
Politecnico di Torino

Politecnico di Torino

Master's Degree in Engineering and Management

Academic Year 2022/2023

March 2023

# Project Risk Management process in IT Audit: An Accounting Firm case study

Supervisors:
Prof. Alberto De Marco
Dott. Filippo Maria Ottaviani
Dott. Matteo Curti

Candidate:
Francesca Bardazzi

March 2023

# Abstract

The following thesis aims at analyzing how Risk Management is approached in one of the Big Four Accounting Firms and the methodology used. In particular, the thesis highlights the role of IT Audit and how the activities carried out by such auditors allow the firm to perform risk assessments and help their clients understand how and where risk is or isn't mitigated by internal controls. For the purpose of such analysis, the thesis is structured as follows:

Introduction to Project Management, Risk Management and Information Systems: in this section a brief description of the main practices is made. Such introduction has the aim to clarify terms and concepts which are the basis for the analysis at hand.

State of the Art Analysis: this chapter highlights what has already been studied regarding risk management and more specifically, information risk management.

Process Analysis: this chapter aims at explaining the risk management methodology used by the accounting firm, starting from the as-is process, and moving on to the to-be process. In particular, the chapter is structured as follows:

- As-Is Process: this first step of the process proposes an overview of the methodology followed by the accounting firm.
- Process Implementation: the process implementation contains evaluations made based on client experiences.
- To-Be Process: this final step aims at proposing improvement methods for the risk analysis process introduced thus far.

## Acknowledgements

# Table of Contents

# List of Tables, Charts, and Figures

# Chapter 1. Introduction to Project Management, Risk Management, and Information Systems

## 1.1. Project Management

According to the Project Management Body of Knowledge (PMBOK)[1], Project Management is the discipline through which knowledge, skills, tools, and techniques are applied to project activities to meet the related requirements.

### 1.1.1. What is a project

To better understand such concept, we can define a project as an effort undertaken to create a unique product, to provide a specific service, or to obtain a desired result.

A project is characterized by a defined beginning and end and its outcome may be tangible or intangible. In addition, all projects have a team, a budget, a planning schedule, and a set of expectations that must be met by the team.

Every project can be seen as a collaboration between different people or groups of people, in charge of taking the project from idea to execution, called Project Stakeholders. The Project Management Institute defines Project Stakeholders as: "*Individuals and organizations who are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or successful project completion*"[2]. Therefore, by definition, stakeholders are all those people who could gain or lose from an interest or an investment according to the project's outcome.

In Project Management, stakeholders can be of two different types, internal or external. Internal stakeholders are those groups of people coming from within the business, for example managers, partners, executives, team members etc. On the other hand, external stakeholders are those people from outside the business which have an interest in the project, such as customers, suppliers, investors and so on.

Stakeholders vary according to the project's type and size, to the scope of the project, and mostly to the industry the project is covering. Nevertheless, a list of the most common stakeholders can be made as follows:

[1] Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fifth Edition

[2] Definition taken by Project Management Institute [https://www.pmi.org/learning/library/stakeholder-analysis-pivotal-practice-projects-8905]

- Project manager
- Teams and team members
- Managers
- Investors
- Suppliers
- Customers
- End users
- Consultants

To understand which stakeholders are most important, a project management team must start from the scope of its project and carry out a project stakeholder analysis, in which the main stakeholders are identified and prioritized according to the level interest that each stakeholder has in the project's outcome. Finally, priority stakeholders must be acknowledged throughout the entire project management lifecycle through face-to-face meetings and interviews.

### 1.1.2. The Project Management Process

A project management process follows a series of well identified steps, also known as Process Groups. The main five process groups are the following:

1. Initiating: this process has the aim to officiate a new project or a new phase of an already existing project. The authorization to begin project activities is given in this phase.
2. Planning: the planning process consists of establishing the project scope, the objectives and all the actions that must be taken to achieve them.
3. Executing: the execution of a project is the phase in which the planned activities are carried out according to the workplan.
4. Monitoring and Control: the monitoring and control process is fundamental to track the work being done, review it in case of errors and identify all those areas in which changes should be made to improve the project's estimated outcome.
5. Closing: in this last phase, the project activities are finalized and closed.

In each of these phases, a project management team has the aim to balance out a number or project constraint, which, considered as a whole, lead to the success or unsuccess of the project itself. Such constraints include:

1. Scope
2. Quality
3. Schedule
4. Budget
5. Resources
6. Risks

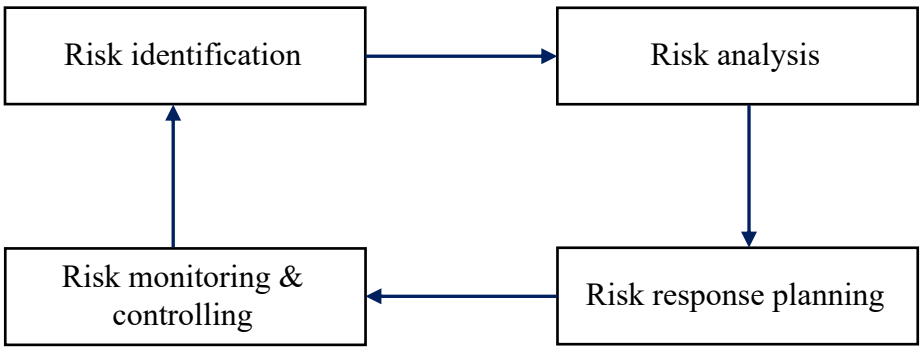
These constraints are linked in a way that if one of them changes, at least one of the others will alter in a meaningful or less meaningful way. For example, it's safe to say that if a project's budget decreases, management must concentrate on reducing the number of resources exploited for the scope of the project. On the other hand, if a project's budget increases and a higher number of resources is made possible, the impact could fall on the project's schedule, which could at this point be shortened to reach the desired KPIs in a timelier manner.

## 1.2. Project Risk Management

Project Risk Management (PRM) is a Project Management practice which aims at identifying specific events which could have a negative impact on the project's outcome and trying to reduce the probability of such events occurring.

The Project Management Institute (PMI) proposes a fully structured Project Risk Management framework which allows to carry out this practice effectively and avoid crisis situations.

First, it's necessary to begin from the PRM process which is composed of the four elements shown below:



### 1.2.1. Risk Identification

The risks identified in a project can either be obvious to the project team, and therefore apparent, or they can be predicted but hardly uncovered. Identified risks are recorded in the project risk register, stored at a central level, in the central project server.
The Project Management Institute (PMI) has identified a series of tools and guidelines which can and should be used to identify risks.

First, it's important to point out the sources from which the identified risks are taken. Here are four possible *risk sources*:

- Risk repository: this source is a list of risks that have already been identified for competed projects, which can be filtered according to the categories or projects of interest.
- Checklist analysis: this checklist consists of a questionnaire that helps identify possible gaps or necessities in a project.
- Expert judgement: this is given by the knowledge that the team has of specific risks, and it can come out through brainstorming sessions or interviews.
- Project status: this includes all types of reports which give an idea of how the project is going, such as progress and quality reports. Such report can be useful in the identification phase because they can provide insights on potential new risks.

Second, during the risk identification phase it's useful to classify the risks according to four main *risk categories*:

- Technical risks: these risks can arise from the use of technology, from specific requirements, from performance or from quality.
- External risks: these risks can come from problems with customers, contractors, suppliers, etc.
- Organizational risks: these risks can arise from problems in logistics, lack of resources, budget constraints, project dependencies etc.
- Project Management risks: these risks can come from errors in the main project management phases such as planning, scheduling, estimation, controlling, and communication.

### 1.2.2. Risk Analysis

This phase of project risk management aims at examining how the outcomes and the objectives of a project can change due to risks' impact. For each risk identified, it's possible to measure the impact it has on a project both quantitatively and qualitatively.

First, for a proper quantitative analysis, the *probability of risk occurrence* must be established and according to the Project Management Institute (PMI), the following classification holds valid:

1. High probability, which goes from $80\% \leq x \leq 100\%$
2. Medium-high probability, which goes from $60\% \leq x < 80\%$
3. Medium-low probability, which goes from $30\% \leq x < 60\%$
4. Low probability, which goes from $0\% < x < 30\%$

Where x is the probability of the risk occurring.

Second, every specific risk can be given a more quantitative level of impact, according to the following *risk impact* categorization:

1. High impact: Catastrophic (Rating A – 100)
2. Medium impact: Critical (Rating B – 50)
3. Low impact: Marginal (Rating C – 10)

The Project Management Institute (PMI) created the following matrix as a guideline to classify the risk impact according to the categorization introduced above:

| Project Objective | Rating C - 10 | Rating B - 50 | Rating A - 100 |
|---|---|---|---|
| Cost | Cost increase > 0% or > 0 € | Cost increase 5-10% or > 50000 € | Cost increase > 10% or > 100000 € |
| Schedule | Overall project schedule delay > 0 days | Overall project schedule delay > 1 week | Overall project schedule delay > 2 weeks |
| Scope | Scope decrease is barely noticeable | Minor areas of scope are affected | Major areas of scope are affected; scope reduction unacceptable to the client |
| Quality | Quality reduction is barely noticeable | Quality reduction does not affect vital functionality | Quality reduction requires client approval |

*Table 1. Impact Classification Guideline*

The following step of the risk analysis phase is that of defining the *risk exposure*. To do so, it's necessary to first define risk as the multiplication between the probability of risk occurrence and the risk impact, as shown in the formula below:

$$Risk = Probability \times Impact = p \times i$$

Taking this as a starting point, the risk exposure can be calculated with the Impact-Probability Matrix introduced by the Project Management Institute (PMI) methodology, illustrated below:

| | | **Probability** | | | |
|---|---|---|---|---|---|
| | | **1=high (80% ≤ x ≤ 100%)** | **2=medium high (60% ≤ x ≤ 80%)** | **3=medium low (30% ≤ x ≤ 60%)** | **4=low (0% < x < 30%)** |
| **Impact** | **A=high (Rating 100)** | Exposure=Very High (Score 100) | Exposure=Very High (Score 80) | Exposure=High (Score 60) | Exposure= Moderate (Score 30) |
| | **B=medium (Rating 50)** | Exposure=High (Score 50) | Exposure= Moderate (Score 40) | Exposure= Moderate (Score 30) | Exposure=Low (Score 15) |
| | **C=low (Rating 10)** | Exposure=Low (Score 10) | Exposure=Low (Score 8) | Exposure=Low (Score 6) | Exposure=Low (Score 3) |

*Table 2. Impact-Probabilty Matrix*

The final step of the risk analysis phase is to assign a timeframe to each risk identified. This classification can be done according to the following timeframes:

- Near, meaning from now until a maximum of one month
- Mid, meaning probable to occur in the next 2-6 months
- Far, meaning probable to occur in more than 6 months

### 1.2.3. Risk Response Planning

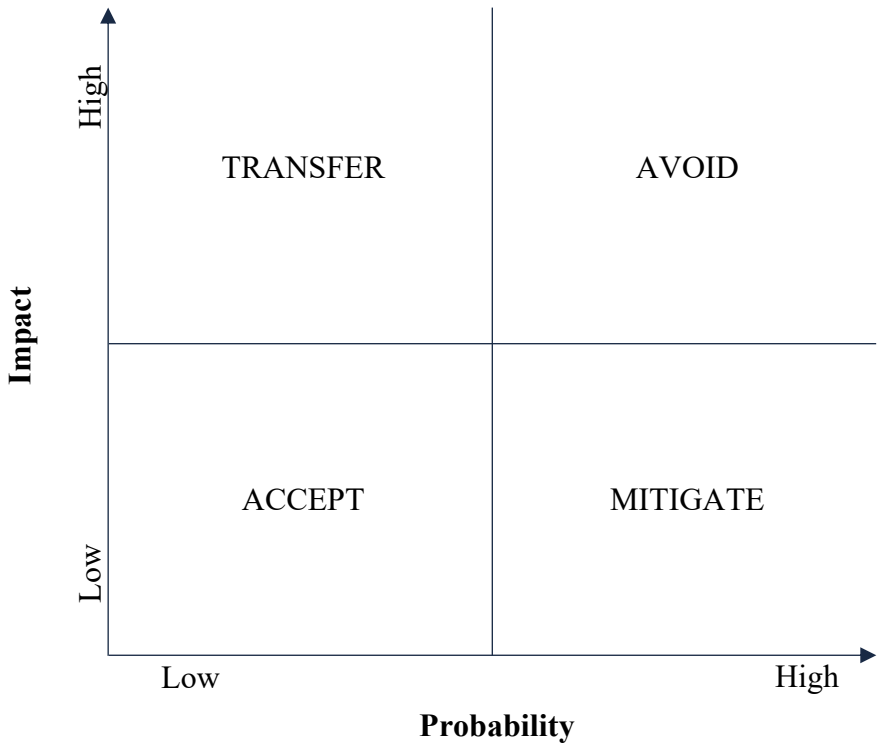
Throughout a project, the risk management team could identify numerous different risks which could have a specific impact on the desired output, so it's important to respond to each risk in a way to reduce catastrophic results as much as possible.

The Project Management Institute (PMI) proposes a series of tools and techniques to choose the most proper response strategy, such as decision trees.

There are four main strategies that deal with risks which could have an impact on projects:

1. Avoid: with this strategy, the project team tries to eliminate the threat to protect the project from any impact. This can involve changing plans, objectives, and schedules. The most extreme avoidance strategy is that of fully shutting down a project.
2. Transfer: with this strategy, the team tries to shift the threat to a third party, to protect the project directly. By doing so, the responsibility of managing a risk simply goes to another party but it doesn't disappear.
3. Mitigate: with this strategy, the team's aim is to reduce the probability of the risk occurring and to reduce the impact it could have. This is done through actions that can be taken early in the project to prevent risks from occurring and this strategy is usually more effective than trying to fix a damage after it has already come up.
4. Accept: with this last strategy, the team acknowledges the risk and decides to take no action whatsoever unless the risk ends up occurring. This strategy entails no change to the project plans, but it requires the establishment of a contingency reserve, meaning an amount of money, resources, and time which can then be used in case of emergency to handle risks.

The following diagram helps determine which response strategy should be implemented according on the probability and the impact of the risk considered:



### 1.2.4. Risk Monitoring and Control

This last phase includes activities which must be carried out to keep risks under control and not receive any unexpected consequences. In particular, the steps taken to monitor and control risks are the following:

- Keep identifying new risks and plan for them
- Keep track of already existing risks, make sure that the assessments made still hold valid, and monitor their developments.
- Reclassify risks is necessary
- Report risks and the

## 1.3. Information Systems

### 1.3.1. What are Information Systems

Information Systems surround us daily and are becoming a more and more integrated part of today's businesses all over the world.

An Information system can be defined as: "*a set of interrelated components that collect, process, store, and distribute information to support decision making and control in an organization*"[3]. The five major components of Information Systems are hardware, software, data, people, and processes, where the first three make up what we call "technology", whereas the last two link these concepts to everyday life. For each of these five components, a brief description can be made:

1. Hardware: hardware is the tangible portion of the information system, meaning that it includes every item that can be touched such as computers, smartphones, monitors etc.
2. Software: software is the non-tangible portion of the information system, meaning that it's the part we can't see but use in every step of our technological actions. Software is created by programmers through a set of written instructions which communicate to the hardware what must be done. There are two main categories which make up software: Operating System and Application system. An operating system is that portion of software which provides an interface between the user and the application, whereas application software is what allows a user to perform a specific task.
3. Data: data is another intangible part of information systems. Data can be defined as a collection of different facts that, put together, can give a business an entire database

[3] Laudon, K.C. and Laudon, J. P. (2014) Management Information Systems, thirteenth edition. Upper Saddle River, New Jersey: Pearson

that can be used for decision making, analysis, and organizational improvements. The main role of an information system when dealing with data is that of taking such data, transforming it into information and then ultimately transforming the obtained information into organizational knowledge.

4. People: many different users are involved in the making of an information system, the main ones being everyday users, the support staff, system analysts, developers, and the chief information officer (CIO) of a company.
5. Process: information systems are taking more into account organizational processes every day, making it essential introduce them into the present description. A process is a set of steps undertaken to reach a desired goal or outcome. Nowadays processes are being more and more automatized and re-engineered, with the ultimate goal of improving business processes and enhancing their interfaces with customers and suppliers.

### 1.3.2. Information Systems through time

Over time and decades, technology has evolved and adapted to social change, nevertheless it has always remained the backbone of every business and as we reach the era of digitalization, integration of information systems into organizations over time and the specific elements through which they reached users:

| Era | Hardware | Operating System | Applications |
|---|---|---|---|
| Mainframe (1970s) | Terminals connected to mainframe computer | Time-sharing (TSO) on Multiple Virtual Storage (MVS) | Custom-written MRP software |
| PC (mid-1980s) | IBM PC or compatible. Sometimes connected to mainframe computer via network interface card. | MS-DOS | WordPerfect, Lotus 1-2-3 |
| Client-Server (late 80s to early 90s) | IBM PC “clone” on a Novell Network. | Windows for Workgroups | Microsoft Word, Microsoft Excel |
| World Wide Web (mid-90s to early 2000s) | IBM PC “clone” connected to company intranet. | Windows XP | Microsoft Office, Internet Explorer |

| | | | |
|---|---|---|---|
| Web 2.0 (mid-2000s – present) | Laptop connected to company Wi-Fi. | Windows 10 | Microsoft Office |
| Post-PC (today and beyond) | Smartphones | Android, iOS | Mobile-friendly websites, mobile apps |

*Table 3. Information Systems through time. Reference below[4].*

### 1.3.3. The Competitive Advantage of Information technology

As we live in the era of digitalization, it's important to value the competitive advantage that information systems, more specifically information technology (IT), can bring to companies.

