Journal of *Cybersecurity and Privacy*

MDPI

Article

Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal

Mário Antunes [1,2,*], Marisa Maximiano [1], Ricardo Gomes [3] and Daniel Pinto [3]

[1] Computer Science and Communication Research Centre (CIIC), School of Technology and Management, Polytechnic of Leiria, 2411-901 Leiria, Portugal; marisa.maximiano@ipleiria.pt
[2] INESC TEC, CRACS, 4200-465 Porto, Portugal
[3] School of Technology and Management, Polytechnic of Leiria, 2411-901 Leiria, Portugal; ricardo.p.gomes@ipleiria.pt (R.G.); daniel.m.pinto@ipleiria.pt (D.P.)
* Correspondence: mario.antunes@ipleiria.pt

Abstract: Information security plays a key role in enterprises management, as it deals with the confidentiality, privacy, integrity, and availability of one of their most valuable resources: data and information. Small and Medium-sized enterprises (SME) are seen as a blind spot in information security and cybersecurity management, which is mainly due to their size, regional and familiar scope, and financial resources. This paper presents an information security and cybersecurity management project, in which a methodology based on the well-known ISO-27001:2013 standard was designed and implemented in fifty SMEs that were located in the center region of Portugal. The project was conducted by a business association located at the center of Portugal and mainly participated by SMEs. The Polytechnic of Leiria and an IT auditing/consulting team were the other two entities that participated on the project. The characterisation of the participating enterprises, the ISO-27001:2013 based methodology developed and implemented in SMEs, as well as the results obtained in this case study, are depicted and analysed in the paper. The attained results show a clear benefit to the audited and intervened SMEs, being mainly attested by the increasing of their information security management robustness and collaborators' cyberawareness.

Keywords: information security; cybersecurity; small and medium-sized enterprises; ISO-27001:2013; auditing

check for updates

Citation: Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. *J. Cybersecur. Priv.* **2021**, *1*, 219–238. https://doi.org/10.3390/jcp1020012

Academic Editor: Nour Moustafa

Received: 16 February 2021
Accepted: 6 April 2021
Published: 8 April 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Enterprises have increased their level of consciousness regarding cybersecurity and information security management, as it has been assumed that these are relevant issues regarding competitiveness and survival in global markets [1,2]. The importance that has been gained by information security and cybersecurity management in enterprises worldwide has been enormous. On one hand, management boards are becoming aware about the need to protect data and information [3] and, on the other hand, cyberattacks are booming, as documented by worldwide cybersecurity institutions [4], and the level of consciousness about the need to implement countermeasures have comprehensively increased [3]. The COVID-19 pandemic has also had a detrimental impact in cybersecurity world wide, as more collaborators are working from home, which led to accelerate digital transformation in enterprises [5,6].

Small and Medium-sized Enterprises (SMEs) play a key-role in economy, as they represent a large band of the wealth produced worldwide [7,8]. However, their intrinsic characteristics, namely their small dimension, the fact that they are grounded on traditional and familiar structures, and their financial resources typology [9], put them in a second plan in what information security and cybersecurity awareness concerns. The difficulties in accessing funded projects for cybersecurity, the collaborators' level of cyberawareness, and

the eventual lack of resident Information Technology (IT) staff are also important issues regarding the implementation of best practices in cybersecurity [10–12].

This paper presents the results that were obtained with the implementation of an information security and cybersecurity management project, funded by IAPMEI though an European funding for regional development, and promoted by NERLEI (https://www.nerlei.pt/en/home, accessed on 7 April 2021), a business association located in Leiria that has about two thousands affiliated SMEs and micro enterprises. The project, named "Log In Innovation" (https://www.logininnovation.pt/projeto, accessed on 7 April 2021), aims to implement a digital transformation process in SMEs that may boost their competitiveness in global markets. Besides information security and cybersecurity, the project has four additional core axes: lean manufacturing, balanced scoreboard, digital marketing, and quality management. The total amount of the project is around 1,304,000.00 € and it plans to cover a total of 80 eligible SMEs operating in the following Portuguese regions: North, Center, and Alentejo. Regarding information security and cybersecurity, fifty SMEs, mainly from the center of Portugal, and operating in several activity areas, benefitting from the interventions realised.

The project was implemented in the period between 2018–2020 and it embodied the following entities: NERLEI, Polytechnic of Leiria (https://www.ipleiria.pt/home/, accessed on 7 April 2021), a consulting company, and the SMEs. Regarding information security, the overall results achieved by the project are two-fold. Firstly, to give the the companies the opportunity to increase their level of cyberawareness and competitiveness, and to help mitigate some of their organisational, IT, and human resources flaws, by applying the funding available for cybersecurity management. Secondly, at a regional level and involving solely local partners and SMEs, to strength the cooperation between a business association, academia, and a consulting team working together, to foster cybersecurity in SMEs and mitigate their information security flaws.

The paper is organised, as follows. Section 2 summarises the fundamentals of information security and cybersecurity, the standard ISO-27001:2013 and the most relevant case studies on information security in SMEs. Section 3 describes the project and the methodology developed to apply ISO-27001:2013 in SMEs. Section 4 depicts the results obtained in the project, that are analysed and discussed in Section 5. Finally, Section 6 presents the relevant conclusions to the project and delineates some directions for future work.

2. Literature Review

This Section concisely describes the literature review that is relevant to the overall paper understanding. Section 2.1 focus on the fundamentals of the information security and cybersecurity management. Section 2.2 summarises the ISO-27001:2013 framework, namely its relevance, scope, and general organisation. Section 2.3 summarises a list of similar case studies, being related to the implementation of information security projects in SMEs.

2.1. Information Security Management and Cybersecurity

Nowadays, information security is an important concern to all businesses, as they operate in a global market, are highly IT dependent, and have a fully online and digital presence. Information security management is a crucial challenge for the companies, as they aim to prevent the exposure to security and privacy threats to information systems and networking infrastructure. Although many of SMEs may have a minimal IT infrastructure to fight cyberattacks [13,14], they can act on a preliminary phase in order to gradually improve their security level. Therefore, organisations must ensure that their businesses processes, policies, and workforce behaviour allow them to minimize and mitigate some of the risks that are involved in their information systems and IT infrastructures [15,16].

Confidentiality, integrity, and availability, which are also known as the CIA triad [17], is a design model to define organisations' policies for information security [18]. Because data are to many of the operations inside an organisation, its confidentiality is a major

concern, requiring that a set of procedures and rules inside the organisation must be applied to define who and whom has access to the data and information. Integrity and availability focus on the data trustworthiness and accuracy accessed by authorised people. Hence, information security standards and frameworks are grounded on the implementation of policies and controls, to manage security and risks at an organisational level.

The best practices inside an organisation are vital and they represent the front line inside information security. The definition of cybersecurity policies should be the first challenge to protect organisational data and define procedures to be followed. The aim is to define a level of protection to assure that organisational data and networks are safe and secure. SMEs may not be able to afford implementing complex and costly effective security procedures, which may make them more vulnerable to cyberattacks and with less controls inside the organisation, as pointed out by several authors [19–22]. Promoting educational activities inside an organisation should be the first step in contributing to collaborators' cybersecurity awareness and helping to protect organisational data and operation [23].

2.2. Standard ISO-27001:2013

ISO-27001:2013 [24] is an international standard that defines a list of controls that are to be considered in the implementation of an Information Security Management Systems (ISMS) [25]. Because organisations of all types and sizes collect, process, store, and transmit data and information, electronically, physically, and verbally, the standard was designed to be used as a reference and a proposal of best practices, when implementing an ISMS in a wide set of scenarios and businesses.

The ISO-27001:2013 standard [24] defines 114 controls, grouped into 14 thematic categories. Each control is analysed, and a score is assigned, according to its level of conformity. A control can be in three distinct states: fail, pass, or not applicable. A control that fails means that it has a level of conformity of 0%. A control that passes means that it is accepted with an acceptance level above 0%, which should be the highest possible. The control may also not be applicable to the enterprise being audited, as it is not relevant in the scope of its activity or organisation.

