Universidad del País Vasco Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

MÁSTER UNIVERSITARIO EN

PROJECT MANAGEMENT

TRABAJO FIN DE MÁSTER

PROJECT MANAGEMENT APPROACH TO THE IMPLEMENTATION OF AN ISMS AND ITS CERTIFICATION AGAINST THE ISO/IEC 27001

Estudiante *de Basterretxea Ibilcieta, Guillermo*

Director/Directora *Zuazo Urionabarrenetxea, Iñaki*

Departamento *Departamento de Expresión Gráfica y Proyectos de Ingeniería*

Curso académico *2020 - 2021*

Bilbao, 09, 09, 2021

Index

Table index

Figure Index

Abbreviation Index

ANSI	American National Standards Institute
BS	British Standard
BSI	British Standards Institution
CASCO	ISO's Committee on Conformity Assessment
CIA	Confidentiality, Integrity, Availability
CRM	Customer Relationship Management
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity
ERP	Enterprise Resource Planning
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technologies
LOPD-GDD	Ley Orgánica de Derechos Personales y Garantía de los Derechos Digitales
MSS	Management System Standards
PM	Project Management
PMBOK	Project Management Book of Knowledge
PMI	Project Management Institute
PMM	Project Management Methodologies
RACI	Responsible, Accountable, Consulted, Informed matrix
SME	Small and Medium-Size Enterprises

1. INTRODUCTION:

Project management literature reflects the growth that the discipline is undergoing in organizations worldwide (Simard et al., 2018; Papke-Shields, et al., 2017; Bredillet et al., 2010). In particular, the influence of the Project Management Book of Knowledge Guide (PMBOK Guide), published by the Project Management Institute (PMI) is widely acknowledged (Shi, 2011; Papke-Shields, et al., 2017; Fernandes et al., 2013). However, despite the impression of a generally recognized and accepted trend in management, in reality, the idea that PM practices vary quite significantly from one context to another is widely accepted (Besner and Hobbs, 2013).

Researchers have dedicated ample attention to study the implementation of PM methodologies in organizations, and they have done so from different perspectives. On the one hand, there are a number of research papers that analyze the advantages and disadvantages of adapted procedures as opposed to structured frameworks (Andersen and Vaagaasar, 2009; Besner and Hobbs, 2013; Fernandes et al., 2013 and 2015).

On the other hand, the efficacy of PM systems has been questioned and the relationship between PM performance, investment in PM and project success has been revised (Thomas and Mullally, 2007; Pace, 2019). However, the conclusion of this revision suggests that there is a direct relationship between the adoption of PM practices and project success (Mir and Pinnington, 2014; Shi, 2011). Achieving this efficacy is a "process" that requires the implication of the organization (Siriram, 2017). Andersen and Jessen (2003) see this process as the steps of a ladder that ultimately conducts the organization towards project maturity. According to Shi (2011) the combination of two dimensions are necessary to achieve this kind of success, a soft system, which consists of the general environment of the organization and the PM culture, and a hard system, which consists of the actual PM processes, PM tools and technics and PM training.

Different circumstances can influence the materialization of these methodologies. Change resistance can be a major issue that undermines the adoption of new strategies, national cultural factors can have a significant impact in the way PM principles are actually implemented (Bredillet et al., 2010) and the specificity of context, industry and the organization's culture can also shape the approach to PM in each particular case (Fernandes et al., 2015).

Different case studies have highlighted the need to adapt the methodology to the particular circumstances of each organization (Besner and Hobbs, 2013) and the

PMBOK Guide itself recognizes the need to determine what is appropriate for each given project (PMI 2017, 28). There are many different ways in which organizations can adopt PM strategies and the implementation of PM methodologies varies considerably from very adapted and informal approaches to more formally defined practices (Fernandes et al. 2015; Shi, 2011).

This paper analyzes the efficacy of an informal project management approach to the development, implementation and certification against the ISO/IEC 27001 standard, of an Information Security Management System (ISMS), by a medium-sized production company.

The aim of the study is to verify to what extent a PM approach to the project helped achieve higher levels of efficacy, even if the circumstances in the organization hampered a more formal implementation of what the PMBOK Guide describes as best practices.

Rich with the experience of implementing and certifying the ISO/9001, quality management standard; the ISO/14001, environmental management standard; and the ISO/45001, occupational health & safety standard; the company decided to embark in this project to minimize the risks related to information security.

The top management of the company explained that they took this decision for three reasons:

- Information security needed to be properly addressed in the organization and, at the moment in which the decision was taken, it was not.
- The company needed to reassure all the stakeholders in the supply chain, from the first provider to the last customer, that the information they shared with the company was secure.
- The certification is necessary to be able to apply to tenders that increasingly demand evidence of compliance with information security regulations.

The company is undergoing changes in its procedures to try to accommodate to the challenges of accelerated growth. Among those changes, the company is adopting project management principles. To a certain extent, the PMBOK Guide inspires those principles.

The project manager and his team, while addressing the ISMS project, favored a rather informal PM approach, largely based in the previous ISO certification experiences.

It was assumed that this approach, supposedly adapted to the particular circumstances of the company and its employees, would better suit its purpose than a more systematic and formal one.

All the information gathered to carry out the study comes from the direct participation of the author in the project, albeit with a minor role, from interviews

with the project manager and other stakeholders and from the documentation produced by the organization for the realization of the project.

……

In order to conduct the analysis, the study is divided in various chapters, each addressing one particular aspect of the analysis:

- Chapter 2 underlines the context of the company in which the project was developed
- Chapter 3 establishes the scope of the study
- Chapter 4 analyses the ISO/IEC 27001 standard
- Chapter 5 presents the basic PM principles as stated by the PMBOK Guide
- Chapter 6 presents the methodology used in the study and the matrix that has been developed to facilitate the comparison between the requirements of the standard, the principles of the PMBOK Guide and the actual procedures followed by the project team
- Chapter 7 discusses the results of the study
- Chapter 8 presents the lessons learnt from this comparison
- Finally, Chapter 9 presents the conclusions drawn from the study

2. CONTEXT

The organization that decided to develop, implement and certify an ISMS as a response to perceived risks related to information security is a Spanish medium sized company, dedicated to the design, production and commercialization of refrigerated display cabinets for supermarkets, department stores and malls.

A family run company created in 2005, its added value lies in its focus on innovation and advanced engineering that translates into highly competitive products.

In a short period of time, besides an important presence in Spain, the company has succeeded in acquiring relevant market shares in such distant and competitive scenarios as Germany, France, Mexico, Chili, Portugal or China. This competitive edge is due to its technological innovation, product development, design, performance, reduced energy consumption, sustainability and reasonable price.

This rapid international expansion provoked an accelerated growth that stretched the structures of the organization to a point in which it was threatening its capacity to remain in control of the operations including production, timely delivery of the merchandise, adequate attention to customers or product development.

The risks related to this accelerated expansion together with the opportunity to consolidate a relevant position in the industry led the management to introduce changes in the structure and the culture of the organization. One of these changes was the decision to implement and certify international management standards such as the ISOs 9001, 14001, 45001 and 27001. In order to address these and other projects, the company decided to adopt PM methodology, and in particular, the PMBOK Guide as a useful reference to manage its projects.

However, the functional organization of the company and the urge to prioritize production demand hampers a truly systematic approach to the introduction of culture changes that naturally take time to materialize. As a consequence, the adoption of PM principles remains an ongoing process and, to a certain extent, depends on the decision of the project manager and the project team, rather than being an embedded feature of the company which remains far from the versatile organization advocated by Turner (Turner, 2014).

In the case of the ISO/IEC 27001 implementation project, the project manager, who is the head of the IT department, favoured a selective approach to the

management of his project. Together with the key stakeholders, they sought to adopt the PM processes recommended by the standard and adapt general PM principles, as presented by the PMBOK Guide, and other referents, such as the Association for Project Management's APMBoK (APM, 2019), to the priorities and circumstances of the project. The main goal being to keep the core team engaged and actively committed to the success of the project.

Determined to improve project management in the IT department, the project manager decided to select from the PMBOK Guide the processes that intuitively and from a practical point of view, would help finalize the project successfully, that is, with the desired certification, in the shortest period of time and with the least possible cost. Other processes, less directly involved with the progress of the project or simply not relevant in this particular case, were discarded.

All together, the project was a success as the company had its ISO/IEC 27001 certification in about a year. The general conclusion was that the introduction of PM principles had had a significant impact in improving project management skills and procedures among the team members and that it had been key in the successful outcome of the project. However, further analysis will provide insight about what worked well and what could have been done differently.

Numerous research papers have pointed out the advantages and disadvantages of adapted approaches versus a standardized model. As it could be anticipated, the former lie in the capacity to fit the specific requirements of the project and the project team, the latter in the structured approach that through repetition ends up becoming part of the culture embedded in the organization (Andersen and Vaagaasar, 2009).

3. SCOPE

This paper presents a project management case study of a Spanish international company of relatively recent creation and discusses the efforts it has made to improve its project management skills by adapting established PM principles and practices to the project of developing, implementing and certifying an ISMS against the ISO/IEC 27001 standard.

The goal of the study is to verify the impact of the measures taken in the successful completion of the project, to analyze the reasons why certain processes were adopted whereas others were not and to gauge the consequences of those decisions for the outcome of the project.

Therefore, the study will focus on the development of the project and its management, with special attention to the following:

- Overview of the ISO/IEC 27001, object of the project
- PM principles as presented by the PMBOK Guide, which was the main reference for the project manager
- Analysis of the PM strategy adopted by the project manager and his team. Processes adopted and discarded: reasons and consequences
- Lessons learnt
- Conclusions

4. THE ISO/IEC 27001

The ISO/IEC 27001 is the international standard for information security. It provides specifications for the development and implementation of a custom made Information Security Management System (ISMS) in all sorts of institutions. The aim of the norm is to help organizations keep their information assets secure.

Risks related to cyber-attacks and data breaches are increasing rapidly with the widespread use of information technologies. The security of assets such as intellectual property, financial information, personal data or information entrusted by third parties has become critical for organizations.

4.1. INFORMATION SECURITY AND RISK MANAGEMENT

Information is a valuable asset that organizations need to protect from fortuitous hazards and from deliberate attacks either internal or external. Information related risks grow with its abundance and its importance.

Information security has become a priority for risk managers in large, medium size and even small companies. The protection of intellectual property and the information that the company deems critical for its competitiveness and, ultimately, its survival, has always been important, but the universal use of information technologies has multiplied the amount of data generated, shared and stored. Among this information, classified documents, personal data, financial operations conducted on-line, sensitive information from the different stakeholders in the supply chain, etc., become valuable assets that the organization is responsible for preserving. Unless properly protected, this information will be vulnerable to cyber-attacks. Any computer linked to the company network and connected to the Internet represents a potential security risk. The security of information assets acquires a completely new dimension.

Amongst the most remarkable risks related to information security are cybercrime, corporate espionage, compliance risks and reputational risks. Security breaches, on the other hand, can be the consequence of premeditated attacks or simple human errors, and the perpetuators can come from within the organization as well as from outside. Other risks include hardware and software failure, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods.

Cybercrime can be defined as the criminal use of information technologies to commit cyberattacks against governments, businesses and individuals. Cybercrime knows no borders and evolves at a phenomenal pace. Cloud security, malicious domains, ransomware, data-harvesting malware, botnets, crypto-jacking, the dark net...

