to the Control and Management Systems Core and the other to the Enterprise Applications Service.

The coordinator of the Control and Management Systems Core suggested as an improvement, *"A criterion must be established at the beginning of the audit project in which those responsible for each application must assume responsibility for all requests related to that application, even if they are not to provide the information requested by the auditors. This avoids confusion when exchanging information, with those responsible for the applications forwarding the request to the person on the correct team who must respond."*.

This improvement suggestion is related to the feedback cycle on the *Connect* platform, which, as explained previously in the project, is a platform that allows the request and sharing of information between PwC and the client during an audit. At the beginning of an audit, a website is created on the *Connect* platform for the audit project that will be developed for the client, and several requests are subsequently created by the auditors for different analyzes and to which the appropriate responsibility on the part of the client is associated and must provide the requested information. This issue caused some alarm during the project, as the individuals assigned to the orders were not always responsible for them, making it difficult to

exchange information at the beginning of the project. For this situation to be avoidable, we consider the suggestion for improvement provided by the customer to be valuable and constructive.

The Enterprise Applications Service team suggested another improvement opportunity, which was also related to communication between the client and the auditor on the *Connect* platform. As a suggestion for improvement, he mentioned that *"It is essential that all requests have clear and highly detailed language in their description about what is being requested and, if possible, in cases most likely to cause doubts, files should be attached to the requests with examples of what should be provided.".*

This suggestion for improvement is related to enhanced communication since doubts often arise from the client about what is being requested by the auditor during the IT audit project, which leads to the exchange of wrong or incomplete information. Another reason for this situation may be related to the fact that the individual assigned to the request is not responsible for providing the requested documentation. As this topic has already been the focus of attention on the part of auditors, we consider the client's improvement suggestion to be relevant.

In conclusion, with this survey, it was possible to recognize that the IT audit work positively impacted all individuals, as everyone considered several benefits in carrying it out. Additionally, the audit team could understand from the client what aspects they should pay attention to and improve in the future, namely the communication exchange on the *Connect* platform.

6. CONCLUSIONS

6.1. SYNTHESIS OF THE DEVELOPED WORK

This project was developed in the Risk Assurance department at PwC Portugal, where it was possible to practically carry out an IT audit for an external client in the Industry & Services sector.

The project consisted of three phases, with the main focus in the first phase being to invest in the training of team members involved in the IT audit project, the second phase comprised the execution of the project itself, and the last phase carrying out a questionnaire to the audited client to receive more detailed feedback on the impact the project had, as well as which aspects should be improved in the future.

By carrying out this project, it was possible to understand the impact of the work of IT specialists when carrying out financial audits. This is because financial reports are issued through various information systems, and given the risks they entail, it is necessary to audit the IT systems. Additionally, this project allows us to have a more comprehensive view of the IT auditor's work, as in addition to supporting financial teams, it is mainly fundamental to improving the information systems of audited clients and consequently improving the quality of the audits carried out.

The project was based on good practices and methodologies, with the ISA (International Standards on Auditing) essential to ensuring high-quality IT audit work.

To aid the financial audit work, the IT specialist team performed several tests in the different ITCCs (General Information Technology Control) domains to ensure the controls were working correctly. Given the importance of correctly managing access to information to ensure that there are no distortions in financial items and the risk associated with improper access to data and programs that could compromise their integrity, the most impactful area of the audit project was *Access to Programs and Data*.

The execution of the ITGCs tests was also crucial from a personal point of view, as they allowed me, as a member of the project team, to acquire various knowledge, which allowed me to gradually build a critical approach in identifying and evaluating the risks associated with the information generated by the systems information, particularly in the Industry & Services sector.

In addition, participation in this project made it possible to monitor the various stages of an IT audit and acquire a holistic view of the client's industry sector.

Overall, the project fulfilled its main objective, adding value to the financial audit team and the audited client.

6.2. LIMITATIONS AND RECOMMENDATIONS FOR FUTURE WORK

This project highlights the potential for additional improvements. It presents some limitations, so it is essential to mention the prospect that it will continue to be carried out in the next auditable year, in which additional analyses will be developed.

The main limitations of the project are related to its evaluation of the impact. They are reflected in the need for more availability of the client, specifically those responsible for the Information Systems department, to collaborate on the prepared questionnaire. For more reliable and authentic results, the questionnaire could have been carried out to more people from different teams in the department and possibly extended to a more in-depth study.