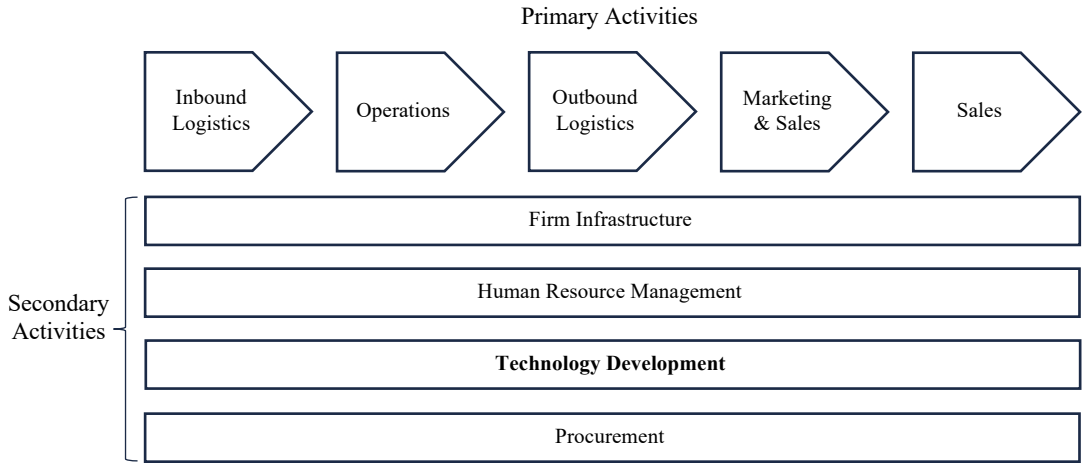
Information technology is the portion of an information system which groups the use of hardware, software, and data, in which the information or data is designed and then implemented.

According to Michael Porter in his book *Competitive Advantage: Creating and Sustaining Superior Performance*[5], a company is said to have a competitive advantage over its competitors when it has profits that are higher than the average profit in that specific industry. There are two ways to achieve such advantage: through a cost advantage or through a differentiation advantage. According to Porter, Information technology can be a factor in both of these two methods, and he demonstrated this using two analytic tools: the value chain and the five forces model.

The Value Chain is a diagram representing a series of activities that a company undertaken to produce a service or a product, the aim of which is to show how value in built. The value chain is made up of primary activities (inbound logistics, operations, outbound logistics, marketing and sales, services) and of secondary activities (firm infrastructure, human resource management, technology development, procurement). The analysis of a value chain can provide insights on hoe information technology can lead a company to have competitive advantage over other companies, given that the technology development activity supports the main primary activities leading them to become more innovative and therefore generating more value. A graphical representation of the Value Chain is shown below:

[4] David Bourgeois, Joseph Mortati, Shouhong Wang, and James Smith (2019) Information Systems for Business and Beyond.

[5] Porter, M (1985). Competitive Advantage: Creating and Sustaining Superior Performance. New York: The Free Press




The Five Forces Model is used to understand to what degree a company is competitive and to analyze its strengths and weaknesses. This model is made up of five elements:

- Threat of substitute products or services
- Bargaining power of suppliers
- Bargaining power of customers
- Barriers to entry
- Rivalry among existing competitors

According to Porter, technology can have an impact on each one of these elements and change the overall profitability.

Having analyzed these two tools introduced by Porter, it's possible to summarize the main goals of a strategic information system implemented by a company:

1. To deliver a service or a product at a lower cost compared to other companies
2. To deliver a differentiated service or product
3. To help the organization focus its attention on a specific market segment
4. To enable innovation

There are many information systems capable of achieving such goals, a few of which are listed and explained below:

- Business Process Management Systems: the competitive advantage of these systems is given by the fact that they can integrate business processes with information systems and/or information technology.
- Electronic Data Interchange: this system integrates the supply chain electronically, leading to a clear competitive advantage.

- Collaborative Systems: these systems create competitive advantage because they allow a company's employee to collaborate in different ways while working. Common use examples of collaborative systems are Google Drive, Microsoft SharePoint, Cisco WebEx, and GitHub.
- Decision Support Systems: these systems facilitate decision making processes within different levels of an organization. They receive specific inputs and provide the necessary information to make a decision of any kind and this process can also be automatized.

In 2008 a study regarding competitive advantage brought by IT was published in the Harvard Business Review by researchers Brynjolfsson and McAfee[6].

According to such study, it appeared that IT could play a big role in a company's competitive advantage if implemented wisely and strategically. The following three conclusions were made to this regard:

1. First, it appeared that IT has in fact highlighted the differences between companies instead of reducing them, meaning that it made way to the most competitive companies to stand out. This shows that technology has given companies the opportunity to change in their own way, according to their own approaches to technology.
2. Secondly, technology improved management skills, allowing process innovations to be delivered on platforms implemented by vendors, consultants, and IT departments.
3. Finally, the competitive advantage brought to companies by IT is worldwide, meaning that it has touched, and it continues touching every country in the world, as IT investments grow more and more everywhere.

[6] McAfee, A. and Bryonjolfsson, E. (2008, July-August). Investing in the IT That Makes a Competitive Difference. Harvard Business Review

# Chapter 2. State of the Art analysis

Having Introduced the main concepts of Project Management, Project Risk Management, and Information Systems, it's now possible to focus on previous research that that been carried out in this field.

The examples proposed in this section have the aim to demonstrate how the discipline of Information Risk Management has been addressed up until now, specifically through IT audits and continuous improvement methodologies.
Before making a deep dive into the state-of-the-art analysis, it's important to introduce the concept of continuous improvement.

## 2.1. Introduction to Continuous Improvement

Continuous Improvement is a concept which had been introduced in the business industry through the Lean Manufacturing/Production philosophy, more specifically with the creation of the Six Sigma methodology. Such methodology can be applied through numerous frameworks such as the DMAIC framework, which will be introduced in detail more ahead.
Continuous Improvement is a never-ending strive to reach perfection in every business process. According to the Lean methodology, continuous improvement aims at improving every process in a company by enhancing those activities that generate the most value and generate the least waste in terms of resources, costs, and time.

There are different tools and techniques which can be implemented to create a suitable environment in a company and adopt continuous improvement. In Lean Manufacturing, the following approaches are the ones that mainly stand out:

1. **Plan-Do-Check-Act** (PDCA): this model is a cycle that aims to set an improvement starting from results that have already been achieved, and this is carried out by these four phases, which each have a specific role:
    - Plan: in this phase, the objectives are set, and the processes needed to give the desired outputs are identified.
    - Do: during this phase, everything that has been laid down during the planning phase is executed.

- Check: after the execution, this phase requires to check the results that have been achieved and compare them to what was expected.
- Act: finally, according to the comparison analysis, it's important to act in the right way to keep changing steps in a process to continuously improve it.

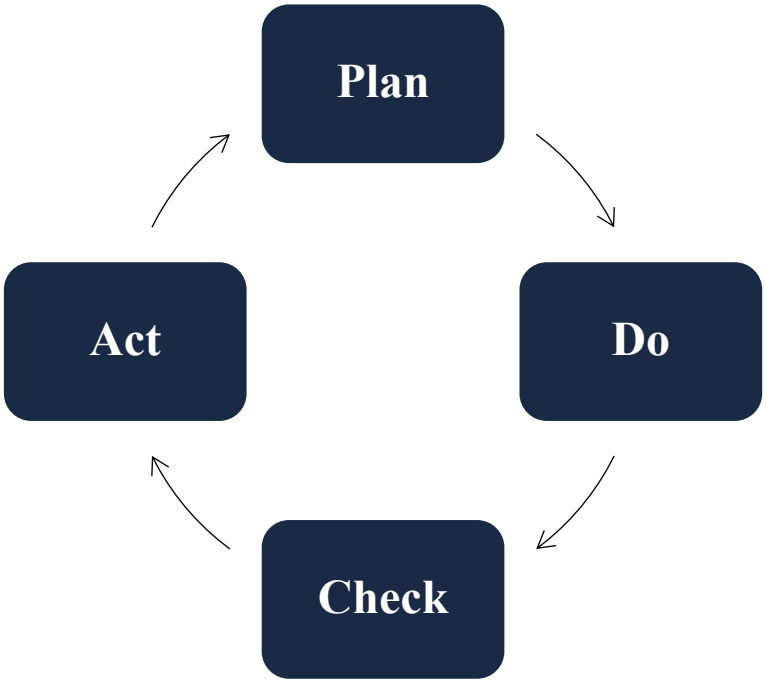



*Figure 1. PDCA model*

2. **Root Cause Analysis** (RCA): this next model is an iterative process which tries to improve or solve a problem by analyzing the root causes that caused it in the first place. The process continues until the final negative effect is reached.

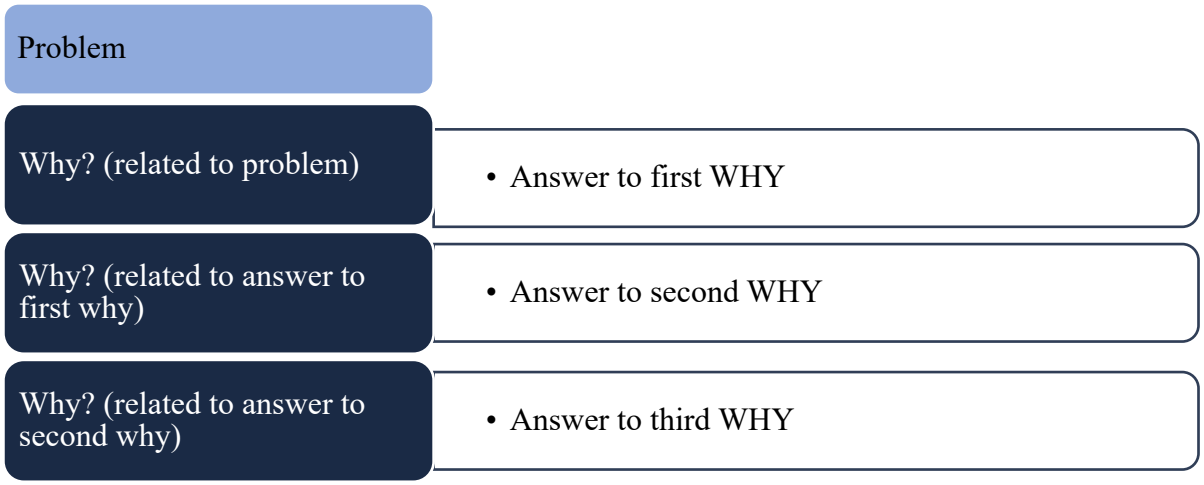



*Figure 2. Root Cause Analysis model*

3. **Lean Kanban**: Kanban is a system that was first used by Toyota to improve the workflow efficiency in a production process and was then adapted by numerous realities as a method to achieve continuous improvement. The model proposed by Kanban is based on six practices which should be put into place to minimize waste in a process:

- Visualize the workflow
- Eliminate any interruption
- Manage flows
- Make policies more explicit
- Generate feedback
- Improve collaboratively

The Kanban method relies on a series of whiteboards that help visualize a workflow by mapping every step of a process. A typical Kanban board is divided into three rows, each containing a series of Kanban cards representing the single activities. For the workflow to be considered complete, each card must pass through every stage. An example of a Kanban board is illustrated below:

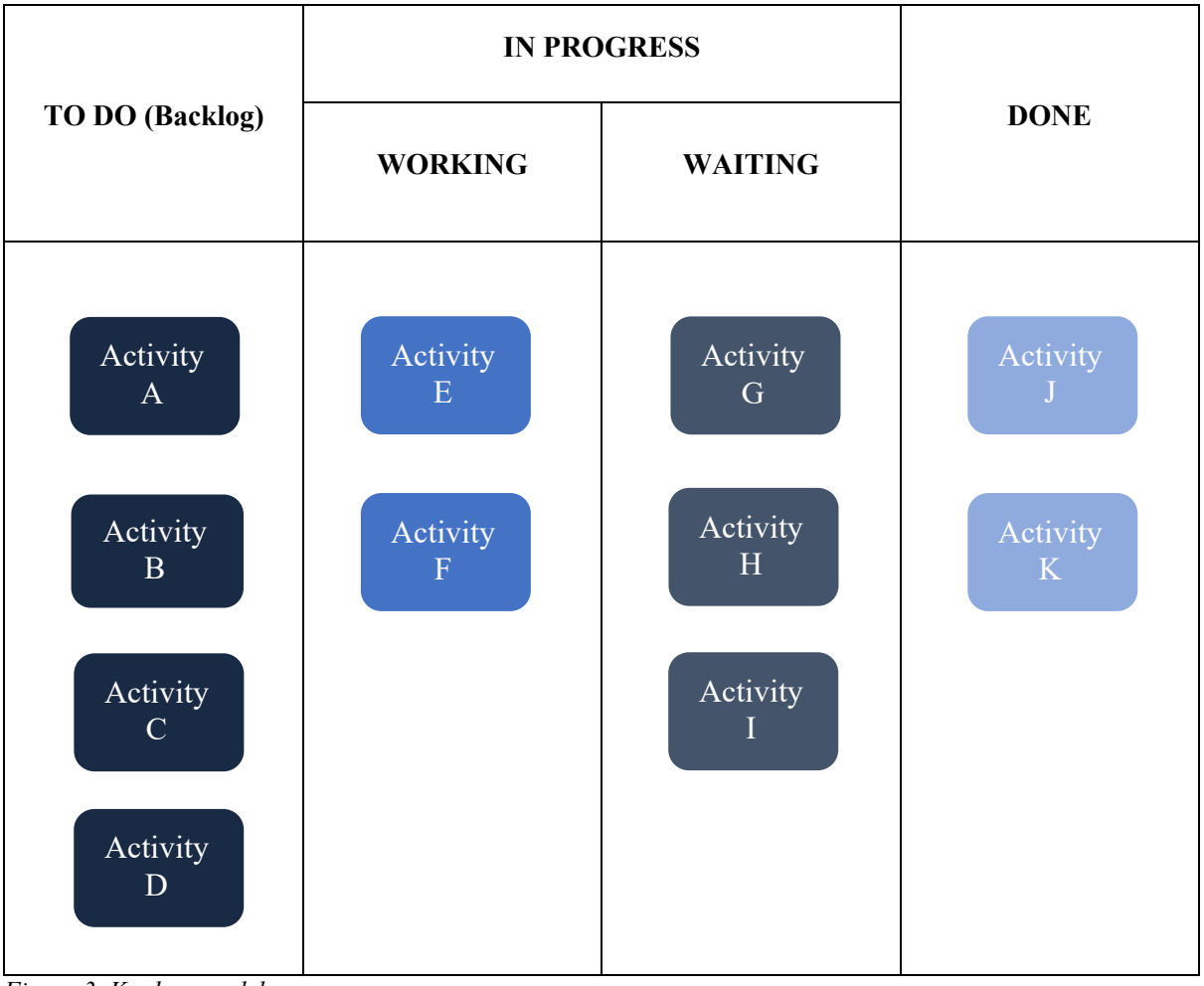



*Figure 3. Kanban model*

## 2.2. 4D-ISS: New proposal for the continuous improvement model of information risk management

In 2018, during the IEEE 27th International Conference on Enabling Technologies, a new approach to information system security governance was proposed and later reported through a dedicated article[7].

The article focuses on introducing the Information System Security Governance (ISSG) framework, particularly the first brick related to Risk Management (ISSRM), and on proposing a new process model for the improvement of the framework. Such model is called 4D-ISS and it's made up of four phases: Define, Direct, Deploy and Decide.

After having described the new proposed model, the article also explains how it can be deployed using the Business Process Modeling Notation (BPMN).

### 2.2.1. Introduction

In this framework, information security risk is defined as the possibility that a given threat could harm the organization by exploiting the vulnerabilities of an asset or group of assets, where assets are referred to as all those resources which are valuable to the organization for their proper functioning.

Such assets can be split into two separate categories: business related assets and information system related assets.

The first ones consist of information and processes which are often managed entirely through information systems, whereas the latter (IS assets) include an organization's technical elements such ad hardware, software, networks, users, and infrastructures.

The Information System Security Governance Risk Management (ISSRM) equation for the determination of risk is slightly different from the commonly known one, as it includes the concept of asset vulnerability: *Risk = Vulnerability x Threat x Impact*.

### 2.2.2. Proposition of the new ISSRM model: 4D-ISS

The scope of this model is to try to align the foundations of the ISSRM with business strategies and to do so, a cyclical and continuous process is introduced. The process is broken down as shown in the cycle below:

[7] "A new approach of information system security governance: a proposition of the continuous improvement process model of information system security risk management: 4D-ISS". Mounia Zaydi, Bouchaib Nassereddine, 2018.

