Project Management approach to the implementation of an ISMS and its certification against the ISO/IEC 27001

Author: Guillermo de Basterretxea Ibilcieta

Director: Iñaki Zuazo Urionabarrenetxea

Abstract

The literature on Project Management (PM) emphasizes the importance of adapting the paradigm, as described by such comprehensive bodies of knowledge as the PMBOK Guide (PMI, 2017), to each particular situation, taking into account the specificities of context, industry and, of course, the project itself.

This paper analyzes the PM processes completed during the implementation of the ISO/IEC 27001 information security standard in a medium size company, and discusses the adequacy of the choice of processes adopted and discarded, by means of a contrastive matrix that confronts classic PM processes, the ISO recommendations and the strategy followed by the project team.

The results confirm that despite some inconsistencies in the strategy, the application of PM theory had a significant impact in the success of the project.

Keywords

Project management practices and processes, ISO standard, information security

1. Introduction

PM literature describes the importance that the discipline has acquired in organizations worldwide (Midler, 1995; Munns and Bjermi, 1996; Simard et al., 2018). The acquisition of this kind of competence and expertise has become a priority for companies that seek to expand and consolidate their position in their industry.

On the other hand, case studies have highlighted the need to adapt PM 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.

2. Literature survey

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.

Finally, K. Best (2012) has highlighted the shared views about PM between the International Organization for Standardization (ISO) and the Project Management Institute (PMI). In fact, when the ISO developed its PM standard, the ISO/21500 *Project, programme and portfolio management — Context and concepts*, 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.

3. Case study

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 information security management system (ISMS) against the ISO/IEC 27001 standard.

The goal of the study is to verify the impact of the PM 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.

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. The security of assets such as intellectual property, financial information, personal data or information entrusted by third parties has become critical for organizations.

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.

Organizations need to consider the impact the way they manage information security can have in the network environment in which they operate. In the global market, business operations require the participation of numerous stakeholders who inevitably share valuable 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.

4.1. Information Security Management System

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 and other controls involving people, processes and technology, managed by an organization to protect its information activities (ISO /IEC 27000: 2018, 11).

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.

5. Methodological framework

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.

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). It is important to remember that, at least to a certain extent, the standards defined by the International Organization for Standardization (ISO) share many of the principles of PM methodology.

The comparison has been carried out through a matrix 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

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

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 1. Matrix entry for PM process "Develop project charter".

The 49 processes described in the PMBOK Guide have been studied similarly in the matrix, so that it facilitates the analysis and the drawing of conclusions as most of the relevant information is readily available.

The purpose of the matrix is to facilitate the analysis and the drawing of conclusions by presenting the data in a practical way.

6. Results

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

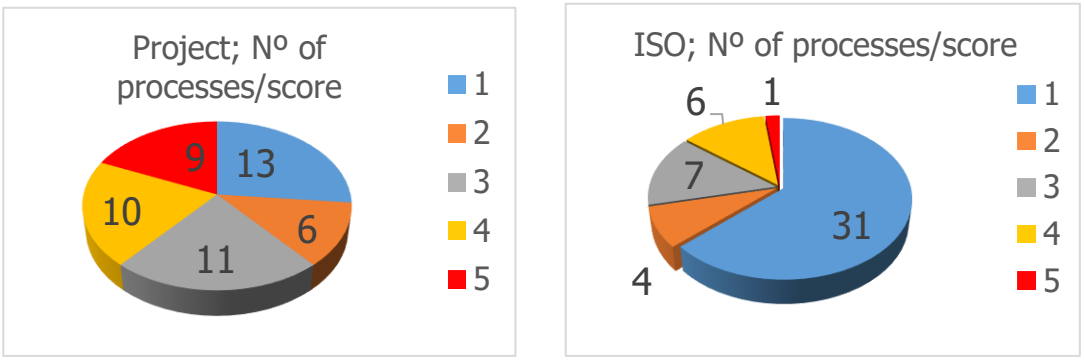

Fig. 1. Number of PM processes per score in the project and in the ISO/IEC 27001

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. Therefore, of the 49 processes, 31 are not even mentioned in the definition of the standard. On the contrary, the project manager, in his endeavor to accomplish his project, has adopted all the processes considered by the ISO as well as many others of his own choice. However, it is also evident that the project manager has discarded a significant number of processes described in the PMBOK Guide. Thirteen processes are not mentioned, and six other processes are considered of minor importance.