Experts, such as the National Cyber Security Centre, in the UK, describe the growth of cybercrime as "rampant" and recognizes it has impacted businesses worldwide. According to the 2019 Internet Crime Report, issued by the FBI, in 2019, the cost of cyberattacks was estimated at 3.5 billion USD, in the US only. In their opinion, it should be considered a major threat for the security of organizations worldwide and adequate measures should be taken accordingly.

As it has always been the case, organizations need to protect their valuable property from criminals, but cybercrime represents a new dimension in security and risk management and a new field of expertise is required to face it. The measures taken will have to evolve at the same pace as the technology and will need to be sufficient to reassure clients, partners and insurers alike.

Corporate espionage is the practice of using espionage techniques for commercial or financial purposes. The nature of the information stolen can be as varied as the reasons for stealing it, intellectual property, techniques and processes, recipes and formulas; or it could be operational information, such as pricing, sales or marketing strategies; or any other information that could be valuable for competitors. The magnitude of corporate espionage has led to escalating international conflicts such as the trade war of the United States of America against China during the Trump Administration.

According to the Spanish Chamber of Commerce (De Miguel et al, 2020), digital transformation is adding significant complexity to information security and risk management in organizations, and they recommend companies to prioritize critical information protection to mitigate the risk of both internal and external attacks.

Compliance risks refer to the abundance of laws and regulations organizations have to comply with, in relation with information and personal data protection. Since companies and institutions have become real information processors and since phenomenal amounts of sensitive personal data are gathered in their IT systems, European and national lawmakers have issued a number of regulations to protect the interests and the privacy of individuals. Article 8(1) of the Charter of Fundamental Rights of the European Union declares that *The protection of natural persons in relation to the processing of personal data is a fundamental right*.

The European Union issued the General Data Protection Regulation (GDPR) in 2016. This regulation establishes the terms for privacy and data protection in the European Economic Area (EEA). It also addresses the transfer of personal data

outside the EU and EEA areas. The GDPR makes organizations responsible for the provision of the necessary safeguards to guarantee the safety of data of European citizens. They are requested to put in place appropriate technical and organizational measures to comply with the data protection principles. IT processes that handle personal data must be designed according to these principles and provide safeguards to protect citizen's rights.

In 2018, Spain enacted the *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* (LOPD-GDD). Its purpose is to adapt Spanish internal law to the General Data Protection Regulation. There are also other regulations in Spain that affect data protection and procedures in companies, such as the *Ley de servicios de la sociedad de la información y del comercio electrónico*, or the *Ley de propiedad intelectual*.

The legislative environment in which organizations operate is increasingly complex. Keeping up to date with all this legislation becomes a heavy burden, especially for international companies that have to follow different legislations. If they fail to comply, sanctions can be severe. Thus, compliance risks have become a concern for risk managers.

Reputational risks refer to the impact the way an organization manages information security can have in the network environment in which it operates. In the global market, business operations require the participation of numerous stakeholders who inevitably share valuable, sometimes critical, information (most payments, transfers and other financial operations are usually conducted on line, for example). Everybody is therefore concerned by how information security is handled by all the members of the supply chain. Bad practices can eventually lead to a serious reputation loss and to be considered as non-eligible by potential partners, suppliers or customers. It is increasingly common for tenders to include clauses related to information security requests. Therefore, it is important not only to manage information security properly, but also to be able to make it apparent, thus the relevance of a well-known international accreditation such as the ISO/IEC 27001.

The ISO/IEC 27001 covers all the major risks associated with Information security including issues such as human errors, system failures, natural disasters, etc. To help organizations protect their information assets from this varied display of perils, the ISO/IEC 27001 advocates and conducts the design and implementation of a customized ISMS. In the early twentieth century, banks were expected to invest heavily in hipper secure vaults to protect their customer's money and assets. The bank's reputation could depend on the size and might of the vault. Now all companies store valuable information, their own and their stakeholder's, clients included, which also needs to be securely protected. Most financial operations are nowadays conducted on line, creating important potential security hazards. A proper ISMS might represent in the twenty first century what the bank vaults did in the twentieth, and with equal reputational implications.

4.2. BASIC PRINCIPLES OF INFORMATION SECURITY

Experts consider confidentiality, integrity, and availability the fundamental principles or tenets of information security (ISO/IEC 27000:2018; ISO/IEC 27001: 2013; Burnette, 2020). Basically, all the endeavors of an information security program should try to achieve one or more of these principles. Together, they form the CIA Triad.

Confidentiality refers to the fact of preventing unauthorized access to private, sensitive information. The principle is to make sure that private information remains private and that only authorized individuals can access it. Often, assuring confidentiality requires defining and enforcing access levels of information within the organization.

Integrity involves protecting data from deletion or modification from any unauthorized party. The purpose of integrity is to ensure that data can be trusted to be accurate and that it has not been inappropriately modified. If any deletions or changes are attempted, good practices will ensure that they are not saved or that the eventual damage can be traced and reversed.

Availability refers to the fact that data can be accessed when needed. It aims to make sure that information is fully accessible in due time and to the right people. The importance of availability is obvious, because it is not enough to protect information if in doing so, it becomes unavailable or difficult to access.

The ISO/IEC 27001 shares this same approach, and proposes how to deal with confidentiality, integrity and availability of information in the particular case of each organization (Kosutic, 2017).

4.3. WHAT IS AN ISMS?

An ISMS is a holistic approach to securing the confidentiality, integrity and availability (CIA) of corporate information assets. It consists of a set of requirements for *establishing, implementing, deploying, monitoring, reviewing, maintaining, updating and improving a documented ISMS with respect to an organization's overall business risks and opportunities* (ISO/IEC 27000:2018, 19).

It includes the policies, procedures, guidelines, associated resources, activities (ISO /IEC 27000: 2018, 11), and other controls involving people, processes and technology, managed by an organization to protect its information.

It is based on regular security risk assessments that help monitor and control the efficiency of the system. In order to be successful, according to the standard, the implementation of the ISMS requires awareness of its need, assignment of responsibilities within the organization, commitment of the managers,

appropriate controls, active prevention, a comprehensive approach and continual reassessment.

The implementation of an ISMS is a strategic decision that should be seamlessly integrated, scaled and updated according to the organization needs. It goes beyond information technologies to address risks related to all the different supports in which information can be stored, and to security habits developed by all the individuals that work in or collaborate with the organization.

Ultimately, an ISMS is a documented, efficient, risk-based and technology-neutral approach to keeping information assets secure.

4.4. THE ISO/IEC FAMILY OF STANDARDS

ISO stands for the International Organization for Standardization, an independent nongovernmental organization and the world's largest developer of voluntary international standards. Organizations accredited with an ISO certification are proving to all interested parties that they work to comply with the highest standards.

IEC stands for the International Electrotechnical Commission, the world's leading organization for the preparation and publication of international IT and ICT standards. It is a non-for-profit organization that works independently of any government.

Both organizations, the ISO and the IEC, have constituted a technical committee, to develop the standards applicable in the domains of information and communication technologies.

The ISO/IEC 27000 family is a series of complementary information security standards that can be combined to provide a framework for best-practices in information security management, assuring the confidentiality, the integrity and the availability of information and containing measures that address three key elements for information security: people, processes and technology.

The series deals with the management of risks related to information security through the design and implementation of an ISMS that consist of processes, procedures and controls. It provides best practice recommendations to help implement a customized ISMS in any given organization. It is part of the ISO framework of management standards such as management systems for quality assurance (the ISO 9000 series), environmental protection (the ISO 14000 series) and other management systems.

The series covers all aspects of information security, and goes beyond IT or cybersecurity issues, including the protection of information in all possible formats and from all imaginable threats. It aims to be applicable to all sorts of organizations, irrespective of type and size. It encourages organizations through

a systematic approach to define, implement, monitor and improve a customized ISMS to suit its specific needs. Because information security deals with a rapidly evolving technical environment, continuous monitoring and improvement is another of the features of the ISO/IEC 27000 series.

The mainstay of the series is the ISO/IEC 27001, which provides a systematic approach to establish, implement, operate, monitor, review, maintain and improve an organization's ISMS. It is the only standard in the series that organizations can be audited and certified against.

Within the family of standards, the following can be of particular interest for organizations seeking to implement and certify the ISO/IEC 27001:

ISO/IEC 27000:2018, Information security management systems overview and vocabulary

ISO/IEC 27002:2013, Information technology. Security Techniques. Code of practice for information security controls

ISO/IEC 27003, Information technology. Security techniques. Information security management system implementation guidance

ISO/IEC 27004, Information technology. Security techniques. Information security management. Measurement

ISO/IEC 27005, Information technology. Security techniques. Information security risk management

ISO 31000:2009, Risk management. Principles and guidelines

ISO/IEC Directives, Part 1, Consolidated ISO Supplement. Procedures specific to ISO, 2012

4.5. ISO/IEC 27001: THE INTERNATIONAL STANDARD FOR INFORMATION SECURITY MANAGEMENT

ISO and IEC official documents define the 27001 standard as the norm that *specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security management systems within the context of the organization's overall business risks* (ISO/IEC 27000: 2018, 19). It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. It provides the requirements to establish information security controls according to the needs of each specific organization regardless of its type, size or nature.

The first edition of the ISO/IEC 27001 was published in 2005. It was based on the British standard BS 7799-2, which was a precursor of the ISO/IEC 27001. When the new international standard was issued the British Standards Institution

(BSI) withdraw the BS 7799-2 and adopted the ISO/IEC 27001 as the new British standard (Kosutic, 2016. 26).

The ISO/IEC 27001 belongs to a well-known group of international standards known as the Management System of Standards (MSS) that includes among others, the ISO/ 9001, Quality Management System; the ISO/ 14001, Environmental Management System or the ISO/ 22301, Business Continuity Management System.

The second and current valid edition of the ISO/IEC 27001 was published in 2013, after a thorough revision that benefited from the experience and contributions of the SC 27[1] member bodies and cooperating organizations, and it takes into account the new MSS approach (Humphreys 2016, 22). This second edition represents a significant step forward that incorporates the experience and the conceptual evolution of the standard.

One of the remarkable differences with the 2005 edition is the suppression of the Plan-Do-Check-Act process model that was one of its outstanding characteristics. This model has been excluded in the new edition, however, the process-based approach and the continual improvement philosophy continues to be very much part of the ISO/IEC 27001.

In its introduction, the ISO/IEC 27001 claims to provide the necessary requirements for any organization, irrespective of size and type, to protect the security of its information via an ISMS, assuring the confidentiality, integrity and availability of the information assets.

Risk management is one of the key axes that permeates the norm. Regular information security risk assessments will determine the security controls that need to be implemented.

The adoption of an ISMS is a strategic decision that should be determined by the specific needs and objectives of the organization. However, these may evolve over time.

4.6. STRUCTURE OF THE STANDARD

The ISO/IEC 27001:2013 is a 34-page[2] document, which contains a foreword, an introduction, ten short clauses, plus a long annex.

Clauses one to three give some preliminary indications and clarify aspects such as the use of specific terminology. Clauses four to ten are compulsory for certification purposes. These clauses describe the necessary steps to define, implement, certify and maintain an ISMS.

[1] ISO Information Technology Security Techniques Subcommittee.

[2] This refers to the Spanish version: UNE-En ISO/IEC 27001, from May 2017.

The first set of clauses refer to all the preliminary measures that need to be taken to prepare the development of the ISMS. They propose a previous analysis of the context and the environment of the organization, a definition of the desired scope of the ISMS, as well as the identification of the stakeholders and their expectations. Finally, they mention the importance of securing top management support from this early stage.