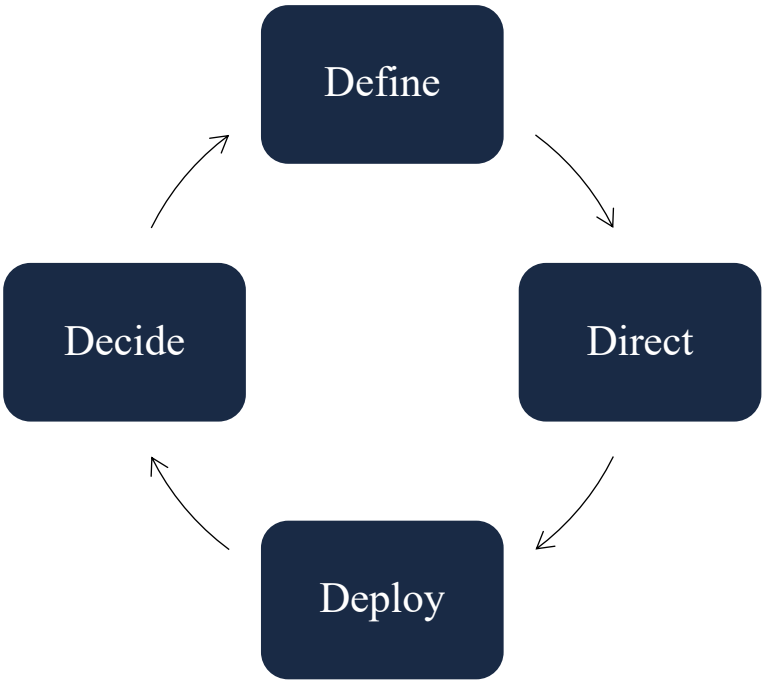



*Figure 4. 4D-ISS model*

In the "Define" phase, risks are identified, evaluated, and prioritized; the "Direct" phase controls such risks and chooses the treatment strategy (transfer, avoid, accept, mitigate) which best fits; during the "Deploy" phase the measure chosen are effectively implemented; finally, during the "Decide" phase, the relevance and degree of the identified risks are measured.

The implementation of the 4D-ISS process has the final aim to integrate risk management processes with business processes and to continuously improve the alignment between the two. For this reason, the assignment of defined roles and responsibilities becomes a critical success factor throughout an organization, to improve the interactions between responsibility groups and divisions. To do so, the R.A.C.I. (Responsible-Accountable-Consulted-Informed) matrix is used. Such matrix links a level of responsibility to each human resource working for an organization for each task they carry out. The general outline of the R.A.C.I. matrix is shown below:

| | Person A | Person B | Person C | Person D |
|---|---|---|---|---|
| Task 1 | **Responsible** | C | A | R |
| Task 2 | C | **Accountable** | I | I |
| Task 3 | A | I | **Consulted** | C |
| Task 4 | R | C | A | **Informed** |

*Table 4. R.A.C.I matrix*

To better read the matrix, Person A is taken as an example: Person A must perform all 4 tasks but has been assigned a different level of responsibility for each of them. In Task 1 and in Task 4, the organization expects Person A to be the main responsible and so to carry out the tasks as project manager/group leader. For Task 2, Person A will be consulted but will hold no direct responsibility over the outcome of the task. Finally, for Task 3, Person A isn't directly responsible but can still be held accountable for the way the task is carried out.

### 2.2.3. 4D-ISS process modeling and conceptualization

Before applying the 4D-ISS model introduced, an organization must first assess its level of maturity with respect to their risk management strategies and guidelines, therefore a proper assessment of the maturity degree must be made. To do so, the organization can choose whether to create a personal evaluation grid or to use a structured framework such as the well-known COBIT framework.

## 2.3. Continuous Improvement for Risk Management in a construction project.

In 2018, an analysis of a subsea pipeline construction project was carried out by the Industrial and Mechanical Engineering Departments of the National Institute of Technology in Indonesia and was then documented in a research article[8]. The scope of such analysis was to identify, assess, mitigate, and monitor all the risks arising from the project and highlight how the risk management was integrated by continuous improvement concepts and methods.

The main methods used for the improvement of the construction project were the Delphi method, the FMECA method, the DNV RP F107 method, and the PDCA model described at the beginning of this chapter.

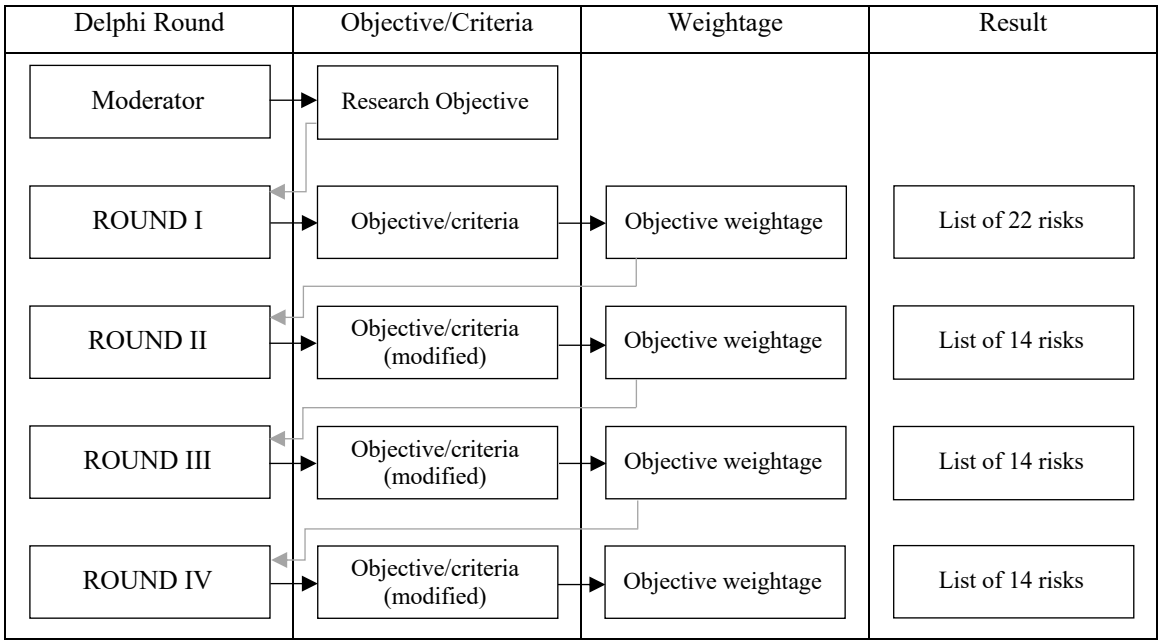
The construction of the subsea pipelines project described in the considered article took place starting from the Offshore Production platform Sepinggan, all the way to the Sejadi Platform in East Kalimantan in Indonesia and the pipelines installed were used to drain the oil and the gas production from the Sejadi to Sepinggan. At the initiation of the project, it was settled that a major risk assessment would take place, to identify and try to avoid the major risks at hand.

[8] "Risk Management in subsea pipelines construction project using Delphi method, FMECA, and continuous improvement". Ellysa Nursanti, Sibut, Julianus Hutabarat, and Ardi Septiawan. National Institute of Technology ITN Malang, Indonesia.

In particular, the highest risks that could arise from this type of project were those on a construction and on an operational level.
Furthermore, such project had to take into consideration external risks which could have a major impact on the construction, such as the risk of a ship sinking and falling on the pipelines, an anchor dropping or dragging, causing scratches or severe damage to the pipelines.

Having established the need for a specific risk assessment, the team carried it out following a specific research method, which was put into place following the 4 phases of the PDCA model: Plan, Do, Check, Act.

PLAN Phase: during the plan phase, which in risk management is commonly known as the risk identification phase, the main activity consisted in providing a list with all the potential risks that could occur. This task was carried out by a senior engineer, a project manager, a marine specialist, and by an operation specialist with many years of experience on the field. Such research was then integrated by the **Delphi method**, which was conducted through a questionnaire with the intention to identify the risks and then to assess the actual probability of the specific risk to occur, providing the possibility to answer on a scale from 1 to 5. The Delphi method, following it an iterative approach, continued with a third round in which a summary of the previous results was made, and then finally concluded with a fourth round which confirmed and validated the results of the entire iteration. In the end, a total of 22 risks was identified and 14 risks were selected and verified. The rounds of the Delphi method applied throughout the "plan phase" can be summarized in the following way:



DO Phase: the second phase was the do phase, which in risk management can be commonly referred to as the risk measurement phase. The main aim of this phase was to analyze the risk at hand, and this was done with the integration of the **FMECA method**.

The FMECA takes into consideration the three core parameters of risk management which are likelihood, impact, and detection. Each of these parameters is described with a value from 1 to 10 and then the FMECA method proceeds by multiplying the values of such parameters with eachother. The result obtained is the Risk Potential Number (RPN), and so by the end of the FMECA process, each risk had an RPN. Once all the RPNs had been calculated, they were ranked from the lowest to the highest, and the risk with the highest RPN was assesses as the most influential risk which had the priority to be mitigated. An example of the FMECA method result is shown below:

| **Risk No.** | **Risks** | **Likelihood** | **Impact** | **Detection** | **RPN** | **Impact** (USD) |
|---|---|---|---|---|---|---|
| 8 | Project delayed | 8 | 9 | 8 | 576 | 2.100.000 |
| 5 | Failure of pipeline laying (failure of design) | 7 | 9 | 8 | 504 | 1.500.000 |
| 10 | Leakage of hydro test | 8 | 9 | 6 | 432 | 900.000 |
| 3 | Pipe failure (due to anchor, leakage, drop anchor, corrosion, fatigue) | 8 | 6 | 8 | 384 | 653.000 |
| 1 | Poor of stakeholder communication | 6 | 7 | 9 | 378 | 165.000 |
| 12 | Error calculated of engineering design | 8 | 9 | 5 | 360 | 1.800.000 |
| 2 | Fisherman friction | 9 | 3 | 9 | 243 | 16.500 |
| 7 | Failure of existing facility | 6 | 8 | 4 | 192 | 82.500 |
| 9 | Error of *equipment/ tools* due to installation | 7 | 6 | 4 | 168 | 33.000 |
| 14 | Fire | 7 | 6 | 4 | 168 | >8.700.000 |
| 4 | Drop object | 4 | 8 | 5 | 160 | 30.000 |
| 11 | *Personal injury* | 8 | 4 | 5 | 160 | >8.700.000 |
| 6 | Sea wave / weather | 8 | 7 | 2 | 112 | 8.250.000 |
| 13 | Difficulty of permit | 7 | 6 | 2 | 84 | 16.500 |

*Table 5. Risk analysis result with FMECA*

CHECK Phase: the third phase is the check phase, which in risk management can commonly be defined as the risk mitigation phase. Once the FMECA method gave as an output the risk with the priority to be mitigated, the check phase structured and put into place the adequate mitigation strategy. The table below shows the comparison between the identified risks before the mitigation strategy was put into place and the risks remained after the mitigation strategy:

| **Before risk mitigation** | **After risk mitigation** |
|---|---|
| **A. Major risks**<br>1. Project delayed<br>2. Failure of pipeline laying (failure of design)<br>3. Leakage of hydro test<br>4. Pipe failure (due to anchor, leakage, drop anchor, corrosion, fatigue)<br>5. Poor of stakeholder communication<br>6. Error calculated of engineering design<br>**B. Moderate**<br>7. Fisherman friction<br>8. Failure of existing facility<br>9. Error of equipment/tools due to installation 10. Fire<br>11. Drop object<br>12. Personal injury<br>**C. Minor**<br>13. Sea wave / weather<br>14. Difficulty of permit | 1. Sea wave / weather<br><br>2. Difficulty of permit |

*Table 6. Comparison before-after mitigation*

ACTION Phase: the final phase was the action phase, in which the continuous improvement concept was integrated. The main purpose of this phase was to understand whether the mitigation strategy had worked or not, and only then to calculate the impact value before and after the mitigation had been put into place.

The research method carried out by the team for the construction project and briefly described above can be schematized in the following way:

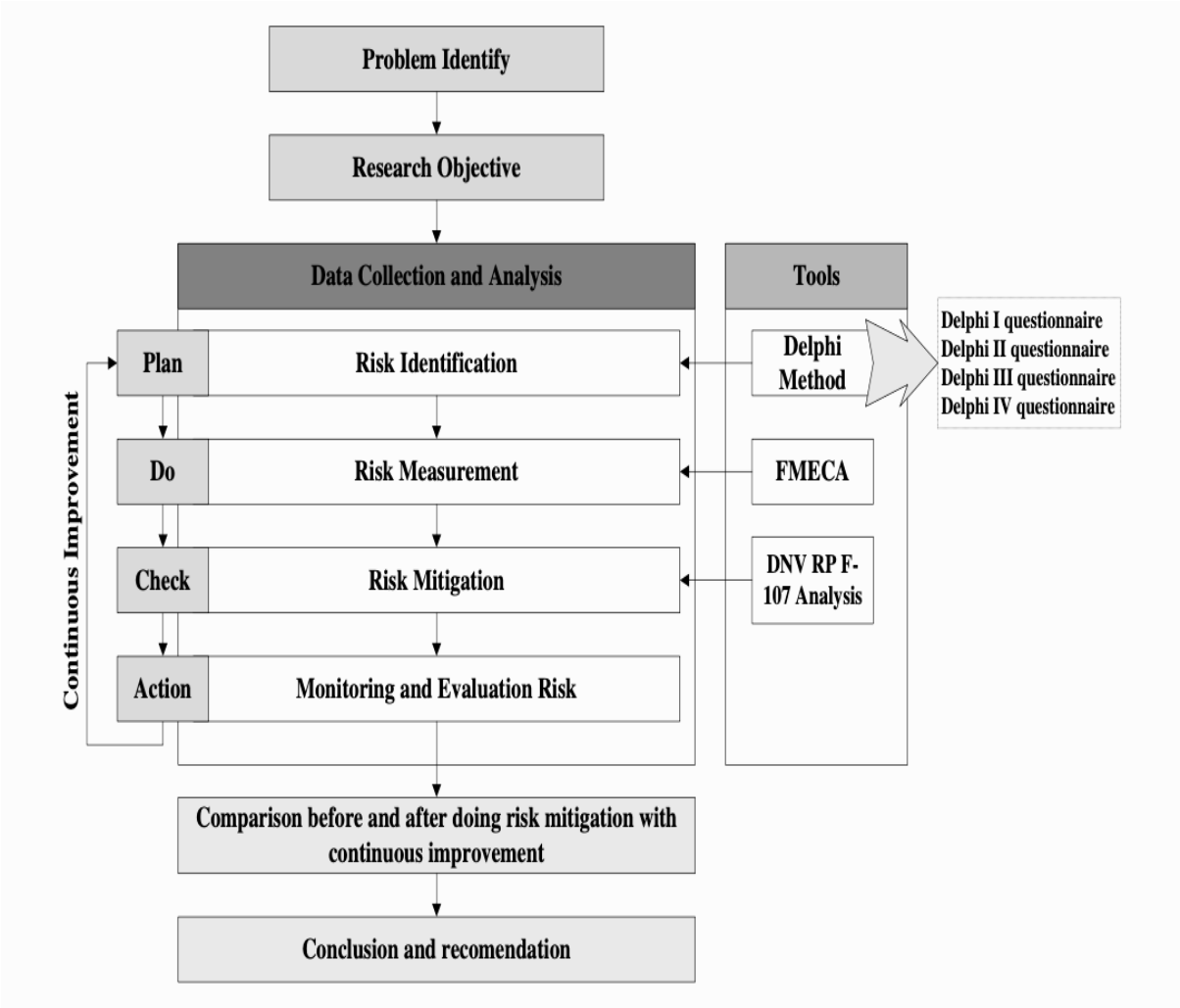



*Figure 5. Research Method*

# Chapter 3. Process Analysis

The following chapter introduces a case study with the scope of further breaking down the Project Risk Management concepts introduced up until now.
The Accounting Firm case study presented from here on out wants to examine the way the entity addresses cases of Risk Management, more specifically of Information Risk Management, through the IT audit process and how such process could be improved.
For the purpose of such analysis, a specific framework has been chosen as a benchmark, to better map the risk assessment phases and the continuous improvement approach.

