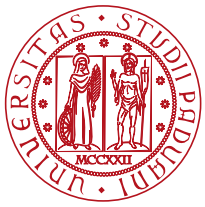

UNIVERSITA' DEGLI STUDI DI PADOVA

DEPARTMENT OF ECONOMICS AND MANAGEMENT "MARCO FANNO"

MASTER'S DEGREE IN BUSINESS ADMINISTRATION

GRADUATE THESIS

THE FUTURE OF INTERNAL AUDITING: HOW TECHNOLOGY IS SHAPING THE PROFESSION

SUPERVISOR: PROF. ENRICO RETTORE

EXTERNAL SUPERVISOR: DOTT. DIEGO BENETELLO

CANDIDATE: EDOARDO PERON

ID NUMBER: 2034486

ACADEMIC YEAR 2022 – 2023

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) ……  ……

Table of contents

Tables, boxes and figures

Figure 13 – Pyramid of risks.

Source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf [Access date: 21/08/2023]

Figure 14 – Regulation timeline.

Source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf [Access date: 21/08/2023]

Executive summary

The goal of the thesis is to investigate the possibility of internal auditing methods becoming more effective and efficient by incorporating technology and specific information technology, tools, and mechanisms.

The thesis's first chapter reviews internal auditing, outlining its origins, objectives, and core theoretical frameworks as COSO, CobiT, COSO ERM, and COSO ERM – Strategy. The chapter also emphasizes how important it is to maintain the independence and objectivity of internal audit operations as well as the role that internal auditing serves in corporate governance and risk management inside organizations, with a focus on the interaction with other organs and functions.

The second chapter describes the planning and daily operations that the internal audit function must perform. The various steps in the internal audit process will be explained, including identifying the items to be audited, identifying the procedures and controls that are currently there, drafting an audit plan to test and strengthen the controls just mentioned, executing the plan, and then creating useful reports to be given to the board of directors to highlight gaps for improvement and provide suggestions; and to the staff for the follow-up phase where the entire process will be improved.

The third chapter of this thesis will be the core of it, within it will be highlighted how technology in its various aspects is helping and will be increasingly pervasive in the internal audit function. Initially, how technological change is affecting the internal auditing profession will be explained. Then, one by one the technologies with the most relevance will be exposed, such as: Data Analytics and Big Data, Robot Process Automation, Process Mining, and Artificial Intelligence.
The ultimate goal of implementing these technologies is to simplify and streamline the repeated tasks of professionals, but most importantly to have a continuous auditing and continuous monitoring approach.

The fourth and last chapter looks at how technological advancements are changing established frameworks like COSO, CobiT, and COSO ERM, leading to increased efficiency and changing risk dynamics. It highlights how technology is changing how human engagement is defined, affecting the sorts of controls and testing procedures, and leading to more successful

compliance operations. The importance of the AI Act in governing AI technology is also discussed in the paper, with special attention paid to its measures for risk management, transparency, and user information. It is emphasized that the internal audit's dual function in assisting AI compliance, spotting gaps, and preserving ethical norms is essential for navigating the rapidly changing technology world.

Chapter 1: Internal Auditing

1.1 Introduction

This chapter aims to analyze Internal Auditing, with a focus on the definition of this activity, its principles, and its history. It will also examine the Standards to be followed, the relationship with control functions and the board of directors, and three important frameworks used to manage business risks: COSO, CobiT, and COSO ERM. The objective of this chapter is to provide a comprehensive and in-depth overview of Internal Auditing, with the goal of supporting the understanding and evaluation of this activity within organizations.

1.2 Definition of Internal Auditing

Internal auditing is a crucial function that supports organizations to accomplish their objectives by delivering a systematic and disciplined approach to assessing and improving the effectiveness of risk management, control, and governance processes.

The professionals that are in charge of doing so are called “internal auditors”, they represent trusted advisors who provide an independent and objective assurance as a service to organizations.

Their main activities are focused on risk management, strengthening internal controls, and ensuring compliance with laws and regulations.

Internal auditors' role is developing fast in today’s complex and dynamic business environment. Organizations need to prevent internal and external risks, such as regulatory compliance, supply chain disruptions, or information technology threats. It’s in the organization’s interest to have robust systems useful to reduce at an acceptable level and manage the risk associated with the just mentioned threats.

Internal auditors are trained and certified to professionally perform; they must follow the International Standards for the Professional Practice of Internal Auditors established by the Institute of Internal Auditors (IIA). These Standards arrange a framework to perform internal auditing and cover other aspects such as consulting, governance, control, and assurance.

The definition of internal auditing is given by the just-mentioned Institute of Internal Auditors (2023a), and it is stated as follows: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

From the definition, we can already explore some of the characteristics that the internal auditor function has and its aim. Starting from the word “independent”: expressing the need for the internal auditor function not to have a bias, that is, a tendency about a specific matter that would not lead to an objective analysis, or an external influence. Independence helps ensure a smooth working process for internal auditors because they do not be afraid of retribution or interference. In a further section of this chapter, we will explore this key characteristic.

The next analyzed word is “objective”, which means that the suggestions and conclusions reported must be based on objective data or real evidence. This feature also helps internal auditors be unbiased and free from conflicts of interest.

"Assurance", on the other hand, refers to the guarantee that professionals are requested to provide and implement adequate control systems in the organization. Which offers adequate and effective risk management, internal controls, governance structure, and management of processes. The assurance function is crucial to boost shareholders’ confidence in the organization.

Internal auditors do also a "consulting activity," that is, the provision of a service for the organization they work for. The service is composed of increasing the efficiency and effectiveness of internal operations, achieving established goals, and suggesting process improvements.

Having listed the principal characteristics that an internal auditor must have lets us move into the service offered, the areas that the internal auditing function directly goes to monitor and analyze.

The first area that the internal auditing function covers is risk management intended in a wide way: to guarantee that they are proficient in recognizing, evaluating, and managing risks at all levels of the organization. This makes it possible to ensure that the organization is ready to handle potential risks and can prevent potential losses.

The second area concerns internal controls, which ensure effectiveness in mitigating risks and verify that the operations performed by the organization are conducted in compliance with laws and regulations.

Certainly, these are preventive measures aimed at reducing losses in case of unforeseen events.

The last area concerns governance processes, it is closely related to the above-mentioned characteristic "consulting activity," because through governance internal auditors can guide corporate management and thereby avoid mistakes.

1.3 Mission and core principles of Internal Auditing

In this section, we will go on to explore the mission of Internal Auditing to understand what the ultimate purpose of the function is, and then proceed to explain the core principles that every internal auditor should follow to make sure that his or her role expresses maximum effectiveness. In addition, for each key principle, we will analyze what are the negative aspects that the organization will incur if the above principles are not met.

The Institute of Internal Auditors (2019a) states that the mission of Internal Auditing is "to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

We can infer from the sentence that the internal auditing function is capable, if it expresses its full potential, of maximizing the value created by the company. But the function also has a role as a protector of corporate value itself.

As mentioned earlier for Internal Audit to accomplish its mission there is a need for it to comply with the core principles.

To ensure that internal auditing is working professionally the Institute of Internal Auditors (2019b) has established a set of core principles that internal auditors should follow.

First principle: Demonstrate integrity

Internal auditors are required by these regulations to uphold the law and refrain from participating in any illegal or unethical behavior that could harm their profession. Reporting the opinions, findings, and suggestions from their engagements is one of the most crucial ways internal auditors demonstrate integrity. If integrity isn't shown, the internal audit activity loses the trust that has been placed in it, and as a result, its credibility to offer independent and unbiased assurance and advice. The internal audit activity is rendered incapable of adding value to the organization as a direct result of a lack of integrity, which also affects the function and the people who work in it. In this case, the organization will probably look for alternate assurance methods.

Second principle: Demonstrates competence and due professional care

Internal auditors must limit the services they provide to those for whom they have the required knowledge, expertise, and experience. They also must constantly work to increase their competence and the efficiency and caliber their services. If internal auditors are unable to complete all or part of an assurance engagement due to a lack of knowledge, expertise, or other capabilities, they may coordinate with other assurance providers, collaborate with subject

matter experts as guest auditors, or hire outside consultants. Before advancing into higher-level internal audit positions and/or specializing in a particular field, such as fraud, data analytics, or IT, internal auditors may be needed to achieve or possess specialized qualifications. On the other hand, professional care is applied when internal auditors comply with the protocol to organize and execute engagements, record their work, and communicate the results. The results from the internal audit activity may include the following if the internal audit activity does not demonstrate competence and proper professional care: other communications, like audit reports, could also be late, erroneous, or poor in quality or uselessness.

Third principle: Is objective and free from undue influence

The third principle is strictly related to the first one "Demonstrate integrity", both demand for internal auditors to behave in the company's best interests. Internal auditors must maintain an unbiased mindset known as objectivity in order to perform their duties impartially. Independence refers to the absence of any circumstances that can compromise the internal audit activity's capacity to operate in this manner. Management and the board are unlikely to believe internal audit findings to be accurate and comprehensive if internal auditors are not perceived as being objective. If the internal audit activity is not independent, it can come under pressure to curtail its engagement, bury results, or alter its perspectives.

Fourth principle: Aligns with the strategies, objectives, and risks of the organization

Internal auditors have a duty to benefit the organization they work for. Connecting internal audit engagements to the risks that could have the biggest effects on the organization's capacity to achieve its goals is one of the best ways to deliver that value. The Chief Audit Executive (from now on we will refer to the Chief Audit Executive but there is an option for companies to have an Audit Committee) interacts with senior management and the board of directors to develop a comprehensive understanding of the organization's main goals, its strategies for achieving those goals, and the risks that might prevent it from achieving those goals. The Chief Audit Executive is also required to interact with important senior management personnel and participate in senior management committees' strategy meetings in several areas (e.g., assets and liabilities committee, operations committee, enterprise risk management committee). The just explain activities of the Chief Audit Executive are also called top-down perspective. From a bottom-up perspective, the Chief Audit Executive may designate specific internal auditors to evaluate various areas inside the organization in order to understand how strategy is executed at the business unit/operational level. If the internal audit function is not in line with the organization's strategic goals, objectives, and risks, it runs the danger of spending resources on

evaluating areas, procedures, or problems that do not aid in the management of the organization's major risks and the accomplishment of its goals.

Fifth principle: Is appropriately positioned and adequately resourced

Without the proper positioning and authority inside the business, it is challenging for the Chief Audit Executive and the internal audit activity as a whole to uphold integrity, independence, and objectivity. When the internal audit activity is properly positioned and suitably resourced, it can effectively deliver value to the organization. The internal audit activity's operating budget and other resources should be confirmed by the board of directors as adequate for the internal audit activity to meet its goals. The Chief Audit Executive and the board of directors may periodically compare the resources of the internal audit activities to those of comparable organizations to support the evaluation. The results and recommendations of internal audit work could not be given enough attention to drive management to take action if the internal audit activity is not positioned properly. Furthermore, the board of directors might not be directly accessible to the Chief Audit Executive, making independent reporting challenging. Internal audit activity cannot openly discuss delicate issues concerning management without access to the board of directors.

Sixth principle: Demonstrates quality and continuous improvement

The Chief Audit Executive must put into place policies and processes that are specific to the organization's needs for assurance and advisory services in order to direct the internal audit activity. In addition to allocating sufficient resources to carry out the engagement, the Chief Audit Executive should also develop and monitor key performance measures, which include routinely reviewing the documentation. The internal auditing process needs to be evaluated and updated on a regular basis. The Chief Audit Executive may conduct surveys or use other methods to ask relevant stakeholders inside the internal audit process for their opinions in order to continuously assess the effectiveness of the work produced by the internal audit activity. Internal audit services may be enhanced by modifying the process in consideration of the feedback. Weaknesses linked to persons, processes, and methodology may go undetected and unaddressed in an internal audit procedure that does not value quality and continuous improvement, leading to inefficiencies and failing to offer trustworthy assurance and recommendations.

Seventh principle: Communicates effectively

The mission, role, value, and effectiveness of the internal audit activity are aggressively promoted as a key component of communication. Internally, spreading the information within the organization is facilitated by pursuing opportunities to reach large audiences. To describe the duties and responsibilities of the internal audit activity and demonstrate the value it can provide to organizational success and efficiency, multimedia approaches can be used to create a slide show or a brief video. These initiatives show how the internal audit activity communicates the importance and role of its work. A communication plan could be part of the Chief Audit Executive's internal audit rules and processes. The communication plan may outline how internal auditors will distribute information about individual engagements, from planning and task programs through results and monitoring. It should be in line with communication-related Standards. If the communication is not done correctly, it will affect the execution of the internal audit activities in all respects. Without an effective communication, the internal audit activity might find it difficult to get the authority, resources, and data necessary to carry out engagements and successfully communicate its findings, recommendations, and opinions to management and the board of directors. In essence, internal auditing will become ineffective and without adding value to the board of directors and management.

Eighth principle: Provides risk-based assurance

The Chief Audit Executive should begin with an internal audit strategy based on a risk assessment of the entire business that is in line with the risk universe of the firm and considers its risk tolerance. The Chief Audit Executive often considers the organization's culture and the level of risk management maturity when developing a suitable strategy for evaluating the governance, risk management, and control procedures. To obtain information useful to assess the risk, the Chief Audit Executive may meet with those in charge of sustaining the organization's risk management framework. The Chief Audit Executive may utilize a specific framework that the organization has established as a basis for evaluating the risks connected to its risk management procedures. By using a predetermined framework, internal auditors and staff members can communicate in a shared language. Additionally, it offers a framework for connecting the organization's goals with the internal audit plan. If the internal audit effort does not result in risk-based assurance, the management or the board will not have a third-party confirmation that the controls are correctly implemented and mitigating risks as planned.

Ninth principle: Is insightful, proactive, and future-focused

First of all, the internal auditing function needs to analyze the past only when root causes are identified and used as the foundation for recommendations for future improvement and is it possible to evaluate past activities in a way that is meaningful. The next step is to identify and describe the potential effects of the threats that have been discovered, and they should examine the data they have obtained to determine the causes. The internal audit team should look beyond the firm's immediate strategic plan and assess how developing risks may influence the organization and the process under examination in addition to delving deeply into results to determine underlying causes. The Chief Audit Executive should direct the internal audit function trying to seek out information on new risks, including those coming from the environment like the organization's market sector or industry, the geographical areas, and regulatory jurisdictions in which it competes. The internal audit activity should ideally make use of these new thoughts to broaden the scope of the organization-wide risk analysis and notify the board and management of any emerging or modifying risks. Finally, internal auditors should perform surveys and interviews with the aim of determining whether stakeholders regard the contributions made by the internal audit activity as insightful, proactive, and future-focused. The internal audit activity exposes the organization to threats for which it could have been prepared and the value-added of the function will be reduced. Moreover, these shortcomings are likely to cause management and the board of directors to lose faith in the audit function.

Tenth principle: Promotes organizational improvement

The main Chief Audit Executive responsibility is to have a preliminary discussion with senior management and the board of directors to comprehend the company's plans and business objectives and evaluate its risk management, control, and governance procedures, and collaborate with other assurance and consulting service providers in order to maximize effectiveness in delivering assurance over the organization's top priority risks. The internal audit activity should provide a comprehensive report on the organization, taking into account its plans, objectives, specific business concerns, and operational procedures. The audience that receives communications should be taken into consideration a pragmatic approach to governance, risk management, and control that may be tailored by the organization with the assistance of the internal audit activity, which may also encourage organizational improvements through benchmarking and the exchange of best practices. If this principle is not met, so when internal audit fail in terms of advising and advisory services and may ignore chances to suggest ways the business could boost productivity or streamline the delivery of assurance services and

eventually save money and resources the direct consequence could be a reduction of resources for the audit practice and a lack of trust in the internal audit's work.

1.4 The evolution of Internal Auditing

The core principles just mentioned will be recurring throughout this first chapter as they subsequently guide both the drafting of the standards used by practitioners and in the creation of the frameworks used.

They have, however, been elaborated and modified throughout the history of internal auditing, therefore understanding the history of internal auditing and how it has changed over time is crucial, and in this section, we will go over the major steps that have led this profession to be developed and mature.

The first step toward internal auditing was taken, according to Pickett (2010), when as an extension of external auditing, organizations began to test accounting data, so it is possible to say that at the beginning of its development internal auditing was limited to increasing the level of adequacy and appropriateness of financial statement accounts.

The difference between an internal audit and an external audit is as follows: in order to improve the functioning of internal controls in the evolution of the work performed by internal audit has increasingly focused on internal aspects of organizations, precisely to broaden the spectrum of assurance, while the external audit is by definition concerned with certifying and giving assurance that financial statements are correct in form and substance. Internal audit, as we will see later in this section, will increasingly focus on the internal workings of the organization and the regulations it must and does comply with.

The next step there was when non-accounting data also began to be verified, simply double-checking to be sure of the correctness and accuracy of the data being considered. At that time small audit teams were formed and they were under an assistant chief accountant. They were not independent.

The probity work was developed subsequently as an adaptation of the audit of accounting records, in which auditors would visit various locations and local offices on an unannounced basis and conduct a thorough set of tests in accordance with a pre-established audit schedule. The auditors would provide management with a list of the mistakes and queries they had found. The auditors had a dual assignment, where they had specific auditing obligations in addition to their usual accounting responsibilities. Audit visits typically concentrated on cash receipts, inventory, purchases, petty cash, stamps, contracts, and other small accounting operations.

Subsequently, the internal audit function has obtained a separation from the accounting function. And due to this evolution of audit management, the presence of audit management was a straight consequence that followed predetermined audit programs. Being able to transcend fundamental financial practices gave freedom to address greater priorities. With the ability to now include a wider range of disciplines audit work may now be expanded.

Employing Chief Audit Executive with a significant organizational rank offered another push toward a professional audit department. They could represent the audit function in meetings with senior management at all levels. Additionally, this includes hiring individuals who may use this audit expertise to advance their managerial careers. The audit function may continue to grow the professional status that is the sign of an acknowledged discipline from the current position, which is established in many large organizations. Nowadays the internal audit function has the capacity, and from a certain perspective is obliged to handle significant problems with a significant influence on success, as an example of professionalism.

The idea of the audit function reporting to the highest levels was introduced by the Chief Audit Executive and expanded through audit committees, and this had a favorable effect on perceived status. A path for high-level audit work capable of addressing the most delicate business issues is to attract the attention of the board of directors, chief executive, managing director, non-executive directors, and senior management. From the earlier duties of inspecting the inventory and petty cash, this is a long way.

The last step done so far by the internal auditing professionalism path was in 1942 when the Institute of Internal Auditing was launched in New York, directly followed by Chicago. Those who were given the title of internal auditor by their employers and wanted to learn and share experiences with colleagues in this new professional discipline founded the Institute of Internal Auditing.

According to Ramamoorti (2003), the Institute of Internal Auditing’s first research director played a crucial role in 1947 by publishing the organization's Statement of Responsibilities of the Internal Auditor. Internal auditing is largely concerned with accounting and financial issues, but it also covers issues of an operating character, according to the Statement of Responsibilities of the Internal Auditor. The Declaration of Internal Auditing's Duties had been significantly expanded by 1957 to cover a wide range of management services.

Later, in 1971, Lawrence Sawyer took on the responsibility of successfully rewriting the Statement of Responsibilities as head of the Research Committee. Further updates to the Statement of Responsibilities were made in 1976, 1981, and 1990 to reflect the profession's fast and ongoing development.

The Standards for the Professional Practice of Internal Auditing were formally accepted by the Institute of Internal Auditing in 1978.

The last milestone from the Institute of Internal Auditing was in 2000 implementing the Professional Practice Framework and then updating it in 2009 and becoming International Professional Practices Framework (IPPF).

1.5 International Professional Practice Framework (IPPF)

As already discovered in the previous paragraphs, internal auditors have a framework for professional practice thanks to the International Professional Practice Framework (IPPF, see Figure 1), which was developed by the Institute of Internal Auditors (2023b). The IPPF is widely regarded as the definitive source of advice for the field of internal auditing.

With the aid of the IPPF, internal auditors make sure that the assurance and consulting services they offer are of a professional level, impartial, and unbiased. The goal of this tool is to assist internal auditors in addressing the changing requirements of their constituents, such as management, the board of directors, and audit committees.

The IPPF is a detailed framework that sets norms and guidelines for the internal audit profession. It assists in making sure internal auditors carry out their duties in accordance with best practices and add value to their organizations.

In this paper we have already set out parts of the International Professional Practice Framework, such as the definition of internal auditing and the core principles that internal auditors must adhere to in order to maximize efficiency and add value for the organization.

In the next paragraphs, we will go through each section of the cited framework and explore each section forming it.

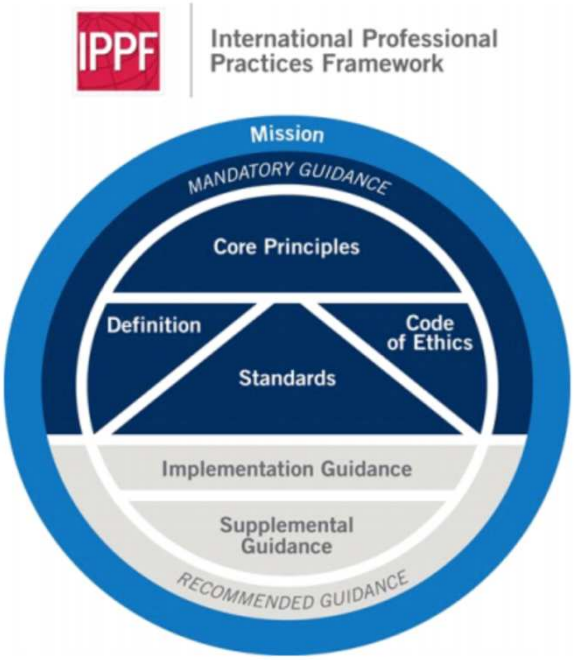

Figure 1: International Professional Practice Framework (IPPF).

1.5.1 Binding guidelines from the association

There are two different categories of guidance in the IPPF: mandated guidance and recommended guidance. The International Standards for the Professional Practice of Internal Auditing represent the mandatory guidelines; Practice Guides, Practice Advisories, and other auxiliary guidelines serve as the suggested guidelines.

The Standards are a set of guidelines and concepts that specify the essential conditions for efficient internal auditing. Attribute Standards, Performance Standards, and Implementation Standards are the three categories into which they are divided.

The traits of the internal audit activity and the people who carry out internal audit work are defined by Attribute Standards. These requirements involve things like independence, objectivity, proficiency, and due professional care.

In this essay, we are going to investigate Attribute Standards and Performance Standards, next you will find an explanation of the main ones.

- Attribute Standards, which are listed in Appendix A and are numbered from 1000 onward, offer guidelines for evaluating the personal qualities, abilities, and organizational structure of internal audit in order to make sure that internal staff has the abilities, information, and resources required to carry out their duties successfully.
- Performance Standards, which you can find listed in Appendix B, numbered 2000 onwards, specify the nature of internal audit work and offer benchmarks for measuring

the effectiveness of the internal audit activity. These guidelines cover subjects including planning, executing, reporting, and follow-up.

