applied sciences

MDPI

Article

A Client-Centered Information Security and Cybersecurity Auditing Framework

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

[1] Computer Science and Communication Research Centre (CIIC), School of Technology and Management, Polytechnic of Leiria, 2411-901 Leiria, Portugal
[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
* Correspondence: mario.antunes@ipleiria.pt (M.A.); marisa.maximiano@ipleiria.pt (M.M.)

Abstract: Information security and cybersecurity management play a key role in modern enterprises. There is a plethora of standards, frameworks, and tools, ISO 27000 and the NIST Cybersecurity Framework being two relevant families of international Information Security Management Standards (ISMSs). Globally, these standards are implemented by dedicated tools to collect and further analyze the information security auditing that is carried out in an enterprise. The overall goal of the auditing is to evaluate and mitigate the information security risk. The risk assessment is grounded by auditing processes, which examine and assess a list of predefined controls in a wide variety of subjects regarding cybersecurity and information security. For each control, a checklist of actions is applied and a set of corrective measures is proposed, in order to mitigate the flaws and to increase the level of compliance with the standard being used. The auditing process can apply different ISMSs in the same time frame. However, as these processes are time-consuming, involve on-site interventions, and imply specialized consulting teams, the methodology usually adopted by enterprises consists of applying a single ISMS and its existing tools and frameworks. This strategy brings overall less flexibility and diversity to the auditing process and, consequently, to the assessment results of the audited enterprise. In a broad sense, the auditing needs of Small and Medium-sized Enterprises (SMEs) are different from large companies and do not fit with all the existing ISMSs' frameworks, that is a set of controls of a particular ISMS is not suitable to be applied in an auditing process, in an SME. In this paper, we propose a generic and client-centered web-integrated cybersecurity auditing information system. The proposed system can be widely used in a myriad of auditing processes, as it is flexible and it can load a set of predefined controls' checklist assessment and their corresponding mitigation tasks' list. It was designed to meet both SMEs' and large enterprises' requirements and stores auditing and intervention-related data in a relational database. The information system was tested within an ISO 27001:2013 information security auditing project, in which fifty SMEs participated. The overall architecture and design are depicted and the global results are detailed in this paper.

Keywords: cybersecurity; information security; auditing; ISO 27001:2013; SME

check for updates

Citation: Antunes, M.; Maximiano, M.; Gomes, R. A Client-Centered Information Security and Cybersecurity Auditing Framework. *Appl. Sci.* **2022**, *12*, 4102. https://doi.org/10.3390/app12094102

Academic Editors: Howon Kim and Thi-Thu-Huong Le

Received: 30 March 2022
Accepted: 13 April 2022
Published: 19 April 2022

1. Introduction

Information security and cybersecurity have gained enormous importance by enterprises' management boards, as they are becoming more aware about the need to protect data and Information Technology (IT) infrastructure against cyberattacks [1,2]. Information security self-diagnosis, awareness sessions, investment in cybersecurity technology, and the hiring of more qualified technical human resources are among the most relevant actions adopted by enterprises to raise the IT protection and to reduce the risk of cyberattacks.

Micro- and Small and Medium-sized Enterprises (SMEs) contribute substantially to income, output, and employment, play an important role in the world economy, and represent a large slice of the wealth produced worldwide [3]. Micro- and SMEs are defined as non-subsidiary, independent organizations that have to meet the maximum values fixed by the national statistical systems, for the following two dimensions: number of employees and annual turnover [4]. In Europe, a micro-company has up to 10 employees, while small and medium-sized enterprises have up to 50 and 250 employees, respectively. The criteria for micro- and SMEs includes also annual turnover and balance sheet total [5]. Due to their intrinsic characteristics, namely the small dimension in the number of employees, the lack of resident IT infrastructure and staff, and the adoption of more traditional and familiar business models, the information security and cybersecurity management may usually be neglected and put in a second stage regarding what auditing and certification concerns are about [6].