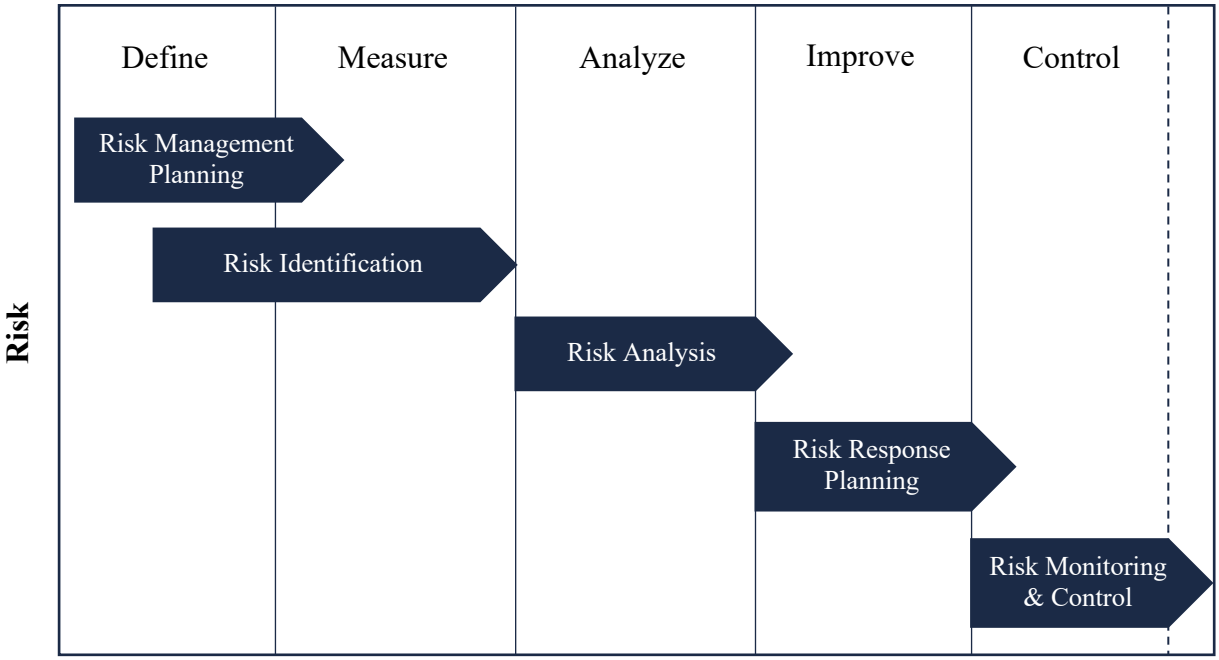
## 3.1. DMAIC Framework

DMAIC stands for Define, Measure, Analyze, Improve, and Control and it's a framework which implements the Six Sigma methodology for continuous process improvement.
The framework introduces five phases which can be linked to the Project Risk Management phases in the following way:

- During the Define phase, the project team identifies the problem at hand which needs a solution and defines the scope of the project itself. A Gantt Chart or a more general plan for future activities is made at this moment. In Project Risk Management, such phase is present during the Risk Management Planning phase and the Risk Identification phase.
- During the Measure phase, the data needed is collected and the problem is quantified. Data collection consists in studying process maps to identify possible bottlenecks and then determining how the process at hands meets expectations. In Project Risk Management such phase is translated into Risk Identification, during which there is a determination and documentation of where the project might be at risk.
- The Analyze phase has the aim to analyze cause-effect relationships in a process, to find which process input factor has the most influence on the desired output. In the Six Sigma Methodology, such phase is based on statistical significance and is therefore carried out using statistical tools such as hypothesis testing, correlation and regression, and the analysis of variance (ANOVA). In Project Risk Management, this phase is identified in the Risk Analysis, in which the actual assessment of the risk's probability and impact is brought out and such analysis can be both quantitative and qualitative.

- The Improve phase takes all the information that has been gathered in the previous phases and determines whether the project process can be changed in a way for the final output to improve. In other words, this phase aims at developing potential solutions based on the main causes identified before. In Project Risk Management, this phase is translated into Risk Response Planning, in which the actions taken to enhance opportunities and reduce risk are decided on.
- The Control phase is the last one, during which statistical process controls are implemented to ensure that results are sustainable, and a control plan is stipulated, to make sure that processes are monitored in the future and that action plans are put into place when needed. In Project Risk Management, the Control phase is identified in Risk Monitoring and Control. In such phase, the project team keeps good track of the risks which have been highlighted in the previous phases.

A summarization graph of the five phases described for the DMAIC framework and their link with the main Project Risk Management phases is shown below:




*Graph 1. DMAIC and Risk Management*

## 3.2. AS-IS Process in the Accounting Firm.

We will now analyze the AS-IS Project Risk Management Process brought out by the Accounting Firm and we will make a deep dive into a specific field of Project Risk Management which is Information Risk Management.

Information Risk Management (IRM) is a line of service dedicated to evaluating and managing the possible risks arising from the technologies which support a business. Such service includes the process of IT Audit.

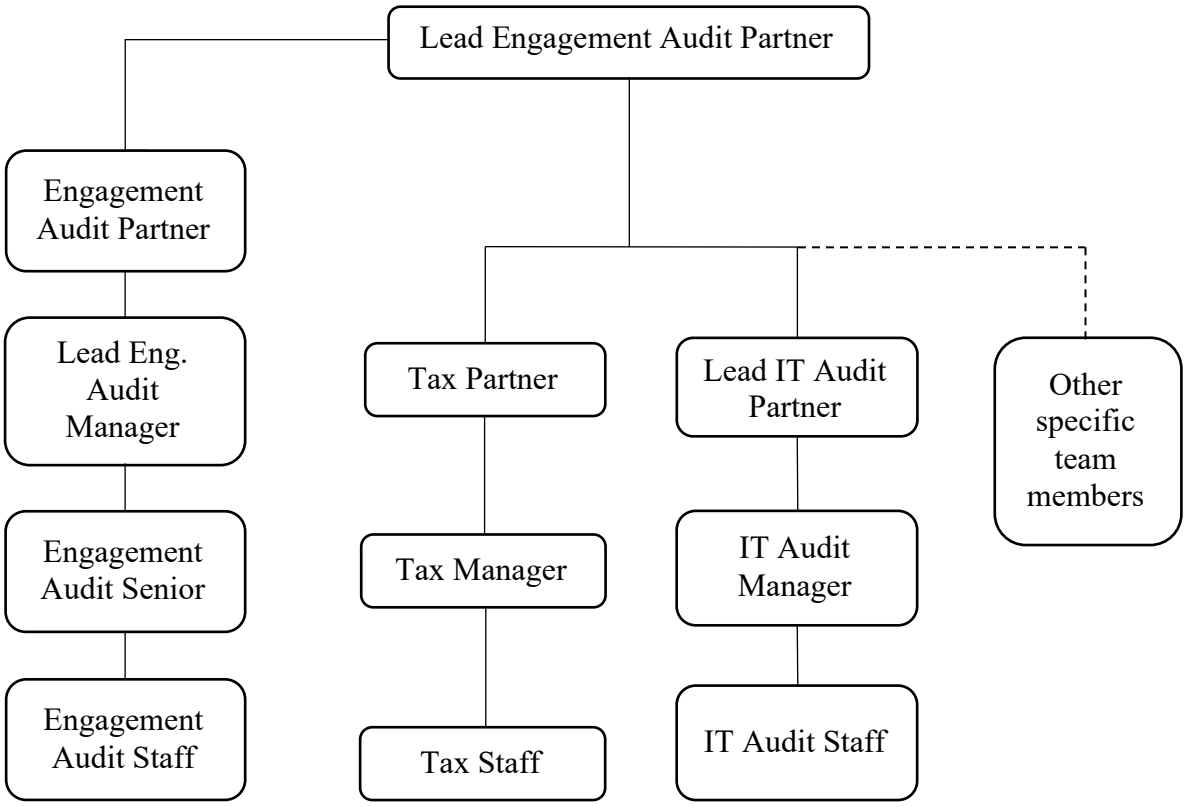
An IT audit is an examination of the management processes and controls within Information Technology structures and business applications. The aim of an IT auditor is that of ensuring the quality of an organization's IT systems and databases and verifying that the methodologies applied are compliant with specific standards.

The role of an IT auditor is mainly that of supporting the activities of the general audit team, responsible for reviewing a client's financial reports. There are in fact specific situations and reasons for which IT auditors get involved in an audit, such as the following:

- To assist the audit team in helping them understand how the client at hand manages it transactions using IT systems
- To understand which IT systems are important and significant for the scope of financial reporting.
- To highlight the major risk points while analyzing the entity's processes
- To highlight all the risks that could arise from the use of IT systems
- To identify all those controls that the entity should carry out to mitigate the risks identified
- To evaluate if such controls have been designed and implemented correctly and to test their effectiveness

As specified in the Accounting Firm's Audit Execution Guide, the audit activity must be conducted in accordance with the International Standards on Auditing (ISAs) to enable a consistent and high-quality audit and with three main frameworks: COBIT, COSO and ISO 27001.

An audit, with the support of IT auditors is carried out by a so-called engagement team, which has a specific structure, represented in the diagram below:




The following analysis describes the role of the IT audit approach in the project phase of Risk Assessment and in the processes through which a client's IT related risks are identified. The audit process in this case can be described through the following phases, which will be further explained:

1. Risk assessment
2. Design of audit procedures
3. Audit procedures
4. Evaluation of results
5. Final issue of an opinion

Finally, the specific audit procedures brought out by the IRM engagement team can be summarized with the conceptual flowchart below, each point of which will be further explained later in this analysis:

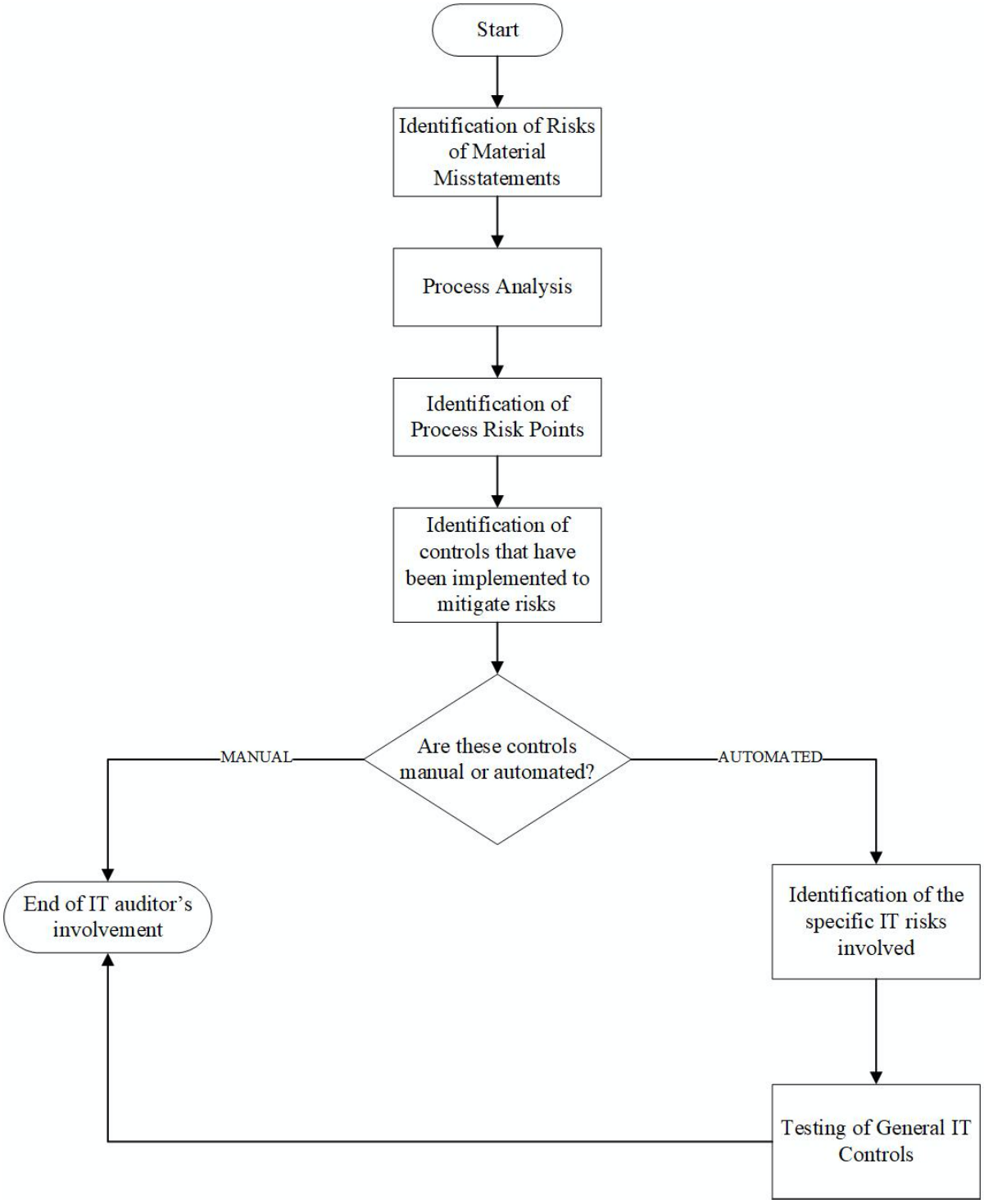



Figure 6. Audit procedure flowchart

### 3.2.1. Risk Assessment and Process Understanding

**Types of Risk**

There are three main areas of risk that must be taken into consideration while carrying out a risk assessment. The macro area is that of Risks of Misstatements (RMs) which contains Risks of Material Misstatements and Significant Risk. It's critical to underline that the IT audit

response is only requested when considering Risks of Material Misstatements (RMMs) and Significant Risk.

According to literature, the Risk of Material Misstatements is the susceptibility of the financial statements, accounts, and assertions to material misstatement, and the risk that a client's current internal controls would be ineffective in identifying and correcting such misstatements. Such risk exists at the financial statement level when they can affect and have a major impact on several assertions. There are specific factors which can lead to a higher risk of material misstatement, such as:

- Incompetence at a managerial level
- Poor oversight by the board of directors
- Inadequate records and accounting systems
- Decreasing economic conditions
- Operating in rapidly altering industries

For each risk that could lead to a misstatement, the audit team must assess the level of inherent risk, which is defined as the likelihood and magnitude of the potential misstatement that could result from each risk identified. The categorization of a risk's significance level is made possible because of professional judgement of the audit team, reached through experience on the job.

**IT Understanding**

The Risk Assessment phase begins with the understanding of an entity's processes and its environment, and this is done through a specific meeting in which a relevant inquiry is conducted.

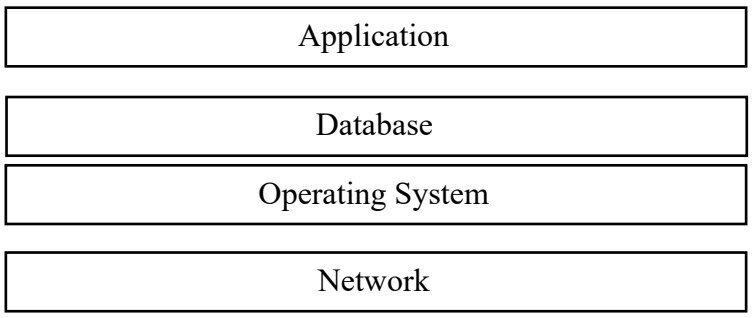
This specific phase of understanding has the aim to clearly highlight how the entity uses IT systems, how dependent the entity is on IT processes, and how such use affects their financial statements and transactions.

The first aspect to document throughout this phase is the specific IT systems used by the entity and the purpose of each of them. Specific IT systems include:

- Financial reporting applications
- Ticketing systems or utility tools
- Robot Process Automation (RPA)
- Business Process applications
- Report writers

- Data warehouse

The IT systems implemented by an entity are categorized according to the layer in which they operate. In particular, the 4 IT system layers are:




1. **Application**: this is the case in which the system performs numerous activities or tasks and includes an interface with the user.
2. **Database**: in this layer the system stores data and information and organizes it in a way for it to be easily accessed, managed, and updated.
3. **Operating System**: in this following layer, the purpose is to control more complex computer operations, which are not directly witnessed by end users.
4. **Network**: this last layer consists of the transportation and migration of data and information from one computer to another.

After having thoroughly analyzed an entity's IT organization, the audit team must also identify the key members involved in the IT organization and the specific roles that they carry. Furthermore, it's important to take into considerations not only the IT functions which are internally managed, but also those which are outsourced by the company.
The next step is to understand the entity's IT policies and procedures and how they are implemented in the processes. Finally, it's also fundamental to understand how the entity deals with cybersecurity risks and incidents and how the controls put into place are useful to mitigate such risks.

**Process Understanding**

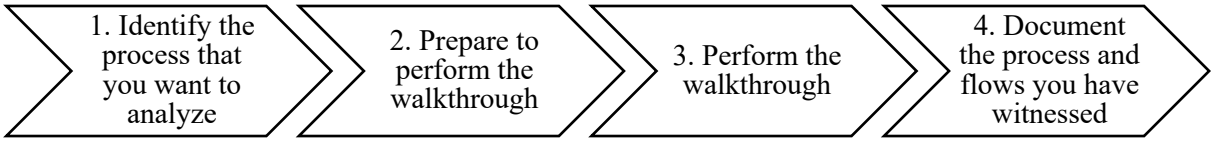
To perform a risk assessment, it's necessary to understand the processes that an entity must undergo to achieve their final target. A business process is a collection of steps that a company uses to develop, purchase, produce, sell, and distribute an entity's products and services.

Understanding and analyzing a process is important because it allows the audit team to clearly identify those points in the process where a risk of material misstatement could arise.

To understand a specific process, the methodology proposes to perform a walkthrough. A walkthrough is an audit procedure in which a process or task owner helps the audit team members understand a process by demonstrating a transaction from its origin all the way until such process is reflected in the financial statements.

The main objectives of a walkthrough are to understand the flow of transactions, to identify the points in the process where it's most likely for a risk to arise, to identify the controls that have been put into place by the entity to mitigate such risks, and finally to verify that the controls have been designed and implemented correctly.

A proper walkthrough requires 4 main steps:




It's important to highlight that a walkthrough should be brought out only for those business processes that may have a risk of material misstatement (RMM) and it's not necessary for every single process.

Once a specific process has been analyzed, it's useful for the purpose of audit activities to create descriptive flow charts, which are in fact graphical representations of a process or of a system in which process steps are showed in a logical sequence.

Flowcharts are very commonly used tools because of their visual simplicity: they are in fact built with basic shapes and symbols to represent different functions.

Furthermore, the use of flowcharts allows the audit team to identify gaps and to understand the actual information and transactional flows.