The project memorandum also defined two distinct auditing types to be considered within the scope of the project, namely "Type 1" and "Type 2". Although both types are detailed in Section 3, a general definition is as follows. Type 1 auditing, which is also termed "Standard", is composed of subset of 30 controls and only these will be analysed and mitigated. In the Type 2 auditing, also named as "Full", all of the 114 controls are going to be analysed and those that did not pass are mitigated. Table 1 shows the list of categories considered in each auditing typology of the project.

Table 1. Identification of the categories considered to "Type 1" and "Type 2" auditing.

Categories	Type 1—Standard	Type 2—Full
(A.5) Information security policies	X	X
(A.6) Organization of information security.		X
(A.7) Human resource security		X
(A.8) Asset management	X	X
(A.9) Access control	X	X
(A.10) Cryptography	X	X
(A.11) Physical and environmental security		X
(A.12) Operations security	X	X
(A.13) Communications security	X	X
(A.14) System acquisition, development and maintenance	X	X
(A.15) Supplier relationships		X
(A.16) Information security incident management		X
(A.17) Information security aspects of BCM		X
(A.18) Compliance	X	X

Information security is addressed inside an organisation when cybersecurity challenges emerge and, therefore, a set of procedures is defined to answer to controls demands, namely policies, processes, procedures, organisation structures, software, and hardware functions. By establishing, implementing, and monitoring these controls, a higher level of awareness toward the importance of security and business objectives of the organisation are met.

The ISO-27001:2013 belongs to a family of Information Security Standards. One of the core concepts of ISO-27001 is to identify information security risk and to further apply the appropriate controls that can evaluate and mitigate the risk. Under this family of standards, the ISO-27005 [26] describes risk management methods. Interrelated to cybersecurity, the ISO-27037 [27] defines guidelines that are related to security techniques that may identify, collect, acquire, and preserve a digital evidence.

2.3. Case Studies and Related Work

IT infrastructure has become a very critical asset in SMEs operations as a whole. The increasing of cyberthreats in SMEs has raised the management boards' consciousness about the need and importance of dealing with the risk that is involved with the overall dependencies of business on information systems. A comprehensive set of related case studies regarding information security and cybersecurity management in SMEs is described below.

Javaid et al. [28] point out the fact that the standards available are scarce and usually focused on large companies, who have a well-structured business process to some extent. The authors proceed to point out that the available standards are too generic or too specific to some specific business domains. Therefore, they proposed an approach on how to apply risk management in information systems on SMEs, by analysing the available standards and their integration with various risk management frameworks.

Saravanan et al. [29] evaluate the extent of the impact of measures (controls) applied to cybersecurity threats as a preventive control in SMEs. The focus was on identifying ISMSs to provide a systematic approach to manage sensitive data in terms of maintaining its confidentiality, integrity, and authentication. The outcomes have allowed the SMEs to determine which ISO-27001:2013 practices are more suitable to use. Wanyonyi [30] analysed the ISO-27001:2013 standard and a toolkit was proposed to help SMEs implement the requirements of the standard. The aim of this toolkit was to guide SMEs to implement and evaluate the ISO-27001:2013 controls.

Several works addressing cybersecurity threats and information security have been published [31]. They explore three distinct goals: to raise awareness on information security; to evaluate how ISO-27001:2013 standard may be used to improve the assets protection and, at same time, to identify the risk they are exposed to; to guide SMEs on the adoption of ISO-27001:2013 standard; and, to improve information security and cybersecurity.

Having in mind the increasing cybersecurity risks and their impact to SMEs, in [32], the authors propose an approach for SMEs to assess and improve their cybersecurity capabilities, by integrating key elements from existing industry standards. The results were obtained by defining an assessment questionnaire; however, validation and monitoring of its applicability in real-world implementations is required.

Ponsard et al. [33] try to develop a cybersecurity label for SMEs supported and accredited by third party cybersecurity risk experts. The defined goals were to raise the awareness of SMEs to the risks that they are facing in European countries. In [34], the same authors present a case study that is focused on the evolution of a Belgian program that is related to good practices of self-assessment to a lightweight certification scheme fitting the needs and capabilities of SMEs.

Furthermore, a case study in the UK [35,36] investigates the possible reasons for SMEs apparent lack of interest in securing data, or developing information security management systems. The authors focus on cyber liability insurance, which provides the basis for a cost-effective solution to encourage good information assurance across the SMEs supply chain, by protecting their own data and the data that they share with the supply chain

partners. A different case study in UK from Rae et al. [37] addresses the increasing amount of cyberattacks and threats for SMEs and identifies the influencing factors that are needed to improve security behaviours and engagements with information security best practices. The authors propose a cybersecurity rating scheme for SMEs in the UK, with the potential to scale internationally.

Overall, the increasing of cyberattacks towards SMEs brings to light specific information security and cybersecurity standards and guidelines that are grounded on well-known best practices that are being developed. In Belgium [38] a survey was implemented to compare different initiatives, aiming to enable a long-term convergence with a European scheme. Their outcomes allowed for reporting some findings regarding how to set up the overall organisational structures, basic management processes, and some supporting tools for SMEs. In [11,39,40], Ozkan et al. describe several information security and maturity models that can be applied to SMEs characteristics, in which ISO-27001:2013 is one of the available frameworks.

The key factors that influence SMEs cybersecurity practices in the technological innovation era were studied on three SMEs of industrial services in Thailand [41]. A qualitative approach was used to collect data to access insights and a decision-support framework was deployed.

Mubarak et al. [42] described a systematic literature review on information security in SMEs, highlighting that one of the proven ways to manage information security is through applying available international standards, frameworks, and best practices. Due to the difficulty of developing and applying a model to address SMEs needs, a systematic review was presented as one of the analytic phases of a project in which different models were analysed. It was shown that most of the models are theoretically conceived, and there is a need to find a suitable model that could be better applicable to SMEs.

An easy-to-use cybersecurity canvas was modelled and proposed by Teufel et al. [43] to allow SMEs pragmatic access to protect their valuable data against cyberattacks. The framework is made of building blocks that can be put individually according to the SMEs requirements and needs. It has been put through an application test with a European SME, which was well received by the participants. Finally, in [44], the author suggests that there are additional issues for SMEs being more often cyberattacked than larger enterprises. The authors propose a theoretical framework for cybersecurity that comprises organisational, technological, and psychological issues, with the insights being analysed based on the data collected from interviews with IT professionals.

Information security frameworks and standards are crucial in improving cybersecurity and minimizing the risk in enterprises. Small Business Standards (SBS) defined a guide to implement ISO-27001:2013 in the context of SMEs information security [45,46]. In the project described in this paper, a ISO-27001:2013 based methodology was defined and implemented in the participating SMEs, following the trends and recommendations that were observed on the adoption of information security frameworks. The number of SMEs involved in the project and the positive impact on their information security and cybersecurity awareness give a higher confidence level regarding the outcomes of the project.

3. Methodology Based on ISO-27001:2013

This Section describes the ISO-27001:2013 based methodology that was adopted in the project, namely the adjustments made to accommodate the original guideline into an SME context, the checklists, and templates to be used by the auditing team. Section 3.1 describes the auditing types that were defined in the scope of this project. Section 3.2 describes the documents that were designed in the scope of the project and illustrates the auditing checklist and templates. Section 3.3 summarises the web-based application developed to collect auditing interventions data, which was used to produce the results that are presented and analysed in Sections 4 and 5.

3.1. Auditing and Intervention Types

The memorandum of the project considers two types of auditing and intervention, based on the ISO-27001:2013 standard, namely "Type 1" (standard) implementation with thirty controls being evaluated, and "Type 2" (full) implementation composed by the whole 114 controls (see Table 1). The idea behind the use of these two typologies was to define two distinct intervention paths, according to the SMEs' profile. Type 1 auditing was directed towards enterprises whose aim was to obtain an initial diagnosis of the cybersecurity risk, and to correct the identified flaws as much as possible. Type 2 was mainly chosen by SMEs with the aim to audit a vast number of controls and reevaluate the corrective measures applied to have at least 60% of compliance with the standard. The funding available for the enterprises that enrolled in each typology was different, as well as the minimum self-investment that each enterprise had to have.