The Attribute and Performance Standards can be applied with the help of Implementation Standards. They address topics including governance, risk management, control, and quality assurance and improvement initiatives.

Also exists position papers, global technology audit guidelines, and other documents that offer extra guidance on particular internal auditing-related subjects, these are examples of additional supplemental guidance.

In the next section, we are going to analyze first the main Attribute Standards and then the main Performance Standards.

1.5.2 The independence role and others attribute Standards

The characteristics of the internal audit activity and the individuals responsible for carrying out internal audit work are defined by attribute standards.

We will not now analyze all nineteen attribution standards proposed by the Institute of Internal Auditors, which you can find in Appendix A for a complete list, but we will explain the rationale for the most relevant ones.

1100 – Independence and objectivity

This standard is perhaps the most important and crucial; we have talked before about independence, and we have seen how the lack of it can lead to biased conclusions and thus underestimation of possible threats, which if they materialize could harm the organization.

Independence is the absence of circumstances that might compromise the ability of the internal audit activity to perform its duties objectively. The Chief Audit Executive has direct and full access to senior management and the board in order to attain the level of independence required to successfully carry out the duties of the internal audit activity. A dual-reporting arrangement can help with this. Obstacles to independence must be controlled at the organizational, functional, and individual auditor levels.

Davis and Stark (2001) in their paper expose all the types of conflict of interest that can arise, the first type highlighted there is when the service provider uses confidential and privileged information for their own gain, this practice is also called "insider trading" or "improperly signaling the marketplace about their client's affairs".

We can have another type of conflict of interest when financial service providers offer their clients auditing and other financial services. Due to the fact that the examined company is a significant client for financial services organizations, conflicts of interest arise since auditors'

decisions are frequently influenced by the need to maintain client satisfaction and avoid losing business. In general, managers of audited companies desire positive evaluations. They have the right to terminate financial service providers whose auditors give them cause for complaint. The impartiality and independence of the auditors are thus compromised because the managers of financial service providers and the auditors who work for them are aware of this.

Another type of conflict of interest is called "personal trading", it is very similar to the first mentioned, but here the service provider does not benefit from the information obtained by working for the company by making profits but manipulates it. That is, if he/she bought the stocks he will make sure to enhance the positive aspects of the analysis, or if he/she sold the stocks he will enhance the negative aspects analyzed.

The paper enunciates how conflicts of interest cannot be eliminated, but only managed, and proposes solutions to this end.

The first proposed solution deals with the competition the service provider has in the market. If the customer is able to leverage competitors, the negative effects of conflicts of interest are limited. In a highly competitive market, financial service providers will struggle to attract customers if they act against the interests of their clients and consequently diminish returns to them.

The second solution concerns the obligation that service providers should have to say whether there are conflicts of interest in place.

The third solution state that there should be a sort of legislation, regulatory organizations, business groups and exchanges, as well as financial services companies themselves, have the power to establish specific regulations requiring persons to avoid conflicts of interest or forbidding behaviors that do so. For the internal auditing industry, this is what the Institute of Internal Auditors is aiming to do.

The last solution proposed when there are conflicts of interest arising from offering multiple products from one company is to implement a structural change in the organization receiving the service, that is, to divide the management responsible for the two or more products/services, in this specific case there will be managers in charge of the auditing function, and other managers in charge of other related services.

Along with independence we also have objectivity, which is an impartial mental attitude. Objectivity is essential to the work of internal auditors because only then can they not create work with bias. As mentioned earlier when the third core principle was expressed when objectivity is not met that it is possible for the organization to be exposed to risky occurrences and repercussions such as regulatory penalties, reputational harm, sanctions, and other

stakeholder losses if biased observations and conclusions are used that either underestimate or conceal the magnitude of risk exposures.

The final thought of the section must be answered in understanding how to position the internal auditing function within the company to make sure that independence and objectivity are respected.
In order to ensure that the internal auditing function is compliant with the Standards there is a need to understand what the best corporate organizational structure and its positioning at the organizational chart level is, it must always provide a reporting channel to the board of directors.
But independence and objectivity in practice are achieved primarily at the level of the organizational chart by positioning the internal auditing function at the staff level, not dependent on any business or control function but instead will have to report directly to the board of directors.

Others attribute standards
Speaking about the standard number 1000, is the first Attribute Standard referring to the documentation that internal auditors need to sign in concomitance with the organization to have the objectives, scope, and responsibility for performing the internal audit activities. This document is called the "internal audit charter". It establishes the role of the internal audit activity inside the company and the nature of the Chief Audit Executive's functional organizational hierarchy with the board of directors. It also grants access to personnel, physical assets, and records necessary for the execution of engagements, as well as defining the internal audit activities' authority.
The board of directors has the power to approve or decline the internal audit charter.
Another important attribute standard is the 1111, the aim of this Standard is to guarantee that the internal audit function can provide its findings and recommendations without interference from management to the board of directors or audit committee.
Direct communication with the board contributes to promoting accountability and honesty inside the company. The board can use this information to better inform their decision-making processes by having a comprehensive awareness of the actions of the internal audit function and the risks that the firm confronts.
The internal audit function must have a direct reporting line to the board or audit committee, as well as adequate access to information and resources, in order to comply with the requirements of this standard.

The last relevant one is the standard number 1230, explaining the importance of a continuous professional development. To stay informed with changes in their field, new risks, and new technology, they should participate in a program of continuous learning, training, and development. To increase the overall effectiveness of the internal audit function, they should create a personal plan for continuing professional development, take part in pertinent training and seminars, stay current on new developments in the internal audit profession, ask for feedback to identify areas for improvement, and share their knowledge and expertise with others within the organization.

1.5.3 Performance Standards

Internal auditing can be carried out effectively and efficiently with the help of the Institute of Internal Auditing performance standards. These guidelines are used by internal auditors to direct their work and make sure they are satisfying stakeholder expectations. The standards serve as a foundation for evaluating the effectiveness of internal audit activities and encouraging the ongoing development of the internal audit function.

The first seven performance standards (2000, 2010, 2020, 2030, 2040, 2050, 2060) talk about the responsibilities of the Chef Audit Executive, namely leading the internal auditing function, drafting an action plan to prioritize risks, communicating changes and discoveries by following standard procedures and policies, and creating periodic reports for top management on the work done, enunciating the authority enjoyed by internal auditing, its responsibilities, and overall performance.

Other Attribute Standards speak to the nature of the work to be done by the internal audit function, and about each professional aspect that the internal audit team will explore, such as Governance (2110), Risk Management (2120), and Control (2130).

The list then discusses engagements, which are particular projects or assignments in that internal auditors participate in order to assess and enhance an organization's operations. It identifies its objectives (2210), scope (2220), resource allocation (2230), work plan (2240), and final monitoring (2300).

All performance standards, as done for attribute standards will be listed in a separate appendix (B).

1.5.4 Code of Ethics

The expectations and standards regulating people's and organizations' conduct during internal auditing are stated in the Code of Ethics (Institute of Internal Auditors, 2023c). It outlines the basic standards for behavior and behavioral expectations instead of specific activities.

The institute's Code of Ethics seeks to advance an ethical mindset throughout the internal auditing industry.

There are four basic principles in the Code:

- Integrity – In their interactions with others, internal auditors are anticipated to be truthful, honest, and transparent. They should refrain from any actions that can undermine their honesty or the integrity of their line of work;
- Objectivity – Internal auditors are supposed to fulfill their responsibilities with impartiality and objectivity. They shouldn't let personal or outside circumstances influence their conclusions or suggestions;
- Confidentiality – Internal auditors are bound to maintain the confidentiality of any information they obtain while doing their duties. They have the duty to avoid sharing any private information unless it's necessary by law;
- Competence – Internal auditors must have the knowledge, abilities, and practical experience required to do their jobs well. They should continue their education and training in order to preserve their professional competence.

The Code of Ethics also contains precise guidelines for behavior that internal auditors must adhere to, such as preventing conflicts of interest, declining gifts or favors that would undermine their objectivity, and refraining from any actions that might damage the reputation of the industry, these additional orders are called "Rules of Conduct".

1.6 Mapping the interactions of Internal Auditing and control functions

Internal audit and other control functions need to find a way to cooperate through specific interactions in order to enlarge the spectrum of assurance following specific accountabilities.

The goals of having a constructive dialogue are to have a clear division of duties and responsibilities, and to assure the company that each control function and internal audit function are working synergistically to give more assurance and transfer as much value as possible to the organization.

These moments of information exchange occur in committees or more simply in regular meetings on a monthly or quarterly basis.

The relationship between internal auditing and other control functions refers to how internal auditors collaborate with and rely on control functions within an entity. The term "control functions" refers to the many organizational units and individuals in charge of establishing internal controls over financial reporting and other corporate processes, such as risk management, compliance, information security, etc.

As already said, the purpose of internal auditing is to add value and enhance an organization's operations by offering independent, objective assurance and advisory services. Internal auditors evaluate the efficiency of the governance, control, and risk management procedures within a business and offer suggestions for enhancement.

Internal auditors depend on control functions to give them the information and assistance they need to do their jobs, so establishing relationships between internal auditing and control functions is crucial. For instance, internal auditors might collaborate closely with the compliance function to make sure the company is sticking by all applicable rules and laws. To identify and evaluate risks that potentially have an influence on the organization's operations, they might also collaborate with the risk management function.

On the other hand, internal auditors are used by control functions to assist in identifying areas where controls should be reinforced or improved. Internal auditors can offer an unbiased assessment of the efficiency of controls and assist control functions in identifying any potential holes or flaws in their control frameworks.

The Institute of Internal Auditors (2020) has updated an already existing model, shown in Figure 2, that assists companies in identifying the structures and procedures that will best help them achieve their goals and support effective governance and risk management.

Within any corporate structure, the internal control system is defined as a three-line model of defense where the first line is represented by the default controls established by already existing procedures, the second line by supporting and monitoring organizational units, and the third line is always represented by internal audit.

This framework is used to understand that internal audit is not isolated from the organization as a whole, but it needs to have a dialogue with other control functions; in the absence of control functions, it will refer to the Chief Financial Officer and the Board of Auditors.

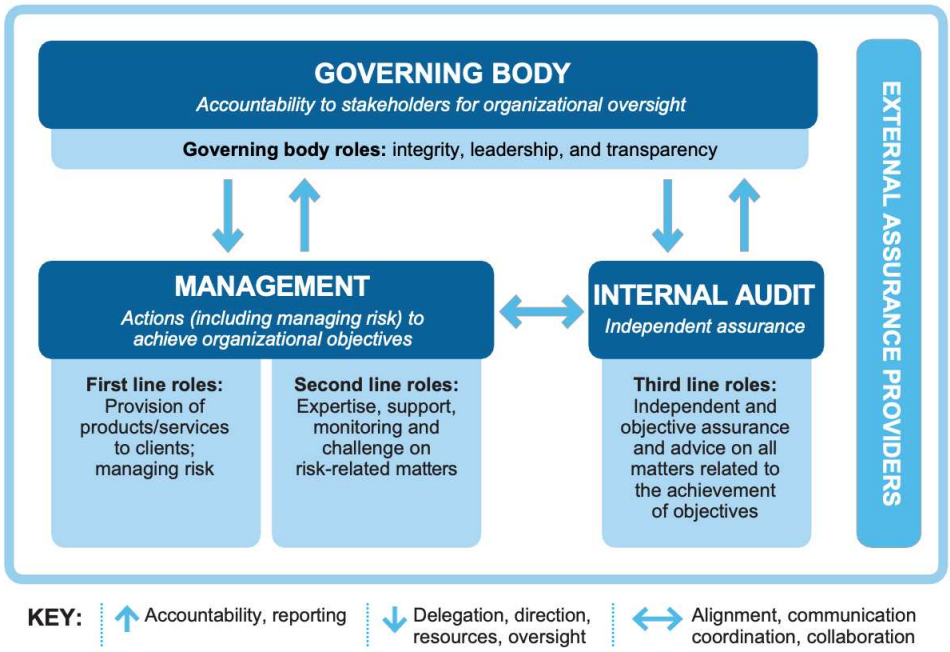

Figure 2: The IIA's Three Lines Model.

Three types of stakeholders can be seen in the proposed model: the governing body, which is most commonly represented by the board of directors, which reflects the will of the shareholders, its role is to establish governance procedures, delegate responsibilities to management, determine the level of riskiness desired within the organization, and finally to declare and monitor the independence, objectivity, and competence of the internal audit function.

Next, we have management, as just explained it is decided by the governing body and must be supervised by it. In turn, management is divided into first-line roles and second-line roles. First-line management is in charge of maintaining direct contact with the governing body, informing it about the plans implemented, the progress of the work, and the output of the work done. They guide and monitor actions aimed at achieving the goals set by the governing body. During daily operations, these structures must identify, measure or assess, monitor, mitigate, and report risks arising from routine business operations; they must adhere to the defined constraints assigned to them in accordance with the risk objectives and procedures in which the risk management process is documented.

Second line managers, on the other hand, are in charge of doing the analyses and reports useful for understanding risk and consequently managing it. The accomplishment of risk management goals including internal control, information and technology protection, sustainability, quality management, compliance with laws, regulations, and appropriate ethical behavior.

The last main actor in the model is internal auditing, having extensively already discussed its role and purpose we simply say that in addition to the tasks outlined above it must interface with management by having a clear and constant exchange of information, while with the governance body, it must play an advisory and consultant role.

For example, within the financial services environment, some regulators highlight the following:

- Bank of Italy (2013), in Circular No. 285, says: “specific attention is paid in the articulation of information flows between the functions corporate control functions; in particular, the heads of the risk control function and the regulatory compliance function inform the head of the internal audit function of critical issues detected in their control activities that may be of interest to audit activities. The head of internal audit informs the heads of the other corporate control functions for any inefficiencies, weaknesses or irregularities that have come to light in the course of audit activities under their responsibility and concerning specific areas or matters within the competence of the latter”.
- IVASS (2018), in Regulation No. 38, says: “ensures that there is appropriate and continuous interaction between all committees established to carry out functions at the group level, within the administrative body itself, the senior management of the ultimate parent company and the group's core functions, and with those who carry out administrative management and control functions in group companies, with particular regard to the companies referred to in Article 210-ter, paragraph 2, of the Code and in other group companies that have a significant impact on the group's risk profile, by proactively requesting information and questioning decisions that may have an impact on the group”.

According to the extent and type of risks, the function aims to identify procedures and regulatory violations as well as periodically evaluate the completeness, sufficiency, functionality (in terms of efficiency and effectiveness), and reliability of the internal control system and information system.

The external assurance provider, on the other hand, possibly serves as support to management and internal auditing, for example, when the latter does not reflect core principles, such as independence or competence.

Now, as the title of the section suggests, we will investigate the relationship that interposes the audit function with management and the governance body.

We start by discussing the connection between first-line and second-line management and internal auditing. Internal auditing is allowed to plan and execute its tasks without interference or bias thanks to management's separation from it. It also has unrestricted access to the people, resources, and data it needs.
The governing body is responsible for it. Yet independence doesn't necessarily mean isolation. To make sure that the internal audit's work is pertinent, aligned with the organization's operational and strategic needs, and relevant, internal audit and management must regularly communicate with other functions of the organization.
Now let's turn to the relationship there is between internal auditing and the government body, let's start by saying that it has to monitor activities on behalf of the government body.
But also, the governing body is in charge of supervising internal audit, which implies: ensuring the establishment of an independent internal audit function, including the selection and removal of the Chief Audit Executive; acting as the Chief Audit Executive's primary reporting line; approving and allocating resources for the audit plan; receiving and evaluating reports from the Chief Audit Executive; and granting the Chief Audit Executive free access to the governing body, including individual meetings without management present.

1.7 Common language: value chain and internal processes

In internal auditing, it's essential to find the right compromise between using standards and customizing for a particular firm. Understanding the appropriate internal auditing standards, such as the International Standards for the Professional Practice of Internal Auditing (IIA Standards), as well as any related rules or regulatory obligations, is the first step. This will make it easier to determine the important rules and specifications that must be adhered to.
The second phase is to evaluate the business environment while taking into account the distinctive qualities of the organization, including its size, sector, complexity, risk profile, and governance structure. This will make it easier to decide the audit's precise focus areas and the necessary level of depth.
At this stage, Porter's Value Chain (De Mozota 1998) visible in Figure 3 helps us understand the specifics of the company under consideration so that we can comprehend its critical issues.

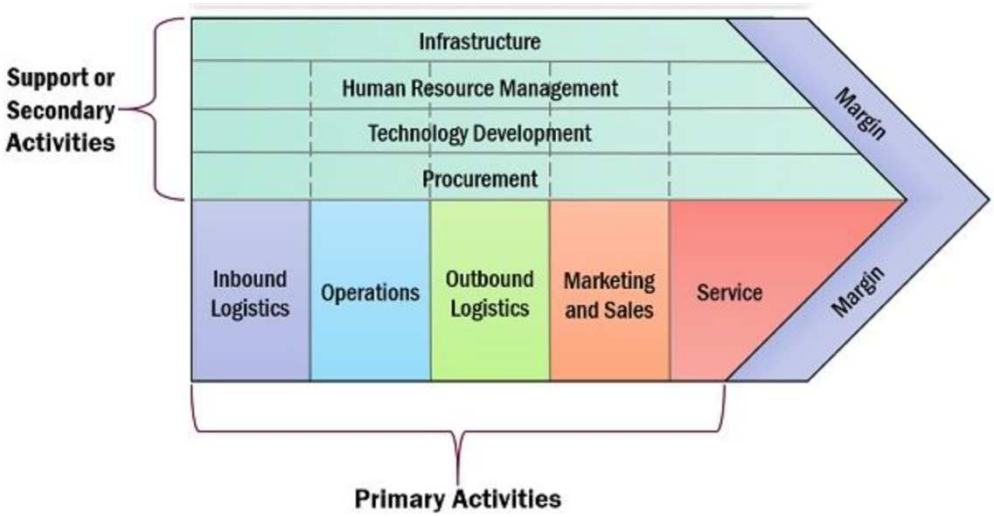

Figure 3: Porter's Value Chain.

The audit committee and senior management are two crucial stakeholders that should be involved in order to understand expectations and priorities. This will make it easier to make sure that the audit is in line with the goals and objectives of the organization. This phase is critical because it brings knowledge to the internal audit function, which transposes information from management and must understand and comprehend the optimal solutions for the type of business, in terms of sector and size that is placed in front of it.

The internal audit team can create a customized audit plan that balances the requirements of the standards with the unique needs of the organization once the appropriate standards and business context have been evaluated. This can imply altering audit methods, picking different audit methodologies, or changing the audit's scope to concentrate on high-risk sectors.

Lastly, maintaining a constant feedback loop with critical stakeholders is crucial throughout the audit process, and the audit strategy should be adjusted as necessary. This will make it more likely that the audit will be valuable to the organization and remain relevant.

Having understood the reasons and procedure for understanding the specifics of the entity you are working with now is the time to create a Process Tree, according to van Zelst S. J. and Leemans S. J. J. (2020) it is defined as "a mathematical model of a process, in which internal vertices represent behavioral control-flow relations and leaves represent process activities."

Typically, the processes analyzed are divided into strategic, business and support.

By dividing the company according to what has just been said, it is possible to understand where the risks are and what controls should be checked.

Processes and their mapping are not only useful to provide assurance by the internal auditing function, but by doing so all people within the organization are aligned and have precisely a

common base of knowledge of their assigned roles and also what their colleagues in other functions are dealing with, by doing this as already mentioned risk identification is more accurate, but also the exchange of information is faster and more efficient, because both actors have understood how the internal processes work.

1.8 Global Frameworks of Internal Auditing

While documenting and evaluating a specific scenario, internal auditors rely on internal control frameworks.

As there are so many frameworks accessible, the management can decide which ones to utilize or even pick an alternative framework depending on the circumstance.

In this section, we'll examine a few of the frameworks that internal auditors frequently employ.

But before we go on to explain in detail, we try to understand what a control framework is.

An organized document that groups and classifies predicted controls or control topics is known as an internal control framework.

Management creates internal control processes using the framework as a starting point when an organization implements a control framework successfully, that usually is an audit risk assessment or risk management. By doing this, the organization is better able to build control methods that maximize value while avoiding risk.

One of the most crucial and essential ideas that company professionals at all levels, as well as external and internal auditors, must comprehend is internal control.

Internal controls are management-implemented procedures that are intended to provide a reasonable level of assurance regarding the observance of laws and regulations, the preservation of the value of the organization's assets, the avoidance or management of risks, and the accomplishment of a mission, objectives, and goals of the organization.

Organizations should equip themselves with methodological tools and frameworks to increase the level of assurance to strengthen control over risks that could impact the company's day-to-day operations.

The main goal of internal audit is to equip itself with methodologies, tools, metrics, and tools that are always directed toward ensuring its enterprise-wide assurance function is optimal. They also help standardize risk assessment procedures.

1.8.1 The COSO standard

The first and most widely used framework is called COSO Internal Control Framework; it is an acronym derived from the "Committee of Sponsoring Organizations." It was published in September 1992 (Moeller 2009, p. 23-51) and it used a three-dimensional model to characterize

an organization's internal control system, three primary internal control components at the top of the model and on the right side the number of layers changes depending on how the business is set up.

The idea behind the model is that the three dimensions, i.e., internal controls, the various functions of the organization, and the segmentation of activities are closely interconnected, and each node that is created by these connections must be analyzed to get a clear and complete view.

We will now analyze, in the proposed framework, the various sections that make it up. (Figure 4)

- Internal controls – This category describes the organization's capacity to establish an efficient system of internal control, which entails identifying and analyzing risks and putting mitigation measures in place, continuously monitoring business operations, managing financial transactions, setting up internal policies and procedures, and adequately training staff. Next this section we will go on to explain all the various subpoints contained by this "face" of the proposed framework.
- Functions of the organization – This category refers to the management of business operations and the establishment of organizational goals. This includes identifying business processes and defining precise goals for each of them, defining roles and responsibilities within an organization, and establishing an innovation process that is centered on ethics and integrity.
- Segmentation of activities – This category refers to the division of business activities into different levels and different facets, ranging from broader elements such as divisions to narrower and more specific ones such as functions.

Figure 4: COSO Internal Control Framework.

Internal controls environment

The control environment serves as the basis for all other internal control measures and has an impact on all unit and entity actions as well as each of the three objectives.

The control environment is a reflection of how the board of directors, management, and other stakeholders feel about the value of internal control in the company as a whole and how they behave accordingly.

The internal control environment is frequently greatly influenced by the history and culture of the organization. When top management continues to stress the necessity of delivering high-quality goods, when this message is conveyed to all levels, and when it has historically been a strong management focus for an organization, it becomes a significant enterprise control environment element.