The next set of clauses focus on two critical aspects of the definition of the ISMS. Risk assessment, the analysis of all the potential information security risks that the organization is exposed to, and risk treatment, the set of measures and controls that can be established to minimize those potential risks.

Then, a set of clauses emphasizes the importance of assuring the necessary resources to conduct the implementation of the ISMS. Human y and material resources, the necessary competence, which if it is not available in house can be hired or acquired through training. The importance of communication to guarantee that all parties involved are adequately informed. Finally, the importance of documenting all these processes, documentation that will be an important part of the certification process.

The last group of clauses addresses the implementation of the ISMS and a quality control system that includes revision, annual audits and the compromise with continual improvement.

Finally, Annex A proposes a list of information security control objectives and information security controls to help decision makers choose the right ones for each ISMS.

4.7. CERTIFICATION

The ISO/IEC 27001 certification is recognized around the world and is considered a valid indicator of the capacity of the holder's information security system. In 2019, there were more than 35.000 organizations with a valid ISO/IEC 27001 compliant certificate in the world.

From an internal point of view, being certified against the ISO/IEC 27001 standard reassures the management and all the members of the staff about the protection of information assets in the organization, both assuring confidentiality, availability and integrity of the information and complying with legislation such as the GDPR.

On the other hand, the certification conveys a powerful message to contractors, suppliers, partners, clients, etc., about the commitment of the organization towards the management of information security, reassuring them that the information they share will be adequately protected. If the organization is also certified against other standards, such as the ISO/ 9001, or the ISO/ 14001, it

will show its compromise with management excellence and best management practices.

No security system is perfect, and despite all the measures taken, breaches can occur. Being certified will allow the organization to prove that it did its best to protect the information for which it was responsible.

4.7.1. Certification Process

At ISO, the International Organization for Standardization, they develop international standards, but they are not directly involved in certification. This is the role of external certification bodies. However, ISO's Committee on Conformity Assessment (CASCO) has produced a number of standards related to the certification process, which are used by certification bodies (ISO certification web page).

When choosing a certification body, it is advisable to evaluate several and check whether they use the relevant CASCO standard and whether they are accredited.

The certification is usually a two-stage process, although some certification bodies propose an optional preliminary assessment to verify the readiness of the organization that seeks to be certified.

The first step consists in a preliminary review of the ISMS, checking thoroughly the completeness of the documentation required and generally trying to identify possible gaps or flaws that can be corrected before the actual assessment takes place.

Once all the requirements are in place, the formal compliance audit can begin. It will consist in a detailed revision of the ISMS, checking it against the requirements specified in ISO/IEC 27001. The auditors will seek evidence that the ISMS has been designed, put in place and is actually working according to the standard. Not only the documentation, but also the measures and controls and the actual operations will be verified. If this audit is passed successfully, it will result in the ISMS being certified compliant with the ISO/IEC 27001.

The certificate is valid for three years. Sometimes certification bodies offer the possibility of regular visits to make sure that the system remains compliant and that it is improving continuously, as is required by the standard. Certification maintenance requires periodic re-assessment audits to confirm that the ISMS continues to operate as specified and intended.

5. PROJECT MANAGEMENT APPROACH TO THE IMPLEMENTATION AND CERTIFICATION OF THE ISO/IEC 27001

Once the management has decided to address the issue of information security in the company via the implementation of the ISO/IEC 27001 and the ISMS that it advocates, including the certification process, the next step will be to define the strategy that will eventually help materialize this project.

Complex projects like this, in order to be successful, in other words, if they are going to be completed in due time, at the right cost and with the expected quality, require the application of knowledge, methods, skills, processes and experience that are best described in Project Management theory.

5.1. INTRODUCTION TO PROJECT MANAGEMENT (PM)

First and foremost, PM is about projects, and projects are defined as *temporary endeavors* with a *defined beginning and end in time.* (Project Management Institute: *What is Project Management?*), whereas the ISO/IEC 27001 norm proposes an ongoing and ever improving process with no eventual end. At first sight, it might seem that PM theory will not be applicable to this case.

Nonetheless, there are at least two phases of the process that ultimately leads to the objective of having an ISMS up and running in the company, that are finite and that can be addressed as a project: the implementation of the ISMS itself and its certification against the ISO/IEC 27001 standard.

Both phases are particularly important to the success of this endeavor, although the process does not end with the certification, on the contrary, all the procedures and controls defined in the ISMS should become common everyday practice throughout the company and continue to be monitored and improved forever. In this sense, the implementation and certification phases are only the beginning of the process.

Therefore, for the purpose of the analysis of the eventual contributions of a PM approach to the implementation of the ISO/IEC 27001 in the organization, only these two phases, definition and implementation of the ISMS as advocated by the standard, and its certification against the ISO/IEC 27001 norm, are going to be considered.

Actually, the reasons argued by the management to explain their decision to implement the ISO/IEC 27001 also indicate that this should be the approach. According to the managers, the reasons that explain their decision are threefold:

- On the one hand, because information security needs to be properly addressed in the organization and, at the moment in which the decision was taken, it was not.
- Secondly, because they wanted to be able to reassure all the stakeholders in the supply chain, from the first provider to the last customer, that the information they shared with the company was secure.
- Finally, because the certification is necessary to be able to apply to tenders that increasingly demand evidence of compliance with information security regulations.

Therefore, the goal is to obtain the certification in the shortest reasonable time so that all three objectives are attained. The organization seeks to pass from an initial state, in which information security represents a potential risk, to another state in which an information security management system has been designed, implemented and certified. It seeks to do so in an orderly manner, controlling parameters such as time, cost, communications, quality, efficiency, etc. In other words, the company is dealing with a project that needs to be managed. Once this stage has been achieved, the ongoing process of managing and monitoring the ISMS can begin.

Project Management can be described as the combination of knowledge, skills and techniques that help define, monitor and travel the journey that leads from the initial state, in which the organization has only made the decision to go for the project, to the final one, in which the certification has been obtained. It is a systematic and knowledgeable approach to the timely and orderly organization of all the different tasks that need to be accomplished in order to obtain the desired result, including the implication of all the necessary stakeholders.

Indeed, given the complexity of the project, that affects all the departments of the organization but that hardly falls into the scope of responsibilities of any of them, sound project management skills are clearly required. The challenge is to organize, plan and execute the different stages described in the norm, including the production of the necessary documentation as described by the standard. To do so, we are going to explore an approach based on PM theory.

5.2. PROJECT MANAGEMENT METHODOLOGIES (PMM)

Project management began to emerge as a discipline at the beginning of the last century, probably with Henry Gantt and his famous chart, and acquired full academic status in the late 1950s (Ungureanu and Ungureanu, 2014). The need to deal with ever more complex projects and the escalating consequences and costs of failure provided powerful stimuli to develop methodologies capable of

helping project managers achieve their goals. Project management methodologies were born to provide the tools knowledge and techniques for leading, defining, planning, organizing, controlling and closing a project; both efficiently (resource utilization) and effectively (customer satisfaction) (Kliem et al., 1997).

Over the years, several different methodologies have proven their efficacy and have been adopted and customized by organizations and project managers throughout the world. Among the best known it might be worth mentioning Agile project management (Hoda et al. 2008), that stemmed from the principles of the Agile Manifesto issued in 2001 by 13 industry leaders. Originally developed by software companies, it is best suited for projects that are iterative and incremental and that require an adaptive approach (Ungureanu and Ungureanu, 2014). Various methodologies or frameworks have evolved within the Agile, such as Scrum, that operates using "roles", "events" and "artifacts". It is best suited for reduced project teams that focus in the delivery of a product or service (Sliger, 2011). In addition, Kanban, that was developed by the Toyota company and that aims to deliver high quality results in complex projects by using visual clues to help identify workflows and possible bottlenecks.

Lean is another well-known methodology that aims to maximize customer value by minimizing waste. Originally developed in Japan, in the manufacturing sector, it is best suited for organizations that need to transform the way they operate (Ballard, 2003).

PRINCE2 was developed by the Central Computer and Telecommunications Agency, a government body in the UK, originally for IT development, and has almost acquired the status of planning and project management standard in the UK.

Motorola engineers, with a focus in reducing errors to improve quality, introduced Six Sigma, a data-driven methodology. It is considered to be particularly adequate for large companies that seek to improve quality and efficiency (Tjahjono et al. 2010).

The International Organization for Standardization, ISO, released in 2012 the ISO 21500 Guidance on Project Management, a generic guidance that provides core principles and good practices in project management. It has been regularly updated since.

The list of PMM is large and continues to grow as does the tendency towards specialization, however, the PMI-PMBOK Guide still keeps its status as reference for project management and it was the guide that, at least to a certain extent, inspired the implementation and certification of the ISO/IEC 27001 in this case study.

PMI stands for Project Management Institute, a non-for-profit membership association, project management certification, and standards organization founded in 1969, in Atlanta (USA).

The PMI issued the Project Management Body of Knowledge Guide, PMBOK Guide, as a white paper, in 1987, for the first time. Not quite a methodology, but a guide providing a set of standards, best practices, conventions and knowledge that represent the core of current PM expertise. *A foundation upon which organizations can build methodologies, policies, procedures, rules, tools and techniques, and life cycle phases needed to practice project management* (PMBOK Guide, 2017). The PMI updates the PMBOK Guide regularly; in 2017, the sixth and latest edition was published both in print and online.

Descriptive rather than prescriptive, the PMBOK Guide provides a thorough set of good practices generally recognized as such by the PM profession. It is the role of project managers and their teams to select the appropriate combination of processes, inputs, tools and techniques to adapt the content to each particular project.

5.3. PROCESS GROUPS AND KNOWLEDGE AREAS

Key concepts to understand the PMI framework of project management are *processes, process groups* and *knowledge areas*. The sixth edition of the PMBOK Guide distinguishes 49 processes and 10 knowledge areas that are interrelated. Processes are grouped in process groups.

- Processes are what the project managing team needs to DO to deliver a project successfully.
- Knowledge areas are what the project managing team needs to KNOW to manage the project successfully.
- Process groups are logical groupings of processes.

The PMBOK Guide re-groups the 49 processes in five process groups based on the five stages of project implementation: initiating process groups, planning process groups, executing process groups, monitoring and controlling process groups, and closing process groups (PMBOK Guide, 2017). The Guide establishes the relationships between Processes, Process Groups, and Knowledge Areas in the "Project Management Process Groups and Knowledge Area Mapping" matrix, found in Table 1-4, on page 25 and in Table 1-1, page 556.

This table maps the 49 project management processes to their corresponding Knowledge Areas, as well as to their corresponding Process Groups.

	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
4. Project Integration Manageent	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work 4.4 Manage Project Knowledge	4.5 Monitor and Control Project Work 4.6 Perform Integrated Change Control	4.7 Close Project or phase
5. Project Scope Management		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.6 Control Scope	
6. Project Schedule Management		6.1 Plan Scheule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Durations 6.5 Develp Schedule		6.6 Control Schedule	
7. Project Cost Management		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
8. Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
9. Project Resource Management		9.1 Plan Resource Management 9.2 Estimate Activity Resources	9.3 Acquire Resources 9.4 Develop Team 9.5 Manage Team	9.6 Control Resources	
10. Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
11. Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perfform Qualitative Risk Analysis 11.4 Perform Quantitative Risk 11.5 Plan Risk Responses	11.6 Implement Risk Responses	11.7 Monitor Risks	
12. Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
13. Project Stakeholder Management	13.1 Identify Stakeholders	12.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Table 1 PMBOK Guide Project Management Process Group and Knowledge Area Mapping

5.4. Project management processes and process groups

A process is simply the way in which an input is transformed into an output using a given set of resources. *Processes produce one or more outputs from one or more inputs by using appropriate project management tools and techniques* (PMBOK Guide, 2017, 22). A set of interrelated actions and activities performed to achieve a specified product, result, or service. Processes, together, accomplish proven project management functions and drive project success.