Table 1 (Section 2.2) lists the *a priori* ISO-27001:2013 categories that were considered in each one of the auditing types. Type 1 auditing encompassed a subset of around 25% of the ISO-27001:2013 categories, which corresponds to 30 controls of the 114 available. The selected 30 controls have a wide range and they can be applied in a multitude of SMEs. It is worth noting that most of the intervened SMEs are going through an information security auditing for the first time and, thus, the selected controls tried to focus on the most fundamental issues of the ISO-27001:2013 standard, not imposing a high level of complexity and procedural maturity that this type of enterprises may not have.

More specifically, in Type 1, the categories, and the corresponding controls, were chosen based on the following general presuppositions:

- No need to acquire infrastructural components, like buildings or specific networking infrastructure components.
- SMEs do not have to have a formal corporate and/or human resources structure in the organisation.
- The selected controls should be directed towards the evaluation and mitigation of the most common cyberattacks described previously.
- There is no need to implement disaster recovery and business continuity procedures, as small businesses and enterprises that chose Type 1 intervention do not have these issues as the main priority.
- Because most of the SMEs in the project do not have a strong business process model representation, the controls included in the proposed methodology tried not to impose a mandatory and existing formal organisation inside the SMEs.
- For some of the SMEs, the aim of their participation in the project was to allow a preliminary check-up of their organisational and security procedures. Therefore, the controls that were included in the Type 1 audit allow for addressing some of the most basic issues without forcing a pre-existence of a formal business and complex IT infrastructure.

For this type of intervention, it was established that no re-evaluation process would be done, and all of the identified flaws were tentatively mitigated during the auditing process. The commitment was to make all of the efforts to have all the controls passed with the highest conformity level, decreasing the risk, and increasing the level of information security. An auditing report was delivered to each SME with the evaluation made, namely the identification of flaws, the countermeasures applied, and a list of recommendations for further interventions.

Cyberthreats are agnostic and they may affect the enterprises as a whole. However, SMEs are prone to be more intensively affected by some specific cyberthreats and attacks, in comparison to larger enterprises. The list below itemizes those cyberthreats, according to the literature [4,8,45,46], and how the ISO-27001:2013 framework and the defined methodology can mitigate them:

- Social engineering attacks, namely phishing, malware, mobile malware, and ransomware.
- Policy management threats, namely weak passwords and inadequate authentication mechanisms and access controls.

- Insider threats, promoted by employees, former employees, business contractors, or associates.
- Hardware based threats, namely the personal electronic equipment used by the collaborators, and those that support the information system and related IT services. Some examples are web servers and database servers.
- Software threads, related with third party applications installed in the SMEs information system.
- Distributed Denial of Service (DDoS) with a higher impact in SMEs that have a big online presence.
- Employees can take advantage of privileged or confidential information to access company resources and steal from or disrupt the business.
- External hackers are not the only cybersecurity threat. A failure to comply with security procedures can lead workers to unintentionally expose an organisation to a cyberattack.

ISO-27001:2013 has a wide scope, being spread by the 14 categories and their 114 controls. Both typologies defined in this project have a set of controls to evaluate the risk SMEs face regarding the cyberthreats described below.

In the Type 2 intervention, the actions that were defined for the 114 were applied and, for those that do not fully passed, countermeasures were defined and applied to reduce the cybersecurity risk. In this audit type, a re-evaluation process was made after the countermeasures were implemented, with the aim to have at least 60% of the controls passed and with the highest level of conformity with the ISO-27001:2013 standard. In this intervention type, SMEs received an intermediate report with the initial diagnostics, and a final report with the evaluation made after the implementation of the proposed list of corrective measures.

For both of the auditing types, the implemented methodology had the following main goals in mind:

1. To apply an auditing checklist, actions and countermeasures lists considered the philosophy behind SMEs functioning and behaviour.
2. To criteriously systematize controls, actions, and corrective measures.
3. To avoid the redundancy between contiguous and/or similar controls.

It is worth noting that, in both auditing types, the enterprises did not become fully prepared to be submitted to an ISO-27001:2013 certification process, and that was not a goal for the project. However, some of the intervened SMEs were in an advanced stage for that purpose. The subset of controls picked in Type 1 auditing does not include controls that are hard to comply in companies that do not have specific business structures, like a HR department, or technical equipment, like a dedicated computer network infrastructure.

3.2. Checklists and Templates

A comprehensive set of documents were produced in the scope of this project, namely:

1. An auditing checklist implemented for each control. The checklist has the instructions that should be followed by the auditing team to assess and validate the control inside the ISMS scope.
2. A list of mitigation activities. For each control, a list of mitigation actions is proposed to be further implemented by SMEs in a control failure scenario.
3. Templates for addressing mitigation measures. A set of templates were proposed to collect information about assets and policies. As an example, a template was defined to collect information regarding the mobile devices that are in use in SMEs.
4. Auditing reports that summarise the results of the auditing processes. The reports are generated by the web-based application, and they can be used by the management board, to evaluate the current position towards cybersecurity and define future improvements.

3.3. Application to Collect Auditing Data

The auditing process, namely the collection of evidences, the automatic processing of auditing reports, and the results analysis, were made available in a web-based application that was developed for this project. It is possible to find a wide set of applications and tools (mostly in Excel files) that allow for the collection and processing of ISO-27001:2013 interventions. However, those tools are mostly devoted to generic and usually large companies in the scope of an ISO-27001:2013 certification process.

The web-based application is versatile and customizable, as it receives a predefined checklist, actions, and mitigation lists. The whole auditing process is stored through the application, starting by the auditing and interventions records, going through the intermediate updates and reports delivery, and finishing in the global results analysis. It was possible to achieve three main goals: harmonizing the auditing process, automatically generating auditing and intervention reports, and processing and analysing the aggregated results. The web-based application overall architecture is organised in three layers: web access through a web browser; application layer developed in Laravel; and, a data layer implemented in a MySQL database.

4. Results

This Section is fully dedicated to the results presentation. It starts with the characterisation of the participating SMEs in Section 4.1, according to the dimensions that were observed in the project: type of SME, main activity, number of employees, type of intervention, activity sector, age, business revenue, and export activity. Subsequently, the results obtained in Type 1 interventions are depicted in Section 4.2, with the overall results being grouped in the dimensions observed in Section 4.1. Finally, in Section 4.3, the results achieved with Type 2 interventions are illustrated in the dimensions previously described.

4.1. Characterization

The project targeted globally 50 SMEs and micro enterprises, affiliated with NERLEI business association and mostly operating in the center of Portugal. From those 50 SMEs, 30 received a Type 1 auditing and the remaining 20 were intervened with a Type 2 auditing, as depicted in Figure 1A. Regarding the characterisation by the types of enterprise, Figure 1B illustrates the distribution by size, namely between small, medium, and micro enterprises, while Figure 1C depicts the distribution of participating SMEs by geographic region in Portugal.

Figure 2 depicts the characterisation of the companies by the following dimensions: main activity sector (A), activity sub-sector (B), age of the enterprise (C), number of employees (D), business revenue (E), and export activity (F).