### 3.2.2. IT Risks and Controls

**Controls**

A control can be defined as an activity put into place by management to mitigate the possible risks that can affect processes and transactions. Once management has performed such controls, the audit team must proceed by testing them to verify if they operate correctly and effectively.

Controls can be categorized according to different natures and different types. A control can be of two different natures:

1. Manual: a control is manual if it's brought out by a person in a certain point in time. It depends on human actions and can therefore lead to a greater risk of human error. An example of a manual control is the case in which a staff member of an entity must review and give approval for certain proposed transactions.

2. Automated: a control is automated if it relies on computerized actions implemented by IT systems. An example of this is the case in which authentication measures are put in place to authorize access to a system or process a transaction.

Controls can furthermore be of two different types:

1. Preventive: a control is preventive if it protects the entity by identifying and addressing possible risks before they occur. Examples of such controls are:
    - Segregation of duties
    - Authorization requirements
    - Password and information protection
    - Physical control over assets

2. Detective: a control is detective if it's designed to highlight errors in transactions after they have occurred. These controls also aim at determinizing whether preventive controls are functioning properly or not. Examples of detective controls include:
    - Reconciliation, which compares two sets of data to one another and identifies differences.
    - Reviewing statements to check for appropriateness and allowability
    - Conducting post-transaction and analysis reviews

Based on the different nature of the controls, the Information Risk Management (IRM) IT Audit team performs different procedures. For manual controls, the team must understand with what frequency the control is implemented and to what extent the control operator is authorized for such control. On the other hand, when considering automated controls, the responsibilities are more challenging. In particular, the audit team must perform the following activities:

- Identify the layers of technology which are relevant for the considered control
- Understand which IT related risks could arise within each layer and affect the control operation

- Understand how the analyzed entity has responded to such risks.

**IT Risks**

IT Risks are those risks that arise when dealing with Information Technology systems and which could affect the automated control activities or the integrity of an entity's data and information. IT Risks are strictly linked to an entity's process because they can be identified after identifying process risk points, which, as seen above, are the points in the business process at which an error could occur.

The risks related to information systems and technology can be categorized through the following Risk Breakdown Structure:

| Level 0 | Level 1 | Level 2 |
|---|---|---|
| IT RISKS | Risks in Program and Data Access | IT systems and data are accessed by anyone without restriction due to lack of authentication methods |
| | | Logical access permission is given to unauthorized accounts or to users with a different job responsibility |
| | | Logical access permissions are not revoked when necessary |
| | | Physical access in IT facilities is granted to users with a different job responsibility or who are unauthorized |
| | Risks in Program Changes | Unapproved changes made to IT system programs or configurations are wrongly implemented |
| | | Changes to IT system programs or configurations don't function properly |
| | | Logical access to implement IT system changes is given to users who are not authorized or with a wrong job responsibility |
| | Risks in Computer Operations | System jobs, processes or programs do not function as intended to support data processing |
| | | Logical access to make changes to jobs, processes or programs is not authroized or doesn't match job responsibility |
| | | Backups of programs and data are incomplete and can't be restored as needed |
| | | IT system incidents cause unavailable or inaccessible IT systems or data |
| | | IT system incidents cause IT systems to process transactions in an untimely manner |
| | Risks in Program Acquisition and Development | Acquired or newly developed IT systems or improvements to existing IT systems are not authorized |
| | | Improvements made to existing IT systems do not function properly |
| | | Acquired or newly developed IT systems do not function properly |
| | | Acquired or newly developed IT systems or major enhancements to existing IT systems are introduced into the production environment prior to their approval |
| | | Logical access rights are established and implemented for acquired or newly developed IT systems that areunauthorized or not commensurate with job responsibilities |
| | | Incomplete and/or inaccurate data is migrated to the production environment of acquired or newly developed IT systems |

*Table 7. Risk Breakdown Structure*

**IT Application Controls and General IT Controls**

An IT Application Control (ITAC) is a control related to specific computer software applications and individual transactions. These controls are reviewed and tested by auditors and management, and they can be of three types:

1. Input Controls: they verify that a transaction has been captured, recorded accurately and properly authorized.
2. Processing Controls: these controls verify that transactions have been performed as they were intended.
3. Output Controls: these controls verify the accuracy of the results obtained throughout processing controls.

For an audit, IT Application Controls are taken into consideration because an entity relies on specific applications needed to deliver services, therefore it's necessary to rely on those specific controls which ensure that data is correctly processed and maintained.

General IT Controls (GITCs) are basic controls which can be applied to IT systems such as applications, operating systems, databases and supporting IT infrastructures. Such controls enable automated control activities to work properly when they are first developed and implemented and to continue to function properly after their implementation.

The difference between General IT Controls and IT Application Controls is given by the fact that the first govern the use of all systems within a company, from ERPs to servers, directory platforms, and project management tools, whereas Application Controls restrict what users can do within one platform, and typically these permissions are configured directly within that application and pertain to specific features or use cases.

General IT Controls are helpful to maintain the security and the integrity of information relevant to the financial reporting for IT systems. These controls relate to one or more IT application, and they allow information system operations to continue working properly.

Finally, General IT Controls are important for the audit team to understand how the entity has responded to specific IT risks identified in the process.

The following flowchart highlights how General IT Controls are linked to the IT audit risk assessment process:

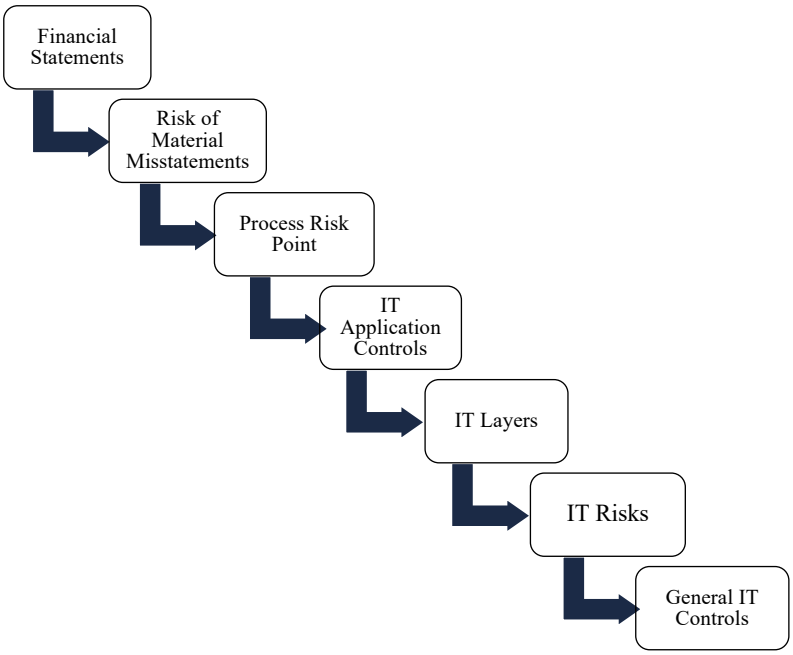



*Figure 7. General IT Controls flow chart*

General IT Controls can fall into e series of categories:

1. General IT Administration: these controls refer to the way IT systems are managed, by whom they are overseen, how risk assessments are conducted and what best practices IT projects should follow. They can also refer to security measure such as email filtering, antivirus software, firewalls and so on.

2. Access Controls: these controls are put into place to prevent unauthorized access and data manipulation and lower the chances of a cyberattack. Such controls include password management and encryption management.

3. System Life Cycle Controls: this control category focuses on monitoring an organization's system updates.

4. Physical and Environmental Security Controls: the aim of this category is to ensure physical security controls such as key badges and intrusion detection systems.

5. Data Protection and Recovery Controls: these controls are implemented to minimize data loss in case of accidents, natural disasters or cyberattacks. This is done through the introduction of backups, database segregation, and business continuity plans.

In setting up their controls, companies refer to the following security frameworks to guarantee the highest level of compliance:

COSO

The Committee of Sponsoring Organizations (COSO) framework integrates controls into business processes to make operations ethical and transparent. The framework achieves this through 5 requirements[9]:

1. Control environments to obtain industry-standard practices and reduce legal exposures for the organization.
2. Control activities to verify they are brought out in a way that risk is minimized, and business objectives are accomplished.
3. Presence of information and communications such as privacy regulations, which help stakeholders understand and comply with legal requirements.
4. Monitoring carried out by internal and/or external auditors to make sure that employees are following existing controls.
5. Risk assessment and management must identify and mitigate as many risks as possible.

COBIT

The Control Objectives for Information Technology framework is based on the theory that IT processes should satisfy specific business requirements to safeguard data. The COBIT framework applies the following five key principles[10]:

1. Meeting stakeholder needs
2. Covering the enterprise end to end
3. Applying a single integrated framework
4. Enabling a holistic approach
5. Separating governance from management

In the USA, this framework is used to assure compliance with the Sarbanes-Oxley Act (SOX), a U.S Congress law created to help protect investors from fraudulent financial reporting by corporations.

[9] Taken from COSO framework: [https://www.coso.org/SitePages/Home.aspx]
[10] Taken from COBIT framework: [https://www.isaca.org/resources/cobit]

ISO 27001

This last framework is strictly related to information security and change management, as it sets policies and procedures aimed at lowering risks related with implementing, monitoring, maintaining, and improving an information security management system. The ISO 27001 attains compliance thanks to the following six steps[11]:

1. Define a security policy
2. Define the scope of the information security management system
3. Conduct a risk assessment
4. Manage identified risks
5. Select control objectives and controls to be implemented
6. Prepare a statement of applicability

### 3.2.3. Control Testing

**Techniques**

Testing a control is an audit activity which consists in examining the internal controls that entities carry out after they have performed them to assess whether the control is effective or ineffective. This allows the audit team to understand whether specific controls are reliable or not for their audit purpose.

Testing controls is very important for financial reporting purposes, given that if a control is strong and implemented effectively by management, then the risks of material misstatements are likely to be lower and cause less damage.

There are four fundamental testing techniques to perform during an IT audit:

1. Inquiry: the scope of an inquiry is to seek information from people who have the proper knowledge of the subject matter. They can be both financial or non-financial individuals and they can be within the company or outside. An inquiry is usually carried out in an informal oral form, but it can also be formally written. The main aim is that of asking the person responsible for the performance of a control how they carry it out, what they look for while performing it and what approach they follow in case of exceptions.
2. Observation: the observation phase consists of observing a process or a procedure up close while it's being performed to fully understand the mechanism behind it.

[11] Taken from ISO 27001 framework: [https://www.iso.org/isoiec-27001-information-security.html]

3. Inspection: during the inspection phase a thorough examination of records and documents is carried out. An inspection can involve checking the evidence that the audit team has asked its clients to check that a control is effective.
4. Reperformance: in this final phase it's the audit team that performs the control according to what has been observed previously. This testing technique is used only when the team wants to test the effectiveness of a control.

The testing techniques listed above are necessary but not sufficient alone. It's fundamental to carefully carry out and inquiry, but an audit team must perform design and implementation procedures at the same time. Determining the design of a control means understanding how an entity expects such control to address the considered risk, whereas determining the implementation of the control means checking whether the control is in fact implemented accordingly to the way it was designed.

To such purpose, it's possible to reach some conclusions regarding the design and the implementation of a control. If a control implemented can address the specific risk and the test procedures are correct, then the control can be considered designed and implemented effectively. On the contrary, is this is not the case, we can conclude that there is a deficiency and therefore it's not possible to rely on the control.

**Control risks**

Another category of risks exists, and these risks are those specifically related to controls. This type of risk can be defined as the probability that financial statements are materially misstated because of failures in the controls of a business.

Each risk is given a level of significance which can be lower or higher according to how much impact it has on the considered control.

When assessing a control risk, there are a few factors which must be taken into consideration:

- The nature of the control
- The type of control
- The frequency of the control, which can be annual, quarterly, monthly, weekly, daily, or recurring
- The competence of the personnel performing the control or analyzing its performance
- Whether there have been changes in the control compared to previous periods
- Whether there have been deficiencies identified in previous periods

**Control sampling**

Because of time and budgets constraints, it's very unlikely for an IT audit team to analyze every transaction, therefore auditors select a representative sample to make assertions about the entire population.

There are specific factors which must be considered while choosing the sample size for a control. First, it's important to define the number of instances, meaning the number of times a control is performed throughout a specific period. Based on the number of instances, the next step is to define the frequency of a control which, as mentioned above, can me annual, quarterly, monthly, weekly, daily, or recurring. By considering both the control frequency and the control risk, it's possible to define the sample size through which the specific control will be tested.

**Testing Operative Effectiveness**

Operating effectiveness testing is performed to understand whether the control at hand operated consistently throughout the considered period. This includes checking how the control was applied, by whom it was applied and whether it operated effectively according to its design and implementation.

The difference between testing the design of a control and testing the operating effectiveness is that in the first case, we consider a test which refers to "a point in time", whereas for the second case we consider an entire period and therefore need samples to understand how the control has evolved in time and how consistent it remained.

Testing Operative Effectiveness requires specific procedures which must be documented. To do so, the audit team must:

- Assess the control risks and link them to the specific test procedures
- Describe the nature, the timing, and the extend of the test
- Obtain the correct evidence
- Document the results obtained from the operative effectiveness test

### 3.2.4. Deficiencies

A control deficiency can occur when an entity's internal controls are designed, implemented, or operated in a way that they don't allow management to prevent, detect or correct misstatements in a timely manner.

According to the ISA standards, it's possible to follow a three-step process to identify and evaluate deficiencies:

1. Determine whether a deficiency exists and describe it: if a deficiency exists it means that a control is missing, it has been designed wrongly or it's not working correctly. A general rule is that a misstatement would not exist without the presence of a deficiency, whereas a deficiency can exist even if a misstatement isn't identified.
2. Evaluate the severity of the deficiency individually: the severity of a specific deficiency is given by the sum of the likelihood that a potential misstatement can occur and the magnitude that it can have.
3. Evaluate the severity of the General IT Control deficiencies: the severity of the general IT control is determined by the sum of the severity of the aggregate deficiencies in a control and the all the additional factors that help evaluate the deficiency's impact.

## 3.3. Process Implementation

We can now focus on elaborating how the framework introduced in the as-is process is carried out in the Accounting Firm case study. The following analysis is based on contents taken from projects with customers who relied on the firm for their IT Audit.

### 3.3.1. Client Inquiry

The purpose of the first inquiry is to understand the entity, its IT environment and how the entity has responded to the related risks. If the client was already present during the previous fiscal year and had already concluded an IT audit with the Accounting Firm., the inquiry can take as a starting point the information provided at an earlier date. In this case, the scope of the meeting with the client is that of understanding whether the entity's environment has in any way changed, if their organizational structure has been modified, if new applications or information systems have been introduced and so on.

On the other hand, if a client is new, the first thing to do is to ask the client for a company overview, including its organizational structure and a description of its IT departments. After this brief introduction, the inquiry should focus on receiving information regarding the following points:

- **The entity's IT infrastructure**: an IT infrastructure is the combinations of all the components used for the management and operation of IT services. In this phase, it's useful for the company to give out information on their software and hardware components, on the number and the location of their servers, how they are managed and how they relate to one another. For the IT audit activity purpose, it's useful to receive documentation such as an infrastructure diagram, shown in the image below.

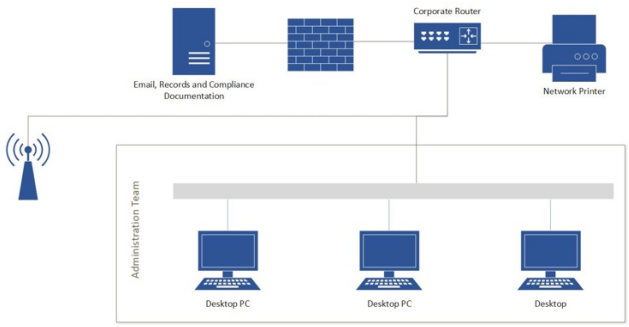



*Figure 8. Example of an Infrastructure diagram*

- **The entity's IT applications**: an IT application is a computer program that the entity uses to carry out a certain task. An entity usually uses different applications for different operations; therefore, it can be useful to receive an IT application diagram which highlights the interfaces between the different applications.
- **The entity's main IT outsourcers**: an entity may sometimes make use of outsourcers for the supply and the management of IT application or any other infrastructure component.
- **The entity's IT projects:** during the inquiry it's important to receive information regarding any projects linked to IT that the entity might have programmed for the fiscal year of interest.
- **The company's adjustments to Covid**: the Covid-19 pandemic has brought inevitable changes to the way work is organized and to the use of information systems within an entity's workplace. This has led to a "new normal" which cannot be ignored while analyzing an entity's use of IT. During the inquiry phase, the IT audit team can ask the client how their organization has adapted to the new normal from an information technology point of view.
- **The entity's Cybersecurity regulations and processes**: nowadays entities are promoting more and more awareness regarding the potential damages of cyberattacks, therefore during this phase of the inquiry it's important to understand what has been done throughout the fiscal year to reduce the risk of such attacks. Clients may provide results of email phishing attack simulations to see how the personnel reacts on such occasion, they may provide results of vulnerability assessments carried out and their internal policies.
- **The entity's General It Controls**: in this phase, the entity exposes the details on the general IT controls regarding the following categories:

    - Information security policy: security policies are posted on the company's intranet to be accessible to every employee from the moment in which they are hired. The IT audit may ask for such documentation and for the evidence that the policies have in fact been shared with the entire organization.