Internal auditors should consistently make an effort to comprehend and assess this entire control environment while conducting nearly all reviews. An internal auditor will almost probably discover more internal control problematic areas when the internal control environment is inadequate.

The following are the standard elements of the control environment: integrity and ethical values transmitted by the top management, commitment to competence, policies established by the board of directors and audit committee, management's philosophy and operating style, a proper organizational structure, how the assignment of authority and responsibility is performed and the human resources policies and practices.

Internal control risk assessment

Several internal and external factors might put an enterprise's capacity to accomplish its goals in danger. A fundamental component of the internal control foundation is the understanding and management of the risk environment, and an organization should have a mechanism in place to assess any potential risks that could affect the achievement of its goals.

The evaluation of COSO internal controls risk should be a proactive procedure that is carried out at all levels and for almost all business operations. Risk assessment is a three-step process, according to COSO:

1. Calculate the risk's importance;
2. Determine how likely or frequently the risk will materialize;
3. Think about risk management strategies and determine what steps need to be implemented.

Risks should be seen from three viewpoints, according to the COSO internal controls framework: enterprise risks resulting from external causes, enterprise risks resulting from internal causes, and specific activity-level risks.

Internal control activities

The rules and procedures known as control activities help make sure that the actions identified to address risks are done after a variety of control activities sub-processes. The idea of control activities is crucial for developing and then implementing efficient internal controls in an organization.

Information and communications internal controls

The firm must transmit pertinent information, assisted by IT systems, in a way and at a pace that enables employees to carry out their duties. Organizations must have effective practices in place to communicate with both internal and external stakeholders in addition to formal and informal channels of communication. Every assessment of internal controls must take into account the organization's information and communication flows.

Monitoring internal controls

Internal control systems will function properly with the right managerial support, control protocols, and information and communication links, but processes must be in place to maintain surveillance of these operations. Internal auditors have always been responsible for monitoring, conducting evaluations, and judging whether established procedures are being followed; however, COSO now considers monitoring in a wider sense. COSO internal control considers

that other systems and control methods evolve over time. What seemed to work when it was first installed might no longer work in the future.

To evaluate the performance of established internal control components and implement corrective action as needed, a monitoring procedure should be in place.

1.8.2 CobiT

The COSO internal controls framework has drawn criticism from certain professionals, who worry that it doesn't place enough focus on information technology (IT) tools and procedures.

As a result, Control objectives for information and related Technology (CobiT), an internal controls framework with a stronger IT focus, was created.

The Information Systems Audit and Control Association issued and governed the CobiT (ISACA).

The main areas of focus for CobiT are organized around the crucial IT governance basic idea that strategic alliances between business operations and information technology operations should be formed.

These interactions between the business and IT worlds fall into several areas, such as value delivery, risk management, resource management, and performance management (Moeller 2009, p. 89-96).

Resources, processes, and information criteria are the three IT-related factors that CobiT also examines for controls. The CobiT cube, which is depicted in Figure 5, describes these three. This CobiT model examines IT controls from a three-dimensional viewpoint and is comparable to the COSO internal controls framework cube.

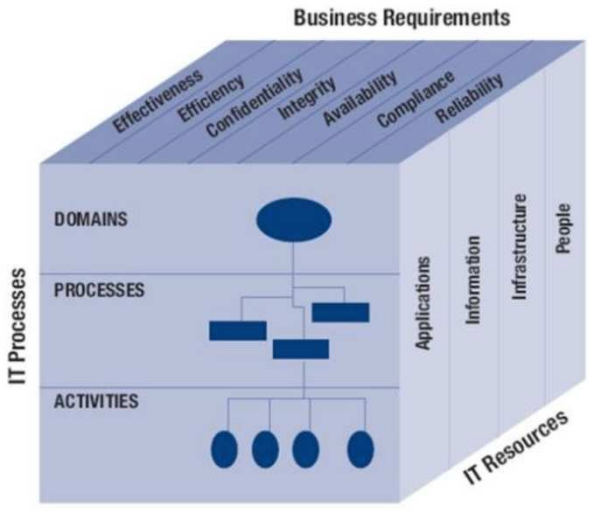

Figure 5: CobiT cube.

IT Processes

The CobiT cube's first dimension, which refers to IT Processes, is divided into three sections: domains, processes, and activities.

- Domains are collections of IT procedures that correspond to organizational responsibility areas, and they include: planning, acquiring, implementing, delivering, monitoring, and evaluating;
- Processes are a set of tasks with built-in rest periods;
- Activities are the steps taken to produce quantifiable results, also explained as the set of tasks that must be carried out in order to obtain the intended results as defined by CobiT. These actions might be seen as specific ones that must be completed in order to carry out the procedure correctly.

Business requirements

Business requirements are the second level of the CobiT cube. For all business requirements, seven components should be taken into account, together with any required IT resources and procedures: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

These seven criteria should be used to evaluate all IT systems as a whole. The emphasis will vary depending on the process type, but these standards should be considered in all IT processes.

IT Resources

The considerations for all the required resources for the functioning of enterprise IT resources are represented on this side of the cube when looking at the CobiT framework.

These resources, which include the following, should be taken into account when assessing controls in an IT environment, either singularly or collectively:

- Software that combines human information processing steps with automated user interfaces;
- Information to be used in business operations;
- Components and facilities that form the technology infrastructure, such as hardware, databases, operating systems and networks;
- It is essential to have key and skilled individuals in order to plan, coordinate, purchase, implement, maintain, monitor, and evaluate IT services.

1.8.3 COSO ERM

When there was the introduction of risk and even more when its identification was methodically processed and documented the Committee of Sponsoring Organizations (COSO) released a version called COSO Enterprise Risk Management Integrated Format (COSO ERM).

This solution enables an organization's internal audit to take into account and evaluate risks at all levels, whether it is in a single area.

The procedure used by COSO ERM is divided into four steps: risk identification, quantitative or qualitative assessment of the documented risks, risk prioritization and response planning, and risk monitoring (Moeller 2009, p. 113-123).

Implementing this four-step risk management method requires the involvement of several professionals at all organizational levels.

Risk identification is the first step and is based not on identifying every possible risk the business may have, but on selecting only those risks that have an impact on the organization's operations within a reasonable period of time. Identified risks can relate to the organization as a whole as well as to a single specific business area. For risks of the whole organization, top management will need to be interviewed, while for risks of each function, reference should be made to the manager managing the function.

Next, an attempt will be made to understand the level of risk exposure the company is experiencing at any given period, as mentioned earlier by interviewing managers and colleagues who interface with the highlighted issues on a daily basis. The best practice usually is to assign a score from 1 to 9, where 1 indicates the near impossibility of the event happening, while 9 there is the near certainty that the event will happen. Averaging within the risk highlighted by the various actors s will subsequently prioritize these risks, from most likely to least likely.

To conclude we will go on to assign each triggered event an associated cost. So as to have, now, a complete picture of the situation.

Key risk identification is never a straightforward, one-time task. When the environment changes, the contexts that surround recognized threats will soon alter as well. Certain risks may become much more dangerous as a result of changing circumstances.

Processes for identifying risks are not recurring. Similar to how a business will create an annual budget that may undergo quarterly modifications, risk identification is frequently an annual or quarterly exercise, of course depending on the size of the organization or the dynamism of the environment. The business must monitor these risks after they have been discovered and continue to make necessary modifications. The process owner or an impartial reviewer can conduct this risk monitoring. Internal audit is frequently a very reliable and effective source to track the progress of identified risks.

The other two faces of the framework are similar to the previously explained framework, standard COSO, while the front face as can be seen from Figure 6 has the exposed elements with the addition of the phases explained earlier in this section.

Figure 6: COSO ERM.

A natural evolution of the framework just explained is when the risk management done by an entity goes together with the vision, mission, and strategy.

In 2017, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) updated the previous version with precisely the implementation of corporate strategy and performance within risk management.

This necessity emerged from two main factors, the first depicts the increasingly turbulent and unstable competitive environment, resulting in concern on the part of the Board of Directors; the second reason lies in the reporting that is obtained after the auditing process, it increasingly needs to be intuitive, readable even by laypersons, concise and effective.

The updated model, called "Enterprise Risk Management - Integrating with Strategy and Performance", takes some elements of the previous models analyzed but drastically changes the point of view from a mere analysis of risks in its various levels and facets to a strategic plan divided into phases and action areas.

The Framework itself is a collection of guidelines divided into five connected areas:

- Governance and Culture – Enterprise risk management is important, as governance establishes supervisory duties and establishes a foundation for the business. Culture has to do with the entity's moral principles, preferred actions, and perception of risk;
- Strategy and Objective-Setting – The strategic planning process integrates enterprise risk management, strategy, and goal-setting. Business goals put the strategy into action

while acting as a foundation for detecting, evaluating, and managing risk. A risk appetite is formed and matched with strategy;

- Performance – Identifying and evaluating risks that might affect how well a strategy and the company's goals are achieved is important. In the context of risk appetite, risks are ranked in order of magnitude. The organization then decides on risk mitigation strategies and evaluates the level of risk it has taken on;
- Review and Revision – An organization can evaluate entity performance by observing how effectively the enterprise risk management components are operating over time and in consideration of significant changes, as well as what improvements are required;
- Information., communication, and Reporting – The act of collecting and distributing crucial information from external and internal sources, which moves across the company, is a constant requirement of enterprise risk management.

Having explained the framework and understood its meaning we can now appreciate the principles and guidelines given in Figure 7.

Following these guidelines can provide management and the Board of Directors with a fair expectation that the organization is aware of the risks related to its strategy and business goals and makes an effort to control those risks.

Figure 7: Enterprise Risk Management - Integrating with Strategy and Performance.

1.9 Conclusions

In conclusion, our analysis gave a comprehensive view of internal auditing by examining at its definition, mission, and guiding principles as well as its history, standards, relationships to the board of directors and control functions, and frameworks used to manage business risks.

The next chapter will be devoted to an in-depth look at the activities performed by Internal Audit, including assessing internal controls, identifying risks and managing them, analyzing business processes, developing an audit plan, and remediating through follow-up adjustments. Also, we will explore the operational framework for internal auditing, which aids in defining the audit process and the roles and activities needed to allow effective and effective audit activities.

We are sure that knowing what the Internal Audit department does and how it operates will help to give a more complete picture of this crucial function within organizations.

Chapter 2: Operating Framework in Internal Auditing

2.1 Introduction

In this first section of the second chapter, we will go on to understand how in practice professionals apply on a daily basis the core principles, standards, and frameworks of internal auditing that we have previously deeply explained.

We start by saying that the auditing process carried out within organizations can be divided into three broad categories:

- The first part is about planning the audit activities, so we will understand what the audit universe is and what are the prerequisites for its use, after that we will understand what it means to carry out the risk assessment, then we will explain the difference between strategic and operational audit plan and their usual duration, and finally we will figure it out the level of resources that internal audit should use in auditing activities and while building the team in the capacity planning.
- The second phase is called the audit cycle, and it shows the stages that make up the internal auditing process, starting with the previously drafted audit plan. The audit selection will be done, then planning, then field work, then reporting, and for constant improvement the last follow-up phase, within the process is included the drafting of final documentation in the form of reports, through which corporate management can obtain advice or be informed of any risks.
- In the third section, we have a recall of reporting, which will already be explained in the second section within the audit cycle but here it will have more of a focus on information effectiveness and more generally on how information is aggregated and selected to be effective communicated to the Board of Directors.

This practical way of proceeding is summarized in the figure below (Figure 8).

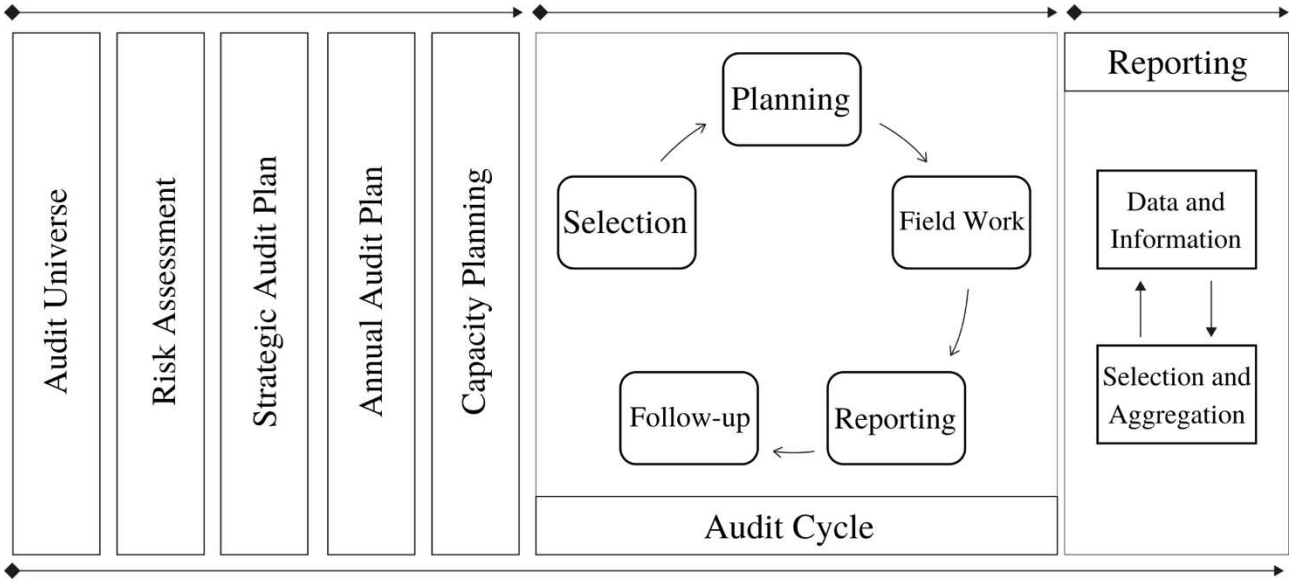

Figure 8: Operating Framework.

2.2 Navigating the process and protocols of Internal Auditing

As outlined in an earlier section introducing the topic, it is essential for the internal auditing function to have a deep understanding of the business that it will be analyzing and evaluating; this preliminary step is useful for identifying the key processes that the organization turns over on a daily basis and then assessing their potential risks.

As a starting point for analyzing a business we have at our disposal Porter's Value Chain, a tool already mentioned and explained earlier in the paper. This tool is critically important, as it highlights the various processes within the company and interactions with third-party entities.

We will now list a number of benefits that internal auditing will enjoy if process mapping is carried out clearly and effectively:

- Understanding the business – The internal auditor can recognize the crucial business processes, risks, and control points by comprehending the organization. The auditor can properly plan and carry out the audit with the aid of this knowledge;
- Identifying critical processes – The auditor can determine which procedures are crucial to the operation of the organization by comprehending the value chain. To make sure that they are working successfully and efficiently, these crucial procedures need to receive a more thorough audit;
- Evaluating controls – The auditor can assess the efficacy of the controls in place with the use of knowledge of the value chain. The auditor can find problems or weaknesses in the control architecture and suggest ways to fill them by looking at the controls at each stage of the value chain;

- Risk assessment – The auditor can evaluate the risks connected to each step of the process, so is better able to concentrate on high-risk areas, prioritizing the actions and organizing audit efforts accordingly;
- Compliance – For the purpose of ensuring compliance with applicable laws and regulations, understanding the value chain is equally crucial. The auditor can evaluate the degree of compliance and offer suggestions for improvement by being aware of the legal requirements at each stage of the procedure.

As I think is now clear, having a strong idea of the business that is going to be analyzed and the internal and external processes that govern the day-to-day operations is a necessary requirement for the internal auditing function.

Following this, the internal auditing function will proceed in identifying the audit universe, which will be explained in the next section.

2.3 Audit universe

The key concept to comprehend in order to understand how to draft an audit plan is that of an "audit universe", according to Majdalawieh and Zaghloul (2009) the audit universe "can be defined as the aggregate of all information systems (IS) related activities that are available to be audited within an organization". It gives a static snapshot of the elements to be considered when is going to draft the audit plan.

So, the audit universe is the list of elements that the internal audit function will go to analyze after prioritizing them, on which the risk assessment will subsequently be carried out for each of them and in each area of the organization.

A structured method of internal auditing is provided by the audit universe, allowing auditors to systematically assess an organization's risk exposure and control environment. All of an organization's key functional areas, including finance, operations, information technology, compliance, and human resources, are often included in the audit universe, but as explained in the previous section, it is important to understand the specifics of the individual company with whom you are working and not follow a standard pattern for all of them, otherwise you risk being too rigid and not capturing the key processes that that company has and therefore need to be audited.

The audit universe is often kept up to date by the internal audit department on a regular basis to reflect changes in the organization's business environment, risks, and priorities. The internal audit team uses the audit universe as a guide to concentrate their efforts on the organizational areas that are most important to the accomplishment of the organization's goals.

Based on the best practices proposed by Sturgis and Loftus (2023) the audit universe can also be drafted on multiple levels within the organization, these are divided into:

- Process level – A process is a set of procedures or activities carried out methodically to accomplish a certain purpose or target is referred to inside a corporation as a process. It might involve several organizational roles and is frequently concentrated on a single job or activity. These can cover a wide range of activities, from manufacturing and production to sales and marketing, customer service, and financial operations, among others.
- Functional level – In contrast, a function inside a company refers to a particular division or sector within an organization that oversees carrying out a specified set of duties or operations in order to accomplish a particular goal. Functions can vary based on the type of business and its aims, however some typical examples of business functions are operations, finance, human resources, marketing, and information technology.
- Product level – This strategy concentrates on auditing certain products offered by the firm.
- Business level – Risks often relate to the organization's overall strategic direction and performance as they could be financial risks, reputational risks, legal and regulatory risks, and cybersecurity risks.

Listing the elements just outlined is the first step in constructing the also-called "Risk Register." Having understood what audit universe means now in the next section we will go on to understand how risk assessment is performed, which is the evaluation of risks that may threaten the effectiveness, efficiency, and adequacy of business processes.
An example of an audit universe will be proposed below (Figure 9).

Business Area	Overview			
	Audit Ref	Business Area	Audit Topic	Audit Type
Finance	F1	Finance	Billing and Accounts Receivable	Assurance
	F2	Finance	Acounts Payable	Assurance
	F3	Finance	Banking	Assurance
	F4	Finance	Aged Debtors	Assurance
	F5	Finance	Suppliers	Assurance
	F6	Finance	Expenses (including Credit Cards)	Assurance
	F7	Finance	Treasury	Assurance
Human Resources / People	P1	People	New Starters	Assurance
	P2	People	Leavers (Including Movers)	Assurance
	P3	People	Payroll	Assurance
	P4	People	Training (including Induction)	Assurance
	P5	People	Performance Management	Assurance
	P6	People	Employee Satisfaction	Assurance
Information Technology	IT1	Information Technology	Backups	Assurance
	IT2	Information Technology	Patching and Vulnerabilities	Assurance
	IT3	Information Technology	Network Security	Assurance
	IT4	Information Technology	IT Asset Management	Assurance
	IT5	Information Technology	Internet Monitoring	Assurance
Business Area	BA1	Business Area	Topic 1	Strategy
	BA2	Business Area	Topic 2	Strategy
	BA3	Business Area	Topic 3	Third Party / Supplier
	BA4	Business Area	Topic 4	Third Party / Supplier
	BA5	Business Area	Topic 5	Operations

Figure 9: Audit universe example.

2.4 Risk assessment

The process of internal auditing must include risk assurance. It implies assessing the efficiency of a company's risk management procedures and assuring that they are working properly. In other words, risk assurance is the process of determining if existing controls are successful in reducing possible threats to an organization.

The creation of a risk-positioned audit plan may be greatly aided by including the Risk Registry in the Audit Universe and immediately connecting it with the various audit subjects or business processes.

On the practical side, an attempt is made to make a qualitative (low-medium-high, as in the example below) or quantitative judgment (give a rating that, for example, ranges from 1 to 9, where 1 stand for almost impossibility of experiencing the event, while 9 is considered that there is almost certainty that the event will happen).

Below there is an example (Figure 10) showing how each element previously identified in the audit universe has had a risk level associated with it.

Risk				
Risk Ref	Risk Category	Risk Description	Residual Risk	Overall Assurance Rating
1	Strategic	Description	High	High
2	Strategic	Description	High	High / Medium
3	Operational	Description	High / Medium	Medium
4	Operational	Description	High / Medium	Medium
5	Financial	Description	Medium	Medium / Low
6	Financial	Description	Medium	Medium / Low
7	People	Description	Medium / Low	Low
8	People	Description	Medium / Low	Low
9	Legal	Description	Low	Low
10	Legal	Description	Low	Low
1	Strategic	Description	High	High
-	N/A	N/A	N/A	N/A
2	Strategic	Description	High	High / Medium
3	Operational	Description	High / Medium	Medium
9	Legal	Description	Low	Low
10	Legal	Description	Low	Low
-	N/A	N/A	N/A	N/A
8	People	Description	Medium / Low	Low
7	People	Description	Medium / Low	Low
6	Financial	Description	Medium	Medium / Low
5	Financial	Description	Medium	Medium / Low
4	Operational	Description	High / Medium	Medium
3	Operational	Description	High / Medium	Medium

Figure 10: Risk assessment example.

2.5 Audit plan

After listing all possible elements in the Risk Register and identifying their current risk index, we will proceed with the management, possible remedial or limiting suggestions for each individual risk found. This procedure is contained in the audit plan and it's a requirement stated in the Performance Standard number 2010 from the Institute of Internal Auditing (see appendix B).

An audit plan is a written document describing an audit's objectives, scope, and procedures. It offers a guide for auditors to use when performing their job, making sure that all essential areas are addressed, and all required actions are completed. The internal audit function normally creates the audit plan.

According to industry best practices, the internal auditing function should draw up two audit plans, the first one is usually drawn up every five years and is called the strategic audit plan, while the other, called the annual audit plan, as the name suggests is drawn up annually.

The strategic plan of auditing is a high-level document that specifies the general aims and goals of the internal audit function. It usually covers several years and is in line with the strategic goals of the company. The primary risks that the internal audit function will concentrate on, the audit procedures that will be applied, and the resources needed to meet the plan's objectives are all outlined in the strategic plan of auditing. It is a document that looks forward and supports,

ensuring that the internal audit function is concentrated on the most significant risks the firm faces.

KPMG (2022) shows us what the disadvantages can be of not having a clear strategic auditing plan:

- "Not being able to identify (all) internal and external trends that may impact the organization;
- Not achieving the strategic goals;
- Losing market share;
- Spending resources, time and money without achieving the desired results;
- Lacking accurate KPIs to assess the actual situation, leading the organization to steer blindly;
- Having an imbalanced view of the situation by focusing too much on near-term financial goals and losing sight of other strategic and short-term objectives;
- Not linking the strategic plan to the operating plan, resulting in a disconnect between the strategy and the operations."