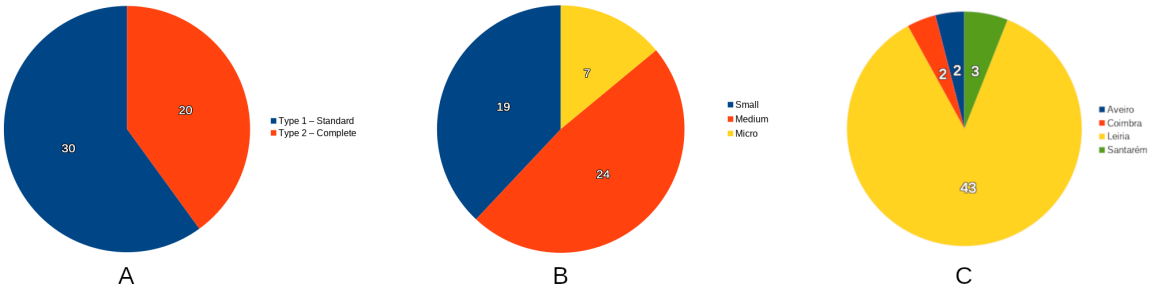

Figure 1. Characterization of the SMEs participating in the case study—(**A**) Type of auditing (Type 1 and Type 2); (**B**) type of company: small, medium, and micro enterprise; and, (**C**) companies per district.

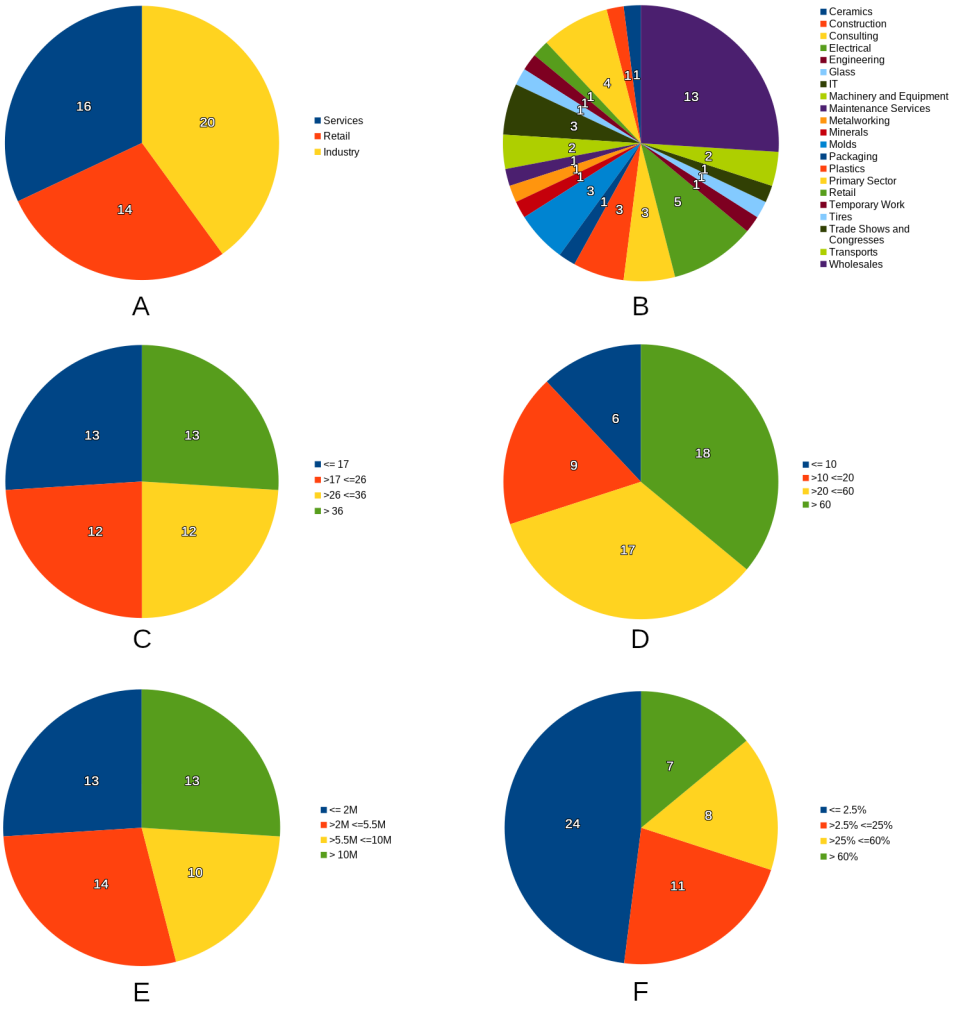

Figure 2. Characterization of the SMEs participating in the case study—(**A**) Main activity sector; (**B**) sub-sectors of activity; (**C**) age of the enterprise; (**D**) number of employees; (**E**) business revenue (scale); and, (**F**) exports as % of business revenue (scale).

By analysing Figure 1, it is possible to observe the following main aspects:

- Regarding the geographic region, all of the participating SMEs operate in the centre region of Portugal, mostly in the Leiria district (43 out of 50).
- We may observe that 48% are medium-sized enterprises and the smaller slice is related with the micro enterprises with 14%.

Regarding the six dimensions that are observed in Figure 2, the global analysis incorporated the already existing quartiles used by NERLEI to classify its affiliated of SMEs, and can be summarised, as follows:

- The main activity sector is equally distributed by industry, commerce, and services, with a slight increasing in the industry sector (20 enterprises).
- The most representative sub-activity sectors are wholesales and engineering services, respectively, with 13 and 5 enterprises.
- The age of companies is equally distributes by the four defined groups (<=17, >17 and <=26, >26 and <=36, >36).

- 70% of the intervened enterprises have more than 20 employees, with 36% having more than 60 employees.
- The business revenue is equally distributed by the four defined scales, namely <=2 M, >2 M and <=5.5 M, >5.5 M and <=10 M, 10 M.
- For almost 50% of the intervened enterprises, the investment in exports only represents 2.5% of the business revenue, which reveals their low level of internationalization. The remaining enterprises are distributed by the other three predefined scales: >2.5% and <=25%, >25% and <=60%, >60%.

By observing Figures 1 and 2, it is worth noting that this project targeted a significant range of the businesses in the region. From enterprise age to business revenue, there is a representative spread of enterprises, even when considering the number of dimensions in analysis. This may infer that the findings of this research work may be applicable to a wider scope.

4.2. Results for Type 1 Auditing

The Type 1 auditing included a subset of 30 controls spread by 14 categories of the ISO-27001:2013 standard. In this intervention type, the auditing process did not have a re-evaluation auditing and the mitigation actions were implemented during the auditing process.

Table 2 aggregates the conformity score of the controls audited, being grouped by the dimensions previously described. The results are summarised in three conformity levels, namely [0% to 50%], [51% to 75%], and [76% to 100%]. It is possible to infer that the more resources a company has, both in size and human resources, the more likely it is going to be able to implement the necessary mitigation tasks to comply with the conformity level of the controls. The industry sector is also the best fitted to comply with these guidelines, probably because it is also the most reliant on standard compliance.

Figures 3 and 4 depict the final snapshot of the auditing process, allowing for an analysis in two distinct ways: by the three predefined conformity levels (Figure 3) and by the 8 categories to which the selected controls belong (Figure 4). Figure 3 reveals that the target companies in this intervention type were mostly micro and small, and most of the controls have an acceptance percentage of over 75%.

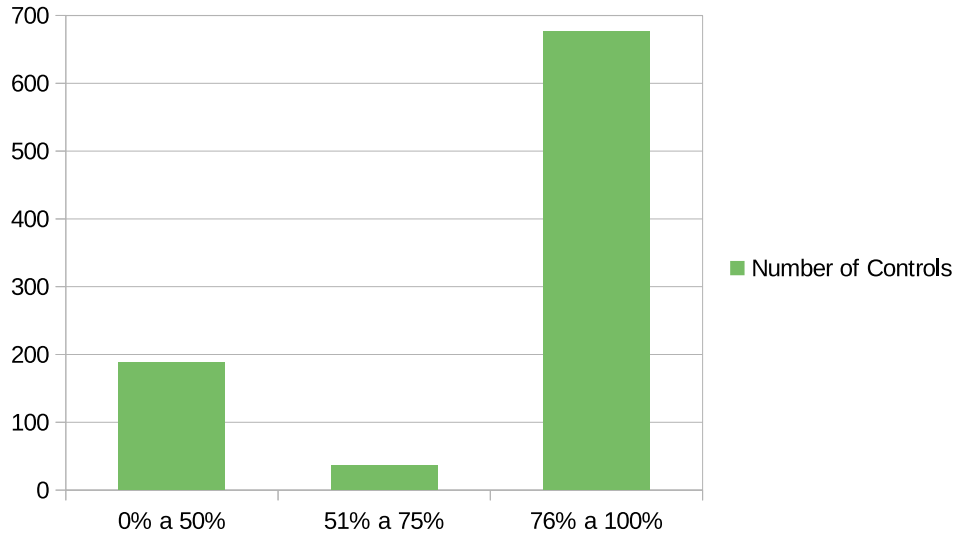

Figure 3. Number of Controls by Acceptance Percentage Intervals.