    - Physical access: in this category there's the explanation of the physical location of servers and any physical component and of which users have access to such locations.

- Backup and job scheduling procedure: for this category the entity must explain its procedures for automatic backups of its data and for how jobs are scheduled.

- Business continuity and disaster recovery procedures: such procedures are important for the understanding of how the entity deals with unexpected interruptions of operations.

- Incident management: incidents at an IT level are generally managed with ticketing systems. It's important for the audit team to understand how incidents are notified, managed, and solved.

### 3.3.2. PBC List and documentation check

The acronym PBC stands for "Provided by Client" and it consists of a list of requests sent by the audit team to the client after the inquiry has come to an end. The documents that the audit team requests and that are sent back after a certain amount of time act as evidence of the fact that the inquired company has in fact carried out specific controls.

The PBC List is structured in a way that for each category of general IT control, distinct requests are listed. Once the list has been sent and the client has provided the requests, the audit team can start reviewing the documentation received. Throughout this phase, it's important to understand whether the information received is compliant with the request, and to check that it's reliable.

The term information includes all the documents or relevant data which the client sends their auditors and which the audit team relies on to carry out their activities. It's important to understand the following things when considering information:

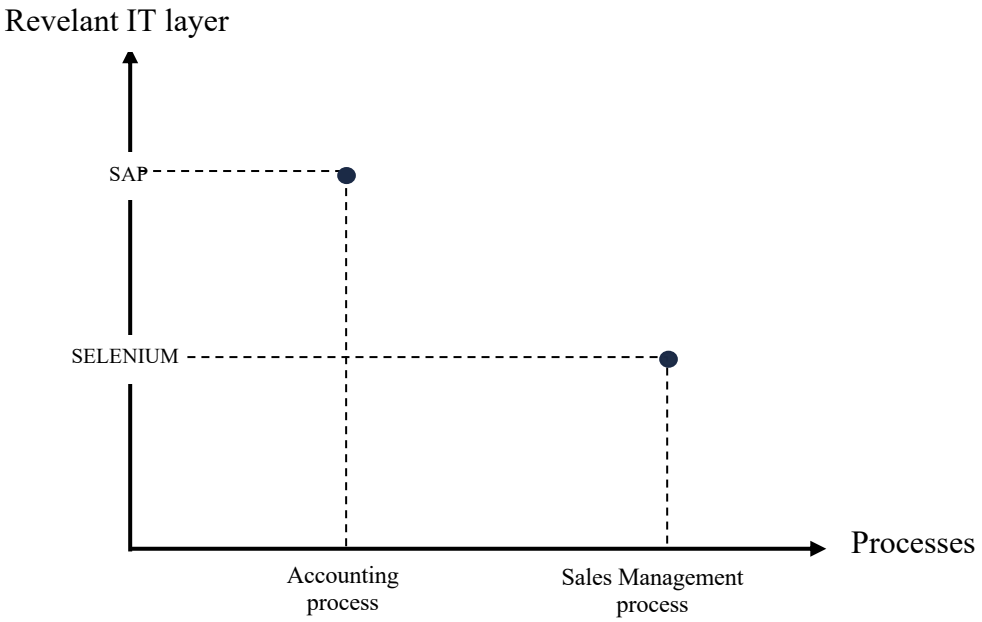
- Out of all the documentation received, it's critical to identify the relevant data elements (RDE), meaning those pieces of information which have something to say to the audit procedures, which are relevant to the controls we are testing.
- It's important to verify that a piece of information contains all the data it should and only the data it should.
- It's fundamental to understand whether the information received is in fact reliable. A common example of this is when the audit team asks the client to send a screenshot of anything regarding their internal server. In a screenshot, one of the first things that must be checked to verify its reliability is the date at which the screenshot was taken, to make

sure that the information sent is up to date and that it can in fact be used to test the control of interest.

Alongside the PBC list, there is another document which must be sent and filled out by the client, the Information System Diagram (ISD). Especially if the audit team is asking requirements regarding the functionalities of a specific application, the Information System Diagram aims at highlighting the IT layer at which it operates and the relevant descriptive information.

The Information System Diagram is a very useful tool because it allows us to visually see which technological layer has an impact on a process. An ISD can be represented on a double axis graph. In particular, on the x axis we can map the relevant processes and on the y axis the relevant IT layers and each intersection represent the layer of IT which has an impact on that specific process.

Example: assume that we must map two processes, an accounting process, and a sales management process. Assume that SAP (ERP system) has an impact on the accounting process and that Selenium (open-source tool for browser automation) has an impact on the sales management process. The ISD can appear like the graph below:




### 3.3.3. Example of control testing

We will now analyze an example of control testing; we will take as a study case the testing of a General IT Control regarding access to programs and data.

Let's consider the case in which identification and authentication mechanisms are not implemented correctly, meaning that the use of passwords is either non-existent or wrongly defined. The IT risk that can arise from such situation is that an unauthorized access to a system is not restricted, giving anyone a free access to confidential information.

To further understand the testing activity for such control, an example concerning the imaginary Company B is illustrated. Company B is a private company which provides retail services to customers. For its purposes, it uses a specific financial reporting system, MacP and the Active Directory (AD) system integrated with the Windows operating system.

After having performed a business walkthrough and having received all the documentation from the PBC list, the audit team must test the following application-level password control: password settings are in line with the defined password policy and appropriately enforced on in-scope systems.

Extra information is given to the audit team:

- Access is authenticated through unique credentials (user IDs and passwords)
- Users are authenticated via a single sign on (SSO) mechanism, meaning that with a single set of credentials a user is allowed to log into multiple independent software systems
- The password parameters are communicated via group policy which is aligned to the password policy
- The password requirements, which are usually very similar from case to case, are the following:
    - Password length: minimum 8 characters
    - Password complexity: Alphanumeric
    - Account lockout: a user is locked out after 10 attempts gone wrong
    - Password expiry: every 90 days

For the purpose of the control test, the audit team prepares a PBC list for the clients with the expected documentation. The client then reads the list, gathers the related content, and sends the evidence back to the audit team. In this example, the evidence provided consists of:

1. The password requirements extracted for the firm's password policy
2. A print screen of the extraction that shows the Windows password settings

Once such evidence has been received, to implement the test the audit team must document the following elements:

1. The nature of the control

2. The control attributes
3. The evaluation of the design of the control and its implementation
4. The evaluation of the test of effectiveness
5. The sample size to consider for the test and the frequency of the test at hand.

As far as the nature of the control is concerned, it's safe to say that it's automated, given by the fact that once a user inputs a password, it's the system which automatically checks that all the parameters are respected and compliant with the password policy.

A control's attributes are those elements that must be taken into consideration to analyze a control and test that it's being carried out in the proper manner. In this specific case, the control attributes to be considered are the password requirements themselves.

The design and the implementation of the control can be evaluated through two of the four main techniques: inquiry and inspection. The inquiry phase consists in asking the company during a settled meeting to present and explain their procedures, whereas the inspection phase consists of checking the evidence received. In this case, during the inspection, the audit team must make sure that the password setting shown on the print screen of the firm's active directory system match with the firm's written policy. In extreme cases, the audit team could also pass on to the observation phase, during which an employee of the client's firm could be asked to insert a set of credentials to observe how the active directory system reacts to wrongly inputted passwords.

Once it has been established that the general IT control is capable of effectively addressing the IT risk related to such control and that the entity is using such control as designed, the test of effectiveness can be performed.

In this specific case, if the risk associated with the control has a low impact (base level), the audit team can consider a single sample and test the effectiveness of the control only once to make sure everything is coherent.

### 3.3.4. Main Risks identified for financial reporting

A further step in this analysis consists of taking into consideration a specific process which is common to a set of different audit clients and identify which risks occur most frequently.

To do so, two approaches are used. First, the single case of an industrial client is assessed. For simplicity, such client will be referred to as Client A. For such client, three main processes have been considered and for each process the main risks that could arise have been

highlighted. Furthermore, for each possible process risk the inherent control activity has been indicated, together with its nature and type. The three processes considered are:

- Financial Reporting
- Inventory Process
- Sales Process

The table below shows the related analysis.

| Business Process | Possible Process Risk | Control Activity | Control nature | Control type | How the control addresses this risk |
|---|---|---|---|---|---|
| Financial Reporting | Manual accounting entries in the management system are not identified, reviewed, and approved | Review of Manually written journal entries | Manual | Detective | The Control Operator conducts an analysis of Journal Entries after determining some High-Risk Criteria to identify any anomalies in the accounting entries. |
| | Credit and Debit invoices don't match in a journal entry | Check that credit and debit match | Automated | Preventive | The system imposes an automatic block that prevents the closing of the accounting entry if credit and debit don't match |
| | Entries are posted in a closed accounting period | Prevent user from posting an entry on an accounting period that has already closed | Automated | Preventive | The system does not allow an accounting entry to be recorded in the accounting period already closed. |
| | The entries posted on the management system aren't transferred to another system correctly | Verification of correct data transfer | Manual | Detective | The Control Operator verifies that data has been transferred accurately |

| | | | | | |
|---|---|---|---|---|---|
| Inventory Management | Inventory cost method (FIFO, LIFO, average cost, retail inventory method) is not appropriately determined or is not consistently applied | Cost Fluctuation Analysis | Manual | Detective | Through the analysis of the main deviations of unit cost (in terms of absolute value), the control allows the identification of material situations of errors resulting from anomalies in the basic information generated during the period. |
| | The valuation of inventories is not correct | Automatic calculation of inventory value | Automated | Detective | The system automatically performs the inventory value calculation, considering inputs and outputs and their values |
| | Difference between goods loaded into the system and goods ordered | Check between goods that have been received and goods ordered | Automated | Preventive | The system has an automatic block that does not allow certain thresholds of difference in the value of purchased goods between what was ordered and what was received to be exceeded. |
| | Inventory receipts and/or shipments are not recorded in the correct accounting period | Following shipment confirmation, the system automatically updates the inventory of goods, depending on the quantities shipped | Automated | Preventive | The automatism tested shows the automatic update of inventories at the time of shipment confirmation |

| | | | | | |
|---|---|---|---|---|---|
| Sales Management | Failure to approve the price list | Price list approval | Manual | Detective | Control owner approves price list |
| | Issuance of Invoice from ERP system is not related to an order | Check that the ERP system generates the invoice based on the sales order | Automated | Preventive | The accounting system requires for invoice issuance that the invoice be linked to previously entered order. This prevents an invoice not related to an order from being issued |

*Table 8. Risks identified for financial reporting*

From the Financial Reporting process, it's evident that the main risks regard the introduction of journal entries into the management system. This includes entry risks such as debit and credit that don't match or entries being posted in periods which are already closed.

From the Inventory Management process, the main risk which emerged involves the way inventory is valued. In fact, this risk can occur on different level, such as the cost method.

From the Sales process, the main risk is given by the fact that a price can be unapproved, or invoices cannot match the related order.

At a later stage, a sample of 11 clients taken from the audit period 2021-2022 has been chosen and examined at the same way.

| Client | Years | Process | Risk description (What Could Go Wrong) | Control Activity |
|---|---|---|---|---|
| Client 1 | 2021-2022 | Financial Reporting | Risk that incorrect accounting entries may be made correct or made by unauthorized persons | System access |
| Client 2 | 2021-2022 | Financial Reporting | Recording of incorrect writing | Verify inability to record a wrong entry |
| | | | Entry of entry in closed accounting year | Verify inability to record an invoice in an already closed accounting period. |
| Client 3 | 2021-2022 | Financial Reporting | Risk of recordings being made by unauthorized personnel | Access to SAP |

| | | | | |
|---|---|---|---|---|
| | | | Incorrect and/or incomplete manual entries | Unbalanced writing block |
| | | | Risk that entries for accounting periods already authorized and closed will be changed | Blocking closed periods |
| Client 4 | 2021-2022 | Financial Reporting | The journal entry is recorded incorrectly or is not properly authorized | Inability to make entries that are not balanced |
| Client 5 | 2021-2022 | Financial Reporting | Risk of entries being made by unauthorized users | System Access |
| Client 6 | 2021-2022 | Financial Reporting | The journal entry is recorded incorrectly or is not properly authorized | Verification of the existence of approval signatures on manual entries |
| Client 7 | 2021-2022 | Financial Reporting | Risk that it is possible to make entries in which credit and debit entries do not equalize | Blocking non-square accounting entries |
| | | | Risk that entries can be made on closed periods | Blocking accounting entries made in closed periods |
| Client 8 | 2021-2022 | Financial Reporting | Entry of manual entries that are erroneous or lack economic/financial justification or are not authorized. | System access authorization for journal entries registration. |
| Client 9 | 2021-2022 | Financial Reporting | Accounting for incorrect or unauthorized entries | System block to unbalanced accounting entries |
| Client 10 | 2021-2022 | Financial Reporting | An employee may have the ability to initiate, authorize and record a transaction or may have custody of assets within the process, such that they are able both to perpetrate and conceal an error or irregularity. | System access |
| | | | Risk that the administrative officer may impute incorrect entries in accounting records | Blocking incorrect inputs |

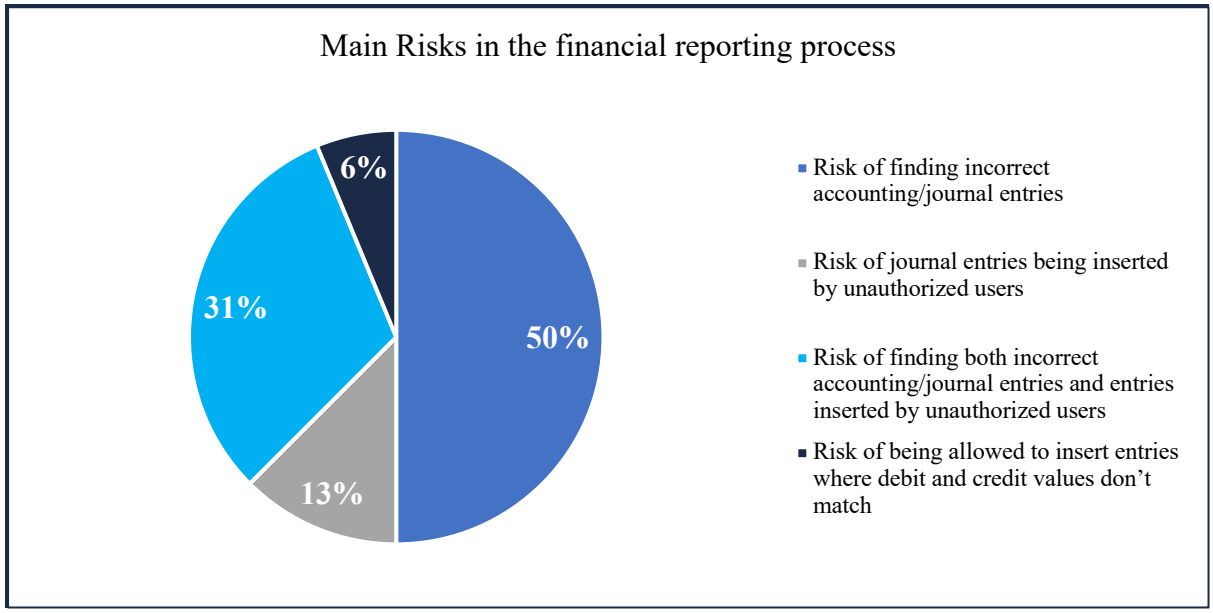
| | | | | |
|---|---|---|---|---|
| Client 11 | 2021-2022 | Financial Reporting | Risk of incorrect and unbalanced accounting entries being made in the accounts | Bank Reconciliations |

*Table 9. Risks identified for sample of clients*

The only process taken into consideration for these clients is the Financial Reporting process and 16 risks have been identified. We can summarize the main risks in the following descending order:

1. Risk of finding incorrect accounting/journal entries (8 risks out of 16).
2. Risk of journal entries being inserted by unauthorized users (2 risks out of 16).
3. Risk of finding both incorrect accounting/journal entries and entries inserted by unauthorized users (5 risks out of 16).
4. Risk of being allowed to insert entries where debit and credit values don't match (1 risk out of 16).

A pie chart representing such summary is illustrated below:




*Graph 2. Main Risks in the financial reporting process*

### 3.3.5. How companies work to mitigate risks

The final step concerns the assessment of what companies do from a risk management point of view. In particular, for the purpose of this analysis, the focus is on the management of IT personnel, meaning how much importance a firm gives to hiring employees qualified in IT.