An annual plan for internal auditing, on the other hand, is a more detailed document that lists the precise audits that will be carried out in the upcoming year. The strategic plan of auditing serves as the foundation for the yearly plan, which adds more specifics about the time, scope, and resources needed for the various audits that will be carried out. This is a vital tool for ensuring that the internal audit function efficiently manages risk and adds value to the firm in the yearly plan.

As you can guess both are functional and dependent on each other, the strategic audit plan shows the key principles to be followed by the annual audit plan, while from the past experience of the various annual audits in the future, the strategic one can be improved to be more effective and efficient.

2.6 Capacity planning

The process of establishing the proper level of resources, including people, technology, and other resources, needed to carry out the internal audit function effectively and efficiently is known as capacity planning in internal auditing.

The internal audit needs and objectives of the business, as well as the risks and difficulties it faces, are often monitored and evaluated as part of the capability plan.

The internal audit team must identify the workforce numbers, skill sets, and training requirements to satisfy these objectives and guarantee that the organization's risks are being properly managed based on this evaluation, this duty is stated in the Performance Standard 2030 (see appendix B).

Finding the technology and other resources necessary to support the internal audit function, such as data analytics tools, audit management software, and other technological solutions may also be part of the capacity plan.

All things considered, a strong capacity plan is necessary to guarantee that the internal audit function is adequately resourced and situated to support the organization's goals and manage its risks.

2.7 Audit cycle

Having finished the planning part just exposed and explained, we will enter the core of auditing practice, which as shown in the operating framework will be explained below.

The Office of Internal Audit at the University of Oregon (2023) identified five main phases that the internal auditing function performs, they are selection, planning, fieldwork, reporting, and follow-up.

Selection

The scope and objectives of the audit, as well as the major risks and controls that will be assessed throughout the audit, are all determined during the selection phase of internal auditing. The audit team and the auditee often work together during this phase to obtain data regarding the business operations, systems, and functions that will be audited. The audit team may also collect data about the auditee's organizational structure, policies, practices, and documentation to better understand the organization and its operations. The selection step, which establishes the framework for the entire audit procedure, is essential to the audit's success and lays the foundation for an informed and effective audit.

Planning

Internal auditing's planning approach involves creating a rigorous audit plan using the data acquired during the selection phase. This plan serves as a roadmap for the audit process from beginning to end, outlining the audit objectives, scope, technique, and timetable.

The audit team may also consider external variables that could affect the audit, such as legal requirements or modifications to the business environment. With this data, a risk-based audit approach is created that prioritizes the highest-risk areas and concentrates on assessing the

efficacy of important controls. Senior management and the audit committee often examine and approve the audit plan once it has been created to make sure it is in line with the goals and priorities of the organization.

Having understood the planning just resumed and previously explained now it is time to get down to practicalities and understand what steps the internal auditor must perform for each auditable object found in the audit universe.

Below is the list of steps that internal audit, following best practices, should follow:

1. Initial announcement – It begins with a formal notice sent to the organizational unit to be audited, informing the head of the unit that the unit's processes will be audited, as stated in the annual audit plan, and also requesting in advance the policies, processes, and procedures in place so that the audit function understands how the unit operates and is organized (as stated in the Performance Standard 2310 and Performance Standard 2330, see appendix B). In this way, after an in-depth study, specific risks are discovered and controls are identified that the internal audit function expects to find and test during the fieldwork phase;
2. Terms of reference – This is the agreed statement of work that lists the exact deliverables and labor that a contractor or supplier is expected to provide. To avoid scope expansion or unpleasant surprises later on, it's vital to have a clear understanding of the work's scope being agreed. The objectives and structure of a project, committee, meeting or negotiation are set out in a so-called Terms of Reference document. It outlines the roles and responsibilities of the participants and provides instructions on how the work has to be carried out and reported;
3. Audit planning memorandum – An audit memorandum is used to inform everyone involved of the findings reached by the authorized professionals involved in the process, which may need certain modifications as part of adhering to the policy and for the benefit of the firm as well. In the day-to-day operations of the internal audit function, the memorandum is represented by a summary document where within it are all the findings made in terms of risks, management of them or any controls to be put in place to ensure the truthfulness and minimize errors in the organization's internal procedures;
4. Draft risk and control matrix (RACM) – An organization can use a risk and control matrix as a tool to recognize, prioritize, and put control measures in place to mitigate risks. In simple terms, a risk and control matrix provides a picture of an organization's risk profile by comparing the risks to the official steps taken to reduce the likelihood of undesirable results. A risk and control matrix's success mostly depends on an organization's capacity to create a thorough list of risks (external and internal) that might

have a negative influence on it, as well as the controls in place to protect against such risks.

In practice, the risk and control matrix is composed of a spreadsheet where each row corresponds to an auditable item identified in the audit universe, while the columns are divided as follows: in the first column, there is the name of the process or at least a reference to identify the auditable item; then a brief description of the risk associated with it and, if possible, placing it in a risk category; then a specific risk to understand its magnitude and the impact it would have on the organization; and finally, the controls performed on that item and the result of the controls to understand its robustness.

Fieldwork

Executing the audit plan that was created during the planning phase is what the fieldwork part of internal auditing consists of. The purpose of this phase is to gather data in order to assess the efficiency and effectiveness of the auditee's controls and procedures.

The audit team may carry out a range of tasks during the fieldwork phase, including document review, interviewing, testing controls, and data analysis. These processes are intended to give the audit findings and conclusions a solid and acceptable foundation.

Fieldwork is the core of the audit activity because once the activity of understanding the audited elements and identifying the risks and controls of the processes implemented by the organizational unit is completed, those controls are tested.

The tests performed can be of two types:

- Design – The internal control's design test would confirm that the control, which the company claims to have in place, has been developed and implemented.
- Operational effectiveness – A particular internal control's efficacy is determined by whether or not it performed consistently over an interval of time in past periods (typically 12 months).

Reporting

Internal auditing's reporting phase includes informing the auditee, senior management, and the audit committee or Chief Audit Executive of the findings. In order to ensure that the stakeholders are aware of the significance of the audit findings, this phase aims to give a brief and clear information regarding the findings, conclusions, and recommendations of the audit's work.

A written report summarizing the audit findings, including any weaknesses or inadequacies in the auditee's controls or procedures, may be prepared by the audit team during the reporting

phase. The report might also point out any potential risks or opportunities that were found during the audit, as well as suggestions for improvement or correction.
We need to understand this reporting phase as the internal communication between insiders who coordinate to present the final document to the Board of Directors, because they will be the final beneficiaries of all the work done so far.
The reporting part will be further explained and described in a later section of this chapter.

Follow-up
After the audit fieldwork and reporting are over, a crucial follow-up phase occurs. It requires evaluating the application and efficacy of any suggestions or corrective measures found during the audit process.
The internal auditor should check that the recommendations have been implemented and assess their efficacy in fixing the problems found during the process. The auditor may conduct interviews, review documentation, and perform diagnostics to confirm that the corrective steps have been done and are functioning as planned.

2.8 Reporting

The last section of the operational framework for internal auditing focuses on reporting, having already explained the relationship between the internal audit function, control function, and management in the previous chapter, explained what steps need to be followed to design an internal audit plan properly, and shown the steps that make up an internal audit plan in this chapter, we will now proceed to list what principles need to be followed outlined by the Institute of Internal Auditing (2022):

- An operational approach should be used and not merely a compliance approach, by doing so management will feel helped and not judged;
- Sometimes going outside the box and presenting documents other than the traditional can help capture the attention of management who will have to implement the proposed solutions;
- Use an Executive Summary to summarize the work done on one page so as to give a general overview;
- In providing the increase in value through the internal audit processes use numbers and data so that the work done is tangible;
- Use tables, indicators and other graphic effects so as to capture attention to key information;

- Suggested observations and recommendations must be previously agreed upon between the internal audit function and management; nothing not previously discussed must be in the final documentation;
- Try as much as possible to remove technicalities and terms used only by internal audit, because the staff who will use them will be managers and not audit technicians;
- Also, highlight the positives found in the auditing process and not just the things that did not work;
- Include wording indicating "conducted in accordance with the International Standards for the Professional Practice of Internal Auditing", as stated in the Performance Standard 2430, see appendix B.
- Include the cost incurred for the audit operation in question to show whether the budget was met.

Following and adhering to these simple guidelines will make the report clear for management. It is critically important that the internal auditing function and management constantly interact to make sure that the final document delivered to the client is as complete and understandable as possible, only then will corrective actions be executed and the true value of internal auditing be expressed.

The internal audit will have to report its findings and suggestions in the form of a final report to the Board of Directors, so once the process audit is completed, the head of the internal audit function will also have to do reporting to its Board of Directors or other relevant bodies, depends on how the organization is structured.

Furthermore, the reporting activity by the internal audit function also requires the head of the internal audit function to inform, in a predefined sequence, certainly the Board of Directors and other internal organs of the company that need information regarding the results of the audits performed by the internal audit function, as stated in the Performance Standard number 2060 (see appendix B).

Direct interaction with the Board of Directors is essential, so as to ensure the independence of the work performed (the internal auditing function being, as explained above, a staff function).

2.9 Conclusions

We conclude this chapter by saying that the entire internal auditing process has been outlined from the operational aspect that the internal auditing function will have to perform, right from the start there should be a clear identification of the auditable objects in the organization, determine the current risk of each object, and then try to actuate useful plans for risk reduction

or management. This is done through an auditing plan and through constant communication between the internal auditing function and management responsible for each audited object.

The goal of explaining how the internal audit function works was accomplished in order to, as will be explained in the next chapter, understand what processes implemented by the internal audit can be automated or how technologies available nowadays and still being developed can support this function to be increasingly effective and efficient.

Chapter 3: How Technology is Changing the Internal Auditing Function

3.1 Introduction

Organizations are continually looking for innovative methods to improve their internal audit procedures in today's quickly changing business environment. Utilizing technology improvements has become essential for internal auditors to keep ahead of the curve as the digital age continues to disrupt industries. The cutting-edge trends in internal audit are examined in this chapter, which also examines the revolutionary possibilities of continuous auditing, continuous monitoring, data analytics, big data, robotic process automation, process mining, and artificial intelligence.

The chapter starts by looking at the technical development of internal audit, emphasizing how businesses are utilizing cutting-edge technologies and methods to improve their auditing processes. To increase their efficacy, efficiency, and risk coverage, internal auditors are using more automated procedures and high-end technologies. The gradual transition from conventional audit techniques to technologically advanced procedures is highlighted in this section.

The combination of continuous monitoring with continuous auditing is one of the most significant technology developments in internal audit. In order to quickly detect risks and abnormalities, this section examines how various approaches provide real-time insights into an organization's activities.

Big data and data analytics are crucial to improving the internal audit process. The chapter describes how auditors may evaluate huge amounts of organized and unstructured data to find hidden patterns, trends, and abnormalities. It examines the advantages and drawbacks of applying big data analytics and internal audit, highlighting the significance of context and effective implementation to realize their full potential.

The chapter also dives into the field of robot process automation (RPA), looking at how businesses use software robots to automate routine and rule-based audit duties. It covers RPA's advantages, as well as its drawbacks and potential implementation difficulties.

Another technique covered in this chapter is process mining. It explains how process mining makes use of data from different systems to view, examine, and improve business processes.

The section gives a summary of process mining's operation, and its effect on internal audit, stressing both its advantages and disadvantages.

The final section of the chapter explores artificial intelligence (AI) and its varied effects on internal audit. It examines how AI may be used in auditing procedures across a variety of contexts. The debate covers the advantages and drawbacks of applying AI, highlighting the necessity for a well-balanced strategy that takes ethical issues, human discretion, and AI system limits into account.

3.2 Technological change and trends

Recent years have seen a considerable transition in the internal auditing sector, partly due to the growing use of technology. Internal auditors now have access to a variety of technologies and techniques that may help them do their work more successfully and efficiently than ever before, thanks to the growth of automation, big data analytics, and artificial intelligence (Pizzi et al. 2021).

The effects of digital transformation on firms have been disruptive. The speed of innovation in the current environment sets it apart from other technological revolutions, which had varied consequences on organizations (Al-Taee & Flayyih 2023).

The power of visualization tools, which are helpful for identifying patterns, connections, and anomalies is also expanding. But, users are also vulnerable to a number of cognitive and perceptual biases when depending on visualizations and experts should be mindful that visualizations can be manipulated to highlight particular findings or represent a desired, and alternative narrative (Christ et al 2021).

According to Ettish et al. (2017) and Ming-Hsien et al. (2011) the use of information technology (IT) can lead to various benefits, such as enhanced operational efficiency, less human error, faster transaction processing, cost savings, and better accuracy. Additionally, it may greatly boost productivity and improve an organization's performance, creating value for all parties involved. Another benefit is lifted up by Al-Taee & Flayyih (2023), stating that there’s also a reduction in the overall risks while using technology.

The rise of technologies has facilitated and is still helping professionals but with associated risks (Kotb & Roberts 2011):

- Legal risks are associated with an increasing reliance on foreign business partners, but, due to the fact that applicable laws and regulations differ between nations, it can be challenging to identify and comprehend the pertinent rules and regulations;

- IT risks are those hazards resulting from greater dependency on quickly changing technology that enables e-business applications.

Key enabling variables that can support the effective deployment of a technical solution inside an internal audit team are performance expectation, effort expectancy, social influence, and facilitating circumstances (Bierstaker et al. 2014).

- Performance expectation describes how much the audit team members view a technological solution as beneficial and useful. Team members are more willing to adopt new technology if they think it will make their work simpler or more efficient;
- The degree to which a technological solution is seen as being simple to use and pick up pertains to the concept of effort expectation. Team members may be reluctant to accept new technology if they think it would take a lot of work to use it;
- The term "social influence" describes how much team members are influenced by the thoughts and actions of their coworkers. The adoption of the technological solution by the audit team may be encouraged if important organizational stakeholders support it;
- In order to make the adoption of the technological solution easier, the company must, to some extent, give the resources and assistance required. To ensure that team members have the knowledge and resources they need to utilize the technology effectively, this includes giving them the necessary training, assistance, and resources.

Additionally, Curtis & Payne (2008) suggests that within a three-year budget/evaluation cycle, rather than a shorter period, auditors are more likely to use a new audit system. Initial start-up expenditures will be more evenly distributed if there is a longer budgeting and review period, allowing them to be matched to cost reductions in subsequent years.

According to the previously mentioned study, auditors are more inclined to adopt new technology when they are aware that the managing partner is supporting adoption across the organization.

Compared to smaller or state-owned businesses, the Big 4 enterprises employ technology more frequently compared with smaller organizations or state-owned organizations (Bierstaker et al. 2014; Janvrin et al. 2009). When compared to their smaller competitors, these major corporations have been able to invest far more in technology, this is the first reason why this happens. Big 4 companies have been able to use their worldwide reach to create and put into practice cutting-edge technological solutions that can help them do their jobs more quickly and effectively. On the other hand, smaller businesses can lack the financial means to invest in

advanced technological solutions and rely more on manual procedures or antiquated technology.

In addition, bureaucratic procedures and rules may restrict the speed with which state-owned organizations may embrace new technology. The Big 4 firms are therefore frequently seen as pioneers in adopting and applying technology in the auditing sector.

Internal auditing businesses want to advertise their pioneering and inventive character, therefore technology adoption is motivated by more than just technical considerations (Manson et al. 2001). Businesses may show their dedication to offering their clients the most modern and effective services by investing in the latest technological solutions. This may send a strong message to potential clients, who may be more inclined to pick a business that comes out as creative and forward-thinking. Additionally, the utilization of technology may be a useful tool for attracting and retaining personnel, especially those seeking a contemporary and exciting work atmosphere.

Companies that are viewed as technology leaders are frequently successful in recruiting top individuals, who are willing to work with the newest tools and methods in their industry. Overall, the use of technology in the internal auditing sector is not only motivated by technical factors but also by strategic and branding factors that may aid businesses in maintaining their competitiveness in a continually changing market (Kotb & Roberts 2011; Manson et al. 2001).

In response to the attractiveness given by employers' use of technology, they demand that new recruits must have the skills and expertise required. As a result, internal audit teams can be particularly interested in individuals with great technological aptitude and expertise (Cangemi 2015).

Furthermore, growing the acceptance and utilization of technological solutions may be done in a very effective way by having an IT specialist on the team (Vasarhelyi & Romero 2014). IT specialists may assist in troubleshooting problems, ensuring that technological solutions are used properly, and training and supporting team members in the use of technology. This might make it easier for the team to properly utilize technology's advantages and remain abreast of current best practices and trends in the market.

3.3 Continuous Auditing and Continuous Monitoring

Internal auditing techniques such as continuous auditing and continuous monitoring are crucial if you want to improve the efficacy and efficiency of your auditing procedures. Continuous auditing is the process of continuously reviewing operational and financial data in real-time or very close to real-time (Cangemi 2010; Chiu et al. 2014). It requires the application of cutting-

edge technology and automated systems to routinely and methodically review transactional data to spot abnormalities, mistakes, or fraudulent activity. With this proactive approach, auditors may quickly identify problems, reduce risks, and offer pertinent suggestions for process improvement. Continuous monitoring, on the other hand, entails the routine observation and evaluation of important controls and performance indicators (Chiu et al. 2014). It focuses on the assessment of risk management procedures, control actions, and adherence to rules and regulations.

Continuous monitoring makes it possible for the frontline operational teams who form the first line to react quickly and effectively to new risks. A constant monitoring of the organization's risk exposure is simultaneously gained by the second line of defense, which includes risk management and compliance operations, allowing them to improve tactics and controls. Continuous auditing, on the other hand, mainly benefits internal audit, the third line of defense. Continuous auditing enables independent and objective evaluations by automating the testing of controls and periodically reviewing processes, improving the overall assurance of the risk management system. After recalling the three lines of defense, it is appropriate to say that continuous monitoring is done by the first two lines of defense, namely business and internal controls; while continuous auditing is done by the third line of defense, internal auditing (Littley 2012).

Internal auditors may quickly identify control weaknesses, spot developing risks, and guarantee compliance with company policies by employing continuous monitoring. Continuous monitoring and auditing provide firms with more certainty about their internal controls, data integrity, and compliance initiatives, which eventually leads to increased operational effectiveness and risk management.

Continuous auditing and continuous monitoring have opposite relationships (Coderre & Police 2005). The efficacy of risk management and control is measured and improved by using all three lines of defense.

If the level of monitoring is low, it will be necessary to increase the effort made by the third line of defense, and hence improve and implement new continuous auditing applications; vice-versa, if the level of continuous monitoring is high, the effort of the third line of defense can be reduced.

In order to ensure the correct use of continuous auditing and monitoring tools, internal auditors are required to improve their technical capabilities to stay up-to-date on new technological

developments (Braun & Davis 2003; Almaqtari et al. 2020; Lois et al. 2020). Auditor education on pertinent software, tools, and data analytics methodologies is necessary as firms become more dependent on digital systems and processes. This gives them the ability to use automation, artificial intelligence, and machine learning to successfully carry out continuous audit and monitoring tasks. Internal auditors may evaluate huge amounts of data rapidly, spot patterns, identify possible risks, and detect control gaps more precisely by adopting these technological innovations.

The whole organization gains advantages from the use of artificial intelligence technologies for continuous monitoring and continuous auditing that go beyond the scope of audit procedures. Internal auditors may offer insights to the company by utilizing AI's capacity to spot patterns, risks, and abnormalities in real-time. Through rapid decision-making and risk reduction, this proactive strategy improves operational effectiveness and protects the organization's reputation. By using these insights to streamline procedures, cut costs, and stimulate innovation, the company acquires an advantage over the competition. For this reason, internal auditors are essential in encouraging their firms to use software and tools for ongoing auditing and monitoring (Cangemi 2010). The effectiveness and efficiency of audit processes might be considerably improved by these technologies. Auditors may accelerate data collection, analysis, and reporting while minimizing manual labor and human mistake by utilizing automation and sophisticated analytics. Additionally, with the use of technological tools, auditors may give management real-time information and recommendations that will help them improve operational performance.
There are currently over 50 software alternatives for continuous auditing on the market (Rikhardsson et al. 2019), which reflects the rising demand for these solutions. Finding the best software for each organization's particular needs, nevertheless, is a challenge. Software vendors are attempting to create and market solutions that can be customized for different sectors and business sizes as part of a drive toward standardization. Big 4 companies are essential to this standardization process because of their depth of industry knowledge and experience. They may aid businesses in choosing the best software and successfully installing it by drawing on their experience and knowledge that have a track record of success.

Alles et al. (2006) point out how the formalization of procedures in the implementation of continuous auditing methodologies is crucial and very often underestimated. The goal of implementing continuous auditing systems should on the one hand help the organization in terms of efficiency, effectiveness, timeliness, and cost reduction and, on the other hand,

automate activities, which, however, can only be so provided that there are not too many variables influencing the auditing and monitoring operation.

This need for formalization is also given by the enormous amount of data that companies collect and have at their disposal (Almaqtari et al. 2020).

Organizations frequently gather data from several sources, which can lead to information silos and fragmentation. Organizations require a strong data integration system to overcome this issue. The process of merging data from many sources, formats, and systems into a single, cohesive picture is known as data integration (Zhang et al. 2015).

Organizations may get rid of data silos, improve the accuracy of their data, and establish a single source of truth by putting in place a sound data integration strategy. Better decision-making, enhanced data analysis, and a more thorough awareness of the business environment are all made possible by this unified data ecosystem.

Coderre & Police (2005) states the steps to implement effective continuous auditing inside the organization:

1. Implementing a strategy and plan for ongoing audits;
2. Getting data for regular usage;
3. Creating indicators for continuous auditing (recurrent risk and control evaluation);
4. Managing and reporting results.

Peirson published a report in 2010, where it explains the benefits of continuous monitoring and auditing:

Benefits of continuous monitoring:

- An organization may increase value through better financial and operational controls and accelerate reporting to facilitate quicker decision-making and business improvement by using continuous monitoring;
- Real-time exception detection for real-time answers;
- Reduce and eventually eliminate ongoing compliance expenses. Substitute automated detective controls with human preventive controls. Create a more automated, labor-efficient risk-based control environment;
- Increase shareholder value and competitive advantage.

Benefits of continuous auditing:

- Improve risk and control certainty, typically in the same or less time than traditional methods;

- Reduce expenses, including internal audit fees and fees related to unresolved control inadequacies;
- Expanding internal audit coverage with little or without additional expense, achieving a more comprehensive, effective auditing process, reducing audit cycles, and spotting control concerns in real time are all goals.

Process and Methodology in Continuous Auditing

Continuous auditing involves constant and ongoing monitoring of financial data to improve the efficacy and efficiency of the auditing process. The uniformity of data is a major problem (Zabihollah et al. 2002), but it is essential for the effective use of continuous auditing. It is essential to create uniform formats, structures, and definitions across many systems and sources so that software can analyze and understand the data properly. This standardization guarantees that possible dangers, mistakes, and abnormalities may be reliably detected by the program. Additionally, continuous auditing includes various levels of automation, from the fundamental data collection and uploading to the incorporation of sophisticated software that enable continuous monitoring of financial occurrences.