Table 2. Type 1—Acceptance percentage intervals of the controls in the predefined dimensions.

Dimension		0% to 50%	51% to 75%	76% to 100%
Classification	Micro	27.14%	8.10%	64.76%
	Small	23.06%	4.44%	72.50%
	Medium	14.55%	0.91%	84.55%
Main Activity Sector	Retail	17.50%	2.92%	79.58%
	Industry	9.09%	2.73%	88.18%
	Services	35.15%	6.06%	58.79%
Number of Employees	<=10	25.33%	8.00%	66.67%
	>10 <=20	22.59%	3.33%	74.07%
	>20 <=60	22.08%	5.83%	72.08%
	>60	15.00%	0.42%	84.58%
Sub-activity Sector	Ceramics	0.00%	0.00%	100.00%
	Construction	26.67%	0.00%	73.33%
	Consulting	40.00%	8.33%	51.67%
	Electrical	0.00%	0.00%	0.00%
	Engineering	0.00%	0.00%	0.00%
	Glass	0.00%	0.00%	0.00%
	IT	23.33%	7.78%	68.89%
	Machinery and Equipment	13.33%	13.33%	73.33%
	Maintenance Services	0.00%	0.00%	0.00%
	Metalworking	0.00%	0.00%	100.00%
	Minerals	20.00%	0.00%	80.00%
	Molds	0.00%	0.00%	0.00%
	Packaging	13.33%	0.00%	86.67%
	Plastics	0.00%	3.33%	96.67%
	Primary Sector	0.00%	0.00%	100.00%
	Retail	16.67%	5.00%	78.33%
	Temporary Work	66.67%	0.00%	33.33%
	Tires	13.33%	6.67%	80.00%
	Trade Shows and Congresses	60.00%	0.00%	40.00%
	Transports	0.00%	0.00%	0.00%
	Wholesales	16.67%	2.86%	80.48%
Company Age	<=17	21.82%	4.24%	73.94%
	>17 <=26	12.50%	2.50%	85.00%
	>26 <=36	33.33%	5.42%	61.25%
	>36	10.00%	2.86%	87.14%
Revenue	<=2 M	25.45%	6.67%	67.88%
	>2 M <=5.5 M	26.30%	3.70%	70.00%
	>5.5 M <=10 M	10.00%	2.22%	87.78%
	>10 M	11.43%	0.95%	87.62%
Exports as % of Revenue	<=2.5%	21.19%	5.48%	73.33%
	>2.5% <=25%	19.05%	1.43%	79.52%
	>25% <=60%	30.00%	6.67%	63.33%
	>60%	11.67%	0.00%	88.33%

By analysing Figure 4, controls that rely on processes and documentation are significantly easier to comply with, while comparing with those that are more technical and that have an intrinsic need to install additional equipment and implement more refined technical procedures. ISO-27001:2013 standard Sections 9.4, 14.1, and 14.2 (Table 1) have the most compliance level, which is interpreted as the process based controls are the most easily achieved for small companies, because no prior knowledge is required to implement mitigating actions. On the opposite direction, Sections 10.1 and 12.1 achieved the worst

compliance results, however by two distinct reasons. Regarding Section 10.1, the reasons are related to the technical complexity in implementing and validating cryptographic controls. In Section 12.1, it is emphasised the difficulty in specifying and validating strict operational and responsibility procedures, in the scope of SMEs.

Figure 4. Type 1—Cumulative Acceptance Percentage of ISO-27001:2013 standard sections, by intervals.

4.3. Results for Type 2 Auditing

Type 2 auditing targeted 20 companies of the overall participating SMEs. Figure 5 depicts the total amount of controls by the three predefined conformity levels in the first (Figure 5A) and second (Figure 5B) auditing. A control that fails means that it is not in conformity with the ISO-27001:2013 standard and it has an acceptance of 0%.

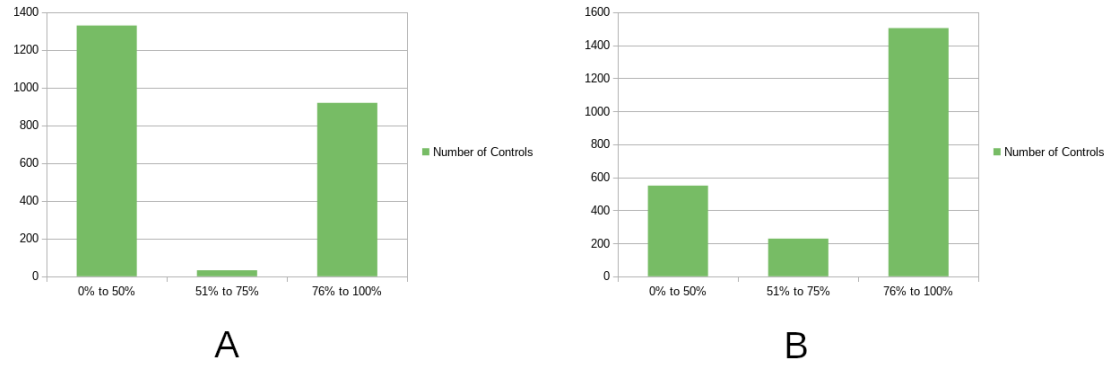

Figure 5. Type 2— Number of Controls by Acceptance Percentage Intervals on the first auditing (**A**); and on second auditing (**B**).

By analysing Figure 5, we may observe the overall evolution from the first to the second auditing process, namely by observing the increasing on the number of controls in the levels [51% to 75%], and [76% to 100%], and the corresponding decreasing on the level [0% to 50%]. This behaviour is directly influenced by the interventions made after the first auditing and the appropriate diagnosis of the aspects that should be fixed to accomplish a higher conformity level with the ISO-27001:2013 standard.

Tables 3 and 4 summarise the global conformity results of the 114 controls that are audited in Type 2 intervention. The results are grouped by the dimensions itemized in the SMEs characterisation (Section 4.1), which were analysed and classified according to the three predefined conformity levels. In a broad sense, from the presented results, we may observe an increase in the percentage of controls classified in each conformity level, from the first to the second auditing.

Table 3. Type 2—First Audit—Acceptance percentage intervals of the controls in the predefined dimensions.