A Project Management Process Group is a logical grouping of project management processes to achieve specific project objectives. Project management processes are grouped into the following five Project Management Process Groups:

- **Initiating Process Group**: Processes carried out to define a new project or phase, align the project objectives with the expectations of the stakeholders, including the decision to go ahead and start de project.
- **Planning Process Group**: Processes carried out to determine the scope of the project, its objectives, and define the roadmap of actions that will lead to the completion of the project. Planning is an iterative and ongoing process, that needs to be revisited and refined continuously, this ongoing refinement is called progressive elaboration (PMBOK Guide, 2017, 565).

- **Executing Process Group**: Processes carried out to execute the previously established project management plan, which will require the coordination of resources and stakeholders. Eventually, these execution processes might require changes that could trigger modifications in the management plan.
- **Monitoring and Controlling Process Group**: Processes carried out to verify the progress and adequate development of the project management plan, identify the eventual non-conformities and take the necessary action to redress them. Monitoring consists in collecting performance data and disseminating performance information appropriately. Controlling consists in comparing actual performance with planned performance and apply corrective action as needed.
- **Closing Process Group**: Processes carried out to conclude all activities across all Process Groups, formally closing the project, phase or contract. This Process Group verifies that all processes are complete and that they are closed appropriately. This Process Group will also address the early closure of a project in the case of the project being cancelled or aborted.

As the PMBOK Guide remarks, project management processes and process groups may be related to each other so that the output of one process can become the input of another (PMBOK Guide, 2017, 23).

5.4.1. Project Management Knowledge Areas

A large part of what constitutes the body of knowledge that has been gathered and proven by the Project Management profession thus far is presented in the PMBOK Guide in ten Knowledge Areas that summarize the state of the art of Project Management.

According to the Guide, Knowledge Areas categorize processes as well as Project Groups. *A Knowledge Area is an identified area of project management defined by its knowledge requirements and described in terms of its component processes, practices, inputs, outputs, tools, and techniques* (PMBOK Guide, 2017, 23).

The ten Knowledge Areas identified in the Guide are the following:

1) Project Integration Management:

This knowledge area covers all five Process Groups, from project initiation to closure. It helps to link processes and tasks together. This creates a single, coherent project lifecycle.

Integration management is a specific competence of project managers. Other knowledge areas might be managed by specialists, such as cost management, for instance, but not integration. Integration includes the *processes and activities to identify, define, combine, unify, and coordinate the various processes and*

project management activities within the Project Management Process Groups (PMBOK Guide, 2017, 69).

The processes involved are developing the project charter and project management plan, directing and managing project work, managing project knowledge, monitoring and controlling project work, performing integrated change control, and closing the project.

2) Project Scope Management:

Project Scope Management defines the boundaries of the project. The goal is to make sure that the project covers all the work required and only the work required so that all the stakeholders share a common understanding of what is part of the project and what it is not. This is defined during the planning process and is validated, controlled, and eventually updated during the monitoring and controlling process.

A good scope definition is essential to avoid the addition of unauthorized or unnecessary tasks, which would imply waste of time, resources and money.

The processes involved are planning scope management, collecting requirements, defining scope, creating work breakdown structure (WBS), validating scope and controlling scope.

3) Project Schedule Management:

Project Schedule Management is one of the most sophisticated among all the knowledge areas and it constitutes a true PM skill. It requires a thorough understanding of the project and it is a key element in the planning process. The aim is to plan, develop, manage, execute and control the project schedule, which is necessary for the orderly and timely completion of the project. All the stakeholders should approve and commit to the schedule.

Often the schedule will need to be revised and updated during the monitoring and controlling process.

The processes involved are planning the schedule management, defining the activities, sequencing the activities, estimating activity duration, developing the schedule, and controlling the schedule.

4) Project Cost Management:

Project Cost Management is essential for an efficient control of the project costs and as such, it is an important part of the planning and control processes. This knowledge area provides effective estimation techniques that help define and anticipate the project costs. This process is also important to ensure that the necessary resources for the completion of the project are timely allocated.

The processes involved are planning cost management, estimating costs, determining the budget and controlling costs.

5) Project Quality Management:

Project Quality Management is another important part of the planning, executing and controlling processes. The organization's quality policy is applied to the project so that quality criteria and requirements are defined for the different deliverables of the project in order to meet the expectations of the stakeholders.

The processes involved are planning quality management, performing quality assurance and controlling quality.

Project Quality Management also involves continuous improvement processes as well as documenting how the project demonstrates compliance with quality standards.

6) Project Resource Management:

This knowledge area refers to the competences and capacities necessary to define, acquire, and manage the resources that the project needs in its different phases and according to the Project Management Plan. The aim is that the right resources are available at the right time and place, so that the project can progress according to the schedule.

Resource Management includes team resources and physical resources. The skills and competences required to manage both types of resources can be very different. The management of the project team requires the ability to select, recruit, motivate and empower the team, whereas physical resource management concentrates in identifying, acquiring, allocating and using those resources as the completion of the project demands.

In the case of human resources, procuring training for the acquisition of necessary competences can also be part of the responsibilities of the project manager.

Processes included are planning, estimating, acquiring and controlling resources, and developing and managing the project team.

7) Project Communications Management:

Project Communications Management refers to the definition and execution of all the necessary measures to ensure an effective and efficient exchange of information between project team members and stakeholders during the entire lifecycle of the project.

Communication is a vital element for the success of the project and can become a quite complex issue if team members do not share the same space or location and if their involvement in the project is only part-time.

The processes involved are planning, managing and monitoring communications.

8) Project Risk Management:

Project Risk Management deals with the analysis and identification of potential risks along the life cycle of the project in order to try to minimize any negative impact through response planning and preparation.

The processes involved are planning risk management, identifying risks, performing qualitative and quantitative risk analysis, planning and implementing risk responses, and monitoring risks.

9) Project Procurement Management:

Project procurement management deals with the purchase of products and the contract of external or internal services necessary for the completion of the project, and identified in the planning process.

Depending on the size and nature of the project, procurement management can be a phenomenal endeavor, or almost irrelevant. In the former cases, often, the purchases department in the organization will be involved.

Project Procurement Management processes include planning procurement management, and conducting and controlling procurement.

10) Project Stakeholder Management:

Project Stakeholder Management deals with the identification of all those who are in any way related to the project, either because they can be affected by the project or because they can affect the project. Once identified, stakeholder management will imply developing a strategy to engage those stakeholders so that their expectations are met and their implication is guaranteed.

A structured approach to the identification and prioritization of those stakeholders can have a significant impact on the development of the project and, consequently, an adequate strategy to ensure their support can sometimes mean the difference between project success and failure.

The implication of stakeholders begins in the early stages of the project and should continue during its entire life cycle. The processes included are identifying stakeholders, and planning, managing and monitoring stakeholder engagement.

5.5. PROJECT MANAGEMENT IN THE CONTEXT OF THE ISO/IEC 27001

The norms issued by the International Organization for Standardization, ISO, by definition, always try to reflect the state of the art and best practices of each area of activity. *Standards are the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent* (ISO web page).

Therefore, it is no surprise that certain PM principles permeate those standards specifically addressed at organizations that seek to implement projects to improve their processes and procedures.

In fact, the ISO issued in 2012 a PM standard, the ISO/21500 *Guidance on project management*, that has become in its latest edition the ISO/21500: 2021 *Project, programme and portfolio management — Context and concepts*, which *specifies the organizational context and underlying concepts for undertaking project, programme and portfolio management* (ISO web page). The PMI, who participated in the committees that developed those standards on behalf of the American National Standards Institute, ANSI, played a very significant role in their definition. As a result, the ISO/21500 is largely influenced by the PMBOK Guide approach (Best, 2012).

The ISO/IEC 27001 is no exception, and some of the processes and process groups described in the PMBOK Guide can be found, at least partially, in the recommendations of this standard. The following table shows the processes that are described in the PMBOK Guide and mentioned in the standard (Color code: green refers to the processes that are mentioned in the ISO/IEC 27001, red to those that are not. Paler shades reflect less coincidence between the two):

KNOWLEDGE AREAS	PROCESS GROUPS				
	Initiating Process Group	**Planning Process Group**	**Executing Process Group**	**Monitoring and Controlling Process Group**	**Closing Process Group**
4. Project Integration Manageent	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work	4.5 Monitor and Control Project Work	4.7 Close Project or phase
			4.4 Manage Project Knowledge	4.6 Perform Integrated Change Control	
5. Project Scope Management		5.1 Plan Scope Management		5.5 Validate Scope	
		5.2 Collect Requirements		5.6 Control Scope	
		5.3 Define Scope			
		5.4 Create WBS			
6. Project Schedule Management		6.1 Plan Schedule Management		6.6 Control Schedule	
		6.2 Define Activities			
		6.3 Sequence Activities			
		6.4 Estimate Activity Durations			
		6.5 Develp Schedule			
7. Project Cost Management		7.1 Plan Cost Management		7.4 Control Costs	
		7.2 Estimate Costs			
		7.3 Determine Budget			
8. Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
9. Project Resource Management		9.1 Plan Resource Management	9.3 Acquire Resources	9.6 Control Resources	
		9.2 Estimate Activity Resources	9.4 Develop Team		
			9.5 Manage Team		
10. Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
11. Project Risk Management		11.1 Plan Risk Management	11.6 Implement Risk Responses	11.7 Monitor Risks	
		11.2 Identify Risks			
		11.3 Perfform Qualitative Risk Analysis			
		11.4 Perform Quantitative Risk			
		11.5 Plan Risk Responses			
12. Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
13. Project Stakeholder Management	13.1 Identify Stakeholders	12.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Table 2 PMBOK Guide Knowledge Areas and Process Groups in the ISO/IEC 27001

It is not the purpose of the ISO/IEC 27001 standard to indicate how organizations should manage the process of defining and implementing their ISMS. However, the norm does mention certain aspects that have been considered particularly relevant by the technical committee and have therefore been included in the norm.

In particular, the ISO/IEC 27001 highlights the importance of the following:

- Consider the context in which the organization operates. Which will have an impact in the definition of the ISMS. This aspect is also mentioned in chapter 2 of the PMBOK Guide: *The environment in which projects operate*.

- Identify stakeholders. The norm states the importance of the identification of the stakeholders' expectations and particularly the commitment of the top management to guarantee the allocation of resources and the implication of the organization.

- Define scope. Information security policy, boundaries and applicability of the ISMS.

- Define roles within the organization. Define and create the team that is going to lead and manage the project.

- Plan the information security management system and the actions to identify and treat the potential risks.

- Estimate resources. To guarantee the adequate completion of the project.

- Assure competence. The organization has to determine the competences necessary to carry out the project and make sure that the team has or acquires the said competences.

- Plan and manage communications. Decide and organize what, when, how and to whom communicate.

- Document the procedures. The norm establishes what needs to be documented and how it needs to be documented. This is particularly relevant when the organization seeks to certify the ISMS against the standard.

- Plan and control operations to implement the ISMS. Including change management.

- Evaluate. Monitor the implementation process.