Another limitation is that both PwC and the client that was audited by IT specialists, according to the terms of confidentiality and data privacy they apply internally, did not allow the sharing of documents and more precise and in-depth information about the context and controls carried out. This information would have helped mainly in the illustrative part of the project.

As a recommendation for future work, we highlight the perspective of specializing communication between auditors and the client, as it would be interesting to develop solutions that facilitate the exchange of information while providing IT audit services.

It would be interesting to delve deeper into this topic applied to a real context, in which the creation of a program that identifies the client, the applications in scope, and the IT dependencies, and consequently, can generate templates that would be imported into the *Connect* and *Aura* platforms. In the first platform, a template document would be imported with all relevant requests for each ITGC domain, and those responsible for the requests would also be identified based on information from previous audited years. This would contribute to the accuracy of the information requested and the exchange of information between people.

In the *Aura* platform, a template document would also be imported with the procedures for carrying out the tests and documentation of the test results, which would be edited whenever necessary. This would facilitate the accuracy of documenting the work carried out and save time for the internal team of auditors.

BIBLIOGRAPHICAL REFERENCES

Alao, B. B., & Gbolagade, O. L. (2019). *An Assessment of How Industry 4.0 Technology is Transforming Audit Landscape and Business Models.* (SSRN Scholarly Paper 3512124). https://papers.ssrn.com/abstract=3512124

Ayinde, L., & Omotayo, F. (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review*, *36*. https://doi.org/10.1177/0266382119831458

Barta, G. (2018). The increasing role of it auditors in financial audit: Risks and intelligent answers. *Business, Management and Education*, *16*, 81–93. https://doi.org/10.3846/bme.2018.2142

Bellino, C., Wells, J., Hunt, S., & Llp, C. H. (n.d.). *Global Technology Audit Guide (GTAG) 8: Auditing Application Controls*.

COSO. (2023). *About Us*. COSO. https://www.coso.org/about-us

Dai, J., & Vasarhelyi, M. A. (2016). Imagineering Audit 4.0. *Journal of Emerging Technologies in Accounting*, *13*(1), 1–15. https://doi.org/10.2308/jeta-10494

Estep, C. (2021). *Auditor Integration of IT Specialist Input on Internal Control Issues: How a Weaker Team Identity Can Be Beneficial* (SSRN Scholarly Paper 2980792). https://doi.org/10.2139/ssrn.2980792

Evans, N., & Price, J. (2016). Enterprise information asset management: The roles and responsibilities of executive boards. *Knowledge Management Research & Practice*, *14*(3), 353–361. https://doi.org/10.1057/kmrp.2014.39

IAASB. (2009a). *International Standard on Auditing 620: Using the Work of An Auditor's Expert*.https://www.ifac.org/_flysystem/azure-private/publications/files/A035%202013%20IAASB%20Handbook%20ISA%20620.pdf

IAASB. (2009b). *International Standard on Auditing 230: Audit Documentation*. https://www.ifac.org/_flysystem/azure-private/publications/files/A012%202012%20IAASB%20Handbook%20ISA%20230.pdf

IAASB. (2009c). *International Standard on Auditing 300: Planning an Audit of Financial Statements*.https://www.ifac.org/_flysystem/azure-private/publications/files/A016%202013%20IAASB%20Handbook%20ISA%20300.pdf

IAASB. (2009d). *International Standard on Auditing 500: Audit Evidence*. https://www.ifac.org/_flysystem/azure-private/publications/files/A023%202012%20IAASB%20Handbook%20ISA%20500.pdf

IAASB. (2009e). *International Standard on Auditing 530: Audit Sampling*. https://www.ifac.org/_flysystem/azure-private/publications/files/A028%202012%20IAASB%20Handbook%20ISA%20530.pdf

IAASB. (2009f). *International Standards on Auditing 200: Overall Objectives of The Independent Auditor and The Conduct of An Audit In Accordance With International Standards On Auditing*. https://www.ifac.org/_flysystem/azure-private/publications/files/A009%202012%20IAASB%20Handbook%20ISA%20200.pdf

IAASB. (2019). *International Standard on Auditing 315 (Revised 2019)*. https://www.ifac.org/_flysystem/azure-private/publications/files/ISA-315-Full-Standard-and-Conforming-Amendments-2019-.pdf

Institute, I. G. (2006). *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*. ISACA.