Dimension		0% to 50%	51% to 75%	76% to 100%
Classification	Micro	0.00%	0.00%	0.00%
	Small	70.72%	0.94%	28.34%
	Medium	35.21%	2.26%	62.53%
Main Activity Sector	Retail	46.20%	2.19%	51.61%
	Industry	66.76%	1.17%	32.07%
	Services	57.54%	0.88%	41.58%
Number of Employees	<=10	19.30%	2.63%	78.07%
	>10 <=20	0.00%	0.00%	0.00%
	>20 <=60	49.61%	1.75%	48.64%
	>60	70.00%	0.96%	29.04%
Sub-activity Sector	Ceramics	0.00%	0.00%	0.00%
	Construction	0.00%	0.00%	0.00%
	Consulting	0.00%	0.00%	0.00%
	Electrical	11.40%	3.51%	85.09%
	Engineering	4.39%	0.00%	95.61%
	Glass	30.70%	0.00%	69.30%
	IT	0.00%	0.00%	0.00%
	Machinery and Equipment	93.86%	0.88%	5.26%
	Maintenance Services	99.12%	0.00%	0.88%
	Metalworking	0.00%	0.00%	0.00%
	Minerals	0.00%	0.00%	0.00%
	Molds	100.00%	0.00%	0.00%
	Packaging	0.00%	0.00%	0.00%
	Plastics	53.07%	3.07%	43.86%
	Primary Sector	58.77%	0.00%	41.23%
	Retail	27.19%	2.63%	70.18%
	Temporary Work	0.00%	0.00%	0.00%
	Tires	0.00%	0.00%	0.00%
	Trade Shows and Congresses	0.00%	0.00%	0.00%
	Transports	81.58%	0.00%	18.42%
	Wholesales	45.18%	2.49%	52.34%
Company Age	<=17	21.82%	4.24%	73.94%
	>17 <=26	12.50%	2.50%	85.00%
	>26 <=36	33.33%	5.42%	61.25%
	>36	10.00%	2.86%	87.14%
Revenue	<=2 M	25.45%	6.67%	67.88%
	>2 M <=5.5 M	26.30%	3.70%	70.00%
	>5.5 M <=10 M	10.00%	2.22%	87.78%
	>10 M	11.43%	0.95%	87.62%
Exports as % of Revenue	<=2.5%	21.19%	5.48%	73.33%
	>2.5% <=25%	19.05%	1.43%	79.52%
	>25% <=60%	30.00%	6.67%	63.33%
	>60%	11.67%	0.00%	88.33%

Table 4. Type 2—Second Audit—Acceptance percentage intervals of the controls in the predefined dimensions.

Dimension		0% to 50%	51% to 75%	76% to 100%
Classification	Micro	0.00%	0.00%	0.00%
	Small	18.42%	15.66%	65.91%
	Medium	27.13%	6.95%	65.92%
Main Activity Sector	Retail	23.39%	19.44%	57.16%
	Industry	26.51%	5.17%	68.32%
	Services	20.53%	7.37%	72.11%
Number of Employees	<=10	20.18%	30.70%	49.12%
	>10 <=20	0.00%	0.00%	0.00%
	>20 <=60	21.73%	12.57%	65.69%
	>60	26.58%	5.61%	67.81%
Sub-activity Sector	Ceramics	0.00%	0.00%	0.00%
	Construction	0.00%	0.00%	0.00%
	Consulting	0.00%	0.00%	0.00%
	Electrical	11.40%	17.54%	71.05%
	Engineering	3.51%	5.26%	91.23%
	Glass	30.70%	0.00%	69.30%
	IT	0.00%	0.00%	0.00%
	Machinery and Equipment	31.58%	0.00%	68.42%
	Maintenance Services	25.44%	0.00%	74.56%
	Metalworking	0.00%	0.00%	0.00%
	Minerals	0.00%	0.00%	0.00%
	Molds	33.33%	1.75%	64.91%
	Packaging	0.00%	0.00%	0.00%
	Plastics	16.67%	11.84%	71.49%
	Primary Sector	31.58%	0.00%	68.42%
	Retail	28.07%	29.82%	42.11%
	Temporary Work	0.00%	0.00%	0.00%
	Tires	0.00%	0.00%	0.00%
	Trade Shows and Congresses	0.00%	0.00%	0.00%
	Transports	25.88%	0.44%	73.68%
	Wholesales	22.37%	19.59%	58.04%
Company Age	<=17	23.25%	12.28%	64.47%
	>17 <=26	19.74%	9.76%	70.50%
	>26 <=36	22.37%	23.90%	53.73%
	>36	31.29%	0.29%	68.42%
Revenue	<=2 M	16.23%	14.47%	69.30%
	>2 M <=5.5 M	28.07%	10.18%	61.75%
	>5.5 M <=10 M	23.68%	7.89%	68.42%
	>10 M	23.83%	10.82%	65.35%
Exports as % of Revenue	<=2.5%	23.07%	13.68%	63.25%
	>2.5% <= 5%	19.74%	14.91%	65.35%
	>25% <=60%	29.82%	0.29%	69.88%
	>60%	27.49%	0.88%	71.64%

Figures 6 and 7 depict the evolution of conformity for each of the ISO-27001:2013 standard categories and their included controls. The conformity index is classified in three levels, namely [0–50%], [51–75%], and [76–100%]. By analysing the figures, one may note that the green spot widens in all the categories, which is the result of the flaws that were observed in the first auditing and the mitigation measures implemented and re-evaluated in the second auditing. This fact is explanatory of the evolution observed, from the first to the second auditing. The yellow spot, which corresponds to a positive level of conformity

(above 50%), has also increased from the first to the second auditing. At the same time, the red spot is reduced in the second auditing, reflecting the decrease of the number of controls with a low acceptance score.

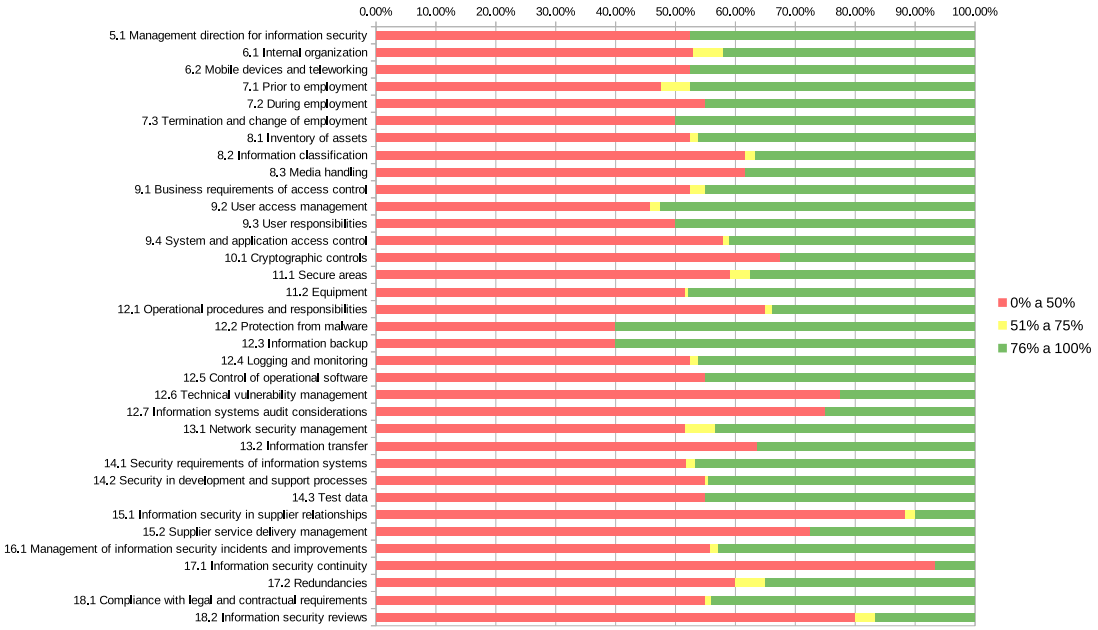

Figure 6. Type 2—Cumulative Acceptance Percentage of ISO-27001:2013 standard sections, by intervals—First Auditing.

Figure 7. Type 2—Cumulative Acceptance Percentage of ISO-27001:2013 standard sections, by intervals—Second Auditing.

5. Results Analysis

The results analysis is split into three main dimensions: global results, Type 1 auditing results, and Type 2 auditing results.

Regarding global results, the implementation of the project brought visible benefits to the intervened SMEs, mainly to their perception of cybersecurity. The benefits are visible when comparing Figures 6 and 7.

By analysing Figures 3 and 5, with the distribution of conformity by predefined groups for Type 1 and Type 2 auditing schemes, it is possible to note the existence of a considerable number of controls with a low level of conformity (below 50%). This is related to the fact that a set of ISO-27001:2013 standard controls are difficult to apply in SMEs. Besides that, while comparing the evolution from the first to the second auditing stages in Type 2 auditing, it is possible to observe an overall positive evolution in the acceptance level higher than 70%, as depicted in the comparison between Figures 6 and 7.