Due to this automation, auditors can quickly discover problems and take appropriate action. Privacy is still a problem with ongoing audits, though (Lois et al. 2020). Authorized auditors are the only people with access to the data, which helps to protect sensitive information's security and maintain confidentiality. Strict processes and controls are implemented to guarantee data security and follow legal requirements for confidentiality and privacy.

3.4 Data Analytics and Big Data

We will now concentrate on the relationship between internal audits, big data, and data analytics. This chapter emphasizes the crucial role that data analytics and big data approaches play in accomplishing continuous auditing goals, building on the preceding exploration of the idea of continuous auditing and monitoring.

We will examine the benefits and drawbacks of adding big data and data analytics into internal auditing, emphasizing their potential to transform audit procedures and motivate more powerful risk management approaches.

The term "audit data analytics" refers to the use of sophisticated analytical methods and equipment to analyze vast amounts of data while conducting an audit. In order to analyze risks and help auditors spot any mistakes, fraud, or noncompliance, it entails analyzing and

interpreting data to find patterns, anomalies, trends, and other pertinent information (Council 2017).

Benefits of Audit Data Analytics:

- Increased efficiency: audit data analytics speeds up the processing and analysis of enormous volumes of data, automating tedious operations and lowering manual labor. Auditors may concentrate more on data analysis and decision-making because of this efficiency;
- Enhanced risk assessment: audit data analytics assists auditors in identifying and comprehending possible risks related to financial reporting, internal controls, and regulatory compliance by analyzing large data sets. It helps auditors to reach more well-informed conclusions about the areas demanding deeper investigation (CaseWare Analytics 2017), sometimes more sophisticated methods are able to completely replace the sampling methodology and act on the entire population, improving the quality of the test and decreasing the risk involved, because the entire reference population has been tested;
- Increased detection of anomalies and irregularities: data anomalies, unusual trends, and exceptions that can point to fraud, mistakes, or noncompliance can be found using audit data analytics. This makes it easier for auditors to conduct inquiries and audits that are focused and risk-based;
- Continuous monitoring and control testing: as already explained, internal auditors can conduct ongoing monitoring and real-time control testing thanks to audit data analytics, they visualize via dashboard or receive notifications when certain limits have been exceeded, being updated instantly. Continuous data analysis enables auditors to quickly spot control flaws, variances, and developing risks, enabling immediate remedial action;
- Data-driven insights: Internal auditors are given data-driven insights and important knowledge about the operations, procedures, and performance of the company using audit data analytics. These can aid in making decisions, enhancing processes, and boosting organizational efficiency.

Issues and Challenges of Internal Audit Data Analytics:

- Data quality and integrity: the data utilized for audit data analytics must be precise, comprehensive, and reliable. The reliability of analysis and the accuracy of audit conclusions may be impacted by poor data quality, inconsistent data formats, and difficulties integrating data. Problems with data capture and extraction might also make

it difficult to use internal audit data analytics (Ramlukan 2015). The efficacy of data analysis is hampered and the amount of knowledge that may be gained is constrained by incomplete or unavailable data sources. To overcome these obstacles, organizations must assure reliable data collection procedures, accurate data source integration, and efficient data cleansing methods;

- Data governance and access: access to pertinent and thorough data from many systems and departments is required by audit data analytics. To safeguard data integrity and maintain data confidentiality, internal auditors must implement suitable data governance procedures and guarantee appropriate access permissions (Council 2017);
- Data privacy and security: internal auditors are required to resolve data privacy issues and adhere to data protection laws. To prevent unauthorized access or breaches, sensitive and private data should be safeguarded throughout the whole audit data analytics process, including data collection, storage, and transfer (Council 2017);
- Integration with audit processes: it could be necessary to modify the audit process' current reporting, procedures, and techniques in order to incorporate audit data analytics. To get the most benefits, internal auditors must integrate audit data analytics effectively and link it with their entire audit approach;
- Interpretation and judgment: accurately evaluating the findings of complicated dataset analyses may be difficult. Internal auditors need to use sound judgment and skepticism to properly assess the data and reach relevant conclusions;
- Increased costs: costs may increase due to the acquisition and maintenance of software and training of staff in using them. The audit team's limited technical expertise may make it difficult to employ data analytics tools and procedures effectively (Chartered Professional Accountants 2017). Audit professionals must get training and upskilling in order to acquire essential proficiency in data processing, analysis, and visualization.

To fully realize the potential of internal audit data analytics, it is crucial to train staff members in its use and to assemble a team with IT expertise (CaseWare Analytics 2017). Organizations may provide their auditors with the technical know-how they need to properly use data analytics solutions by offering training (Tang et al. 2017). With the help of this training, auditors may rapidly evaluate massive amounts of data, spot risks, detect abnormalities, and gather crucial information for making decisions. A deeper knowledge of the organization's data architecture and systems is made possible by the collaboration between auditors and IT experts that is fostered by the team's inclusion of IT expertise. The team is able to use cutting-edge technology for continuous monitoring and control testing thanks to this partnership, which also improves

the integration of data analytics into the audit process. It also assures the quality and integrity of the data.
Organizations may exploit the advantages of internal audit data analytics, enhance audit quality, and provide value by investing in training and developing a multidisciplinary team (Deloitte 2016).

Several elements that affect its acceptance and efficacy have an impact on the usage of internal audit data analytics. First, client expectations are crucial. Clients want auditors to use data analytics to get deeper insights into business operations, uncover patterns, and give actionable suggestions as enterprises increasingly seek value-added audit services. This requirement encourages auditors to adopt data analytics as a way to fulfill client expectations and provide more thorough audits that are insightful (Chartered Professional Accountants 2017).
The use of data analytics is also driven by competition among audit companies (Walker et al. 2019). Businesses that successfully use data analytics to their advantage can provide more thorough and effective audit services, giving them a competitive edge. Audit companies are aware of the need to invest in data analytics skills and use technology to deliver improved audit outcomes in order to stay ahead of the competition.
Another important element is the availability of qualified auditors who are also data analytics experts (Walker et al. 2019; Li et al. 2018). With the proper technical training and understanding, audit professionals may use data analytics tools and procedures efficiently. The ability to extract valuable insights from complicated datasets and successfully convey their conclusions to stakeholders is a skill that skilled auditors have mastered. These skills include data manipulation, statistical analysis, and programming.
Internal audit data analytics are also more likely to be used by customers that have sophisticated enterprise resource planning (ERP) or information technology (IT) systems (Eilifsen et al. 2020). The abundance of structured data that these systems frequently produce makes it simpler for auditors to acquire, retrieve, and evaluate data. Businesses that have established ERP or IT systems are more likely to use data analytics because they have the infrastructure and standards for data quality in place to facilitate efficient analysis. This factor relates to the fact that the Big 4 are facilitated and have greater degrees of advancement than smaller players or government agencies (CaseWare Analytics 2017; Chartered Professional Accountants 2017). This is because larger clients in terms of size have more advanced procedures and are more structured.

Big data

Due to its major influence on the development of contemporary auditing techniques, big data is strongly tied to the subject of internal audit data analytics. Big data is the term used to describe the enormous amounts of organized and unstructured data that businesses create from a variety of sources, including transactions, social media, sensors, and more (Gandomi & Haider 2015). Big data is used in internal audit data analytics to uncover trends, find anomalies, and improve risk assessment and fraud detection.

Big data requires the use of advanced analytics techniques and tools in order to be processed and analyzed properly due to the massive volume, velocity, and variety of the data (Gandomi & Haider 2015; Zhang et al. 2015). Internal auditors may make sense of the enormous volume of data and gain insightful information by using data analytics approaches including statistical analysis, machine learning, and data visualization.

Big data also makes it possible for auditors to undertake analysis in real-time or very near real-time, improving the flexibility and responsiveness of internal audit activities. With the capacity to process and analyze data in real-time, auditors are better able to spot anomalies, identify developing risks, and provide management prompt suggestions.

Big data presents numerous challenges and gaps that organizations must address to ensure its effective utilization. These gaps include data consistency, data integrity, data identification, data aggregation, and data confidentiality (Zhang et al. 2015).

- Data consistency is the need that data to be consistent and standardized across many systems and sources. Unreliable analyses and insights might result from inconsistent data;
- The correctness, comprehensiveness, and dependability of data are the main topics of data integrity. It is essential to maintain data integrity to guarantee that the analysis and decision-making processes are founded on reliable data;
- The capacity to correctly identify and categorize pertinent data among the enormous amounts of available information is referred to as data identification. The efficacy and efficiency of data analytics activities are increased by using proper data identification to make sure auditors concentrate on the most relevant data sets;
- Data aggregation is the process of compiling information from many sources into a single, cohesive format for analysis. Integrating several data sets is necessary for efficient data aggregation, but it can be difficult and time-consuming;
- When working with large data, data confidentiality is an important factor. Ensuring the security of sensitive data and safeguarding it from unwanted access or breaches is

crucial as businesses gather and analyze enormous volumes of sensitive data. To protect data confidentiality, organizations must establish strong security measures, data encryption, access controls, and privacy rules;

- The idea of the "black box" might also cause opposition to the use of big data (Ramlukan 2015). Some complex data analytics models and procedures are opaque, which may make people wonder about the audit process' dependability and openness. To overcome this obstacle, auditors must work toward openness by outlining the data analytics methodology and underlying assumptions to provide stakeholders with trust in the findings.

3.5 Robot Process Automation

The term "Robot Process Automation" (RPA) refers to the use of software "bots" to automate routine, rule-based processes. By automating data extraction, analysis, validation, and reporting tasks, RPA technology helps auditors speed and improve numerous audit operations (Cooper et al. 2019; Moffitt et al. 2018).

Robot Process Automation (RPA) works best when used with clearly specified procedures. RPA may be used to automate processes that have distinct, consistent phases and little variance (Moffitt et al. 2018). These procedures frequently include numerous, repetitive actions that are prone to human mistakes, take up a lot of time, and demand a lot of resources. Organizations can obtain considerable cost reductions and efficiency advantages by utilizing RPA in these situations. The automation of these repetitive processes frees up human resources to concentrate on more intricate and strategic duties that call for analysis and critical thought. Therefore, RPA becomes a suitable option to simplify operations and improve overall productivity when procedures are well-defined and entail high-volume, repetitive work (Moffitt et al. 2018).

Benefits of RPA

Numerous advantages of Robot Process Automation (RPA) have been cited and debated by Cooper et al. (2019). RPA has a huge benefit in that it may drastically save processing time, especially for routine, repetitive, and rule-based operations. RPA greatly accelerates the process by automating these tasks and removing the need for manual involvement. In addition to boosting efficiency, this accelerated speed also enables auditors to devote more time and resources to value-added tasks like data analysis, risk evaluation, and strategic decision-making. RPA also helps to increase accuracy by reducing human error and ensuring that set rules and processes are consistently followed.

RPA considerably improves the quality and dependability of audit procedures by being able to perform tasks accurately while removing the possibility of human oversight.

Limitations of RPA

While Robot Process Automation (RPA) has many benefits, it's also necessary to take into account its restrictions and potential downsides (Cooper et al. 201). Potential effects on employment are a top worry. Certain jobs and job responsibilities may be replaced as a result of task automation using RPA, especially those that require repetitive and rule-based work. People whose tasks are automated may experience job loss and unemployment as a result of this. It seems sense that people are afraid of losing their jobs because doing so might result in income inequality and societal issues. It is important to keep in mind that the effects of automation on employment are complicated and vary in strength between sectors and job categories.

The introduction of new technology frequently opens doors for the creation of new positions and the development of new skills. These potential difficulties may be reduced, and a seamless transition to a more automated future can be ensured, by properly managing the automation transition and reskilling the workforce.

Robot Process Automation (RPA) deployment has been proven to boost a company's efficiency and effectiveness, according to research done in 2019 by Cooper et al. Intriguingly, the survey found that even though RPA was used, the majority of firms did not report a decrease in headcount or an increase in recruiting. Instead, the emphasis was on increasing the productivity of the current workforce. Additionally, it was shown that the implementation of RPA had favorable effects on employee job satisfaction, work-life balance, and employee turnover rates. According to the study's respondents, exposing staff to programming and automation would be advantageous and encourage them to use new technologies. These results show how RPA has the ability to improve employee satisfaction by bringing about good organizational changes.

To allow intelligent automation, RPA may be combined with other cutting-edge technologies like artificial intelligence (AI) and machine learning (ML). Bots can manage unstructured data, comprehend natural language, and make choices based on established rules or algorithms thanks to AI-powered RPA.

We will examine these technologies and their integration in a next paragraph of this chapter.

3.6 Process Mining

When used in the context of internal auditing, the term "process mining" refers to the methodical examination of operational data by an organization to understand its process, spot inefficiencies in those operations, and identify possible risks and control gaps, using contemporary information technology system, such as the Enterprise Resource Planning systems (ERP) (Jans, Alles, and Vasarhelyi 2013; Eulerich et al. 2021; Jans, Alles, and Vasarhelyi 2014).

Jans, Alles, and Vasarhelyi (2014) state: ‘‘The basic idea of process mining is to extract knowledge from event logs recorded by an information system’’ where an event log is ‘‘a chronological record of computer system activities which are saved to a file on the system.’’

It entails the extraction of event logs from multiple information systems using specialized software tools and methodologies, followed by the analysis and visualization of these logs to reveal the real activity flow, deviations from established protocols, and process bottlenecks.
Process mining for internal auditing is used to give unbiased and data-driven insights into the efficacy and efficiency of an organization's internal control systems. Internal auditors can evaluate the actual execution of processes to prepare process models or benchmarks by looking at the event logs.
Internal auditors can acquire a deep understanding of the organization's processes through process mining, including their execution sequences, times, and resource usage. It makes it possible for auditors to spot process abnormalities including deviations from standard operating procedures, unnecessary manual involvement, or inefficient resource allocation. Process mining enables auditors to identify areas of concern and prioritize their audit efforts by visualizing the process flow and highlighting these deviations.

Process mining is a good internal audit support tool because it possesses three essential features (Jans et al. 2011):

- First off, it makes use of log data, including meta-data (*meta-data describes various attributes of the primary data, helping to provide context, structure, and meaning to it. This extra information may contain specifics like the creation date, author, file size, file type, location, rights, and more*), that is independent of the auditee. This makes it possible for auditors to impartially retrace the real process flow that preceded a transaction, such as the payment of an invoice. Auditors can get a thorough knowledge

of the completed process and spot any deviations or non-compliance by depending on objective data;

- Second, process mining offers a picture of the process that goes beyond just using developed process models. Instead, auditors might use the identified, real process model as a point of departure for their actions. As opposed to depending simply on hypothetical or idealized process models, this enables auditors to match their audit operations with the processes that are taking place in the actual world;
- Process mining's capacity to increase the scope of audits is its third beneficial internal auditing feature. Using process mining techniques, auditors may assess both controls and details. They can assess how well internal controls are working and check the correctness and compliance of individual transaction information. In order to ensure a thorough and effective audit process, auditors may evaluate both the general control environment and the specifics of individual transactions using this all-encompassing methodology.

The data that is routinely gathered in many firm IT systems serve as the foundation for process mining. For each event in this information system, four crucial features must be retrieved in order to provide efficient process mining analysis (Eulerich et al. 2021).

- The first step is identifying and documenting the activities occurring during the event. This might involve doing things like signing, approving, or making payments, and giving information on the particular activities being carried out throughout the process;
- Second, the instance of the process connected to the event has to be recorded. This is the specific thing or things that are connected to the event, such as an invoice, a receipt, or a purchase order. It aids in grouping and evaluating events that pertain to the same process instances;
- Thirdly, it's important to identify the event's creator or accountable party. This feature offers details on who planned or carried out the activity, enabling the study of resource use and accountability;
- The event's timestamp, which captures the precise day and hour it happened, must also be documented. The examination of process lengths, waiting times, and the temporal order of occurrences is made possible by the timestamp, offering important insights into the order and timing of operations.

Businesses may use process mining to assess and enhance their business processes based on the automatically acquired data by extracting these four characteristics from the information system.

Approaches in process mining

Five essential techniques, together known as process mining, enable organizations to extract insightful information from their event data (Eulerich et al. 2021; Jans, Alles, and Vasarhelyi 2014; Jans et al. 2019):

- Process discovery: based on event data, process discovery seeks to automatically build a process model or representation of a business process. It entails examining the event log to determine the order of events, their connections, and the process flow as a whole. Techniques for discovering the true behavior of a process, including variances, exceptions, and possible bottlenecks, can serve as a starting point for further investigation and improvement;
- Conformance checking: to determine the degree of conformity to the anticipated process flow, conformance checking compares the observed event log data with a pre-defined process model. It indicates deviations, non-compliant actions, and dependencies on the control flow that have been broken. Organizations can assess their processes' effectiveness and compliance with specified process models and standards by using conformance checking;
- Performance analysis: by examining temporal factors and resource usage, performance analysis focuses on assessing the efficacy and efficiency of a business process. It assists in locating process bottlenecks, holdups, and potential improvement areas. Organizations may monitor and optimize process cycle durations, waiting times, throughput, and resource allocation using performance analysis methodologies to improve process performance;
- Social network analysis: in process mining, social network analysis focuses on the connections and interactions among the parties (resources or people) participating in the process. Social network analysis may bring light on information flow, bottlenecks, and collaborative effectiveness by examining communication patterns and dynamics. With the aid of this strategy, firms may better comprehend the social components of their operations and spot chances to enhance information exchange and communication;
- Decision mining and verification: decision mining focuses on examining the decision-making behavior inside a process as well as the decision points. It seeks to extract from the event log data decision rules, decision outcomes, and decision dependencies. On the other side, decision verification tries to evaluate the accuracy and conformance of decisions made during process execution. Organizations may learn more about decision-making trends, assess decision compliance, and spot opportunities for decision-process improvement by evaluating decision-related data.

Advantages and limitations of using process mining

Process mining has a number of benefits over conventional auditing techniques, improving the efficiency and worth of the auditing process. First off, it makes it easier for auditors to compare real operations to specified procedures and spot deviations, inefficiencies, and compliance gaps (Jans, Alles, and Vasarhelyi 2013). Event logs' richness, which includes thorough input and meta-data organized logically by time and source, offers a lot of data for analysis (Jans, Alles, and Vasarhelyi 2013). Additionally, process mining enables auditors to examine the full population of data rather than just a small sample, resulting in a deeper evaluation (Jans, Alles, and Vasarhelyi 2013). Process mining enables the creation of fresh analyses that significantly enhance the assurance function by merging data from many corporate departments (Eulerich et al. 2021).

Although process mining has many advantages, its use in auditing has several restrictions. The demand from auditors and the economic and human variables affecting its execution constitute one important restriction. The desire of auditors and the resources available determine whether technology-based auditing procedures are used (Eulerich et al. 2021). It's also crucial to understand that frauds that leave no electronic trail or are not recorded in event logs cannot be caught via process mining (Jans, Alles, and Vasarhelyi 2014). The potential for some fraud types to go undetected emphasizes the need for more fraud detection techniques. Process mining's capacity as a deterrent also depends on the chances and incentives available to those who are inclined to commit fraud.

Below you can see an exhaustive list of all the advantages and disadvantages in the table taken from Eulerich et al. (2021).

Benefits and Advantages	Challenges and Disadvantages
• Transparency: Comprehensive overview of potential risks • Quick identification of risks within the entire company (full population testing) instead of sampling • Detailed identification of risks (cases, documents, employees, etc.) • Data-based decision-making • Generation of necessary information to measure risks • Creation and calculation of KRIs & KPIs • Presentation of correlations between deviations, key figures, and time periods • Identify, assess, and monitor risks and make changes (transform processes) • Saving of costs as well as time and manual efforts • Added value for documentation and communication during risk identification, and	• Need for precise analysis approaches due to complex and uncommon business environment • Challenges posed by data integrity, data availability, or privacy issues related to company-specific IT structure or employee-related data • The evaluation of process mining results requires a very high level of company-, process-, and industry-specific expertise. • False positives versus false negatives influence the overall assessment of specific results. • Use of process mining requires expertise in data analysis and knowledge of relevant systems (e.g., SAP)

Figure 11: Advantages and disadvantages of process mining.

Methodology

To understand the steps and procedure of process mining, let us first understand what an event log is: an event log is a structured data set that records the orderly progression of actions or events carried out inside the information systems of an organization. It acts as the analysis's main input for process mining.

An event log normally consists of discrete entries, also known as events, that detail each activity that takes place while a business process is being carried out. The most common way to display these events is in a table style, where each row corresponds to a particular event and the columns record different information related to that event.

Numerous abnormal transactions were discovered through process mining of event logs, including those involving payments made without authorization, breaches of segregation of duties, and transgressions of the company's internal rules (Jans, Alles, and Vasarhelyi 2013).

Process mining uses information extracted from event logs to find, monitor, and enhance actual processes (van der Aalst 2010).

Using event log data from information systems, the process mining technique uses a systematic way to extract, analyze, and improve business processes developed by Bozkaya et al. (2009). To acquire insights and improve process effectiveness, it includes steps including log preparation, log inspection, control flow analysis, performance analysis, and role analysis.

- Log preparation: in this first stage, the information system's event log is retrieved and ready for analysis. In order to do this, the pertinent event data must be gathered. This data generally consists of timestamps, activity names, case identifiers, and other features. To make sure the log is compatible with the process mining tools and techniques used in later stages, it is cleaned, converted, and formatted;
- Log inspection: the prepared event log is examined during the log inspection step to get an understanding of the procedure. This stage entails studying the event data's contents, visualizing the main events, and figuring out how they happened in order to detect any trends or abnormalities. Log inspection offers a quick overview of the procedure and aids in locating key areas for additional investigation;
- Control flow analysis focuses on recreating and examining the order in which process operations are carried out. This stage seeks to extract the process model or representation from the event log data, such as a process flow diagram. Control flow analysis shows the process's flow of control and uncovers the connections between activities as well as process variations and bottlenecks;
- Performance analysis: performance analysis examines the use of resources and temporal characteristics of the process. It looks at the length of tasks, the intervals between them, and measures for overall process performance including cycle durations and throughput. Organizations may improve the performance of their processes and resource allocation by using performance analysis to discover inefficiencies, delays, and resource bottlenecks;
- Role analysis: understanding the roles and responsibilities of the people or resources engaged in carrying out the process activities is the focus of role analysis. It entails figuring out who or what is involved in each activity and then examining how they interact and cooperate. Role analysis aids in determining possible role conflicts or process inefficiencies as well as task distribution and resource allocation assessments.