The table below 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 2. Analysis of the differences in score for each process 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 above, both for the ISO standard and for the strategy followed by the project team, fall into four main categories:

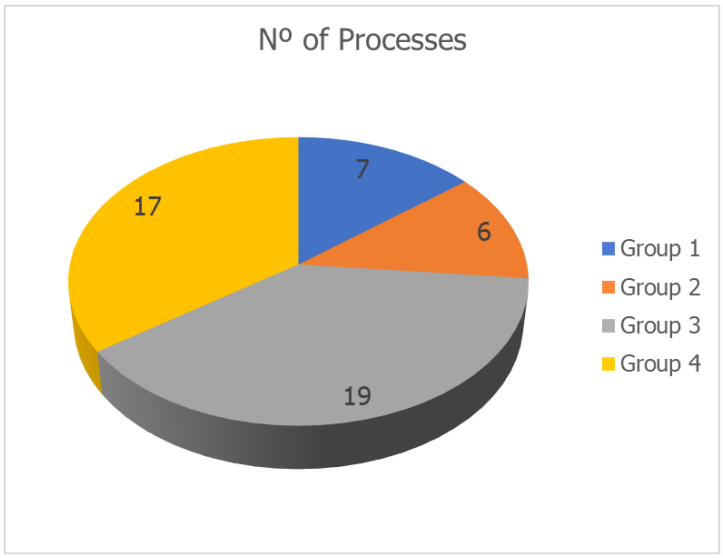

Fig. 2. Processes grouped according to their relative scores in the ISO and in the project

Group 1. Processes considered relevant or very relevant by both the ISO and the project:

The processes Identify Stakeholders, Plan Scope Management, Define Scope, Validate Scope, Define Actitivities, Plan Quality Management and Develop Team have scored four or five in both the ISO and the project. They 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. It is not a surprise that the project team did follow the recommendations of the standard when it suggested that certain processes were particularly relevant.

Group 2. Processes not considered al all by the ISO but regarded as very important by the project team.

There are six processes in which the difference in score between the ISO and the project is three or four (maximal). Significantly, the processes concerned are, Manage communications, Direct and Manage project work, Perform integrated change control, Control scope and Develop schedule:

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.

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

Very significantly, there is a whole set of processes with scores of one or two in both the ISO and the project. They 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. In addition, neither of them value the set of processes related to Cost and Procurement management.

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

A total of 17 processes 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 and Quality management.