Regarding Type 1 auditing, in Table 2 it is visible that most of the selected controls are above 50% and they were evaluated as being in conformity with the standard. This behaviour was observed in the majority of the intervened enterprises. By observing the categories to which the controls belong, cryptographic controls are those that have the worst performance, with a classification below 50%. The remaining controls achieved an evaluation higher than 75%. By observing all of the controls with positive evaluation, the average is 78.06%.

Regarding the dimension of the enterprises, we may observe that the medium-sized enterprises have better performance, with the lowest number of controls being below or equal to 50%. In the reverse way, micro enterprises have the highest rate of controls, being evaluated below 50%. Regarding the analysis by activity sectors, manufacturing enterprises present the highest rate of controls above 75% of conformity (88.1%). In the opposite direction the rate of companies with a conformity level below 50% is observed in service enterprises (35.15%).

By analysing the volume of business, we may observe a direct connection between this parameter and the performance obtained. That is, the enterprises with higher volume of business have reached the higher number of controls with higher than 75% of conformity with the ISO-27001:2013 standard. Regarding the level of exports, we may observe that the enterprises that mostly export have obtained better performance. By analysing this parameter, together with the volume of business, it is possible to infer that the enterprises' wealthiness and the exportation level are related with the level of preparation to adopt good practices of cybersecurity and cyberawareness. The global market presence brings out an obligation to these enterprises concerning cyberawareness and cybersecurity, mainly due to their acquired competitiveness and international activity obtained in international partnerships.

Regarding Type 2 auditing, Figures 6 and 7 compare the benefits obtained from the first to the second evaluation. In the first auditings, the controls that failed represent more 40% than those that passed, while, in the second auditing, the controls that passed are more than the double those that failed. Regarding the analysis by the categories of the ISO-27001:2013 standard, all of the categories improved, by observing Figures 6 and 7. It is also possible to observe that the controls that failed in the first auditing are above 30% when comparing with those that failed in the second evaluation. After the second auditing, we may note that this relation changes, as the number of controls that passed represent the double of those that failed. Figure 7 and Table 4 illustrate this phenomenon.

In Type 2 auditing, we may observe two distinct behaviours in the 20 enterprises intervened: in the first auditing, six enterprises did not pass in any of the 114 controls, while only two achieved more than 100 controls being positively validated. When comparing these results with those obtained in the second auditing, we verify that the number of controls positively evaluated have increased and achieved, on average, 60%. In this topic, the joint efforts between the auditing team and the SMEs to mitigate the flaws that were identified during the first auditing were positive.

Regarding the level of exports, enterprises with a lower level have a better performance. When analysing this parameter, together with the volume of business, it allows for us to conclude that enterprises with less resources and export activity were those that took advantage of the possibility of doing a first auditing, implementing the identified flaws, and correcting them for further evaluation.

6. Conclusions

This paper presented the results that were obtained with the implementation of an information security and cybersecurity management project in SMEs. A comprehensive literature review was made and the deployed ISO-27001:2013 based methodology was described. The characterisation of the participating SMEs according to several dimensions was also made, as well as an analysis of the results that were obtained in this case study.

The attained results have shown substantial benefits to the audited and intervened SMEs, being directly and indirectly related with their information security management robustness and collaborators' cyberawareness. The conclusions to the project implementation and results obtained are grouped into three distinct dimensions: project development and management, impact in the participating SMEs, and global results observed.

Regarding the project development, the aims were well defined *a priori* and they were grounded on embodying the SMEs with better tools to manage information security and cybersecurity. Regarding the collaborators' cyberawareness, a set of seminars and talks along the project were proposed. The adopted methodology for ISO-27001:2013 framework is in line with those that were described in the literature. The scope of application is in the SMEs and micro enterprises, and the aim is to generally improve the information security and cybersecurity. There are other frameworks that could be applied to information security auditing in SMEs (e.g., NIST Cyber Security Framework), but the ISO-27001:2013 framework has been identified in the literature as a best practice in which information security in SMEs is concerned [31,46].

Regarding the impact on the intervened SMEs, the observed improvements must be emphasised, especially on those enterprises that adhered to Type 2 auditing. Nevertheless, without having a second auditing, SMEs that intervened with Type 1 auditing had the opportunity to evaluate 30 controls and, for those, to apply the corresponding mitigation tasks. Despite that this type did not have a re-evaluation process, as the countermeasures were applied during the intervention, a way to enhance the overall methodology is to include this additional step.

The global results seem to be clear regarding the positive impact that the project had in the participating SMEs. It was not expected to have a full success rate in all the controls and SMEs intervened. The SMEs were not at the same organisational, human resources, and IT level, and the cyberawareness level was not also the same in all of the intervened SMEs. These two reasons implied a variation in the results that were achieved by the SMEs in some categories of the ISO-27001:2013 standard.

The consulting team was also challenged to apply the ISO-27001:2013 standard to SMEs, besides their experience in larger and more organised institutions. Having in mind the definition of a unique and harmonised guideline for the whole auditing interventions, one may infer that the work done by the consulting teams embodies the spirit of the original ISO-27001:2013 standard. Broadly speaking, the adoption of information security auditing processes and their continuous improvement, as well as the training and certification of SMEs collaborators, are essential in mitigating the risks in cybersecurity and producing a positive impact in the overall SMEs activity.

Information security and cybersecurity management are wide topics, in which distinct paths could be followed to implement robust and integrated solutions. The adoption of ISO-27001:2013 framework have in mind the literature review concerning the best practices and information security frameworks that should be applied in SME. However, ISO-27001:2013 is a single tool for achieving the project goal and it can be seen as a limitation in this study. In that sense, other best practices and frameworks should be addressed, implemented, and compared, in order to identify the fully appropriateness of ISO-27001:2013 to all of the intervened SME.

Author Contributions: Data curation, M.A., D.P., M.M., R.G.; Formal analysis, M.A., M.M., R.G.; Funding acquisition, M.A.; Methodology, M.A., M.M., R.G.; Software, D.P.; Supervision, M.A.; Visualization, R.G.; Writing—original draft: M.A., M.M., R.G., D.P. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by "POCI—Programa Operacional para a Competitividade e Internacionalização" grant number POCI-02-0853-FEDER-026352. This publication and the APC is funded by FCT—Fundação para a Ciência e Tecnologia, I.P., under the project UIDB/04524/2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy concerns and the need to be made anonymous on request.

Acknowledgments: The authors acknowledge NERLEI business association project team by the support given along the implementation of the project.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

BCM	Business Continuity Management
HR	Human Resources
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
NERLEI	Núcleo Empresarial da Região de Leiria
SBS	Small Business Standards
SME	Small and Medium-sized Enterprise

References

1. Ikeda, K.; Marshall, A.; Zaharchuk, D. Agility, skills and cybersecurity: Critical drivers of competitiveness in times of economic uncertainty. In *Strategy & Leadership*; Emerald Publishing: Bingley, UK, 2019.
2. Huang, K.; Madnick, S.; Johnson, S. Framework for Understanding Cybersecurity Impacts on International Trade. 2019. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3555341 (accessed on 7 March 2021).
3. Al-Sartawi, A.M.M. Information technology governance and cybersecurity at the board level. *Int. J. Crit. Infrastruct.* **2020**, *16*, 150–161. [CrossRef]
4. ENISA Threat Landscape. 2020. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ (accessed on 7 March 2021).
5. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
6. Ahmad, T. Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. 2020. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830 (accessed on 7 March 2021).
7. Nistotskaya, M.; Charron, N.; Lapuente, V. The wealth of regions: Quality of government and SMEs in 172 European regions. *Environ. Plan. Gov. Policy* **2015**, *33*, 1125–1155. [CrossRef]
8. Small Business Standards. Available online: https://www.sbs-sme.eu/sme-involvement/standards-and-smes (accessed on 7 March 2021).
9. Kertysova, K.; Frinking, E.; van den Dool, K.; Maričić, A.; Bhattacharyya, K. *Cybersecurity: Ensuring Awareness and Resilience of the Private Sector Across Europe in Face of Mounting Cyber Risks-Study*; Technical Report; European Economic and Social Committee, The Hague Centre for Strategic Studies: Hague, The Netherlands, 2018. Available online: https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study#downloads (accessed on 7 March 2021).
10. Boletsis, C.; Halvorsrud, R.; Pickering, J.B.; Phillips, S.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021), Vienna, Austria, 8–10 February 2021.
11. Ozkan, B.Y.; Spruit, M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. In *Research Anthology on Artificial Intelligence Applications in Security*; IGI Global: Hershey, PA, USA, 2021; pp. 1252–1278.
12. Whitehead, G. Investigation of Factors Influencing Cybersecurity Decision Making in Irish SME's from a Senior Manager/Owner Perspective. Ph.D. Thesis, National College of Ireland, Dublin, Ireland, 2020.
13. Saleem, J.; Adebisi, B.; Ande, R.; Hammoudeh, M. A state of the art survey-Impact of cyber attacks on SME's. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017.