Institute, I. G. (2007). *COBIT® 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. IT Governance Institute.

ISACA. (2015). *ISACA ® Glossary of Terms English-Brazilian Portuguese Expert Translation*. https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/isaca-glossary-english-portuguese_mis_por_0615.pdf?la=en&hash=F48BE9C8DF19839AD68EF9C8C961476AC4BFC43E

ISO 27001. (n.d.). Retrieved February 28, 2024, from https://www.27001.pt/

Kilgore, A., Radich, R., & Harrison, G. (2011). The Relative Importance of Audit Quality Attributes. *Australian Accounting Review*, *21*(3), 253–265. https://doi.org/10.1111/j.1835-2561.2011.00141.x

Otero, A. R. (2018). *Information Technology Control and Audit, Fifth Edition*. CRC Press.

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2016). *Managing and Using Information Systems: A Strategic Approach*. John Wiley & Sons.

PwC. (2023). *Global Annual Review 2022*. PwC. https://www.pwc.com/gx/en/about/global-annual-review-2022.html

PwC Portugal. (2023). *PwC em Portugal*. PwC. https://www.pwc.pt/pt/quem-somos.html

Sayana, S. A., & CISA, C. (2002). The IS audit process. *Information Systems Control Journal*, *1*, 20–22.

Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners.

International Journal of Accounting Information Systems, *13*(1), 60–79. https://doi.org/10.1016/j.accinf.2011.11.001

Tarek, M., Mohamed, E. K. A., Hussain, M. M., & Basuony, M. A. K. (2017). The implication of information technology on the audit profession in developing country: Extent of use and perceived importance. *International Journal of Accounting & Information Management*, *25*(2), 237–255. https://doi.org/10.1108/IJAIM-03-2016-0022

APPENDIX A

Ethics Committee Report

This is to certify that
Project No.: **OTHER2023-11-199557**
Project Title: **The impact of IT Audit work**
Principal Researcher: **Maria Helena Silva**

according to the regulations of the Ethics Committee of NOVA IMS and MagIC Research Center this project was considered to meet the requirements of the NOVA IMS Internal Review Board, being considered **APPROVED** on 11/19/2023.

It is the Principal Researcher's responsibility to ensure that all researchers and stakeholders associated with this project are aware of the conditions of approval and which documents have been approved.

The Principal Researcher is required to notify the Ethics Committee, via amendment or progress report, of
- Any significant change to the project and the reason for that change;
- Any unforeseen events or unexpected developments that merit notification;
- The inability of the Principal Researcher to continue in that role or any other change in research personnel involved in the project.

Lisbon, 11/19/2023

NOVA IMS Ethics Committee
ethicscommittee@novaims.unl.pt

APPENDIX B

Survey: The impact of IT Audit work

The Impact of IT Audit Work

This survey seeks to explore the influence of an IT Specialist team in their execution of an IT audit project for a client, aiming to gain insights into the project impact.

As you have received this form, it implies that the project undertaken affected your Information Systems Department team. I greatly appreciate your input in helping me understand the extent of his impacts and its implications.

*Mandatory

Q1. Which is your role? *

- ○ Manager of IS Department
- ○ Coordinator of the Control and Management Systems Core
- ○ Team member of Enterprise Application

Q2. How important and useful do you believe IT Audit works are for your team? *

- ○ Very important
- ○ Somewhat important
- ○ Not very important

Q3. What are the benefits of IT Audit work? *

- ○ Improved Security
- ○ Data Integrity
- ○ Cost Savings
- ○ Risk Mitigations
- ○ Compliance Assurance
- ○ Client Trust

Q4. Do you consider that the work carried on fulfilled its main purpose? (Identify risks, vulnerabilities, and opportunities for improvement, helping to maintain the integrity of the IT environment, safeguard data, and meet regulatory requirements,...) *

- ○ Yes
- ○ No

Q5. How frequently do you think an organization should undergo IT audits? *

- ○ Annually
- ○ Bi-annually
- ○ Only when issues arise

Q6. What improvements or enhancements would you like to see in the process of IT audits project?

Desenvolvido pela Qualtrics

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação

Universidade Nova de Lisboa