Security auditing teams, which can be internal or external to the enterprise, bring the intervention and support in information security consulting, namely by regularly auditing the enterprises according to international standards, such as ISO 27001:2013, ISO 27009, and the NIST Cybersecurity Framework (NIST-CSF) [7,8]. Broadly speaking, the auditing process involves the whole organization, as the consulting team has to collect and evaluate a list of predefined controls, which is mostly derived from the standards and documentation and best practices procedures available. Besides the NIST-CSF and ISO 27000 series standards' families, which are the most relevant and the best of breed in what cybersecurity and information security are about, some additional standards and frameworks could also be addressed, being however specific to the business area: ISO 22301:2012 [9] for business continuity management systems and the Health Insurance Portability and Accountability Act (HIPAA) [10] to protect the confidentiality and security of health care information and data.

As these standards have controls, auditing tasks' lists, and mitigation measures, they could also be applied to the framework presented in this paper. However, our case study was the ISO 27001 standard and its adoption by SMEs.

Each auditing process is composed of various auditing interventions, in which the team evaluates the level of compliance of each security control, by applying to it a predefined checklist. For each control, a list of mitigation tasks is already defined and delivered to guide the auditor during the auditing interventions. After assessing all the controls, a global compliance score is calculated. For those controls that are not fully compliant with the standard that is being applied in the auditing, a list of countermeasures and mitigation tasks is proposed to the enterprise, as they can be implemented and further evaluated during the auditing process.

The auditing process can take several weeks or months, depending on several factors, such as the number of employees, the organizational complexity, the preparedness of the information system infrastructure, and the level of knowledge about the business and the technological infrastructure that supports it. During the auditing process, a considerable number of interventions may have to be made, mostly on-site, where physical validation of existing software and hardware takes place, as well as the identification of assets and of business processes.

Data are collected and stored in each auditing intervention for further analysis and reporting. The initial auditing implies an auto-diagnosis of the enterprise regarding cybersecurity. Depending on the score attained, several mitigation tasks may be proposed to be implemented. Each subsequent auditing intervention is essentially dedicated to the evaluation of the impact that each mitigation had on the overall security auditing, that is the aim of the several auditing interventions that may take place is to evaluate and assess the enhancements obtained with the countermeasures that were proposed by the auditing team. At the end, the compliance level of the enterprise regarding cybersecurity and information security issues should increase and may demonstrate the continuous readiness of the enterprise.

Each well-adopted information security, privacy, and cybersecurity international standard has its own set of tools and best practices, available elsewhere to be applied by the enterprises and auditing teams. However, these tools and the existing Information Systems (ISs) that support them to manage cybersecurity and information security auditing processes are mainly oriented toward a particular standard. The reasons are mainly the inflexibility of these tools to accommodate different standards and their corresponding structures and checklists. Some of the existing standards are also hard to apply in a set of heterogeneous enterprises, and in some cases, the supporting tools are shallow and fed by the information security auditing community, which gives less confidence about their adoption in wide auditing scenarios.

These auditing applications usually fall into two distinct groups: proprietary and oriented toward complex auditing processes in big companies; open source, usually free-of-charge, and mainly composed of spreadsheet-based toolkits delivered by the community. This notwithstanding, the various standards are based on assessment checklists; each one delivers its own toolkit to collect and process auditing data, limiting the use of the same IS platform for different enterprises and standards. This fact implies that a consulting team running auditing processes in different companies and using distinct information security and cybersecurity standards has to collect and analyze the resulting data with different toolkits.