14. Carías, J.F.; Borges, M.R.; Labaka, L.; Arrizabalaga, S.; Hernantes, J. Systematic Approach to Cyber Resilience Operationalization in SMEs. *IEEE Access* **2020**, *8*, 174200–174221. [CrossRef]
15. Stoneburner, G.; Goguen, A.; Feringa, A. Risk management guide for information technology systems. *Nist Spec. Publ.* **2002**, *800*, 800–830.
16. Bell, S. Cybersecurity is not just a 'big business' issue. *Gov. Dir.* **2017**, *69*, 536–539.
17. ISO-ISO/IEC 27000:2009—Information Technology—Security Techniques—Information Security Management Systems—Overview and vocabulary. Available online: https://www.iso.org/standard/41933.html (accessed on 2 February 2021).
18. Stallings, W. *Cryptography and Network Security*, 4th ed.; Pearson Education India: Delhi, India, 2006.
19. Mohammed, A.M.; Idris, B.; Saridakis, G.; Benson, V. Information and communication technologies: A curse or blessing for SMEs? In *Emerging Cyber Threats and Cognitive Vulnerabilities*; Elsevier Press: Amsterdam, The Netherlands, 2020; pp. 163–174.
20. Kabanda, S.; Tanner, M.; Kent, C. Exploring SME cybersecurity practices in developing countries. *J. Organ. Comput. Electron. Commer.* **2018**, *28*, 269–282. [CrossRef]
21. Naradda Gamage, S.K.; Ekanayake, E.; Abeyrathne, G.; Prasanna, R.; Jayasundara, J.; Rajapakshe, P. A Review of Global Challenges and Survival Strategies of Small and Medium Enterprises (SMEs). *Economies* **2020**, *8*, 79. [CrossRef]
22. Alahmari, A.; Duncan, B. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 15–19 June 2020; pp. 1–5.
23. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef] [PubMed]
24. ISO-ISO/IEC 27001:2013—Information Technology—Security Techniques—Information Security Management Systems—Requirements. Available online: https://www.iso.org/standard/54534.html (accessed on 2 February 2021).
25. Information Security Management System | ISMS.online. Available online: https://www.isms.online/information-security-management-system-isms/ (accessed on 2 February 2021).
26. ISO-ISO/IEC 27005:2018—Information Technology—Security Techniques—Information Security Risk Management. Available online: https://www.iso.org/standard/75281.html (accessed on 2 February 2021).
27. ISO-ISO/IEC 27037:2012—Information Technology— Security Techniques—Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence. Available online: https://www.iso.org/standard/44381.html (accessed on 7 March 2021).
28. Javaid, M.I.; Iqbal, M.M.W. A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). In Proceedings of the International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 78–90.
29. Muthaiyah, S.; Zaw, T.O.K. ISO/IEC 27001 Implementation in SMEs: Investigation on Management of Information Assets. *Indian J. Public Health Res. Dev.* **2018**, *9*, 2631–2637. [CrossRef]
30. Wanyonyi, V. Information Security Management Toolkit for ISO/IEC 27001 Standard, Case of Small-to-Medium Sized Enterprises (SMEs). Ph.D. Thesis, University of Nairobi, Nairobi, Kenya, 2020.
31. Renvall, A. Improving Cybersecurity through ISO/IEC 27001 Information Security Standard in the Context of SMEs. 2018. Available online: https://www.theseus.fi/handle/10024/157277 (accessed on 7 March 2021).
32. Ozkan, B.Y.; Spruit, M. Assessing and Improving Cybersecurity Maturity for SMEs: Standardization aspects. *arXiv* **2020**, arXiv:2007.01751.
33. Ponsard, C.; Grandclaudon, J.; Dallons, G. Towards a Cyber Security Label for SMEs: A European Perspective-. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), Madeira, Portugal, 2–24 January 2018; pp. 426–431.
34. Ponsard, C.; Massonet, P.; Grandclaudon, J.; Point, N. From Lightweight Cybersecurity Assessment to SME Certification Scheme in Belgium. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 75–78.
35. Henson, R.; Sutcliffe, D. An insurance-based approach to improving SME Cyber Security. In *Special Topics in Economics & Management: An Introduction*; ATINER: Athens, Greece, 2017.
36. Hassinen, T. Enhancing Cyber Security for SME Organizations through Self-Assessments: How Self-Assessment Raises Awareness. 2017. Available online: https://www.theseus.fi/handle/10024/125437 (accessed on 7 March 2021).
37. Rae, A.; Patel, A. Defining a new composite cybersecurity rating scheme for smes in the uk. In Proceedings of the International Conference on Information Security Practice and Experience, Kuala Lumpur, Malaysia, 26–28 November 2019; Springer: Cham, Switzerland, 2019; pp. 362–380.
38. Ponsard, C.; Grandclaudon, J. Survey and guidelines for the design and deployment of a cyber security label for SMEs. In Proceedings of the International Conference on Information Systems Security and Privacy, Madeira, Portugal, 22–24 January 2018; Springer: Cham, Switzerland, 2018; pp. 240–260.
39. Ozkan, B.Y.; Spruit, M.; Wondolleck, R.; Coll, V.B. Modelling adaptive information security for SMEs in a cluster. *J. Intellect. Cap.* **2019** *21*, 235–256.
40. Ozkan, B.Y.; van Lingen, S.; Spruit, M. The Cybersecurity Focus Area Maturity (CYSFAM) Model. *J. Cybersecur. Priv.* **2021**, *1*, 119–139. [CrossRef]

41. Auyporn, W.; Piromsopa, K.; Chaiyawat, T. Critical Factors in Cybersecurity for SMEs in Technological Innovation Era. In Proceedings of the ISPIM Conference Proceedings, The International Society for Professional Innovation Management (ISPIM), Bangkok, Thailand, 1–4 March 2020; pp. 1–10.
42. Mubarak, S.; Heyasat, H.; Wibowo, S. Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review. In Proceedings of the Australasian Conference on Information Systems, Perth, Australia, 9–11 December 2019; pp. 148–154.
43. Teufel, S.; Teufel, B.; Aldabbas, M.; Nguyen, M. Cyber Security Canvas for SMEs. In Proceedings of the International Information Security Conference, Pretoria, South Africa, 25–26 August 2020; Springer: Cham, Switzerland, 2020; pp. 20–33.
44. Zec, M. *Cyber Security Measures in SME's: A Study of IT Professionals' Organizational Cyber Security Awareness*; Linnaeus University: Kalmar, Zugriff unter, Sweden, 2015; Volume 849211. Available online: https://www.diva-portal.org/smash/get/diva2:849211/ATTACHMENT01.pdf (accessed on 7 March 2021).
45. Ozkan, B.Y.; Spruit, M. Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a research agenda. *Int. J. Stand. Res.* **2019**, *17*, 41–72. Available online: https://www.igi-global.com/gateway/article/full-text-pdf/253856&riu=true (accessed on 7 March 2021). [CrossRef]
46. Organizations in Cooperation with ISO—SBS—Small Business Standards. Available online: https://www.iso.org/organization/5100110.html (accessed on 7 March 2021).