These are all well-known concepts in PM and are also emphasized by the technical committee that developed the last edition of the standard. However, in order to manage properly the definition and implementation of the ISMS, and its certification against the ISO/IEC 27001, many other management principles will have to be applied.

Indeed, in our case study, the company, inspired by the PMBOK Guide, developed a roadmap which would eventually lead to the completion of these objectives in due time, at the right cost and with the expected quality.

6. METHODOLOGICAL FRAMEWORK

The purpose of this paper is to study the efficacy of the set of measures and PM processes implemented by the project team and their impact in the successful completion of the project, to analyze the reasons why certain processes were adopted whereas others were not and to gauge the consequences of those decisions for the outcome of the project.

In preparation for this analysis, the study confronts, both quantitatively and qualitatively, the processes adopted by the project manager and his team with the recommendations included in the ISO/IEC 27001 standard and with the whole set of processes and knowledge areas described in the PMBOK Guide (PMI, 2017).

The comparison has been carried out through a matrix (see annex 1) in which the treatment accorded by the ISO/IEC 27001 standard and by the project team to each one of the 49 processes described in the PMBOK Guide has been examined and evaluated according to the following scale:

1. The process has not been considered. It is not mentioned
2. The process might be mentioned but its importance is considered negligible
3. The process is addressed but it is considered of relative importance
4. The process is adopted and considered relevant
5. The process is adopted and considered key to achieve the objective

The scale reflects the importance accorded to each of the processes respectively by the ISO standard and by the project team. Obviously, there is a direct relationship between the actions undertaken by the team and the importance attributed to them in the documentation of the project[3].

The matrix, which is dynamic, admits all kinds of comparisons as well as grouping the processes according to different criteria. For instance, following the knowledge areas described in the PMBOK Guide.

Comments have been added to each process form to explain the reasons for the option selected:

[3] Besides the direct participation of the author in the project, the information used for the study comes from the abundant documentation generated in the process (it is customary in ISO certifications that every step of the project is thoroughly documented) and from direct interviews with the project manager as well as with some of the relevant stakeholders

PM Process	1	2	3	4	5	Score	Comments
Develop Project Charter							
Presence in ISO 27001	x					1	- Not mentioned in the definition of the standard
Presence in the proyect			x			3	- Not documented in the project - Official declaration of the top management assigning the head of the IT department as project manager

Table 3 This entry corresponds to the first process mentioned in table 1-4, part one, of the PMBOK Guide

The aim of the matrix is to facilitate the analysis and the drawing of conclusions by making the relevant information readily available. The complete matrix is available in Annex 1.

6.1. TRANSLATION OF PROCESSES INTO ACTUAL PROJECT ACTIVITIES

Each of the PMBOK Guide processes that is finally incorporated to the project management strategy actually translates into a set of actions that, depending on their nature, can be more or less complex.

If we look at the process "Define activities", for instance, considered very important by both the ISO standard and by the project team, we can see how this apparently simple statement develops into a multitude of different activities that, at the same time, unfold into a myriad of tasks that the project needs to accomplish and, very often, also document.

Pm Process	1	2	3	4	5	Score	Comments
Define Activities							
Presence in ISO 27001				x		4	- The ISO 27001 includes a template that suggests a set of measures to improve the information security but the details have to be tailored to each specific ISMS
Presence in the proyect					x	5	- Definition of every control to be implanted in the organization for each ISO requirement applicable for the ISMS - Detailed descriptions of each activity and control to be implemented

Table 4 "Define Activities" process entry in the matrix

The PMBOK Guide defines the process Define Activities as *the process of identifying and documenting the specific actions to be performed to produce the project deliverables. The key benefit of this process is that it decomposes work packages into schedule activities that provide a basis for estimating, scheduling, executing, monitoring, and controlling the project work. This process is performed throughout the project.*

Among the many activities that the project will have to consider to complete the project planning, one of the most important to define the ISMS is the information security risk assessment. This analysis process will identify all the weaknesses of the company's systems in terms of information security and will trigger the risk treatment process with the assignment of information security controls that will help minimize those risks.

As we can see in the table below, for this activity only, Information Security Risk Assessment (*Seguridad de la información*), twenty-eight sub-activities have been identified, each corresponding to an area of potential information security risks for which treatments and controls, chosen from ISO/IEC 27001 Annex A, are defined in the corresponding column.

At the same time, each of those sub-activities that refer to areas of potential risks, as we will see, will trigger their own subdivisions and will develop into new sets of tasks.

APARTADO 27001	APARTADO 27001	CONTROLES ASOCIADOS
PROCESO Seguridad de la información		Anexo A 27001
Acta constitución Comité Seguridad de la Información		
GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	6.1.1 Acciones para abordar riesgos y oportunidades. Consideración generales 6.1.2 Apreciación de riesgos de seguridad de la información Anexo A - controles	A.8.1.1 - A.8.1.2
DECLARACIÓN DE APLICABILIDAD	4.3 Determinación de alcance del sistema de seguridad de la información 6.1.3 Tratamiento de los riesgos de seguridad de la información	
CONTROL DE ACCESO LÓGICO	Anexo A - controles	A.6.1.1 - A.6.1.2 - A.9.1.1 - A.9.2.3 - A.9.2.4 - A.9.2.5 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.11.2.8
SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS	Anexo A - controles	A.6.1.5 - A.14.1.1
SEGURIDAD EN LOS DISPOSITIVOS MÓVILES	Anexo A - controles	A.6.2.1 - A.8.3.1 - A.8.3.3 - A.11.2.1 - A.11.2.6 - A.14.1.2
GESTIÓN DE DISPOSITIVOS PROPIOS (BYOD)	Anexo A - controles	A.6.2.1 - A.8.3.1 - A.8.3.3 - A.11.2.1 - A.11.2.6 - A.14.1.3
SEGURIDAD EN EL TELETRABAJO	Anexo A - controles	A.6.2.2
GESTIÓN DE USUARIOS Y CONTRASEÑAS	Anexo A - controles	A.7.3.1 - A.9.2.1 - A.9.2.2 A.9.2.6 - A.9.4.1 - A.9.4.2 - A.9.4.3 - A.13.2.4
NORMATIVA DE BUENAS PRACTICAS EN SEGURIDAD DE LA INFORMACIÓN	Anexo A - controles	A.8.1.3 - A.8.1.4 - A.11.2.9 - A.13.2.4
CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN	Anexo A - controles	A.8.2.1 - A.8.2.2 - A.8.2.3
MANTENIMIENTO, REUTILIZACIÓN Y ELIMINACIÓN DE SOPORTES	Anexo A - controles	A.8.3.2 - A.11.2.7
USO DE MEDIOS DE ALMACENAMIENTO EXTERNO	Anexo A - controles	A.8.3.2 - A.11.2.7
CONTROL DE ACCESO A LA RED	Anexo A - controles	A.9.1.2 - A.9.2.3 - A.13.1.1 - A.13.1.2 - A.13.1.3
DESARROLLO SEGURO DE APLICACIONES	Anexo A - controles	A.9.4.5 - A.14.2.1 - A.14.2.2 - A.14.2.3 - A.14.2.4 - A.14.2.5 - A.14.2.6 - A.14.2.7- A.14.2.8 - A.14.2.9 - A.14.3.1
GESTIÓN DE LA FIRMA DIGITAL	Anexo A - controles	A.10.1.1 - A.18.1.5
SEGURIDAD FÍSICA	Anexo A - controles	A.11.1.1 - A.11.1.2 - A.11.1.3 - A.11.1.4 - A.11.1.5 - A.11.1.6 - A.11.2.2 - A.11.2.3 - A.11.2.4 - A.11.2.5
GESTIÓN DE CAMBIOS EN APLICACIONES	Anexo A - controles	A.12.1.2 - A.12.1.3 - A.12.1.4 - A.14.2.1 - A.14.2.2 - A.14.2.3 - A.14.2.4 - A.14.2.5 - A.14.2.6 - A.14.2.8 - A.14.2.9 - A.14.3.1
MANTENIMEINTO DE EQUIPOS	Anexo A - controles	A.12.2.1
CONTROL Y RESPUESTA ANTIMALWARE	Anexo A - controles	A.12.2.1
GESTIÓN DE BACKUPS	Anexo A - controles	A.12.3.1
GENERACIÓN Y USO DE LOGS	Anexo A - controles	A.12.4.1 - A.12.4.2 - A.12.4.3 - A.12.4.4
INSTALACIÓN DE SOFTWARE	Anexo A - controles	A.12.5.1 - A.12.6.2
GESTIÓN DE VULNERABILIDADES TÉCNICAS	Anexo A - controles	A.12.6.1
INTERCAMBIO DE INFORMACIÓN	Anexo A - controles	A.13.2.1 - A.13.2.3
GESTIÓN DE LA PROVISIÓN DE SERVICIOS POR TERCEROS	Anexo A - controles	A.13.2.2 - A.14.1.3 - A.15.1.1 - A.15.1.2 - A.15.1.3 - A.15.2.1 - A.15.2.2
GESTIÓN DE INCIDENTES DE SEGURIDAD	Anexo A - controles	A.16.1.1 - A.16.1.2 - A.16.1.3 - A.16.1.4 - A.16.1.5 - A.16.1.6 - A.16.1.7
CONTINUIDAD DE NEGOCIO	Anexo A - controles	A.17.1.1 - A.17.1.2 - A.17.1.3 - A.17.2.1

Table 5 Project original: information-security activity listing

To illustrate how this process deepens into ever more detail and the definition of more activities until it can be considered complete; we are going to focus on the first proper category of the listing, "Information security risk management" (*Gestión de riesgos de securidad de la información*):

GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	ISO 27001	Código	**PS-08**
		Edición	**0**
		Fecha:	28/07/2020

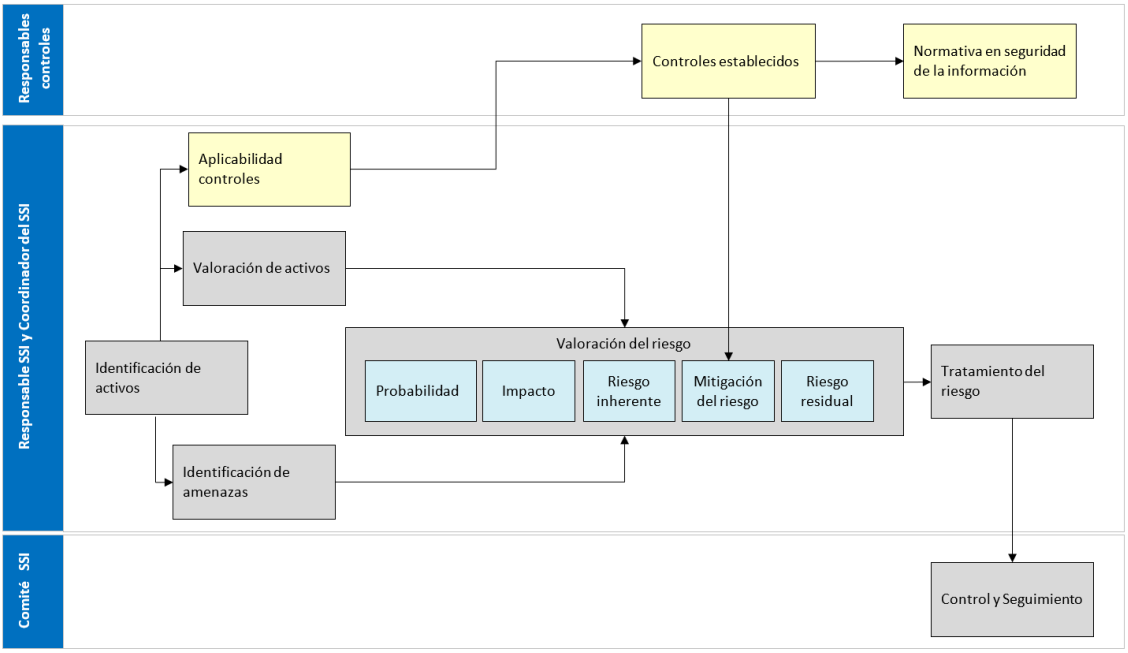

Figure 1 Project original: information-security risk management flow diagram and activity breakdown

Figure 1 illustrates how the task breaks down into a new set of activities that, at the same time, unfold into more actions, "Asset identification" (*Identificación de activos*), "Asset valuation" (*Valoración de activos*), etc.