A sample of 23 firms has been considered, including both industrial firms and financial services firms. Four ranges concerning the number of IT personnel in the firm have been established as can be seen in the chart below:

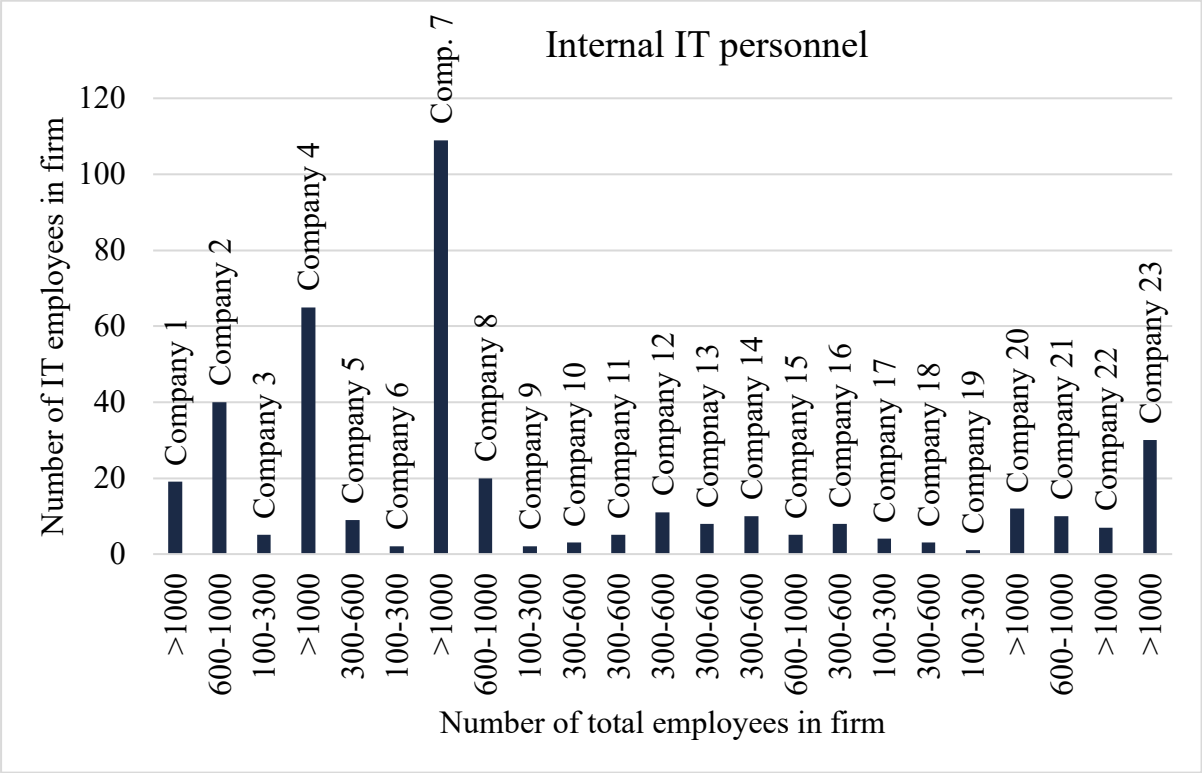
The number of firms belonging to such range has been pointed out, together with the sum of the number of IT employees throughout the number of firms and the average number of IT employees throughout the firms.

| Internal IT personnel range | N° of Firms | Internal IT personnel | Average IT personnel |
|---|---|---|---|
| 100-300 | 5 | 14 | 2,8 |
| 300-600 | 8 | 57 | 7,125 |
| 600-1000 | 4 | 75 | 18,75 |
| >1000 | 6 | 242 | 40,33 |

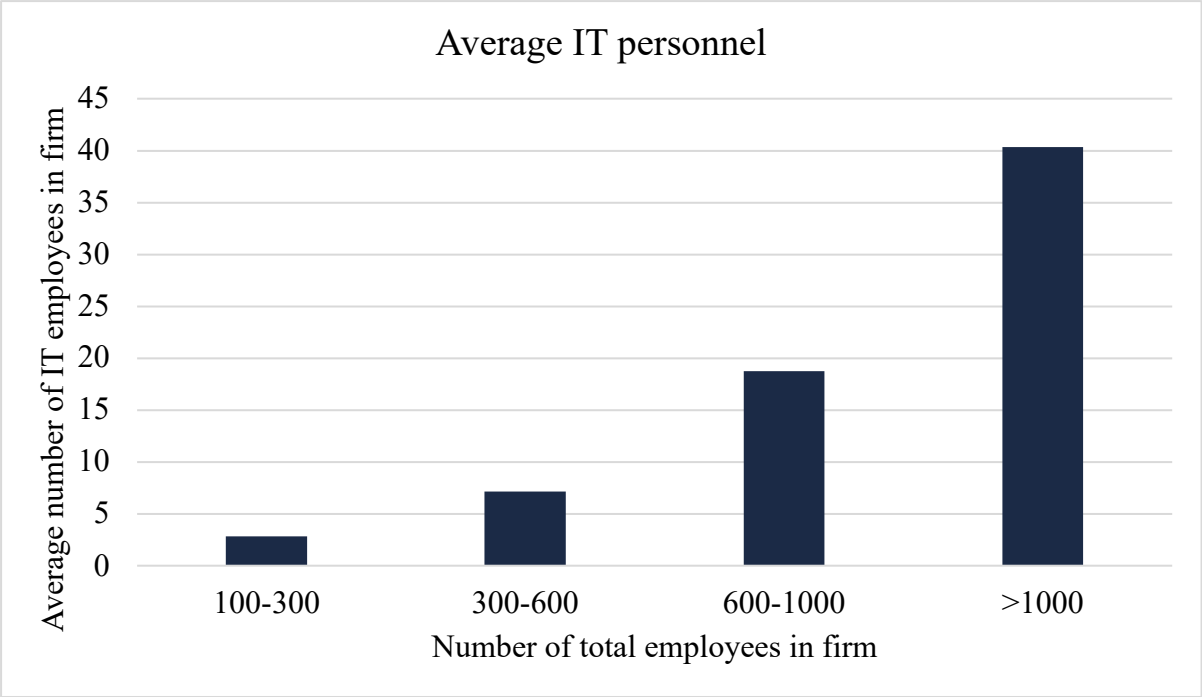
*Table 10. IT personnel ranges*

The following graphs show:

- The relation between the total number of employees and the number of IT employees in each firm
- The relation between the total number of employees and the average number of IT employees in the aggregate number of firms.




*Graph 3. Internal IT personnel*




*Graph 4. Average IT personnel*

## 3.4. TO-BE Process in the Accounting Firm

The present chapter dedicated to the analysis of an IT audit process for Information Risk Management has so far covered four of the five sections which make up the DMAIC framework. The deep dive into the "as-is" process and its implementation has given an overview of how the procedure defines (D), measures (M), analyzes (A), and controls (C) risk. It has in fact covered and explained the following points:

- How the entity plans the risk management audit procedures to be carried out
- What methods the entity implements to identify the major risks affecting their clients' business processes
- How such processes are analyzed to find the major risk points in which an actual risk of a specific nature could arise
- Which controls are put into action by the entity to verify whether their client firm has in fact mitigated the identified risks.

The last phase missing from this analysis is that of proposing methods and approaches which could in some way lead to a continuous improvement (I) of the considered process. This final phase can be applied from two points of views:

- The client's side: in this case, the aim is to propose ways for the client firm to better manage the risks that have been identified by the audit team to lower the likelihood of such risks impacting their operations and business goals.
- The entity's side (Firm): in this case, the aim is to propose improvements that the audit team could implement in their day-to-day activities to better identify risks arising from technology and offer service which is always in continuous evolvement.

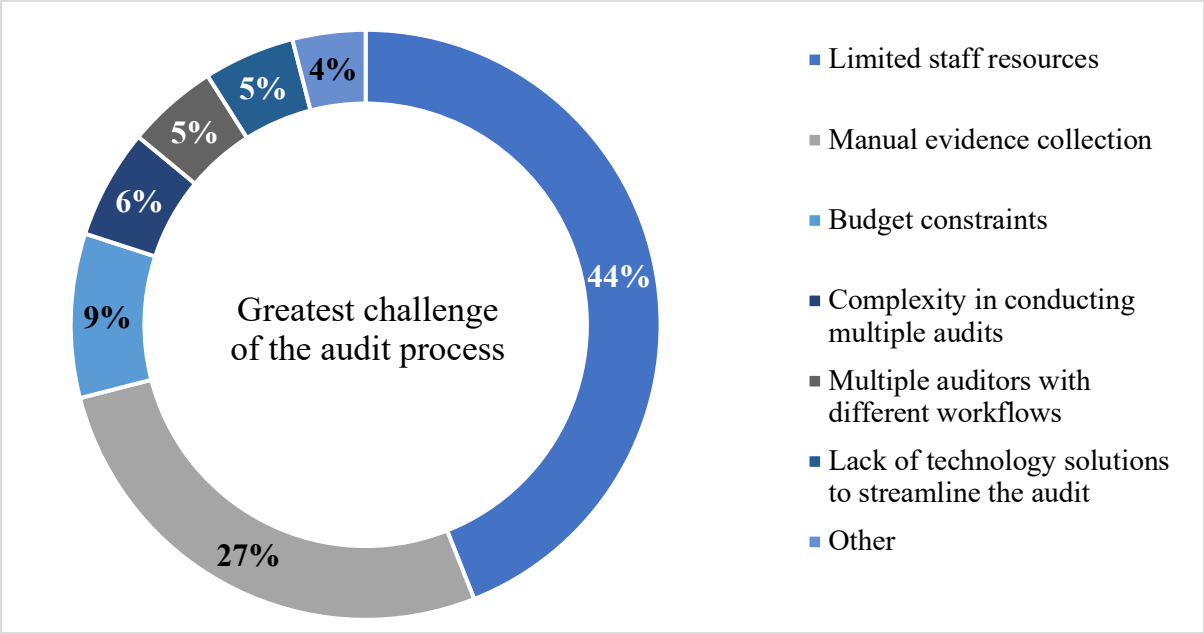
For the purpose of this study, the following sub-chapter will focus on the proposal of continuous improvement methods for the entity's audit management.

### 3.4.1. The challenges in Audit

According to the *2020 Compliance Benchmark Report*[12] prepared by *A-Lign*, a global cybersecurity and compliance solutions provider, there are a few aspects that challenge audit teams in many organizations. To prepare such report, a survey was made and sent out to a set of respondents which had already conducted audits throughout their professional activity. The

[12] Taken from the following A-Lign website: https://www.a-lign.com/articles/common-challenges-audit-process

respondents were asked about their concerns related to the audit process; the answers were then collected and analyzed to give the following output:




Graph 5. Survey responses for audit process challenges

As shown in the graph above, there are several different reasons for which respondents believe that their audit process could be improved in time, lack of resources being the first, strictly followed by the fact that evidence is collected manually as opposed to automatically. This problematic would however require a more thorough reflection, not in scope for this study.
Other challenges of the audit process are given by the fact that an audit is usually carried out in an internal team, and at the same time an auditor is required to work with the audited client/group. Having to respond to an external organization may be tricky because they must for example share documentation with the audit team, allocate time, provide access to their IT systems, and all of this can become a bottleneck to the process if not done in a timely manner or in a precise way. Clearly, it's harder to keep track of an external organization as opposed to an internal one.

Just like any business process, an entity's audit process can be subject to continuous improvement, also known as "*Kaizen*," in the Lean terminology. Such improvement can be reached by incremental changes made over time which can then slowly lead to major changes in the long run. The main reason for the implementation is to reduce waste of time, resources, and budget as much as possible and create a process capable of reaching the required outputs in the best way possible. In fact, with continuous improvement, the aim is to build organizations

capable of effectively balancing what is important with what is urgent. Other characteristics that can be reached with the implementation of continuous improvement are the following:

- A good and steady workflow in every audit group. This would include receiving ad giving fast feedback and support to and from anyone external or internal to the group.
- Minimal amount of waste due to rework of a job, meaning that unneeded work should be minimal.
- Smoother processes as time goes by and as audit projects change.
- Steady reactions to change or unexpected events arising throughout the project.

From here on out, a set of proposals for the continuous improvement of the entity's audit process introduced in the previous sub-chapters will be illustrated and commented.

### 3.4.2. Using Kanban to improve the audit process

As anticipated in chapter 2, the Kanban Method is a Lean methodology tool which can help an organization improve its workflow by generating a visual board containing the main tasks in a project and their status.

To create a Kanban board, the first thing to do is to clearly have in mind all the major milestones that must be reached for the completion of the project. Once such steps have been identified, the Kanban board can be created through the use of dedicated software, open-source websites or manually.

The board consists of a set of columns, each of which represents a completion status for the milestones. The single activities are all placed in the first column, to indicate that they must all be started, and then step by step the activities are all singularly allocated in the successive status phases as they reach completion.

The Kanban board methodology is useful as it helps the project team visually have an idea of how the project is proceeding. It's accessible to all team members, meaning that everyone is aware of the situation, and this improves time management and quality management as a deadline approaches.

The following images show an example of a Kanban board created with the open-source website "Milanote" for the purpose of such example. The Kanban board created below represents the possible project flow of a simplified IT Audit procedure.

For the sake of simplicity, the following example considers a project consisting of a single application used by the client company, meaning that a single PBC list can be prepared. Furthermore, for the sake of simplicity, the General IT Controls considered are only 5 (although such a low number is very uncommon and unlikely in reality), and the IT Application Controls are 2 in total.