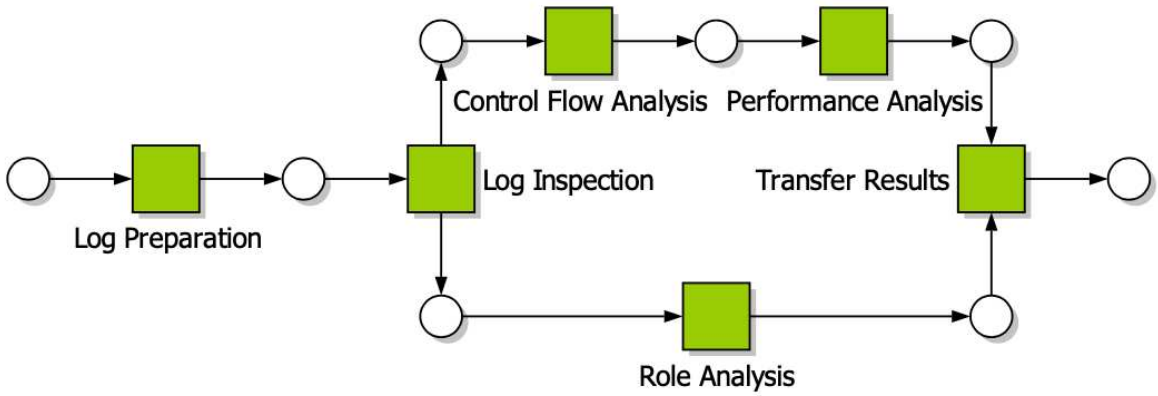

Figure 12: Process mining technique.

3.7 Artificial Intelligence

The application of cutting-edge technologies and algorithms to improve the efficacy, efficiency, and efficiency of auditing procedures is referred to as artificial intelligence (AI) in auditing. It entails using computer systems to execute operations including advanced data analysis, pattern identification, anomaly detection, and decision-making. AI systems can evaluate vast amounts of financial and non-financial data, spot possible hazards, find inconsistencies or fraudulent activity, and give auditors insightful data. By utilizing AI, auditors may increase audit quality, optimize their workflows, and unearth patterns or trends that would not be visible using more conventional audit techniques.

With AI now being used in auditing, there has been a substantial change in the industry, allowing auditors to use technology to provide more thorough and intelligent audit services.

Types of Artificial Intelligence used in Auditing

The three main categories of AI systems used in auditing are: Assisted AI systems, Augmented AI systems, and Autonomous AI systems (Albawwat & Frijat 2021).

- The most popular and least sophisticated are those called Assisted AI systems. They support auditors' decision-making by carrying out routine jobs that people currently undertake. These systems frequently have established workflows and depend on human direction and oversight;
- A collaborative approach to decision-making is required for Augmented AI systems, which entail robots acting. These systems are able to communicate with their surroundings and absorb information from auditors. They take advantage of AI's capabilities to boost the auditor's performance and offer insightful analysis and

suggestions. Despite some autonomy, these systems still need human input to make sure decisions are made correctly;

- Autonomous AI systems, the third category, are more sophisticated and less frequently utilized. These systems are capable of changing to different conditions and acting on their own without the direct involvement of auditors. They are more autonomous and capable of completing activities without human assistance. For efficient and effective auditing procedures, autonomous AI systems rely on cutting-edge algorithms, machine learning, and data analysis approaches.

Areas of application

The use of artificial intelligence (AI) in auditing is widespread and has a positive impact on the industry. Neural networks are one type of application that enables auditors to examine intricate data patterns and spot fraud or irregularities using sophisticated algorithms. Additionally, deep learning (DL) and machine learning (ML) techniques are used (Hasan 2021), enabling auditors to accurately anticipate the future based on previous data and extract useful insights from vast datasets. Natural language processing (NLP) is another significant application that is essential for effectively creating internal and external reporting. NLP improves audit planning and strengthens internal control procedures by automating processes like data extraction, analysis, and summary.

Additionally, internal auditors can resolve ambiguities in daily operations with the use of fuzzy logic (Khamis 2021), a sophisticated mathematical instrument. Keeping up with fuzzy logic developments enables auditors to detect and reduce risks brought on by ambiguous or imprecise circumstances more accurately.

Impact of Artificial Intelligence on tasks, knowledge, training and ethical aspects

The main effect of AI on auditors' jobs is to free them up to concentrate on higher-value work. Audits may be made more efficient by automating basic and repetitive processes, which frees up auditors' time for other responsibilities. To properly deploy AI, however, auditors will need to invest time in learning about AI systems, checking the veracity of the data, comprehending it, and interpreting the outcomes (Henry & Rafique 2021).

The use of new technology, like AI, in the auditing industry has a variety of effects that are not equally felt by all members of the public. Although partners in audit companies profit from higher product quality, more efficiency, and lower human resource expenses, possible difficulties may be encountered by young employees. The roles and responsibilities of junior workers may change as AI investments mature and implementation advances, with the

displacement impact being obvious many years later (Fedyk et al. 2022). In order to ensure that the benefits of technology breakthroughs are spread fairly and that steps are made to help individuals impacted by changes in employment dynamics, it is critical to acknowledge these possible discrepancies and take proactive actions to address the impact on all levels of the workforce.

A larger focus on technological competence is required due to the impact of AI on auditors' knowledge, abilities, and practice. To adapt to the shifting environment, auditors will need to deepen their understanding of AI systems and pick up essential skills (Henry & Rafique 2021). Participants in the debate stressed that humans cannot be substituted by AI for the audit's human components, underlining the growing value put on interpersonal communication and intuitive abilities (Henry & Rafique 2021).

The degree of auditors' comfort and knowledge with such technology has a significant impact on their readiness to accept and use AI solutions (Albawwat & Frijat 2021). Auditors who lack trust or feel uneasy utilizing AI are considerably less likely to use these systems, even if they have major advantages and are thought to be valuable for their companies. The successful integration of AI in auditing methods is greatly influenced by the human component of auditor acceptance and adoption. Therefore, encouraging auditors to actively interact with AI systems might help them overcome their doubts and maximize the potential advantages these technologies may have for auditing businesses by fostering an atmosphere that supports training, assistance, and reassurance.

Auditors will require specific training to get the knowledge and abilities needed for working with AI systems, including having an understanding of AI concepts and coding (Henry & Rafique 2021; Chukwuani & Egiyi 2020).

Benefits of Artificial Intelligence

A number of advantages that result from the use of AI in auditing boost audit quality and overall efficiency. By automating repetitive and regular operations, AI technologies improve efficiency and effectiveness while freeing up auditors' time for more involved and valuable work (Hasan 2021). They guarantee consistent techniques and consistency in audit duties while lowering the risk of human mistakes. By facilitating organized workflows and procedures, AI improves audit engagement efficiency by giving auditors a framework to operate within. AI can evaluate vast amounts of data and give auditors insightful analysis and suggestions. This helps better decision-making and communication (Hasan 2021).

The potential for AI to lessen the likelihood of fraud is a big advantage. Advanced algorithms and data analysis methods are used by AI systems to find abnormalities, unexpected trends, or questionable transactions, which makes it easier for auditors to spot fraudulent activity. Additionally, because AI can evaluate data more accurately and dependably than human analysts, its use helps to enhance the quality of accounting information as a whole (Hasan 2021).

Law & Shen (2020) have revealed a strong correlation between using AI and better audit quality. Auditors may conduct more thorough studies, detect hazards, and find hidden patterns or trends that would not be visible using conventional audit procedures by utilizing AI tools and methodologies. In the end, this results in better audit quality and higher confidence in the audit results.

It is important to note that the use of AI in auditing has the potential to lower audit fees and may cause some human auditors to lose their jobs (Fedyk et al. 2022). However, as already explained, rather than completely replacing auditor functions, this displacement should be seen from the perspective of AI changing the nature of those roles. With AI integration, auditors may broaden their knowledge, concentrate on activities of greater value, and conduct audits that are both more effective and efficient.

Limitations of Artificial Intelligence

A number of hazards and difficulties are presented by the incorporation of AI in auditing, which must be properly handled. These dangers include protracted decision-making procedures since AI systems may consider a lot of options, which might cause delays in coming to a choice or conclusion. Building, maintaining, and upgrading AI systems may be expensive and call for considerable infrastructure expenditures as well as continual technical assistance (Hasan 2021; Goh et al. 2019).

The possible restriction of beginners' knowledge base represents another concern. If AI systems are frequently used, there is a chance that younger auditors won't learn how to use professional judgment and could wind up being unduly reliant on automated decision-making tools (Hasan 2021). Their capacity to independently examine and understand audit findings as well as their overall professional development may be limited by this.

There is also a chance that rivals may acquire AI tools and technology, which might result in a loss of competitive advantage or the abuse of these capabilities against the auditor. Additionally, the legality of the evidence produced by AI systems may be contested, and accusations of excessive reliance on decision support systems may jeopardize the auditor's reputation and responsibility.

Establishing strong governance structures and standards for the creation and use of AI systems in auditing is crucial to reducing these dangers. In order to guarantee the systems' correctness, dependability, and relevance, regular monitoring and upgrading are essential. Auditors should have appropriate training and education, with a focus on the value of sound judgment and analytical abilities. Artificial intelligence systems should be designed and used with ethical issues in mind to encourage accountability, transparency, and justice.

There are also ethical issues that arise with the use of AI in auditing that need to be addressed. Key concerns include issues including ingrained prejudice, probable job loss, excessive dependence on AI, security problems, and a lack of knowledge (Henry & Rafique 2021). It is crucial for auditors to traverse these moral dilemmas and guarantee that AI is applied ethically and in accordance with recognized professional norms.

But, Law & Shen (2020) strongly show that the use of AI in auditing does not result in the elimination of auditor positions, but rather results in a change in the skill set needed by auditors. Auditors can improve the quality of audits by utilizing AI technologies since these tools provide cutting-edge capabilities in advanced data analysis, pattern recognition, and anomaly identification. Due to the emergence of AI, auditors now need to adapt and learn new skills in order to make the most use of and analyze the insights offered by these technologies. Since auditors may use AI to undertake more thorough analyses and acquire deeper insights into financial and non-financial data, this change in the skill requirements for auditor employment adds to an overall improvement in audit quality.

Biases

The integration of AI in auditing also introduces potential risks related to biases that can impact decision-making and outcomes (Khamis 2021).

- Data-driven bias is one such issue, when AI systems provide biased results as a result of errors or skewed patterns in the underlying data. It can reinforce and exacerbate preexisting biases in the auditing process if the data used to train AI models is lacking, prejudiced, or otherwise inaccurate;
- Another issue is prejudice acquired through contact, in which case biases are taught to robots by the people who teach them. The AI system may accidentally accept and perpetuate those biases if the training data represents subjective or biased assessments, which might result in biased decision-making;
- Emergent bias, also known as algorithmic confirmation bias, is when AI systems protect people from opposing ideas and only present them with data that support their

preferences or beliefs. This may lead to the formation of a "personalization bubble" that restricts exposure to many viewpoints, so reinforcing biases that already exist and perhaps impeding the ability to make objective decisions;

- When stereotypical human interactions with the AI system unintentionally affect the system's behavior, conflicting-goals bias might develop. The results of the AI-based auditing process might be impacted by stereotype- or discrimination-based biases;

Auditors and developers must be watchful and dedicated to addressing data quality issues to address these biases, providing representative and objective training data. To detect and correct any establishing biases, AI systems should be regularly monitored and audited. Reduce prejudices by including diversity and inclusion practices in the training and development process. Additionally, building an ethical culture that stimulates critical thinking and increases awareness of biases can assist auditors in identifying and addressing any biases in decision-making.

To reduce the danger of biases and guarantee that AI technologies contribute to more objective and impartial audit conclusions, it is critical to prioritize fairness, transparency, and accountability in the design and deployment of AI systems in auditing.

3.8 Conclusions

This chapter has examined a number of important issues within the field of internal auditing and evaluated both their benefits and drawbacks. There is a recurring theme that emerges from the dynamism of technological change and trends to the potential of Continuous Auditing, Monitoring, Data Analytics, Big Data, Robot Process Automation, Process Mining, and Artificial Intelligence: the potential for improved efficiency, accuracy, and strategic insight. These benefits must be tackled, nevertheless, with careful consideration of obstacles including implementation difficulty, data privacy issues, excessive dependence on automation, and ethical issues.

It takes a careful balancing act of ongoing learning, adaptation, and the preservation of human judgment to successfully integrate these technologies into internal auditing. The wise use of these technologies has the potential to not only raise the position of internal auditors as the business landscape changes, but also significantly contribute to organizational growth and sustainability at a time of fast technological advancement.

Chapter 4: Redefining Risk Management, Controls, and AI Regulation

4.1 Introduction

The development of internal auditing is at a crucial crossroads as the technological revolution redefines company environments. The conventional frameworks explained in the first chapter, such as COSO, CobiT, and COSO ERM, are the foundations of this chapter as it explores the underlying change toward technology-driven internal auditing methods. It focuses on how technological tools like data analysis, artificial intelligence, robotic process automation, and process mining can help create more efficient, self-evident, and responsive control environments. This transformation from manual detective controls to automated preventative controls is specifically examined. Further benefits of this transformation are described in this chapter, including streamlined risk management, proactive controls, automated monitoring, and testing, as well as improved productivity and cost reductions.

The chapter provides the basis for understanding how the integration of technology is changing the fundamentals of internal auditing through this research.

We will go into more detail about the goals organizations should aim for by integrating technology into their internal auditing operations in the next sections. Designing and implementing improved and automated controls is one of these goals. Another is elevating control testing to make sure it's in line with corporate objectives.

In the last section we will try to illustrate the influence on technical innovation, ethical concerns, and regulatory compliance within diverse businesses, remarks will be made discussing the implications and possible regulation issues by the new European legislation controlling the use of artificial intelligence.

4.2 Improving the Framework of Risk Management and Controls

"Design and implement enhanced and automated controls": this approach refers to how businesses improve the efficacy and efficiency of their risk management procedures by incorporating cutting-edge technology into their control frameworks. By using this strategy, businesses may spot parts of their control framework that need extra attention, such as "hot spots" where vulnerabilities are more likely to occur, instances of duplicate controls, or controls that have been rendered obsolete by adjustments to processes or systems (KPMG, 2023). Organizations may make sure that their control environment is optimal and in line with their risk management goals by systematically evaluating and improving these factors. In order to improve control implementation, execution, and monitoring processes, automation is used,

allowing for real-time reactions to risks and reducing manual intervention. This strategy not only improves the organization's risk management, but it also makes sure that controls are adaptable and effective in the context of evolving risks and business conditions.

A variety of technologies that function in the front end and back end of the control framework constitute the tools used for creating and implementing upgraded and automated controls.

- Data analysis, robotic process automation, and process mining are critical components of the back end. The systematic evaluation of huge datasets for patterns, anomalies, and insights that might guide the design of controls is known as data analysis. Artificial intelligence helps by enabling the development of sophisticated algorithms that can identify potential dangers and recommend the best possible management measures. By automating repetitive processes, robotic process automation simplifies control execution and frees up human resources for more strategic initiatives. Contrarily, process mining provides a thorough visual picture of real operations, enabling businesses to see inefficiencies and chances to improve management;
- Key Control Indicators (KCIs) and graphical dashboards offer crucial information on the front end. KCIs are quantitative indicators that measure how well controls are working, enabling companies to keep an eye on the efficiency of controls in real-time. These indicators allow for fast reactions to changes from predetermined control levels. Graphical dashboards provide understandable visual representations of the state of compliance, risk levels, and control performance. This facilitates decision-making by providing complicated information in an understandable way, allowing stakeholders to quickly comprehend the broader control environment.

When front end components like KCIs and graphical dashboards are combined and integrated with back end tools like data analysis, AI, RPA, and process mining, organizations are empowered to not only improve the design and implementation of controls but also to create a more agile, responsive, and adaptable control environment that is in line with the dynamic nature of contemporary business landscapes (KPMG, 2023).

Several control strategies may be used to increase risk management and guarantee regulatory compliance in the context of creating and implementing upgraded and automated controls.

These control choices cover a range of strategies, each with varying degrees of human involvement and technological integration:

- Manual control option: this strategy heavily depends on monitoring and human involvement. This manual process could include written signatures and verbal conversation;
- Semi-automated control option: this strategy optimizes several phases in the control process by combining manual and automated components. However, before moving further, human authorization is still necessary;
- Configured control option: this approach involves standardizing and configuring controls inside systems. Through preset processes, any deviations from the established process are directed;
- Data analytic option: this strategy comprises an automated assessment of the data using data analysis tools. Automated processes are triggered by abnormalities or inconsistencies to do more research;
- Robotic control option: in this case, specialized control duties would be handled by software robots or bots. The bot may start workflows or escalate exceptions for human review based on established rules;
- AI control option: this method, which makes use of artificial intelligence, includes self-learning algorithms. Artificial intelligence digital assistants might review client onboarding paperwork, automatically fill out a checklist, and provide a streamlined summary for a customer service manager's approval. The AI might start resolution procedures if anomalies are found.

It is interesting to notice that less and less human involvement is required in control procedures as technology develops. A commensurate drop in residual risk generally occurs when manual engagement is reduced. Organizations may benefit from the efficiency and accuracy provided by technology by adopting more automated and sophisticated control systems, which will reduce human error and ensure a reduced level of residual risk (KPMG, 2023).

4.3 Improvement of Testing Activities

It is standard practice in organizations to use risk management, internal controls, and compliance. It relates to raising the efficiency of procedures that guarantee the accuracy of financial reporting, deter fraud, and sustain operational effectiveness.

It focuses on using various testing techniques to assess the efficiency of the current internal controls. It entails determining if the controls in place are functioning as expected and producing the desired results. Enhancing the testing of controls entails improving and

optimizing the techniques used to assess these controls, making sure they are thorough and trustworthy.

The following actions are necessary to improve controls testing:

- Risk assessment: recognize the dangers facing the company and find the controls that will handle them. Not every control is created equal; some are more important than others for maintaining financial integrity. Sort controls according to significance;
- Testing Procedures: create methods for testing the effectiveness of the controls. To evaluate the controls' responsiveness, this may entail going over the documentation, having interviews, going through the system, and modeling situations;
- Sample Selection: determine appropriate transactions or processes to test using the sample selection procedure. In order to assure reliable findings, a representative sample is chosen because it is sometimes not practical to evaluate every transaction;
- Testing Tools: implement technologies and methods that can automate some steps in the testing process. For example, data analytics may be utilized to find trends or anomalies that point to control flaws;
- Test Frequency: establish the recommended testing frequency. It may be necessary to test important controls more often than less crucial ones. Controls are continually tested to guarantee their efficacy;
- Documentation: keep complete records of the testing process, including the steps taken, the outcomes attained, and any problems found. These records are useful for audits and evaluations.

Technology provides a variety of instruments that accelerate and strengthen testing processes. Large datasets may be analyzed to find patterns and anomalies that can be used to expose potential control flaws. This is made possible by data analytics and machine learning. Automation makes it easier to carry out testing procedures, enabling thorough analyses free from the limitations of manual work. Technology also helps with continuous review of controls and real-time monitoring, allowing firms to quickly correct any deviations or vulnerabilities that may emerge. Because of this, incorporating technology into these crucial phases improves the precision, effectiveness, and efficiency of internal control systems, supporting organizational resilience and regulatory compliance.

The use of automation provides a variety of compelling benefits in the field of control testing. First off, automation greatly expands the range and depth of testing by making it possible to quickly and thoroughly evaluate greater volumes, including enlarged sample sizes. This improved capability quickens the testing procedure without sacrificing precision or quality. Additionally, automated controls produce standardized outputs that enable a more

comprehensive testing strategy, particularly in the context of global controls. By streamlining the review process with this standardized data, efficiency and effectiveness are both improved.

A market perspective

According to recent experience, (KPMG, 2023) a bank's procedures and controls were recently reviewed, and during the inspection that followed, an astonishing total of more than 4000 controls were found. Surprisingly, more than 90% of these controls were manually operated, demonstrating a heavy reliance on human involvement. In addition, the assessment found that over 65 percent of these controls fell under the category of detective controls, which are intended to find problems or abnormalities after they have already happened. This implied a greater focus on responding to problems than proactively preventing them. The labor-intensive manual control testing procedure was being carried out by a sizable number of people, which emphasized the lack of automated approaches and exacerbated the inefficiencies.

KPMG in the UK conducted a thorough controls study in response to these discoveries using their Decipher Risk and Controls Insights Tool. This investigation produced some astounding revelations and chances for development. Notably, it was determined that the existing controls could be impressively reduced by 40%, leading to a considerable decrease in the overall number of controls. The required risk mitigation strategies would still be maintained while efficiency would be improved. Additionally, the research revealed that more than 50% of the remaining controls had the potential to be automated, indicating a substantial window of opportunity for deploying technology solutions to improve control procedures and decrease the reliance on manual labor.

In addition to these immediate advantages, the research revealed more general trends and patterns in the bank's control environment. These observations were labeled as critical topics for additional transformation programs, indicating that the findings may act as a base for subsequent strategic efforts focused at thorough control improvement. In conclusion, the case study emphasizes the need of carefully analyzing and improving control processes, utilizing automation when practical, and employing cutting-edge analytical tools to find potential for efficiency gains and transformation.

Another example could be the use of controls for optimization and automation, a big financial services firm underwent a remarkable change. A remarkable 50% decrease in quality assurance (QA) time and associated expenses was achieved as a consequence of this project. Building on this outstanding accomplishment, the institution targeted a further 50% decrease in these indicators by implementing controls automation. This phase had a significant influence on the

overall degree of assurance and the knowledge gleaned from the quality assurance processes in addition to resulting in significant cost savings.

The institution switched to an automated risk-based sampling technique from a manual, random 2 percent sampling process. This new strategy was based on studying the complete population as opposed to just using small random samples. This strategy change enabled the company to obtain assurance from a far wider range of data, resulting in a more thorough understanding of risks and control efficacy.

This transformational journey demonstrates how the fusion of control optimization and automation may provide outstanding results. The institution's dedication to use technology-driven procedures led to not just significant cost and time savings, but also improved insight quality and depth. The organization was able to move away from conventional sample techniques and toward a more thorough and all-encompassing risk-based strategy by using the power of automation. Overall, this case study serves as an example of the genuine advantages that may be attained by strategically combining control optimization, automation, and cutting-edge sampling techniques within the context of quality assurance.

The last example refers to a renowned UK retail and commercial bank, KPMG (2023) organized a significant change in control testing. They worked with the customer to create a cutting-edge digital solution that will expedite the procedures involved in control evaluation by utilizing their experience. This ground-breaking approach smoothly automated the gathering of control-related data and its testing, and it also produced work papers for later human evaluation.

The outcomes of this project effort were outstanding. Within the same fiscal year, the client saw a quick return on investment and significant advantages. Notably, there was a significant increase in processing speed. Thanks to the effectiveness of automated bots, what formerly required 53 days of laborious manual work may be finished in just 12 hours. Processing times were significantly cut, which improved operational effectiveness and saved resources for more strategic projects.

The effectiveness of technologically driven solutions in improving control testing procedures is highlighted by this case study. The partnership between KPMG and the bank produced observable improvements in operational effectiveness, testing coverage, and processing speed. In addition to speeding up procedures, automation of control data collection and testing allowed for a more complete and detailed evaluation of controls, which improved the overall assurance and insights from the testing efforts.