This paper describes an IS to support and manage information security auditing processes, regardless of the standard that is being applied. The developed and ready-to-use web-based application was designed to load a predefined list of controls that were extracted from a standard, as well as their corresponding sets of checklists and countermeasure tasks. The IS is thus agnostic to the standard being used in the auditing; it stores the assessment made of the controls and calculates the global score attained by the auditing. The IS was tested in a cybersecurity auditing project, in which fifty SMEs were audited for the ISO 27001:2013 standard [11]. The IS's level of independence regarding the standard being adopted allows the controls' lists and corresponding checklists from other standards to be available. The proposed IS validates the methodology followed in this project, regarding the development of an agnostic tool, due to its possibility of incorporating different standards to be assessed and facilitating the benefits of the outcomes of having a structured and automatized tool to guide the auditing team, providing real feedback any time it is needed. The use of a tailored IS as a tool to facilitate the reporting and monitoring process of an audit team proved, in our scenario, that this is a major advantage of this type of approach.

The remainder of this paper is organized as follows. Section 2 describes the most relevant ISs, tools and applications that are available to support information security and cybersecurity auditing. Section 3 details the information system that was developed, namely its overall architecture, main technological components, and the data model used to store the data collected. Section 4 validates the information system presented in this paper, by depicting the results obtained with a case study, followed by their corresponding analysis. Finally, Section 5 states the main conclusions and delineates some future work.

2. Background

This section describes a subset of known tools available to support auditing interventions. ISO 27001:2013 is the most common and well-known information security standard, and its available tools were analyzed in depth. Table 1 enumerates the most relevant tools for ISO 27001:2013, which are classified into three dimensions: (i) type, which distinguishes the cloud-based tools and those that are based on spreadsheets and other documents; (ii) openness, as the tools can be commercial or supported by the community; and (iii) the technological maturity level.

The analysis was intended to ascertain if the tools require an existing organizational structure, as well as the technological maturity of the companies, that is if the applications can be easily applied to both SMEs and large enterprises. The classification also distinguishes the tools that support different standards or compliance regulations, from those that were only developed to implement ISO 27001:2013 guidelines.

Table 1. ISO 27001 auditing support tools (links accessed on 29 March 2022).

Flexibility	Software	Type	Open Source/ Open Access	Tech Maturity
Supports Other Standard	Mango—Limited Mango [12]	SaaS	No	Yes
	ISO Manager—ISO Manager [13]	SaaS	No	Yes
	Instant Management Systems B.V.—Instant 27001 [14]	SaaS	No	Yes
	Resolver—IT Compliance [15]	SaaS	No	Yes
	NIST—Cybersecurity Framework Reference Tool [8]	SaaS	Yes	No
	OpensourceGRC—ISO 27001 Package [16]	SaaS and Doc based	Yes	No
	Eramba—GRC Software [17]	SaaS	No	Yes
Does not support other standards	SecuraStar—ISO 27001 Software [18]	SaaS	No	Yes
	Advisera—Conformio [19]	SaaS	No	Yes
	Netwrix—ISO IEC Compliance [20]	SaaS	No	Yes
	Certikit—ISO 27001 ToolKit [21]	Doc based	No	Yes
	IT Governance ISO 27001 Documentation Tool Kit [22]	Doc based	No	Yes
	ISO 27K Forum—ISO 27001 ToolKit [7]	Doc based	Yes	No
	Teramind—ISO 27001 Compliance [23]	SaaS	No	Yes

As can be seen from Table 1, the available tools are mostly delivered as a Software-as-a-Service (SaaS) cloud applications. According to the documentation available, it is possible to infer that these applications are less suitable to SMEs or those with a low technological maturity. The cloud-based nature of these applications, such as the SaaS model, brings high flexibility to the end-users, as few technological requests are needed to setup an auditing process. These tools rely heavily on features that fit the organizational structure, such as the definition of strict responsibility assignments or documentation repositories that need to be referenced.

There are a few document-based toolkits available, which are basically composed of general guidelines derived from templates, policies, and spreadsheets, to collect the necessary information about assets when an auditing process is being prepared. The Opensource GRC—ISO 27001 package is open source; the documentation is fed by the ISO 27001 community; it is composed of a web application that can be used for several standards; for each clause and control of the standard, it provides a set of documentation, such as templates or data collection documents. However, it does not have easy support to record auditing interventions, as it is designed to be used internally by companies, to assess and evaluate their compliance with the standards.