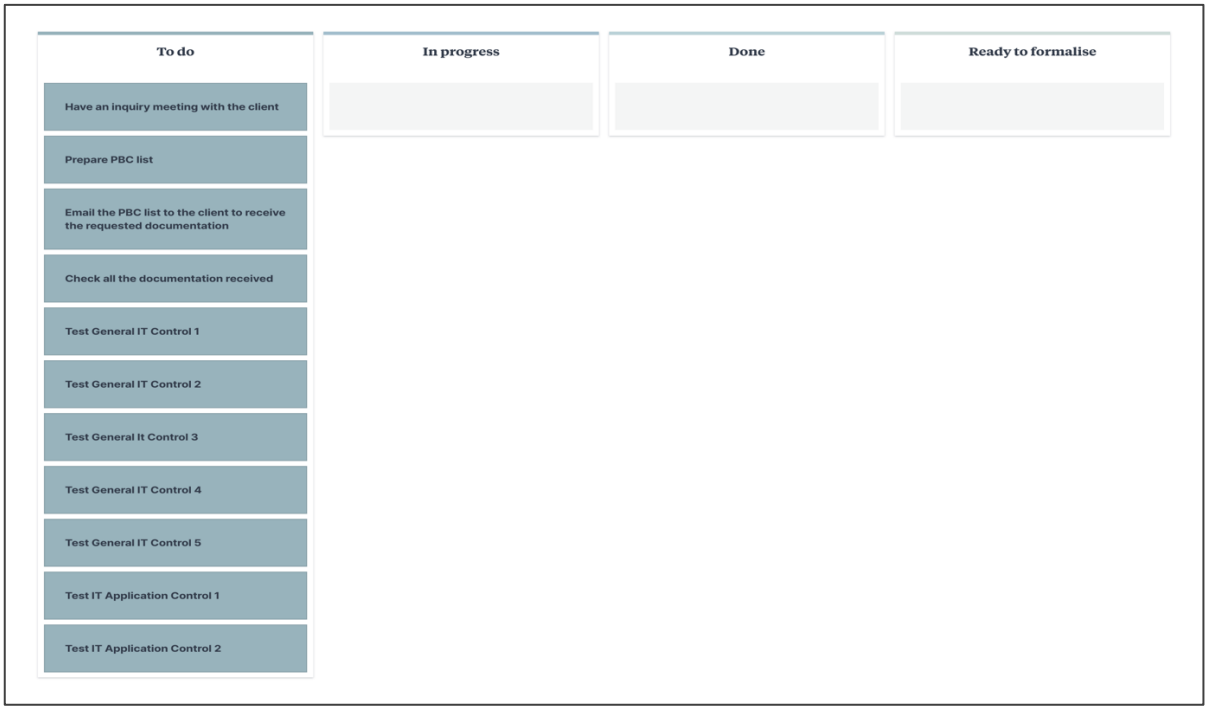



Figure 9. Kanban phase 1

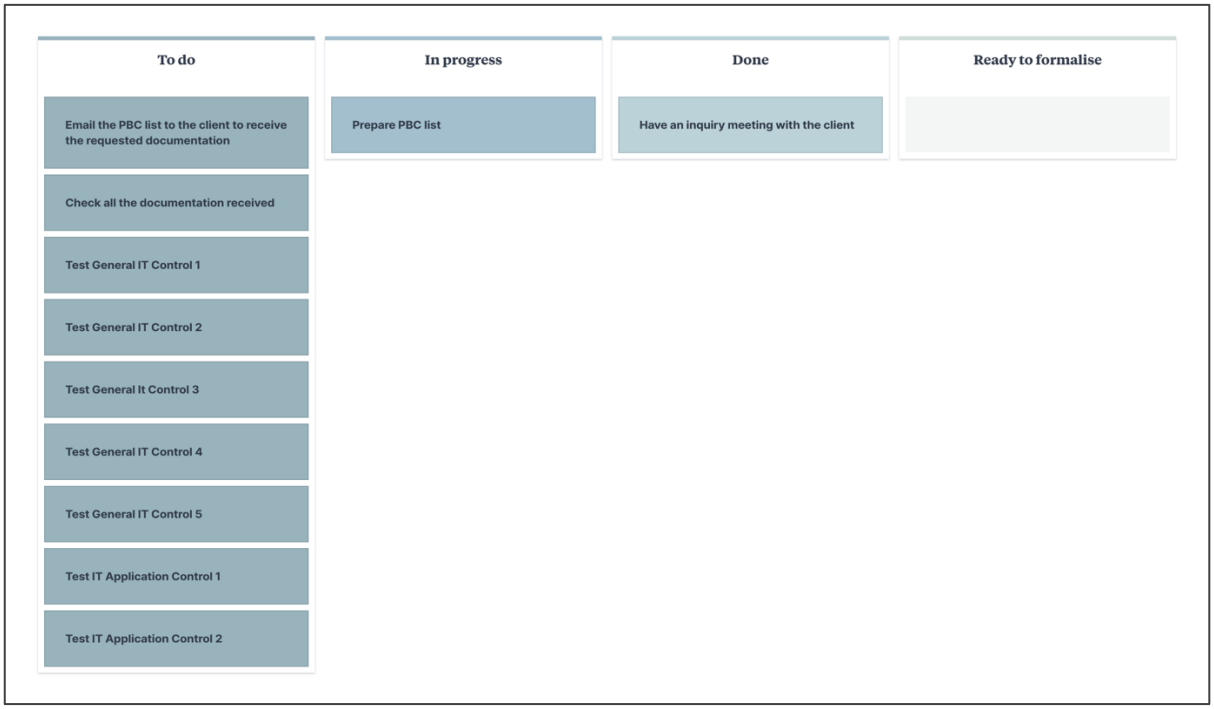



Figure 10. Kanban phase 2

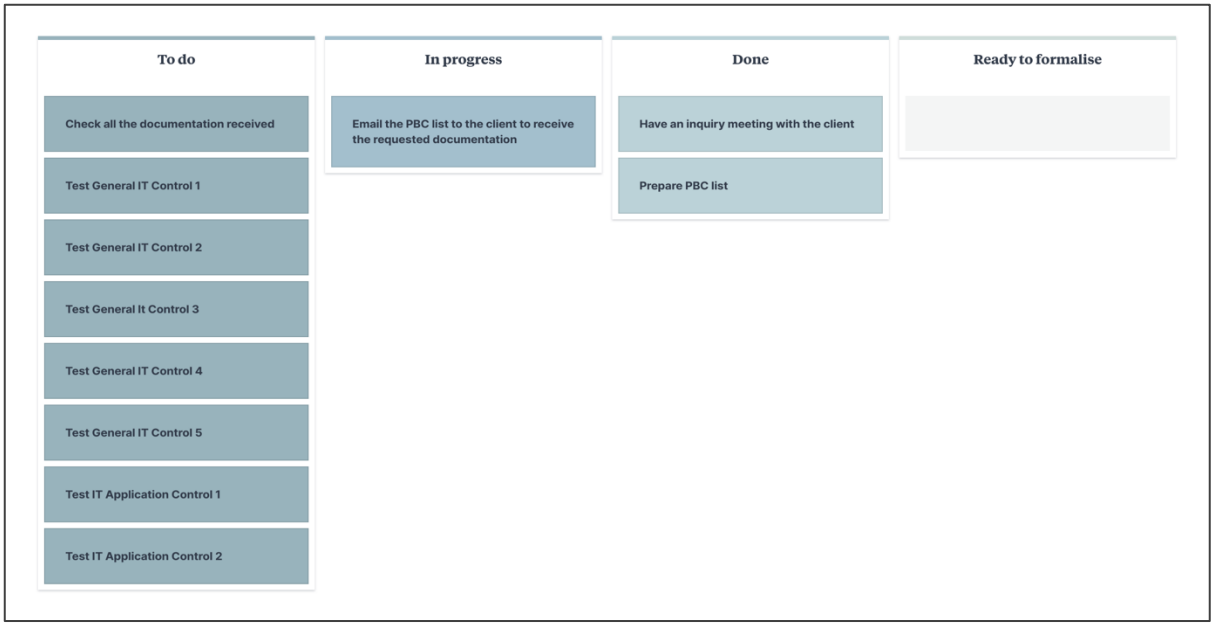



Figure 11. Kanban phase 3

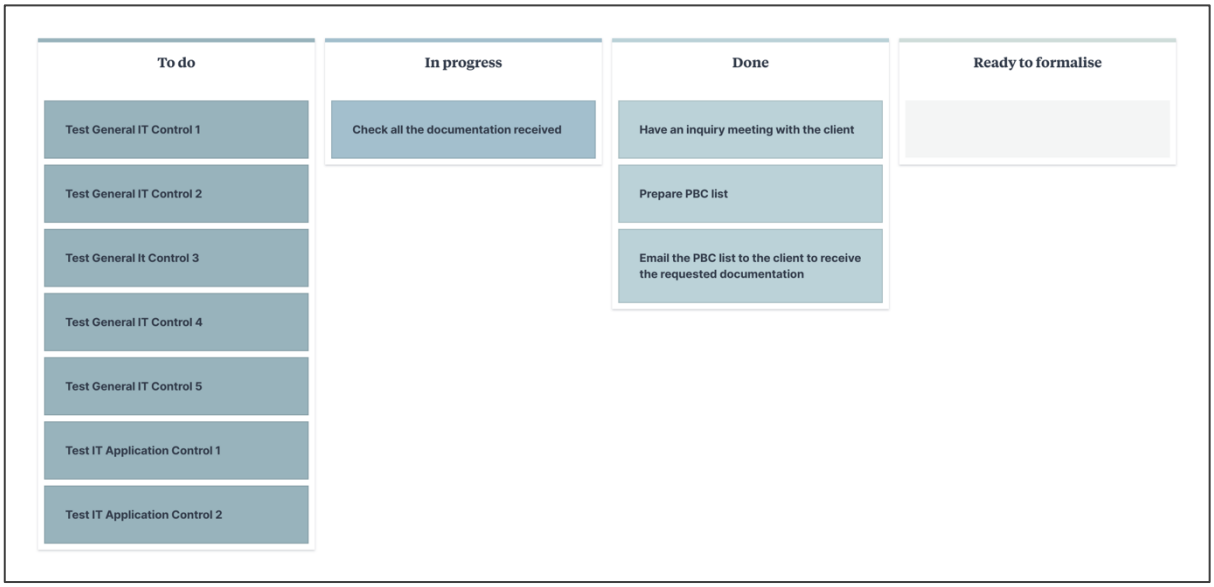



Figure 12. Kanban phase 4

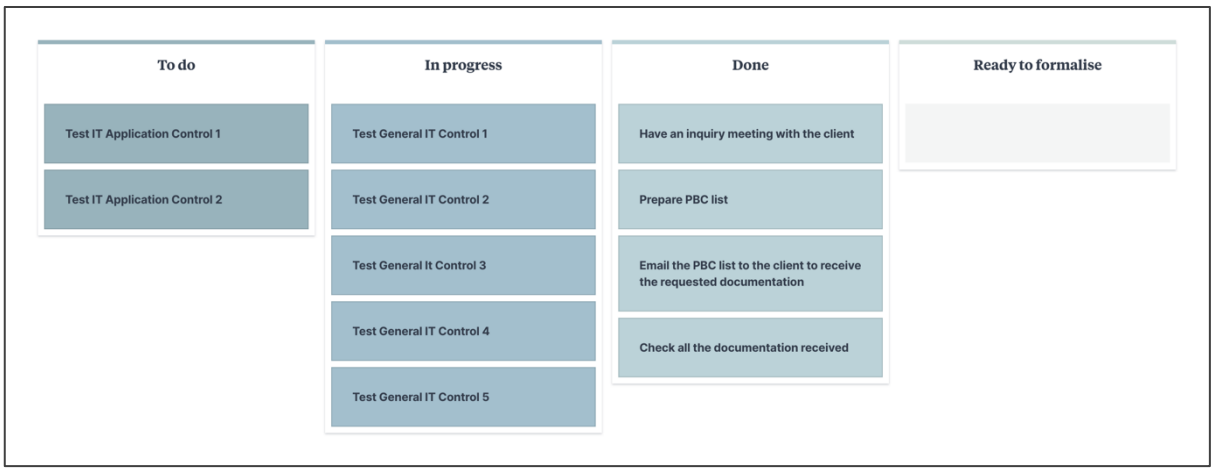



Figure 13. Kanban phase 5

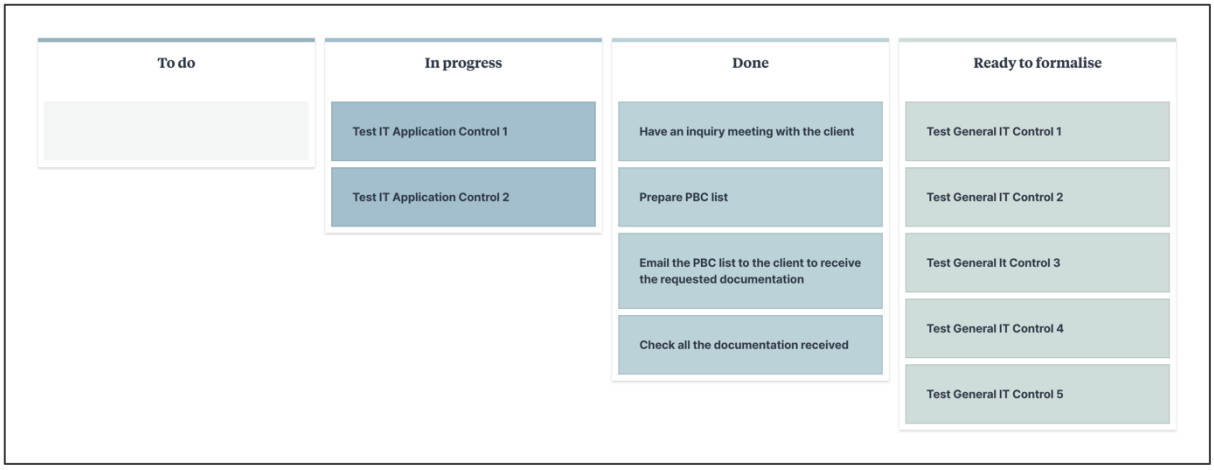



Figure 14. Kanban phase 6

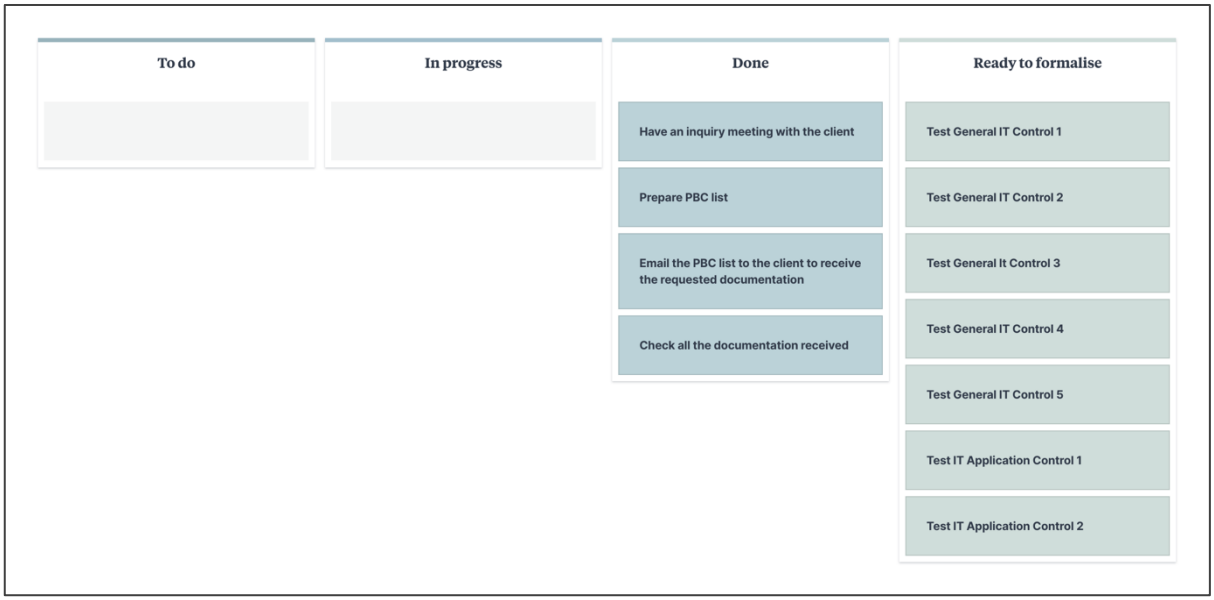



Figure 15. Kanban phase 7

### 3.4.3. Using FMECA to improve the audit process

The Failure Mode, Effects & Criticality Analysis (FMECA) is a method which involves quantitative failure analysis. Such method is proposed for the improvement of risk management in the audit process, in order to better identify and prevent risks and therefore failure. This method consists of creating links between potential failures (the so-called Failure Modes), the impact that a possible failure can have on the scope of the project (the Effects), and the causes of such potential failure (Causes).

The implementation of FMECA can lead to a series of benefits:

- Design and Development benefits: higher quality, more safety, more reliability, less time spent in re-designing project phases.

- Operational benefits: more effective controls and tests, more effective maintenance, less waste.
- Cost benefits: fewer costs given by the fact that failure modes are identified at an earlier stage and are therefore less costly to fix.

To put the FMECA process into practice for the improvement of risk management, 7 steps must be implemented:

1. **Perform the FMEA**: FMEAC is the starting point for the FMECA analysis, as it includes the initial phases excluding the criticality analysis. It provides inputs of failure modes and causes of failure mechanisms.

2. **Determine Severity Level**: in this phase, once the failure modes and effects have been identified, a severity level in assigned to each of them. Severity Levels can differ according to the project or to the considered industry. There are however 4 generic severity levels which are classified as follows:

- Catastrophic: a failure mode or effect falling in this category could lead to a damage having an impact of about $1M USDs.
- Major/High Impact: a failure mode or effect falling in this category could lead to a damage having an impact of about $200K < x < $1M USDs.
- Minor impact: a failure mode or effect falling in this category could lead to a damage having an impact of about $10K < x < $200K USDs.
- Low impact: a failure mode or effect falling in this category could lead to a. damage having an impact of about $2K < x < $10K USDs.

3**. Calculate Failure Effect Probability**: the probability values used in the FMECA methodology are the following:

- Actual loss: 1.00
- Probable loss: 0.10 < x < 1.00
- Possible loss: 0 < x < 0.10
- No effect: 0

4. **Assign a quantitative probability of occurrence**: in this phase the probability values must be assigned.

5. **Calculate the criticality**: in FMECA criticality takes two forms:

- the Modal Criticality, which indicates each single cause of each single failure
- the criticality of an item, which indicates all the failure modes summarized together

6. **Design Risk Mitigation**: in this phase, the actions that must be taken to mitigate risks must be defined.

7. **Perform Maintainability Analysis**: in this final phase of FMECA, the analysis consists of considering the highest risk item and determining which components will fail the fastest. This phase can affect the next steps to be taken in a project.

The FMECA analysis can be visually represented through the use of the FMECA worksheet.

# Conclusions

At the end of the present thesis work, it is possible to state that Project Risk Management is fundamental for the improvement of an entity's processes and scopes.

Information is at the heart of automated processes in today's industries and as innovation makes its way, the role of the IT Auditor will face more and more responsibilities for the risks that IT carries within everyday processes, leading to the greater need for Cybersecurity and IT awareness.

The improvement of the Information Risk Management Auditing procedures through Lean Methodology frameworks can lead to a more precise Project Risk Management Analysis and therefore reduce the IT risks and the major impacts that such risks can have on today's companies throughout every industry.

It is a personal belief that the continuous improvement of such processes must remain a subject to be deepened and enhanced, and for the mitigation of IT risks to become ever more a priority for all entities.

# Sitography


1. https://corporatefinanceinstitute.com/resources/careers/map/accounting-careers/risk-of-material-misstatement/
2. https://www.dfa.cornell.edu/controller/internalcontrols/designing#:~:text=Manual%20vs.%20Automated%20Controls%201%20Manual%20controls%20rely,functions%20can%20ensure%20data%20accuracy%20and%20completeness.%20
3. https://www.swordshieldconsulting.com/itac
4. https://jumpcloud.com/blog/what-are-it-general-controls-itgc
5. https://www.i-sight.com/resources/coso-framework-what-it-is-and-how-to-use-it/
6. https://jumpcloud.com/blog/what-are-it-general-controls-itgc
7. https://www.wikiaccounting.com/audit-internal-control-testing/
8. https://linfordco.com/blog/design-vs-operating-effectiveness/
9. https://www.ibm.com/topics/infrastructure
10. https://goleansixsigma.com/dmaic-five-basic-phases-of-lean-six-sigma/
11. https://www.forbes.com/advisor/business/what-is-process-improvement/
12. https://www.pmi.org/about/learn-about-pmi/what-is-project-management
13. https://www.teamwork.com/project-management-guide/project-stakeholders/
14. https://www.pmi.org/learning/library/stakeholder-analysis-pivotal-practice-projects-8905
15. https://www.pmi.org/learning/library/risk-analysis-project-management-7070
16. https://www.isixsigma.com/new-to-six-sigma/dmaic/dmaic-phases-mesh-project-risk management/
17. https://kanbanize.com/lean-management/improvement/what-is-continuous-improvement

18. https://asana.com/resources/continuous-improvement
19. https://blog.planview.com/using-kanban-to-improve-audit-management/
20. https://www.a-lign.com/articles/common-challenges-audit-process
21. https://milanote.com
22. https://quality-one.com/fmeca/

# Bibliography

1. Shankar, Rama – Process Improvement Using Six Sigma – A DMAIC Guide – American Society for Quality (ASQ) (2009)
2. Charles T. Carroll – Six Sigma for Powerful Improvement – A Green Belt DMAIC Training System with Software Tools and a 25-Lesson-Course-Productivity Press (2013)
3. Lance B. Coleman, Sr. Advanced Quality Auditing – An Auditor's Review of Risk Management, Lean Improvement, and Data Analysis.