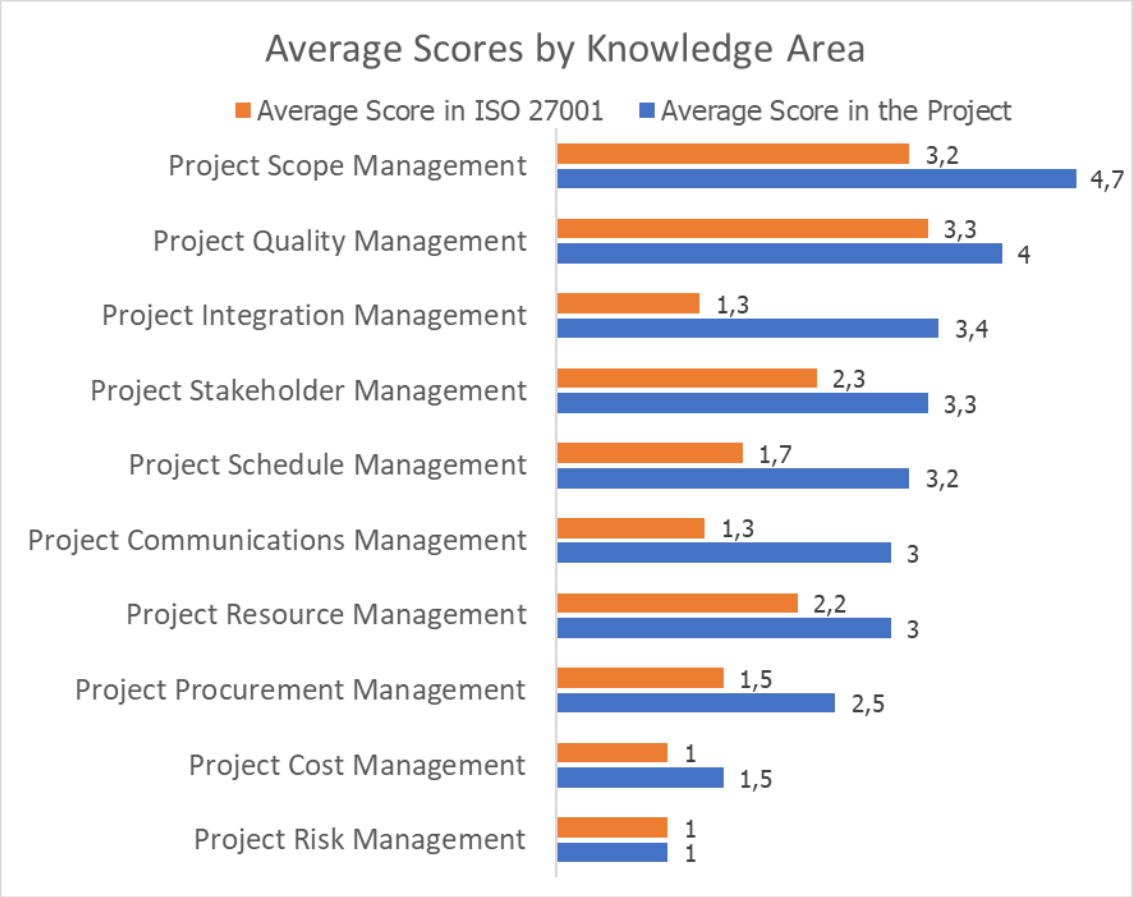

Fig. 3. Average scores by knowledge area

As we can see, with the processes grouped by knowledge areas, on average, in all cases but one, the project accorded more importance to the processes than did the ISO. The knowledge areas with the highest scores coincide 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.

7. 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/
- 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.
- 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.
- 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.

- Midler, Christophe. 1995. ""Projectification" of the firm: The renault case". Scandinavian Journal of Management. Volume 11, Issue 4, December 1995, Pages 363-375.
- Mir, Farzana Asad and Pinnington, Ashly H. 2014. "Exploring the value of project management: Linking project management performance and project success". International Journal of Project Management 32 (2014) 202-217.
- Munns, A.K. and Bjermi, B.F. 1996. "The role of project management in achieving project success". International Journal of Project Management. Volume 14, Issue 2, April 1996, Pages 81-87.
- Pace, Michael. 2019. "A Correlational Study on Project Management Methodology and Project Success". Journal of Engineering, Project and Production Management. July 2019 DOI: 10.2478/jeppm-2019-0007.
- 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).
- 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.
- Siriram, Raj. 2017. "A Hybrid (Soft and Hard) Systems Approach to Project Management". SSRG International Journal of Industrial Engineering (SSRG-IJIE) – Volume 4 Issue 3 – Sep to Dec 2017. ISSN 2349 – 9362.
- Thomas, J. and Mullally, M. 2007. "Understanding the value of project management: first steps on an international investigation in search of value". Project Management Journal 38 (3). 74-89.