Each of these actions is properly defined and the file were they originated and were they have been completed and documented are also identified. Thus, the cycle is completed.

Table 6 shows the description and the reference files of the first two activities:

ACTIVIDAD	ENTRADAS	DESCRIPCIÓN DE LA ACTIVIDAD	SALIDAS
Identificación de activos	FC-S08.01 Mapa de riesgos SI *(Información)*	Teniendo en cuenta la tipología de activos y su descripción, se realiza una lista pormenorizada de los activos que se encuentran incluidos dentro del alcance del Sistema de Seguridad de la Información.	FC-S08.01 Mapa de riesgos SI *(Valoración activo)*
Valoración de activos	FC-S08.01 Mapa de riesgos SI *(Información)*	Hay que conocer la importancia de cada activo en la gestión de la información de EXKAL. Para ello, se valora cada activo en las tres dimensiones de la seguridad de la información (confidencialidad, integridad y disponibilidad), se calcula el **valor total del activo** y se clasifica en función del valor resultante. Se realiza, además, una **valoración global de cada dominio (o tipología de activo)**.	FC-S08.01 Mapa de riesgos *(Valoración activo)*

Table 6 Project original: Activity description

All the twenty-eight activities included in the information-security activity listing (Table 5) have had a similar treatment, as have the controls proposed for each of those identified risks. This gives an idea of the nature and the level of complexity of the project.

6.2. MATRIX VALUATION. SCORE ASSIGNMENT

The matrix and its scores feed from various sources of information. On the first hand, from the documentation of the project that, as we have seen in the previous epigraph, can be very thorough. Secondly, from the comments made from the project manager and other important stakeholders of the project. Finally, from the author's own experience during his participation in the project.

The previous example illustrates how the scores in the matrix scale have been assigned.

We have seen a very small portion of the level of detail in which the project has analyzed and decomposed the activity "Information Security Risk Assessment", one of the many activities of the process "Define Activities". As we can imagine, the entire definition of activities in all its depth represents hundreds of pages of documentation. This detailed activity-breakdown and in-depth analysis of each of the components justifies the maximum score (5) assigned to this process for the project.

On the other hand, we saw in chapter four that the ISO/IEC 27001, also mentions repeatedly the importance of the definition of the activities that the project needs to tackle. In particular, clauses four to ten of the standard focus on a list of activities that the standard deems especially important for the purpose of defining and implementing the specific ISMS that each organization needs. Some of the activities mentioned are, understand organization's context, define stakeholders' expectations, define scope, define information security policy, document the

processes, define roles and responsibilities, conduct information security risk assessment and risk treatment, define best treatment controls, provide resources, review system performance, audit ISMS periodically, conduct continual improvement process.

This thorough description of the activities that need to be carried out by the standard merited a score four for the Process "Define Activities" in the matrix.

In the same way, the ISO/IEC 27001 and the project strategy have been measured and evaluated against the 49 processes described in the PMBOK Guide to complete the matrix and to provide the comparison elements for the study.

7. RESULTS

Committed with the decision of the company to introduce PM methodologies, the manager of the ISO/IEC 27001 project faced the challenge of defining the set of PM principles and processes that would be chosen to attain the goals of the project. The first selection came from the recommendations of the standard that, as it has already been said, advocates certain management practices. All those recommendations were adopted.

The next source of knowledge was the PMBOK Guide, from which the manager and his team selected a number of processes they considered directly relevant for the rapid completion of the project. Certain processes that did not have such a direct impact or that were nor pertinent for the project, were discarded. To a certain extent, the choice was also influenced by the need to limit the amount of extra work that would have to be demanded to the participants, none of whom had exclusive dedication to the project.

Standard PM theory recognizes the need to adapt the paradigm, as described by generic bodies of knowledge, such as the Project Management Institute PMBOK Guide (PMI, 2017), to the particularities of project, context and industry (Besner and Hobbs, 2013). The PMBOK Guide also emphasizes the need to determine what is appropriate for each given project.

The analysis of this case study will look into the particularities of the PM strategy adopted in the project and will discuss the consequences of the decisions taken.

The following chart presents a general overview of the processes mentioned and considered relevant in the ISO/IEC 27001 and in the project:

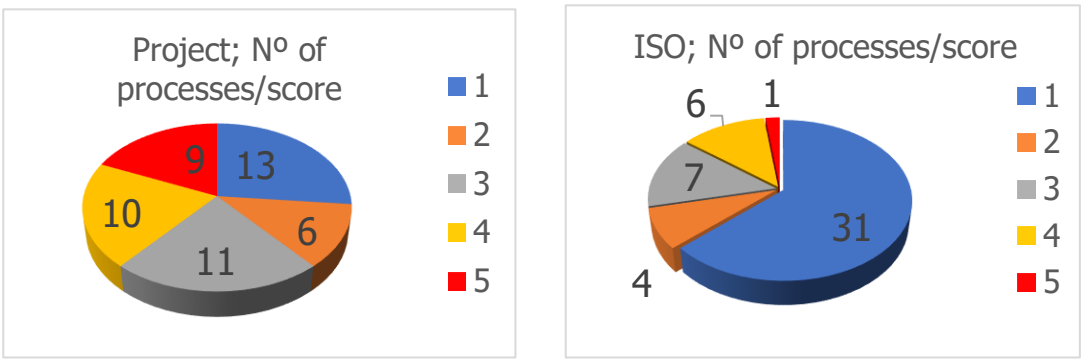

Figure 2 Number of PM processes per score in the project and in the ISO/IEC 27001

It is clear that the ISO focuses in only a minority of very specific processes, as its purpose is not to determine how the project of developing, implementing and certifying the standard should be approached. On the contrary, the project manager, in his endeavor to accomplish his project and in his role as leader of the project, has adopted all the processes considered by the ISO as well as many others from his own choice. However, it is also evident that the project manager has discarded a significant number of processes described in the PMBOK Guide.

The following table compares the score obtained by the processes in the project and the difference of score of those processes in the ISO/IEC 27001.

	Nº of processes with a difference of:					
Project Score	0	1	2	3	4	Total
1	13					**13**
2		6				**6**
3	1	3	7			**11**
4	1	4	1	4		**10**
5	1	5	2		1	**9**
Total	**16**	**18**	**10**	**4**	**1**	

Table 7 Processes grouped by the difference in score between the ISO and the project.

As we can see, in 16 processes, the difference in score between the project and the ISO is cero and in 13 of those cases, neither of them considered the process. On the other hand, in 34 of the 49 processes described in the PMBOK Guide, the difference in the importance accorded to the process by the ISO and the project is cero or one, which shows an important alignment of the project team with the ISO recommendations.

The matrix reveals that the processes described in the PMBOK Guide, once accorded the notations described in the matrix, both for the ISO standard and for the strategy followed by the project team, fall into four main categories:

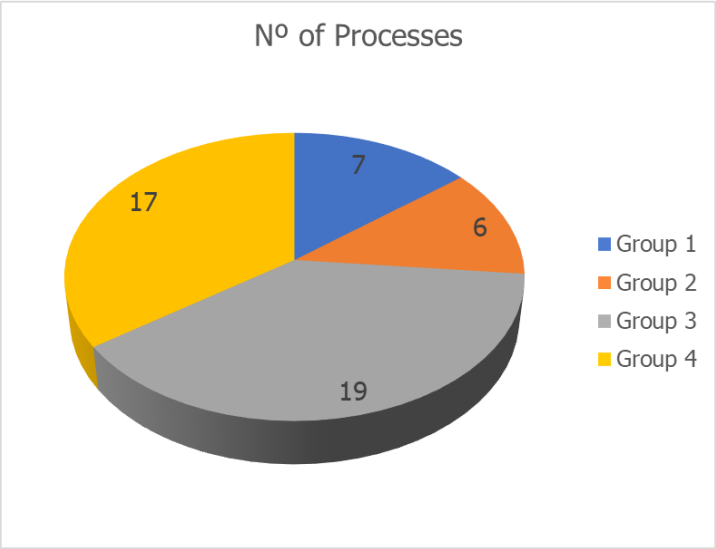

Figure 3 Processes grouped according to their relative scores in the ISO and in the project

Group 1. Processes considered relevant or very relevant by both the ISO and the project (scores four or five in both):

In general, whenever the ISO standard advocates certain management measures the project team follows quite strictly its recommendations. In this sense, the standard determines the strategy. Obviously, when the standard suggests a certain procedure and requests that it should be documented for the certification process, the project managers have little choice.

In the case of seven processes both the ISO and the project have coincided in considering them relevant or very relevant, key, for the successful completion of the project. They are, Identify Stakeholders, Plan Scope Management, Define Scope, Validate Scope, Define Actitivities, Plan Quality Management and Develop Team. In general, they refer to core actions particularly important for the adequate approach to managing the project. Some of the most remarkable refer to such vital elements as the scope of the project, which will be determinant to establish the criteria for the certification, the definition of the activities that will be undertaken to perform the project and the identification of the stakeholders of the project.

The following entries from the matrix reflect the importance attributed by the standard and by the project team to these processes. It is remarkable that in all cases the emphasis attributed by the project team to each of these processes is even higher than that considered by the standard:

Pm Process	1	2	3	4	5	Score	Comments
Define Scope							
Presence in ISO 27001				x		4	- Paragraph 4.3 of the ISO 27001 states that an organization should determine the scope of its ISMS
Presence in the proyect					x	5	- Several meetings were needed to determine the scope of the ISMS - The fifth version of the scope was finally validated and it containsin detail what is going to be included in the ISMS, offices, CDPs, software, hardware, external providers, etc…

Table 8 "Define Scope" process entry in the matrix

Pm Process	1	2	3	4	5	Score	Comments
Plan Scope Management							
Presence in ISO 27001				x		4	- Paragraph 6.1.2 of the ISO 27001 contains guidelines about how the scope of an ISMS should be elaborated
Presence in the proyect					x	5	- The main objective of the project was to achieve the certification against the ISO 27001 and the scope was managed in parallel with the completion of the documentation required for the certification

Table 9 "Plan Scope Management" process entry in the matrix

Pm Process	1	2	3	4	5	Score	Comments
Identify Stakeholders							
Presence in ISO 27001				x		4	- The ISO 27001 stablishes the importance of having the support of the top management - The ISO 27001 does not consider the impact that other stakeholders may have
Presence in the proyect					x	5	- Once the information security risks inventory was completed, all risk owners were identified. - Responsibility for a particular risk could change after further evaluation but no information risk could be registered in the initial inventory without being assigned to a particular stakeholder

Table 10 "Identify Stakeholders" process entry in the matrix

Group 2. Processes not considered by the ISO but regarded as particularly relevant by the project team.