The results of a recent survey conducted by KPMG (2021) of 300 key industry professionals, including Chief Audit Executives, Audit Directors, Vice Presidents, and Senior Managers, representing various sectors across 35 countries and territories, indicate that the internal audit landscape is about to receive a significant transformation. It is noteworthy that 60% of respondents indicated a high degree of technological maturity, highlighting the rising significance of incorporating digital technologies within the audit function. Additionally, 85% of respondents said they planned to hire experts in artificial intelligence (AI) and machine learning (ML), showing that the sector understands the crucial role these technologies play in boosting audit effectiveness and efficiency.

Internal audit teams are clearly adjusting to a changing risk picture as seen by the 49% of them who have already used agile approaches and the 19% who are actively engaged in the design stage of digital transformation. However, there is still room for improvement, as 13% of respondents felt unprepared to assess risks associated with developing technologies. The poll also showed that the demand for specialized subject matter expertise, which was mentioned by 39% of respondents, is what motivates the use of outside experts for Technology Internal Audits. Despite these obstacles, it is certain that technology is transforming internal auditing's future and positioning it to meet the needs of a more sophisticated and digital business environment.

Chief Audit Executives and Directors were thoroughly questioned in a separate poll by the Institute of Internal Auditors in order to acquire insights into the changing audit landscape for their 2023 (d) North American Pulse of Internal Audit report. By making up 19% of respondents' top audit goals, the poll showed how cybersecurity and IT are becoming increasingly important in audit strategies. It is interesting to note that about 70% of these audit units allocated resources to assessing high-risk areas, notably in cybersecurity and IT, at least once a year. Furthermore, over 80% of auditors consistently include fraud and IT issues in their audit procedures.

According to the survey, technology is also the common driving force behind the top three riskiest industries: cybersecurity, IT, and third-party relationships, all of which were rated as high risks by 78%, 57%, and 51% of respondents, respectively. These relationships frequently involve third parties providing crucial IT services. These findings highlight how important technology and cybersecurity are in determining the internal audit environment, indicating their growing importance in modern enterprise risk management.

4.4 Regulation with respect to the use of Artificial Intelligence

The Artificial Intelligence Act (AI Act), a complete framework created to traverse the changing world of AI technology, has several facets, which we shall explore in this paragraph. Artificial intelligence (AI), a rapidly developing field of technical innovation, has the potential to greatly benefit society and the economy across a wide range of business sectors and social spheres. The adoption of AI can create socially and environmentally beneficial outcomes through improved predictive capabilities, streamlined operational processes, resource optimization, and customized service delivery, providing crucial competitive advantages to both businesses and the European economy as a whole.

Although the underlying principles and procedures that enable AI's socioeconomic benefits are clear, they also carry the possibility of introducing new dangers or unfavorable effects on both persons and society. The European Union (EU) is dedicated to developing a well-calibrated strategy in light of the high speed of technological progress and the associated difficulties it poses. The foundation of the EU's strategic view is preserving its technical leadership and making sure that its citizens benefit from new technologies in accordance with EU values, basic rights, and guiding principles.

Scope of the regulation

The AI Act defines its regulatory scope with a set of clear objectives. The Commission has stated the following specific objectives for the proposed artificial intelligence regulatory framework in response to the current environment:

- Safety and Compliance: establishing strict guidelines that guarantee the security and compliance of AI systems released to the Union market is one of the main goals of the AI Act. With the help of these rules, AI technology will be held to the same standards as current legislation pertaining to basic rights and Union values. The Act intends to promote an environment where the integration of AI technologies is in harmony with the rights and values that form the foundation of the Union by requiring AI systems to function within the parameters of these set legal boundaries;
- Legal Certainty: the goal of the AI Act is to establish legal clarity, which is essential for attracting investments and promoting innovation in the field of AI. The Act intends to eliminate any uncertainties that would possibly discourage investors and innovators from participating in AI-related initiatives by establishing a precise and defined legislative framework. The Union's competitive position in the global AI landscape is expected to be strengthened by this clarity, which is expected to act as a spur for additional investments and ground-breaking developments in the AI field;

- Governance and Enforcement: the strengthening of governance structures and the efficient execution of current laws pertaining to basic rights and safety requirements applicable to AI systems are two additional crucial aspects of the AI Act. The Act works to make sure that AI technologies do not violate people's rights or undermine safety standards through strong governance frameworks and proactive enforcement tactics. The Act strengthens the Union's commitment to protecting the welfare of its citizens and creating a responsible AI ecosystem by ensuring adherence to these regulations;
- Market Cohesion: the AI Act also considers the necessity of developing a unified market for trustworthy and legal AI applications. To achieve this goal, market fragmentation must be avoided in order to maintain uniform standards for AI products throughout the Union. The Act intends to hasten the adoption of AI technologies while also increasing public confidence in their use by assisting the creation of a coherent and unified AI market.

Harmonization with pre-existing law inside the European Union

Harmonization inside the European Union (EU) is a crucial matter that needs careful consideration. Due to their broad extent, the proposed restrictions must be in perfect accordance with the present Union legislation regarding the industries that house high-risk AI systems, both in use now and in the near future. A rational and uniform regulatory environment that not only answers the unique needs of AI deployment but also easily interacts with the current legal system is crucial because the idea crosses several sectors. This harmonization is crucial for promoting a uniform approach to AI governance across the EU, expediting procedures, and reducing inconsistencies that can result from conflicting legal interpretations. The EU may get closer to a well-coordinated and comprehensive approach to AI regulation that crosses sectors and protects the Union's collective interests by strengthening this synergy between the AI Act and pre-existing law.

The European Union's complete framework for regulating artificial intelligence is built on the AI Act. A variety of policies have been adopted in addition to this important law to guarantee a responsible and secure AI environment. Among them are the Directive on Network and Information Systems Security (Directive (UE) 2016/1148), which aims to ensure high levels of cybersecurity throughout the Union, the General Data Protection Regulation (Regulation (UE) 2016/679), which protects personal data, and the Directive on Cybersecurity Measures (Directive (UE) 2022/2555), which aims to improve cyber resilience. The Digital Markets Act (Regulation (UE) 2022/1925) and the European Data Governance Regulation (Regulation (UE)

2022/868) are also essential for promoting fair and competitive digital markets. The Digital Operational Resilience Regulation (Regulation (UE) 2022/2554) also guarantees the resilience of the financial sector's digital operations. Finally, to encourage responsible and safe AI innovation inside the European Union, the upcoming Regulation on Crypto-Assets Markets (Regulation (UE) 2023/1114) will regulate the crypto-asset markets.

Policy adopted

The chosen policy alternatives show that the European Union is managing AI technology in a thoughtful and purposeful manner. The introduction of a horizontal EU legislative tool that works in combination with a proportional risk-based methodology is essential to this plan. By accommodating the varied degrees of risk associated with each, this strategy guarantees that the regulatory framework retains its relevance and applicability across various industries and AI applications. The legislation may be adjusted to varied circumstances by using a risk-based lens, making it possible to more precisely match supervision with the real risk of damage or effect.

Additionally, adding codes of conduct for low-risk AI systems gives the regulatory environment a flexible and adaptable quality. These regulations act as guidelines that support the proper design and implementation of AI systems that might not be classified as high-risk. This understanding of various risk levels enables a comprehensive and balanced approach to the handling of AI technology, encouraging innovation and adoption while protecting against any negative effects.

The Regulatory Framework outlines a systematic classification of risk levels for AI systems that is divided into four categories. These levels provide as a unifying framework for evaluating and categorizing the possible dangers connected to diverse AI applications. Each level corresponds to a certain amount of risk and acts as a benchmark for choosing the proper regulatory controls to be implemented (European Commission, 2023).

- Unacceptable Risk: this classification is only given to AI systems that are assessed to pose an intolerable risk to safety, society values, and fundamental rights. Since the introduction of such technologies to the market or society would fundamentally violate existing laws and moral standards, it would be strongly discouraged and subject to stringent regulatory restrictions;
- High Risk: high risk AI systems are ones with a strong potential to harm, whether to specific people, groups, or larger social institutions. These systems run the risk of compromising security, privacy, or the operation of crucial services. To guarantee the

appropriate development, implementation, and use of these high-risk AI systems, strict regulatory standards and oversight are implemented;

- Limited Risk: these systems may be more likely to have negative effects on a smaller scale or with less severity. Regulatory safeguards are in place to ensure the responsible use of AI in this category, even if they are not as strict as high-risk systems;
- Minimal or No Risk: these systems are thought to have a very low risk of injury or unfavorable outcomes. They won't likely violate basic rights or cause major societal problems. As a result, this category receives relatively less attention from regulators, creating a more permissive setting for innovation and agile development.

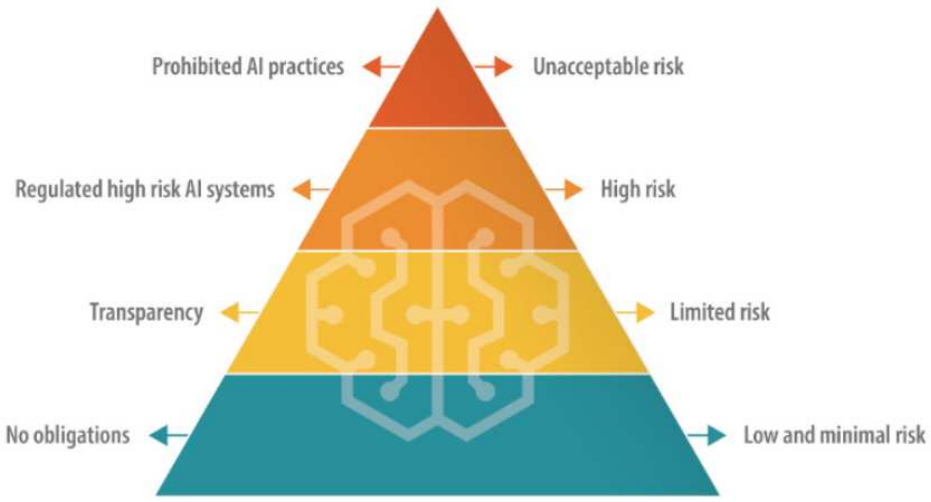

Figure 13: Pyramid of risks.

Last news and next steps

On June 14, 2023, the European Parliament made an important milestone for AI legislation by approving its position on the proposed Artificial Intelligence Act. With 499 votes in favor, 28 against, and 93 abstentions, the adoption of this bargaining stance was decisively supported. The list of AI system applications that are considered invasive and discriminatory was increased during this period by amendments that were presented by the Parliament (Cyber Risk GmbH, 2023).

It's crucial to remember that this development does not represent the Artificial Intelligence Act's final form. Although the European Parliament has made its negotiating stance known, the definitive text of the Act has yet to be finalized.

In the next phases, the Parliament will negotiate with both the EU Council and the European Commission in a trilogue procedure. The goal of the trilogue is to get a temporary agreement

among all parties on the proposed legislation. The Commission takes on the role of a mediator throughout this process, promoting conversations and assisting in the discovery of common ground between the co-legislators, namely the Parliament and the Council. Once a preliminary agreement has been achieved, it must be legally accepted through the appropriate Parliament and Council processes. This will clear the way for the Artificial Intelligence Act to be put into effect.

The European Union is committed to providing thorough and balanced AI rules that safeguard basic rights, social values, and responsible AI innovation, which is demonstrated by this multidimensional approach.

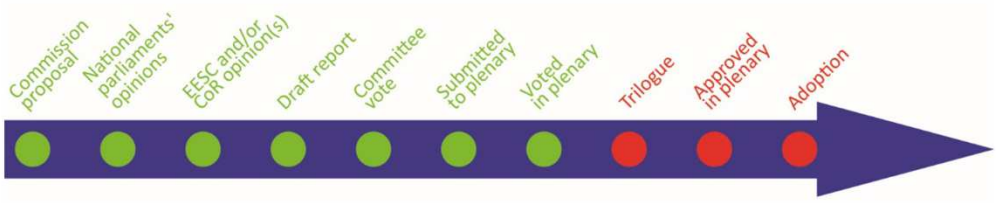

Figure 14: Regulation timeline.

Artificial Intelligence Act

In our exploration, we will examine the preliminary sections of the AI Act that have been released thus far (European Commission, 2021a). We will concentrate on the first three books in particular because they cover key components of this regulatory structure. These are their titles:

- General provisions (TITLE I);
- Prohibited Artificial Intelligence Practices (TITLE II);
- High-Risk AI Systems (TITLE III).

By concentrating on the first three titles of the AI Act, we want to better understand the guiding ideals, limitations, and rules that serve as the cornerstone of this all-encompassing framework. We will learn more about how the AI Act seeks to strike a balance between the potential advantages of AI and the necessity of guaranteeing its ethical, legal, and responsible deployment across a variety of industries and applications as we go deeper into each title.

General provisions (TITLE I)

The scope of the legal system is described in the AI Act's first title, as previously mentioned.

Beyond this description, the Regulation makes it clearer which organizations and people are covered by its provisions. This distinction is crucial for ensuring that the legal framework is correctly implemented and enforced across the many AI members.
Additionally, the Act's first title includes an in-depth explanation of "Artificial Intelligence". This term provides further context for the technical environment that the Act aims to control. In order to maintain the Act's applicability and effectiveness in addressing the changing AI landscape, it is crucial to promote a shared understanding of the technologies that are subject to regulation.

The following categories of actors are covered by this Regulation:

- Providers Putting AI Systems on the Market or in Service in the Union: this category includes organizations that put AI systems on the market or in use inside the Union, whether they are based there or in a third nation. No matter where they are from, companies that implement AI systems are subject to this Regulation;
- Users of AI Systems in the Union: this Regulation's requirements also apply to people or organizations based in the Union who use AI systems. The regulatory framework extends its protection to individuals who use AI systems inside the Union's geographical borders;
- Providers and Users of AI Systems in Third Countries with Union Impact: the Regulation also covers users and suppliers of AI systems situated in third-party nations. This inclusion especially applies to circumstances in which the AI system's output is used inside the Union. Providers and users that contribute to AI-generated outputs that have an influence on the Union are likewise subject to the rules outlined in this framework, even if they are located outside of the Union's borders.

In the context of the AI Act, the word "artificial intelligence" is broad and incorporates a variety of advanced technologies and approaches. This phrase encompasses a range of methods and strategies that make it easier for AI systems to emulate human intellect. The following innovations are listed in the Act's definition of "artificial intelligence" (European Commission, 2021b):

- Machine Learning Approaches: this category includes a variety of machine learning methods that let AI systems recognize patterns, anticipate outcomes, and get better over time. It consists of three types of learning: supervised learning, in which models are taught using labeled data; unsupervised learning, in which patterns are found without the use of labeled data; and reinforcement learning, in which agents are taught by

interaction with their surroundings. When deep learning is used, neural networks with several layers are used, allowing the system to automatically learn features from data;

- Logic and Knowledge Based Approaches: methodologies based on logic and knowledge representation fall under this category. Knowledge bases, which store organized information, and inductive logic programming, which creates logic rules from data, are essential elements. Drawing logical inferences from the data at hand is made easier by inference and deductive engines, while expert systems and symbolic reasoning simulate human knowledge in the solution of challenging issues,
- Statistical Approaches: Bayesian estimation is a probabilistic modeling technique that takes decision-making uncertainty into account. Algorithms used in search and optimization procedures scour problem domains for ideal solutions. With the use of these methods, AI systems can find patterns, connections, and the best answers inside large, complicated datasets.

Prohibited Artificial Intelligence Practices (TITLE II)

The following is a list of forbidden AI practices that are enforced under the AI Act (TITLE II):

- The Act forbids the employment of AI systems that use subliminal tactics outside of a person's conscious awareness to substantially modify their behavior and hurt them or others physically or psychologically;
- It is forbidden for AI systems to manipulate behavior in a way that is harmful to the affected individual or others by taking advantage of vulnerabilities related to age, physical infirmity, or mental illness;
- Public authorities are prohibited from utilizing AI systems to evaluate or categorize people based on their social conduct or other personal traits since this might result in unfair treatment or societal score-based judgments.

TITLE II also explains that law enforcement can deploy "real-time" remote biometric identification systems in open areas only to find specific victims, stop immediate threats, or find, locate, and charge specific significant criminal acts. The use must take into account the circumstances, how they may affect rights and freedoms, and any required precautions and restrictions.

The use of “real-time” remote biometric identification technologies for law enforcement needs prior authorization by a court or administrative body, based on unbiased evidence, taking necessity and proportionality into consideration. While urgent usage might start without permission, a request must come next.

Member States have the option to permit “real-time” remote biometric identification technologies for law enforcement under certain criteria and guidelines defined in their national legislation, including defining approved goals and criminal acts.

High-Risk AI Systems (TITLE III)

The first three articles we will view (Article 9, Article 11 and Article 13) will explain the requirements that any product or service offered within which there is a presence of Artificial Intelligence must have.

Organizations must create a thorough framework for compliance with the AI Act's requirements, concentrating on three crucial elements: risk management, technical documentation, and transparency in providing information to users. The establishment, implementation, documentation, and preservation of a careful risk management system specially created for high-risk AI systems are all required under Article 9 of the Act. This system must be an ongoing, iterative process that covers every stage of these systems and allows for frequent modifications to accommodate changing conditions. Notably, intensive testing is necessary to determine the best risk management strategies for high-risk AI systems.

Article 11 places a strong emphasis on the creation and maintenance of technical documentation for high-risk AI systems before to their release or deployment. This documentation shows how the system complies with the provisions of the AI Act so that national competent authorities and notified entities may assess compliance. It is essential for keeping track of, auditing, and making sure that these systems adhere to predetermined criteria.

For high-risk AI systems, Article 13 emphasizes the value of transparency and user-centric design. These systems need to be transparently designed so that users may understand their outputs and use them correctly. The degree of transparency needs to be adjusted to meet the needs of users and providers. Additionally, these systems must come with user instructions that are presented in a clear, comprehensive, accurate, and understandable in a proper digital format. This supports the appropriate utilization of these cutting-edge technologies and encourages user knowledge. Overall, following these regulations helps to promote ethical and responsible AI practices that put user welfare and well-informed decision-making first while still ensuring regulatory compliance.

The last two articles (Article 17 and Article 21) we are going to examine aim to express the obligations that organizations have to ensure the compliance of the products or services they go to offer in the market.

Article 17 of the AI Act requires developers of high-risk AI systems to set up a formal quality control system to guarantee compliance with the rules. Written policies, procedures, and instructions addressing a variety of topics, including regulatory strategy, design processes, development, testing, data management, risk management, post-market monitoring, incident reporting, communication, record keeping, resource management, and staff responsibilities, should be included in this system's organization. Technical requirements and data processing methods must be provided, taking harmonized standards into account. The system should be implemented proportionally to the provider's size.

If a system that organizations have released into the market or placed into operation is found to be in violation of the rules, the liabilities for suppliers of high-risk AI systems are outlined in Article 21 of the AI Act. In such cases, providers are required to take timely corrective action to make up for the noncompliance. The system may need to be brought into compliance, withdrawn, or a recall may need to be started, depending on the situation. Additionally, the providers must tell the appropriate distributors, authorized agents, and importers of the issue and the corrective actions being implemented.

4.5 Conclusions

This chapter has explored the dynamic interaction between technology and well-known frameworks like COSO, Cobit, and COSO ERM, demonstrating the opportunity for improvement and efficiency. We have looked at how technology is changing the control landscape by redefining human contact and affecting residual risk. The discussion covered a range of control types and showed how those control types' responsibilities have changed as a result of technological development. In addition, a thorough procedural understanding of testing was given, showing how technology not only makes the process more efficient but also improves the effectiveness of control evaluation. Practical examples have clearly shown how technology is a crucial tool in this effort, enabling rigorous testing efforts that reveal weaknesses and guarantee compliance.

The analysis included the AI Act and explained how it had a significant influence on the field of AI. As technology continues to push the envelope, legislative initiatives like the AI Act are essential in guiding the appropriate use of AI. The complexity of the AI Act has been explained in this chapter, along with explanations of its provisions for risk management, technical documentation, transparency, and user information. Technology and regulation together produce a healthy environment that encourages innovation while preserving moral behavior. The fusion of well-established ideas, innovative techniques, and legal frameworks is essential

as the technological environment develops in order to maintain the robustness and adaptability of our approach to controls and testing.

Additionally, internal audit makes a substantial contribution to the compliance journey for organizations utilizing AI. It assists in locating practice gaps, evaluating the efficacy of risk management systems and confirming compliance with requirements for transparency and information availability. Internal auditors are given the tools they need to perform rigorous, data-driven audit activities, resulting in actionable insights for enhanced decision-making.
Internal audit has a dual function in this holistic approach, serving as both a collaborator in assuring ethical and responsible use of AI and a guardian of compliance for the firm as a whole. It is obvious that internal audit's adaptable and comprehensive viewpoint is crucial in ensuring the benefits of AI while keeping ethical norms and legal duties as the parameters of technology and legislation continue to advance.

Appendix A – Attribute Standards

Source: The Institute of Internal Auditors. Attribute Standards.
Available at: <https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/attribute-standards/>
[Access date: 06/03/2023]

1000 - PURPOSE, AUTHORITY, AND RESPONSIBILITY

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework (the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing). The chief audit executive must periodically review the internal audit charter and present it to senior management and the board for approval.

1010 – RECOGNIZING MANDATORY GUIDANCE IN THE INTERNAL AUDIT CHARTER

The mandatory nature of the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the Standards, and the Definition of Internal Auditing must be recognized in the internal audit charter. The chief audit executive should discuss the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework with senior management and the board.

1100 – INDEPENDENCE AND OBJECTIVITY

The internal audit activity must be independent, and internal auditors must be objective in performing their work.

1110 – ORGANIZATIONAL INDEPENDENCE

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

1111 – DIRECT INTERACTION WITH THE BOARD

The chief audit executive must communicate and interact directly with the board.

1112 – CHIEF AUDIT EXECUTIVE ROLES BEYOND INTERNAL AUDITING

Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.

1120 – INDIVIDUAL OBJECTIVITY

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

1130 – IMPAIRMENT TO INDEPENDENCE OR OBJECTIVITY

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

1200 – PROFICIENCY AND DUE PROFESSIONAL CARE

Engagements must be performed with proficiency and due professional care.

1210 – PROFICIENCY

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

1220 – DUE PROFESSIONAL CARE

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1230 – CONTINUING PROFESSIONAL DEVELOPMENT

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

1300 – QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

1310 – REQUIREMENTS OF THE QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

The quality assurance and improvement program must include both internal and external assessments.

1311 – INTERNAL ASSESSMENTS

Internal assessments must include:

- Ongoing monitoring of the performance of the internal audit activity; and
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.