As we have seen, a number of processes were chosen following the recommendations of the standard, and often, the importance attributed to those processes was maximal, however, there is a whole group of processes that were chosen by the project team, despite the fact that the ISO/IEC 27001 does not consider them at all.

There are six processes in which the difference in score between the ISO and the project is 3 or 4 (highest). Significantly, the processes concerned are, Manage Communications, Direct and Manage Project Work, Perform Integrated Change Control, Control Scope and Develop Schedule. All refer to vital aspects of PM determinant for the success of any project. Control of communications, change, scope, schedule and project activities are all core elements of any PM plan.

Here are some of the entries from the matrix:

Pm Process	1	2	3	4	5	Score	Comments
Develop Schedule							
Presence in ISO 27001	x					1	- The ISO 27001 does not provide any guidance to develop a schedule to implement an ISMS
Presence in the proyect				x		4	- Based on knowledge acquired in previous projects and considering past performances of the members of the project team a Gant diagram was developed

Table 11 "Develop Schedule" process entry in the matrix

ACTIVIDADES	2020									
	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4	Semana 1 2 3 4
Fase I: Diagnóstico del Sistema										
Plan de Acción										
Fase II: Elaboración de la documentación del SGSI										
Mapa de riesgos SI										
Documentación Integrada										
Documentación del SGI										
Fase III: Apoyo en la implantación										
Asistencia en la elaboración de registros										
Formación										
Fase IV: Auditoría Interna										
Realización de Auditorías Internas										
Informe de Revisión por la Dirección										
Asistencia Presencial: Plan de Acciones Correctivas (PAC)										

Table 12 Project original: Gantt chart developed by the project team

Pm Process	1	2	3	4	5	Score	Comments
Manage Communications							
Presence in ISO 27001	x					1	- Although the ISO 27001 mentions communication in its section 7.4 it is only in terms of mitigating the information security risks
Presence in the proyect				x		4	- There was no specific action taken to manage communication amongst team members, it was not considered necessary because they were already members of the same department - The deliverables and any other document relevant for the project, used standardized format and were electronically filed in a private server so they were available to all the team - Communication with the consultants was managed via regular meetings and the exchange of information used a shared digital storage device

Table 13 "Manage Communications" process entry in the matrix

Pm Process	1	2	3	4	5	Score	Comments
Perform Integrated Change Control							
Presence in ISO 27001	x					1	- The ISO 27001 does not include indications about for how to introduce changes in the implementation or certification of an ISMS
Presence in the proyect					x	5	- Most project team members were members of the IT department, and automaticaly embraced the integrated change control system used introduce changes in projects developed for other departments

Table 14 "Perform Integrated Change Control" process entry in the matrix

In all those six cases, although the standard does not concede any particular importance to the process, the project team has considered them relevant or very relevant. This management choice, that show how the project manager assumed his role and decided to undertake a number of actions even though they were not included in the suggestions of the ISO, was important for the outcome of the project, in particular, the management of the schedule. According to the project manager, checking the progress against the plan became almost a daily routine.

Group 3. Processes not considered by the ISO nor by the project:

A whole set of processes was not considered either by the ISO/IEC 27001 or by the project team. As a result, they were not incorporated into the project schedule and were not performed. Some were effectively not pertinent, such as the set of processes related to managing and controlling the project budget as, apart from

a minor quantity necessary for the certification process that, by definition, has to be subcontracted, the project did not have external expenses and the internal ones, it was decided, would not be considered. The same could be said about the set of processes related to the managing of procurement, as this aspect had a very minor importance in the project, according to the project manager.

However, there is a whole set of processes that refer specifically to anticipating and managing the risks that the project might face during its lifespan that the standard does not consider and that the project team discarded perhaps too lightly:

Pm Process		Score	Comments
Identify Risks			
Presence in ISO 27001	x	1	- The ISO 27001 greatly emphasizes the importance of identifying possible information security risks as well as their sources but, it does not consider any risk (unrelated to IS) that may threaten the implementation project
Presence in the proyect	x	1	- The project performed risk identification as part of the activities required to develop, implement, and then certificate the ISMS, but no attention was paid to the identification and documentation of eventual risks for the development of the project or their possible sources.

Table 15 "Identify Risks" process entry in the matrix

Pm Process		Score	Comments
Plan Risk Management			
Presence in ISO 27001	x	1	- Although the ISO 27001 extensively covers the subject of risk management for information security and the maintenance of an ISMS, it does not consider what risks may impact its implementation or how to manage them
Presence in the proyect	x	1	- Because of the nature of the ISO 27001 many of the project activities involved risk management (in relation with IS), but there has been no formal treatment of the risks that the project faced in any terms similar to what the PMBOK presents

Table 16 "Plan Risk Management" process entry in the matrix

Lack of project risk anticipation and management had its consequences and the completion of the project was delayed by about two months because of that. A seasonal, and therefore predictable, increase in the demand forced the project team, which do not benefit from the luxury of an exclusive dedication to the project, to shift their attention to their other duties. As a consequence, the project was put on hold for a number of weeks, until production and distribution was able to cope with the orders.

Equally, the project team had to deal with an unexpected delay when certain units, which do not have a particularly close contact with the IT department that managed the project, showed some stubborn resistance to change their habits. The project manager had to invest more time than expected to convince them to accept the new procedures put in place by the project to assure that the information security objectives were attained.

Group 4. Processes considered relevant by the project but not so much by the ISO:

A total of 17 processes that have scored between three and five in the project and between one and three in the ISO, with an average of three point five in the project and two in the ISO. They are generally processes that pertain to some of the knowledge areas that have been considered by the project team, such as Stakeholder, Scope, Schedule, Integration and Quality management. These are knowledge areas that include numerous processes in the PMBOK Guide taxonomy. In this case, the difference can be explained because of the lesser detail provided by the standard when it describes the management procedures that it recommends.

The following figure shows the average score obtained by the ISO and the project in the processes grouped by knowledge areas.

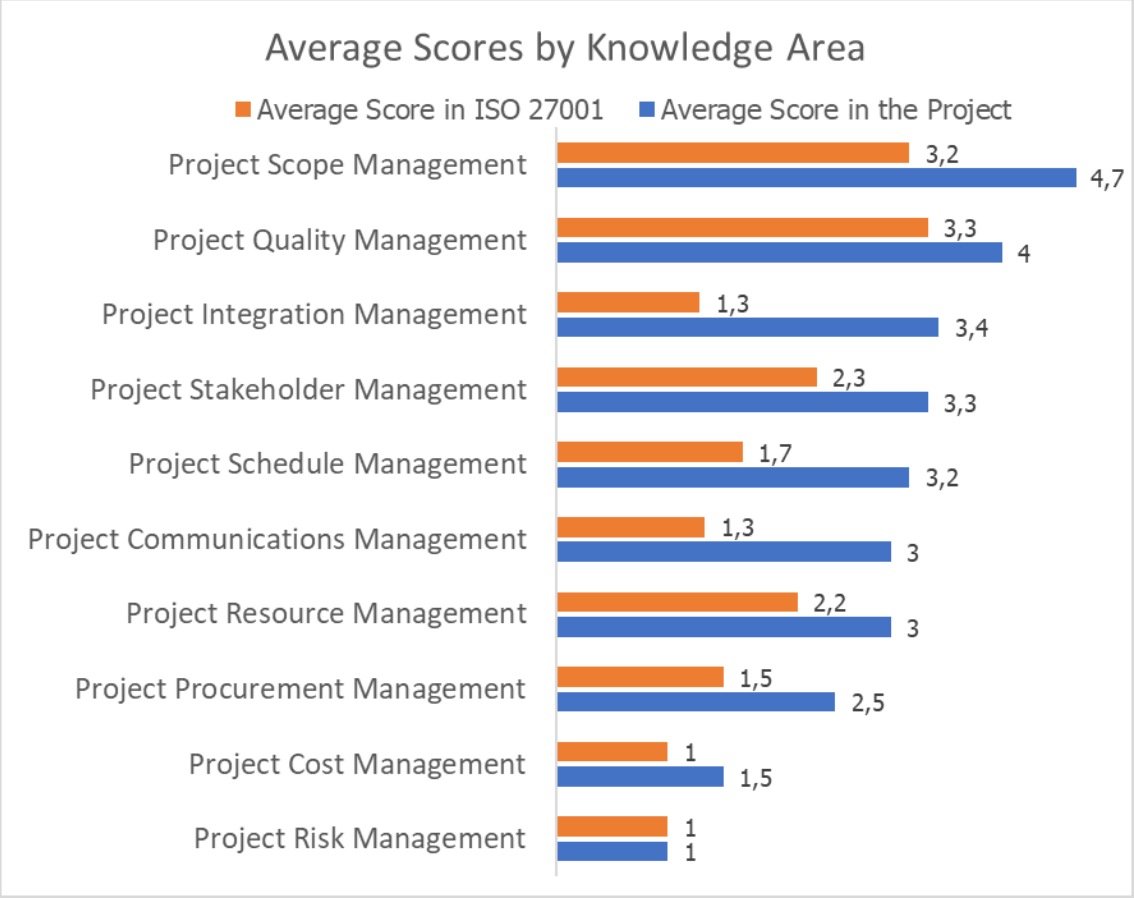

Figure 4 Average scores by knowledge area

As we can see, in all cases but one, the project accorded more importance to the knowledge areas than did the ISO. The knowledge areas with the highest scores coincide more or less in both the project and the ISO. These areas are Scope, Quality and Stakeholder management. Even in these areas that the standard

considers particularly relevant, the project team has gone far beyond, according them the highest importance together with the areas of Integration and Schedule management. This is significant, because all five areas that have had a score above three in the project refer to basic management principles that no project can do without.

Project Communications management and Project Resource management, which have an average score of three in the project, are also vital elements in project management and although the ISO had neglected them somehow, they did receive some important attention by the project team. A possible explanation for their rather low scores in the project might be the fact that most of the project activities were carried out by the members of the IT department whose head also was the project manager and so communications were not perceived as a major challenge. Something similar could be argued about Resource management, as most resources in the project were human resources and they were the members of the IT department.

Interestingly, the three areas that had the lowest scores in both the project and the standard, close to one and always bellow three, Procurement, Cost and Risk management, are related to aspects that were considered irrelevant for the project. Procurement and Cost, effectively, had little or no relevance according to the project manager, as there were hardly any supplies or expenses to consider. However, lack of attention to Risk management did cause the only major problems during the lifespan of the project, as unexpected but predictable circumstances caused a two-month delay in the completion of the project.

Finally, still within a reasonable period of time, the project of defining and implementing an ISMS was considered complete and the certification process was initiated with AENOR, the Spanish certifying body. In the end, the certification was obtained in January 2021 and the project as a whole was considered a success, both by the top managers of the company and by the project team. All the key stakeholders agreed that the introduction of PM procedures had had a major role in this success and the experience was considered an important first step in the new modus operandi and the new culture of the organization.

8. LESSONS LEARNT

PM literature advocates for a hybrid, hard and soft, systems approach to the introduction of PM methodologies (Shi, 2011; Siriram, 2017; Fernandes, et al., 2015). The soft system consists of the environment of the implementation project including the PM culture. The hard system would consist of the traditional implementation strategies, training, PM tools and techniques, etc. Probably the coordination of the soft system and the hard system represents an ideal path to PM implementation in an organization (Shi, 2011). However, in our case study, the circumstances were far from ideal.

Both the company and the project manager were committed to introducing PM principles and methods into the modus operandi and the know-how of the organization, but they lacked the experience and, to a certain extent, even the expertise. To face the challenge, they appealed to the immediate resources available, the ISO/IEC standard itself, with its management recommendations, and the PMBOK Guide. With this guidance and following their own reasoning, they succeeded in completing the project in reasonable time and with minimum cost. The certification was obtained within a year. The project was considered a success and the appeal to PM theories a promising beginning.

- The ISO/IEC 27001 recommendations in terms of PM procedures proved to be extremely useful and paved the way for the selection of a set of procedures presented and described by the PMBOK Guide.
- The PMBOK Guide also proved to be a useful compendium of best practices from which the project manager and his team were able to choose and conform a set of procedures that regulated the development of the project.
- The introduction of PM practices helped motivate and reassure the project team who described an impression of "being in control" during the development of the project.
- The systematic revision and selection of processes as described in the PMBOK Guide helped the project team focus on certain management aspects, such as communications management, that might otherwise have been less carefully approached.
- The lack of experience with certain management practices, such as systematic planning, led to countless revisions and alterations that caused some confusion among the team.
- An excess of zeal to finish the project in the least time possible perhaps led the team manager to discard certain processes, such as the set related to anticipating and managing eventual risks that did have negative

consequences for the development of the project and ultimately caused unnecessary delays.

- The rather amateurish way in which the organization attempted to introduce PM methodologies in its proceedings, probably justified in terms of lack of time and lack of means, did produce some positive results, but surely is no substitute to a proper approach including the soft and hard systems coordination advocated by the aforementioned researchers.

9. CONCLUSIONS

The company and the project manager were committed with the introduction of PM principles in the management of this project. However, this introduction was going to take place in less than ideal conditions, as the company could not afford the time and the resources necessary for a proper integration process including training and the acquisition of PM tools and techniques.

In these circumstances, the project team appealed to the PM recommendations included in the definition of the ISO/IEC 27001 standard and to the PMBOK Guide as a general reference.

The recommendations of the standard proved useful but insufficient. The standard focuses basically in four knowledge areas, Scope, Quality, Stakeholders and Resource management. The project management and his team followed these recommendations with zeal. As the matrix shows, various processes related to these knowledge areas were considered highly relevant: define, plan and validate scope; plan, manage and control quality; identify stakeholders and acquire resources and develop team had a score of four or five in the project. In this sense, it can be concluded that the ISO led the definition of the project team's strategy.

To these four knowledge areas advocated by the ISO, the project team added another three, Integration, Schedule and Communications management. Processes related to these knowledge areas were incorporated to the management of the project, develop project management plan, direct and manage project work and perform integrated change control; define activities and develop schedule, and plan and manage communications also had scores of four or five in the project. In this aspect, the PMBOK Guide proved its capacity as reference to help complete the definition of the strategy.

On the contrary, processes related to three knowledge areas were given minimal relevance, Procurement, Cost and Risk management. According to the project manager, procurement and cost management were indeed minor aspects of the project, as there were minimal supplies or external costs to consider. However, the lack of attention to potential risks for the completion of the project was considered a costly mistake by the project team. Effectively a seasonal, and therefore predictable, increase in the demand forced the project team, which do not benefit from the luxury of an exclusive dedication to the project, to shift their attention to their other duties. As a consequence, the project was put on hold for

a number of weeks, until production and distribution was able to cope with the orders.

In summary, the experience was considered successful by the project manager and by the main stakeholders and the guidance procured by the ISO/IEC 27001 and the PMBOK Guide was highly valued by all the parties involved. The adoption of PM practices was seen as a very important first step towards a systematic change in the culture and the project management practices of the organization.

REFERENCES:

- Andersen, Erling and Jessen, Svein Arne. 2003. "Project maturity in organisations". International Journal of Project Management 21 (2003) 457-461.
- Andersen, Erling and Vaagaasar, Anne L. 2009. "Project Management Improvement Efforts – Creating Project Management Value By Uniqueness or Mainstream Thinking?" Project Management Journal, Vol. 40, Nº 1, 19-27. Available at https://onlinelibrary.wiley.com/
- Asociación Española de Normalización. 2017. Norma Española UNE-EN ISO/IEC 27001. Document owned by the Company. Available through UNE.
- Association for Project Management (APM). 2019. *APM Body of Knowledge*. Seventh edition. Buckinghamshire. United Kingdom. ISBN: 978-1-903494-82-0.
- Ballard, Glenn and Howell, Gregory A. 2003. "Lean project management". Building Research & Information ISSN 0961-3218 print /ISSN 1466-4321 online # 2003 Taylor & Francis Ltd. http://www.tandf.co.uk /journals
- Besner, Claude and Hobbs, Brian. 2013. "Contextualized Project Management Practice: A Cluster Analisys of Practices and Best Practices". Project Management Journal, Vol 44. Nº 1, 17-34. Available at https://onlinelibrary.wiley.com/
- Best, K. 2012. "International standards for project management". Paper presented at PMI® Global Congress 2012—EMEA, Marseilles, France. Newtown Square, PA: Project Management Institute.
- Bredillet, Christophe; Yatim, Faysal and Ruiz, Philippe. 2010. "Project management deployment: The role of cultural factors". International Journal of Project Management 28 (2010) 183–193.
- Burnette, Mark. "Three Tenets of Information Security", 2020. Accessed 12.02.2021. Available at: https://www.lbmc.com/blog/three-tenets-of-information-security/
- De Miguel, Jesús; Marín, Salvador y Mínguez, Raúl (Directores). "Guía sobre seguridad e inteligencia estratégica para PYMES". PDF. Cámara de Comercio de España y Consejo General de Economistas. 2020. Available at: https://www.camara.es/sites/default/files/publicaciones/guia-seguridad-inteligencia-estrategica-pymes.pdf
- Drob, C.; Zichil, V. "Overview regarding the main guidelines, standards and methodologies used in project management". Journal of Engineering Studies and Research. Volume 19 (2013) No. 3. p. 26-31. ISSN: 2068-7559.
- ENISA (European Union Agency for Cybersecurity) "Threat Landscape. The year in review. From January 2019 to April 2020". Accessed 24.02.2021. Available at: https://www.enisa.europa.eu/publications/year-in-review
- Federal Bureau of Investigation. US Government. "2019 Internet Crime Report". Accessed 11.02.2021. Available at: https://www.fbi.gov/news/stories/2019-internet-crime-report-released 021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion.

- Fernandes, Gabriela; Ward, Stephen and Araújo, Madalena. 2013. "Identifying useful project management practices: A mixed methodology approach". International Journal of Information Systems and Project Management. Available at www.sciencesphere.org/ijispm.
- Fernandes, Gabriela; Ward, Stephen and Araújo, Madalena. 2015. "Improving and embedding project management practice in organisations — A qualitative study". International Journal of Project Management 33 (2015) 1052–1067.
- Guasconi, Fabio (Chairman) and Sabatini, Guido (Coordinator). SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security management. Accessed 12.02.2021. Available at: https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-1-1.pdf
- Hoda, Rashina; Noble, James and Marshall, Stuart. 2008. "Agile Project Management". Conference paper. Available at: https://www.researchgate.net/publication/228983124_Agile_Project_Management
- Humphreys, Edward. *Implementing the ISO/IEC 27001 ISMS Standard*, Second Edition. Artech House. Norwood, MA, USA. 2016. ISBN 13: 978-1-60807-930-8.
- *International Standard ISO/IEC 27000. Information technology – security techniques – Information security management systems – Overview and vocabulary*. Geneva. Switzerland. 2018. Available at: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- ISO web page. What is a standard? Accessed 13.02.2021. Available at: https://www.iso.org/standards.html
- ISO/IEC 27000 "Information technology-Security techniques-Information security management systems-Overview and vocabulary". Second edition. 2018
- ISO web site about certification. Accessed 01.03.21. Available at: https://www.iso.org/certification.html
- IT Governance Web Page. The ISO/IEC 27001. Accessed 12.02.2021. Available at: https://www.itgovernance.co.uk/iso27001
- Kliem, R. L., Ludin, I. S., and Robertson, K. L. 1997. *Project management methodology: A guide for the next millennium*. Dekker, New York. ISBN 0-8247-0088-0.
- Kosutic, Dejan. *Seguro y simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios*. Publicado por primera vez por Advisera Expert Solutions Ltd. Zavizanska 12, 10000 Zagreb. Croatia. 2016. ISBN: 978-953-57452-7-3. Available at: https://www.isms.online/iso-27001/#:~:text=ISO%2FIEC%2027001%3A2013%20is,the%20bottom%20of%20the%20page).
- Martinsuo, Miia and Huemann, Martina. 2020. "The basics of writing a paper for the International Journal of Project Management". International Journal of Project Management. Volume 38, Issue 6, August 2020, Pages 340-342.
- Müller, Ralf; Pemsel, Sofia and Shao, Jingting. 2014. "Organizational enablers for governance and governmentality ofprojects: A literature review". International Journal of Project Management 32 (2014) 1309–1320.
- National Crime Agency. National Cyber Security Centre, The cyber threat to UK business. 2017-2018 Report. Accessed 11.02.2021. Available at: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/178-the-cyber-threat-to-uk-business-2017-18/file
- Papke-Shields, Karen E. and Boyer-Wright, Kathleen M. 2017. "Strategic planning characteristics applied to project management". International Journal of Project Management. Volume 38, Issue 6, August 2020, Pages 340-342.

- Project Management Institute (PMI). 2017. *A guide to the project management body of knowledge. PMBOK Guide*. Sixth edition. Newton Square. PA. 2017. ISBN 9781628251845 (paperback).
- Project Management Institute. *Success in Disruptive Times. Expanding the Value Delivery Landscape to Address the High Cost of Low performance.* 2018. Available at: https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf
- Sadeq Alturfi. *Best Practice Project management for the Sustainable Regeneration of Holy Karbala Province in Iraq* (PhD Thesis). UK: The University of Bolton. May 2017. Chapter Two: "Project Management". p 9-66. Accessed 09.03.2021. Available at: https://www.researchgate.net/profile/Sadeq-Al-Turfi/publication/328677271_Project_Management_literature_Review/links/5bdb96f192851c6b27a05b63/Project-Management-literature-Review.pdf
- Shi, Qian. 2011. "Rethinking the implementation of project management: A Value Adding Path Map approach". International Journal of Project Management 29 (2011) 295–302.
- Simard, Magali; Aubry, Monique and Laberge, Danielle. 2018. "The utopia of order versus chaos: A conceptual framework for governance, organizational design and governmentality in projects". International Journal of Project Management 36 (2018) 460–473.
- Sliger, M. 2011. "Agile project management with Scrum". Paper presented at PMI® Global Congress 2011—North America, Dallas, TX. Newtown Square, PA: Project Management Institute.
- Tjahjono, B.; Ball, P.; Vitanov, V. I.; Scorzafave, C.; Nogueira, J.; Calleja, J.; Minguet, M.; Narasimha, L.; Rivas, A.; Srivastava, A.; Srivastava, S. and Yadav, A. 2010. "Six Sigma: a litterature review". International Journal of Lean Six Sigma · August 2010. Available at: https://www.researchgate.net/publication/235262819_Six_Sigma_a_literature_review
- Turner, J. Rodney. 2014. *The Handbook of Project Based Management: Leading Strategic Change in Organizations*. Fourth Edition, 2014. McGraw-Hill Education. ISBN-13: 978-0071821780.
- Ungureanu, Adrian and Ungureanu, Anca. 2014. "Methodologies used in Project Management". Annals of Spiru Haret University Economic Series. 14. 47. ISSN 2393-1795.