1312 – EXTERNAL ASSESSMENTS

External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization. The chief audit executive must discuss with the board:

- The form and frequency of external assessments.
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

1320 – REPORTING ON THE QUALITY ASSURANCE AND IMPROVEMENT PROGRAM

The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board. Disclosure should include:

- The scope and frequency of both the internal and external assessments.
- The qualifications and independence of the assessor(s) or assessment team, including potential conflicts of interest.
- Conclusions of assessors.
- Corrective action plans.

1321 – USE OF "CONFORMS WITH THE INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING"

Indicating that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing is appropriate only if supported by the results of the quality assurance and improvement program.

1322 – DISCLOSURE OF NONCONFORMANCE

When nonconformance with the Code of Ethics or the Standards impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

Appendix B – Performance Standards

Source: The Institute of Internal Auditors. Performance Standards.
Available at: <https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/performance-standards/>
[Access date: 06/03/2023]

2000 – MANAGING THE INTERNAL AUDIT ACTIVITY
The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.

2010 – PLANNING
The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

2020 – COMMUNICATION AND APPROVAL
The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

2030 – RESOURCE MANAGEMENT
The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

2040 – POLICIES AND PROCEDURES
The chief audit executive must establish policies and procedures to guide the internal audit activity.

2050 – COORDINATION AND RELIANCE
The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

2060 – REPORTING TO SENIOR MANAGEMENT AND THE BOARD

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the Standards. Reporting must also include significant risk and control issues, including fraud risks, governance issues, and other matters that require the attention of senior management and/or the board.

2070 – EXTERNAL SERVICE PROVIDER AND ORGANIZATIONAL RESPONSIBILITY FOR INTERNAL AUDITING

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

2100 – NATURE OF WORK

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

2110 – GOVERNANCE

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

2120 – RISK MANAGEMENT

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

2130 – CONTROL

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

2200 – ENGAGEMENT PLANNING

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

2201 – PLANNING CONSIDERATIONS

In planning the engagement, internal auditors must consider:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

2210 – ENGAGEMENT OBJECTIVES

Objectives must be established for each engagement.

2220 – ENGAGEMENT SCOPE

The established scope must be sufficient to achieve the objectives of the engagement.

2230 – ENGAGEMENT RESOURCE ALLOCATION

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

2240 – ENGAGEMENT WORK PROGRAM

Internal auditors must develop and document work programs that achieve the engagement objectives.

2300 – PERFORMING THE ENGAGEMENT

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2310 – IDENTIFYING INFORMATION

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

2320 – ANALYSIS AND EVALUATION

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330 – DOCUMENTING INFORMATION

Internal auditors must document sufficient, reliable, relevant, and useful information to support the engagement results and conclusions.

2340 – ENGAGEMENT SUPERVISION

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

2400 – COMMUNICATING RESULTS

Internal auditors must communicate the results of engagements.

2410 – CRITERIA FOR COMMUNICATING

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

2420 – QUALITY OF COMMUNICATIONS

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

2421 – ERRORS AND OMISSIONS

If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.

2430 – USE OF “CONDUCTED IN CONFORMANCE WITH THE INTERNATIONAL STANDARDS FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING”

Indicating that engagements are "conducted in conformance with the International Standards for the Professional Practice of Internal Auditing" is appropriate only if supported by the results of the quality assurance and improvement program.

2431 – ENGAGEMENT DISCLOSURE OF NONCONFORMANCE

When nonconformance with the Code of Ethics or the Standards impacts a specific engagement, communication of the results must disclose the:

- Principle(s) or rule(s) of conduct of the Code of Ethics or Standard(s) with which full conformance was not achieved.
- Reason(s) for nonconformance.
- Impact of nonconformance on the engagement and the communicated engagement results.

2440 – DISSEMINATING RESULTS

The chief audit executive must communicate results to the appropriate parties.

2450 – OVERALL OPINIONS

When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

2500 – MONITORING PROGRESS

The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

2600 – COMMUNICATING THE ACCEPTANCE OF RISKS

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Bibliography

- Al-Taee, S. H. H., & Flayyih, H. H. (2023). Impact of the electronic internal auditing based on IT governance to reduce auditing risk. Corporate Governance and Organizational Behavior Review, 7(1), 94-100.
  Available at: <https://doi.org/10.22495/cgobrv7i1p9>
- Albawwat, I., & Frijat, Y. (2021). An analysis of auditors' perceptions towards artificial intelligence and its contribution to audit quality. Accounting, 7(4), 755-762.
  Available at: <http://doi.org/10.5267/j.ac.2021.2.009>
- Alles, M., Brennan, G., Kogan, A., & Vasarhelyi, M. A. (2006). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. International Journal of Accounting Information Systems, 7(2), 137-161.
  Available at: <https://doi.org/10.1016/j.accinf.2005.10.004>
- Almaqtari, F. A., Farhan, N. H., Al-Homaidi, E. A., & Mishra, N. (2020). An empirical evaluation of financial reporting quality of the Indian GAAP and Indian accounting standards. International Journal of Accounting, Auditing and Performance Evaluation, 16(2-3), 200-229.
  Available at: <https://doi.org/10.1504/IJAAPE.2020.112717>
- Bank of Italy (2013). Disposizioni di vigilanza per le banche: circolare n. 285. Rome: Bank of Italy, p. 300.
  Available at: <https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/Circ_285_19_Aggto_Testo_integrale.pdf> [Access date: 06/03/2023]
- Bierstaker, J., Janvrin, D., & Lowe, D. J. (2014). What factors influence auditors' use of computer-assisted audit techniques?. Advances in Accounting, 30(1), 67-74.
  Available at: <https://doi.org/10.1016/j.adiac.2013.12.005>
- Bozkaya, M., Gabriels, J., & van der Werf, J. M. (2009). Process diagnostics: a method based on process mining. In 2009 International Conference on Information, Process, and Knowledge Management (pp. 22-27). IEEE.
  Available at: <https://doi.org/10.1109/eKNOW.2009.29>
- Braun, R. L., & Davis, H. E. (2003). Computer-assisted audit tools and techniques: analysis and perspectives. Managerial Auditing Journal.
  Available at: <https://doi.org/10.1108/02686900310500488>
- Cangemi, M. P. (2015). Staying a step ahead: Internal audit's use of technology. The Global Internal Audit Common Body of Knowledge (CBOK), 16.
  Available at: <https://doi.org/10.13140/RG.2.1.4795.5683>

- Cangemi, M. P. (2010). Internal audit's role in continuous monitoring. EDPACS, 41(4), 1-8.
  Available at: <https://doi.org/10.1080/07366981.2010.488571>
- CaseWare Analytics (2017). Data analytics: The key to Risk-based auditing.
  Available at: <https://info.caseware.co.uk/the-key-to-risk-based-auditing> [Access date: 21/08/2023]
- Chartered Professional Accountants (2017). Audit Data Analytics Alert: audit data analytics.
  Available at: <https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/audit-data-analytics-alert-ada-survey-results> [Access date: 21/08/2023]
- Chiu, T., Brown-Liburd, H., & Vasarhelyi, M. A. (2019). Performing tests of internal controls using process mining: What could go wrong? The CPA journal, 89(6), 54-57.
  Available at: <https://www.cpajournal.com/2019/07/10/performing-tests-of-internal-controls-using-process-mining/> [Access date: 21/08/2023]
- Chiu, V., Liu, Q., & Vasarhelyi, M. A. (2014). The development and intellectual structure of continuous auditing research☆. Journal of Accounting Literature.
  Available at: <https://doi.org/10.1016/j.acclit.2014.08.001>
- Christ, M. H., Eulerich, M., Krane, R., & Wood, D. A. (2021). New frontiers for internal audit research. Accounting Perspectives, 20(4), 449-475.
  Available at: <https://doi.org/10.1111/1911-3838.12272>
- Chukwuani, V. N., & Egiyi, M. A. (2020). Automation of Accounting Processes: Impact of Artificial Intelligence. International Journal of Research and Innovation in Social Science (IJRISS), 4(8), 444-449.
  Available at: <https://www.rsisinternational.org/journals/ijriss/Digital-Library/volume-4-issue-8/444-449.pdf> [Access date: 21/08/2023]
- Coderre, D., & Police, R. C. M. (2005). Global technology audit guide: continuous auditing implications for assurance, monitoring, and risk assessment. The Institute of Internal Auditors, 1-34.
  Available at: <https://www.qcpa.org.qa/assets/uploads/documents/library/1563184783.pdf> [Access date: 21/08/2023]
- Cooper, L. A., Holderness Jr, D. K., Sorensen, T. L., & Wood, D. A. (2019). Robotic process automation in public accounting. Accounting Horizons, 33(4), 15-35.
  Available at: <https://doi.org/10.2308/acch-52466>

- COSO (2017). Enterprise Risk Management – Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission, p. 3-11.
  Available at : < https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf> [Access date: 05/04/2023]
- Council, F. R. (2017). Audit quality thematic review: The use of data analytics in the audit of financial statements. The Financial Reporting Council (FRC), UK, London. Retrieved October, 25, 2018.
  Available at: <https://www.frc.org.uk/getattachment/4fd19a18-1beb-4959-8737-ae2dca80af67/AQTR_Audit-Data-Analytics-Jan-2017.pdf> [Access date: 21/08/2023]
- Curtis, M. B., & Payne, E. A. (2008). An examination of contextual factors and individual characteristics affecting technology implementation decisions in auditing. International Journal of Accounting Information Systems, 9(2), 104-121.
  Available at: <https://doi.org/10.1016/j.accinf.2007.10.002>
- Cyber Risk GmbH (2023). The EU Artificial Intelligence Act.
  Available at: <https://www.artificial-intelligence-act.com/> [Access date: 21/08/2023]
- De Mozota B.B. (1998). Structuring Strategic Design Management: Michael Porter's Value Chain. Design Management Journal 9: 26-31.
  Available at: <https://doi.org/10.1111/j.1948-7169.1998.tb00201.x>
- Deloitte. (2016). Internal audit analytics: The journey to 2020 Insights-driven auditing.
  Available at: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-internal-audit-analytics-pov.pdf> [Access date: 21/08/2023]
- Devis Michael & Stark Andrew (2001). Conflicts of interest and self-dealing in the professions: a review essay. New York: Oxford University Press, p. 170-172.
  Available at: <https://www.jstor.org/stable/3857777>
- Eilifsen, A., Kinserdal, F., Messier Jr, W. F., & McKee, T. E. (2020). An exploratory study into the use of audit data analytics on audit engagements. Accounting Horizons, 34(4), 75-103.
  Available at: <https://doi.org/10.2308/HORIZONS-19-121>
- Ettish, A. A., El-Gazzar, S. M., & Jacob, R. A. (2017). Integrating internal control frameworks for effective corporate information technology governance. JISTEM-Journal of Information Systems and Technology Management, 14, 361-370.
  Available at: <https://doi.org/10.4301/S1807-17752017000300004>

- Eulerich, M., Huang, Q., & Vasarhelyi, M. A. (2021). Using Process Mining as an Assurance-Tool in the Three-Lines-of-Defense Model. Available at SSRN 3973155. Available at: <http://dx.doi.org/10.2139/ssrn.3973155>
- European Commission (2023). Regulatory framework proposal on artificial intelligence. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> [Access date: 21/08/2023]
- European Commission (2021a). Proposal for a Regulation of the European Parliament and of the Council. Laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF> [Access date: 21/08/2023]
- European Commission (2021b). Annexes to the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_2&format=PDF> [Access date: 21/08/2023]
- European Union (2023). Briefing EU Legislation in Progress: Artificial intelligence act. Available at: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf> [Access date: 21/08/2023]
- Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. Review of Accounting Studies, 27(3), 938-985. Available at: <https://doi.org/10.1007/s11142-022-09697-x>
- Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. International journal of information management, 35(2), 137-144. Available at: <https://doi.org/10.1016/j.ijinfomgt.2014.10.007>
- Goh, C., Pan, G., Seow, P. S., LEE, B. H. Z., & Yong, M. (2019). Charting the future of accountancy with AI. Available at: <https://ink.library.smu.edu.sg/soa_research/1806> [Access date: 21/08/2023]
- Hasan, A. R. (2021). Artificial Intelligence (AI) in accounting & auditing: A Literature review. Open Journal of Business and Management, 10(1), 440-465. Available at: <https://doi.org/10.4236/ojbm.2022.101026>

- Henry, H., & Rafique, M. (2021). Impact of Artificial Intelligence (AI) on Auditors: A Thematic Analysis. IOSR Journal of Business and Management, 23(9).
  Available at: <https://doi.org/10.9790/487X-2309050110>
- IVASS (2018). Regolamento IVASS n. 38 del 3 luglio 2018. Istituto per la Vigilanza sulle Assicurazioni, p. 69.
  Available at: <https://www.ivass.it/normativa/nazionale/secondaria-ivass/regolamenti/2018/n38/Regolamento_IVASS_38_del_3_7_2018.pdf> [Access date: 05/04/2023]
- Janvrin, D., Bierstaker, J., & Lowe, D. J. (2009). An investigation of factors influencing the use of computer-related audit procedures. Journal of Information Systems, 23(1), 97-118.
  Available at: <https://doi.org/10.2308/jis.2009.23.1.97>
- Jans, M., & Hosseinpour, M. (2019). How active learning and process mining can act as Continuous Auditing catalyst. International Journal of Accounting Information Systems, 32, 44-58.
  Available at: <https://doi.org/10.1016/j.accinf.2018.11.002>
- Jans, M., Alles, M. G., & Vasarhelyi, M. A. (2014). A field study on the use of process mining of event logs as an analytical procedure in auditing. The Accounting Review, 89(5), 1751-1773.
  Available at: <https://doi.org/10.2308/accr-50807>
- Jans, M., Alles, M., & Vasarhelyi, M. (2013). The case for process mining in auditing: Sources of value added and areas of application. International Journal of Accounting Information Systems, 14(1), 1-20.
  Available at: <https://doi.org/10.1016/j.accinf.2012.06.015>
- Jans, M., Depaire, B., & Vanhoof, K. (2011). Does process mining add to internal auditing? An experience report. In Enterprise, Business-Process and Information Systems Modeling: 12th International Conference, BPMDS 2011, and 16th International Conference, EMMSAD 2011, held at CAiSE 2011, London, UK, June 20-21, 2011. Proceedings (pp. 31-45). Springer Berlin Heidelberg.
  Available at: <http://doi.org/10.1007/978-3-642-21759-3_3>
- Khamis, A. (2021). The Impact of Artificial Intelligence in Auditing and Accounting Decision Making.
  Available at: <https://doi.org/10.13140/RG.2.2.20831.18085>

- Kotb, A., & Roberts, C. (2011). The impact of e-business on the audit process: An investigation of the factors leading to change. International Journal of Auditing, 15(2), 150-175.
  Available at: <https://doi.org/10.1111/j.1099-1123.2011.00427.x>
- KPMG (2023). Controls transformation: How to optimize and automate your risk and control lifecycle.
  Available at: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/04/gm-ots-03528-controls-transformation-playbook-V7-Web.pdf> [Access date: 21/08/2023]
- KPMG (2022). Internal Audit of the Strategic Planning Process.
  Available at: <https://assets.kpmg.com/content/dam/kpmg/be/pdf/2022/KPMG-Internal-Audit-of-the-Strategic-Planning-Process.pdf> [Access date: 20/03/2023]
- KPMG (2021). Agile, resilient & transformative.
  Available at: <https://assets.kpmg.com/content/dam/kpmg/jm/pdf/agile-resilient-and-transformative-report.pdf> [Access date: 08/09/2023]
- Law, K., & Shen, M. (2020). How does artificial intelligence shape the audit industry. Available at SSRN.
  Available at: <http://dx.doi.org/10.2139/ssrn.3718343>
- Li, H., Dai, J., Gershberg, T., & Vasarhelyi, M. A. (2018). Understanding usage and value of audit analytics for internal auditors: An organizational approach. International Journal of Accounting Information Systems, 28, 59-76.
  Available at: <https://doi.org/10.1016/j.accinf.2017.12.005>
- Littley, J. (2012). Leveraging data analytics and continuous auditing processes for improved audit planning, effectiveness, and efficiency. KPMG White Paper.
  Available at: <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/Leveraging-Data-Analytics.pdf> [Access date: 21/08/2023]
- Lois, P., Drogalas, G., Karagiorgos, A., & Tsikalakis, K. (2020). Internal audits in the digital era: opportunities risks and challenges. EuroMed Journal of Business.
  Available at: <https://doi.org/10.1108/EMJB-07-2019-0097>
- Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. Journal of emerging technologies in accounting, 15(1), 1-10.
  Available at: <https://doi.org/10.2308/jeta-10589>
- Majdalawieh M. & Zaghloul I. (2009). Paradigm shift in information systems auditing. Managerial Auditing Journal. Vol. 24 No. 4, 2009, p. 354.
  Available at: <https://doi.org/10.1108/02686900910948198>

- Manson, S., McCartney, S., & Sherer, M. (2001). Audit automation as control within audit firms. Accounting, Auditing & Accountability Journal, 14(1), 109-130. Available at: <https://doi.org/10.1108/09513570110381097>
- Ming-Hsien, Y., Wen-Shiu, L., & Tian-Lih, K. (2011). The impact of computerized internal controls adaptation on operating performance. African Journal of Business Management, 5(20), 8204-8214. Available at: <https://doi.org/10.5897/AJBM11.572>
- Moeller R. Robert (2009). Brink's modern internal auditing: A common body of knowledge. Hoboken: John Wiley & Sons, p. 23-51 & 89-96 & 113-123.
- Peirson, J. (2010). Continuous monitoring and continuous auditing: From idea to implementation. Technical report, Deloitte & Touche LLP. Available at: <https://www2.deloitte.com/content/dam/Deloitte/uy/Documents/audit/Monitoreo%20continuo%20y%20auditoria%20continua.pdf> [Access date: 21/08/2023]
- Pickett K. H. Spencer (2010). The internal audit handbook. Third edition. Chichester: John Wiley & Sons, p. 7-10.
- Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. Technology in Society, 67, 101738. Available at: <https://doi.org/10.1016/j.techsoc.2021.101738>
- Ramamoorti Sridhar & Gramling A. Audrey (2003). Research opportunity in internal auditing. First edition. Altamonte Springs: Institute of Internal Auditors, p. 5-8.
- Ramlukan, R. (2015). How big data and analytics are transforming the audit. EY Reporting. Available at: <https://www.ey.com/en_es/assurance/how-big-data-and-analytics-are-transforming-the-audit> [Access date: 21/08/2023]
- Rikhardsson, P., Singh, K., & Best, P. (2019). Exploring continuous auditing solutions and internal auditing: A research note. Accounting and Management Information Systems, 18(4), 614-639. Available at: <https://doi.org/10.24818/jamis.2019.04006>
- Sturgis R. & Loftus A. (2023). Best Practices for a Highly Effective Internal Audit Function. Alexandria VA: Association of Credit Union Internal Auditors. Available at: <https://www.acuia.org/sites/acuia.org/files/1C%20-%20Best%20Practices%20for%20a%20Highly%20Effective%20IA%20Function_0.pdf> [Access date: 15/03/2023]

- Tang, F., Norman, C. S., & Vendrzyk, V. P. (2017). Exploring perceptions of data analytics in the internal audit function. Behaviour & Information Technology, 36(11), 1125-1136.
  Available at: <https://doi.org/10.1080/0144929X.2017.1355014>
- The Institute of Internal Auditors (2023a). Definition of internal auditing.
  Available at: <https://www.theiia.org/en/standards/what-are-the-standards/definition-of-internal-audit/> [Access date: 16/02/2023]
- The Institute of Internal Auditors (2023b). International Professional Practices Framework (IPPF).
  Available at: <https://www.theiia.org/en/standards/international-professional-practices-framework/> [Access date: 21/02/2023]
- The Institute of Internal Auditors (2023c). Code of Ethics.
  Available at: <https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/code-of-ethics/> [Access date: 06/03/2023]
- The Institute of Internal Auditors (2023d). 2023 North American Pulse of Internal Audit: Benchmarks for Internal Audit Leaders.
  Available at: <https://www.theiia.org/en/resources/research-and-reports/pulse/> [Access date: 08/09/2023]
- The Institute of Internal Auditors (2022). Good Practice Internal Audit Reports.
  Available at: <https://www.iia.org.au/sf_docs/default-source/technical-resources/2018-whitepapers/iia-whitepaper_good-practice-internal-audit-reports.pdf?sfvrsn=2> [Access date: 21/03/2023]
- The Institute of Internal Auditors (2020). The IIA's three lines model.
  Available at: <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf> [Access date: 27/02/2023]
- The Institute of Internal Auditors (2019a). The Internal Audit Charter: A Blueprint to Assurance Success.
  Available at: <https://www.theiia.org/globalassets/documents/resources/the-internal-audit-charter-a-blueprint-to-assurance-success-august-2019/pp-the-internal-audit-charter.pdf> [Access date: 16/02/2023]
- The Institute of Internal Auditors (2019b). Demonstrating the Core Principles for the Professional Practice of Internal Auditing.
  Available at: <https://www.iia.org.au/sf_docs/default-source/technical-resources/pg-demonstrating-the-core-principles-for-the-professional-practice-of-ia.pdf?sfvrsn=2> [Access date: 16/02/2023]

- University Of Oregon (2023). Audit process.
  Available at: <https://internalaudit.uoregon.edu/report/audit-process> [Access date: 15/03/2023]
- Van der Aalst, W. (2010). Auditing 2.0. IEEE Computer, 43(3), 90-93.
  Available at: <https://pdfs.semanticscholar.org/1f39/862b94132662801f362ab80db8d7ccc17df5.pdf > [Access date: 21/08/2023]
- Van Zelst S. J. And Leemans S. J. J. (2020). Translating Workflow Nets to Process Trees: An Algorithmic Approach. MDPI, Algorithms, p. 1.
  Available at: <https://doi.org/10.3390/a13110279>
- Vasarhelyi, M., & Romero, S. (2014). Technology in audit engagements: a case study. Managerial Auditing Journal, 29(4), 350-365.
  Available at: <https://doi.org/10.1108/MAJ-06-2013-0881>
- Walker, K., Brown-Liburd, H., & Lewis, A. (2019). The emergence of data analytics in auditing: Perspectives from internal and external auditors through the lens of institutional theory. Working paper May.
  Available at: <https://www.nhh.no/globalassets/departments/accounting-auditing-and-law/digaudit/audit-transformation-5-28-19.pdf> [Access date: 21/08/2023]
- Zabihollah, R., Ahmad, S., & Rick, E. (2002). McMickle Peter L."Continuous Auditing: Building Automated Auditing Capability". Auditing Journal of Practice & Theory, 21(1), 147-163.
  Available at: <https://doi.org/10.1108/978-1-78743-413-420181008>
- Zhang, J., Yang, X., & Appelbaum, D. (2015). Toward effective big data analysis in continuous auditing. Accounting Horizons, 29(2), 469-476.
  Available at: <https://doi.org/10.2308/acch-51070>