Most of the solutions presented are not open source and require that the company has some level of technological maturity, which is not the common scenario in SMEs, if we think of those acting in the manufacturing industry. Those tools that are open source fail to support different standards, which gives less flexibility to the information security auditing and has a strong impact on the way an SME is able to choose and benchmark distinct standards.

Based on the limitations described above and the lack of tailored solutions that could be set for the context of an auditing process, in this paper, we propose a web-based open-source solution that is able to record the auditing activity with different and heterogeneous information security standards. It is possible to support different instances of information security standards and to benchmark the results obtained. Each standard can be easily configured, by importing a list of controls and associated checklist actions and mitigation strategies. Therefore, the software instance can be tailored to support different standards and allows the incorporation of controls that are more suitable to the context of the company.

3. Information System for Security Auditing

The Information System (IS) described in this paper was initially built and tested for ISO 27001:2013 auditing. However, it was designed to support other standard specifications, as the application can be customized to load any ISMS. The customizable approach under the web application was tailored to the following main presumptions:

- A checklist for each control is available as a set of actions to be applied during the auditing.
- These actions are specific elements to check by a "true/false" answer, and the result allows an auditor to better define an acceptable percentage for each control. In a first auditing intervention, the overall checklist is verified and the level of acceptance is calculated.
- A list of mitigation actions is available for each control. Depending on the level of acceptance related to each control, after the first auditing, the team receives an automatically generated list of mitigation tasks to be applied, in order to decrease the risk of the control being evaluated and raise the acceptance level.
- When a second intervention occurs, each control is re-evaluated, to assess the impact of the countermeasures that were identified and applied after the first intervention.

One of the main reasons behind this approach is to allow the IS to be used in companies of different sizes and with distinct technological maturities. The ability to split the objectives of each control into a set of actions to be performed in an audit has the main advantage of providing more flexibility to process the actions' list. The standards are very strict and usually do not allow this kind of flexibility.

In our case study summarized in Section 4 and detailed in [24], it was possible to monitor and make a diagnosis about the cybersecurity and information security risks observed in the fifty intervened SMEs, according to the data collected during the auditing process, namely on both interventions.

The IS was designed as a web application for the benefit of being platform agnostic. This means that any auditor may use the application regardless of his/her own environment or that of the company being audited. As the auditor can define and customize the actions to be validated for each control, the proposed solution can be adjusted to fit the auditing process to the organizational context of each intervened company. The proposed solution can be tailored to the common auditing standards, namely the ISO-27000 family, which contrasts with the overall auditing solutions available (Section 2). The following subsections detail the architecture, the data model, and the reasons behind the choices made during the development.

The IS presented in this work was developed to support the auditing process applied to the fifty SMEs. Indeed, the aim in developing and proposing this tailored software was to allow all the authors to have constant access to the occurring process, making all data available when needed. The challenges and amount of data gathered in a process of this nature are known to be great. Therefore, the scope and aim are essentially to make all the data available when needed. This proof of concept allowed us to focus on and determine the best requirements for a system of this nature. The benefits of having a system that automates the registration and standardization of the data collection are some the key outputs.

3.1. Proposed Architecture

Figure 1 depicts the auditing process, namely the collection of evidence made by the auditing team, the automatic processing of auditing reports, and the results' analysis. The web application is versatile and customizable, as it receives a predefined checklist of actions and a list of corrections to be applied. The whole auditing process is stored in a database, starting with the auditing and interventions' records, going through the intermediate updates and reports' delivery, and finishing with the global results' analysis. This application enabled the achievement of three main goals: (1) to harmonize the auditing process; (2) to automatically generate auditing and intervention reports; (3) to process and analyze the aggregated results, at different stages of the auditing process.

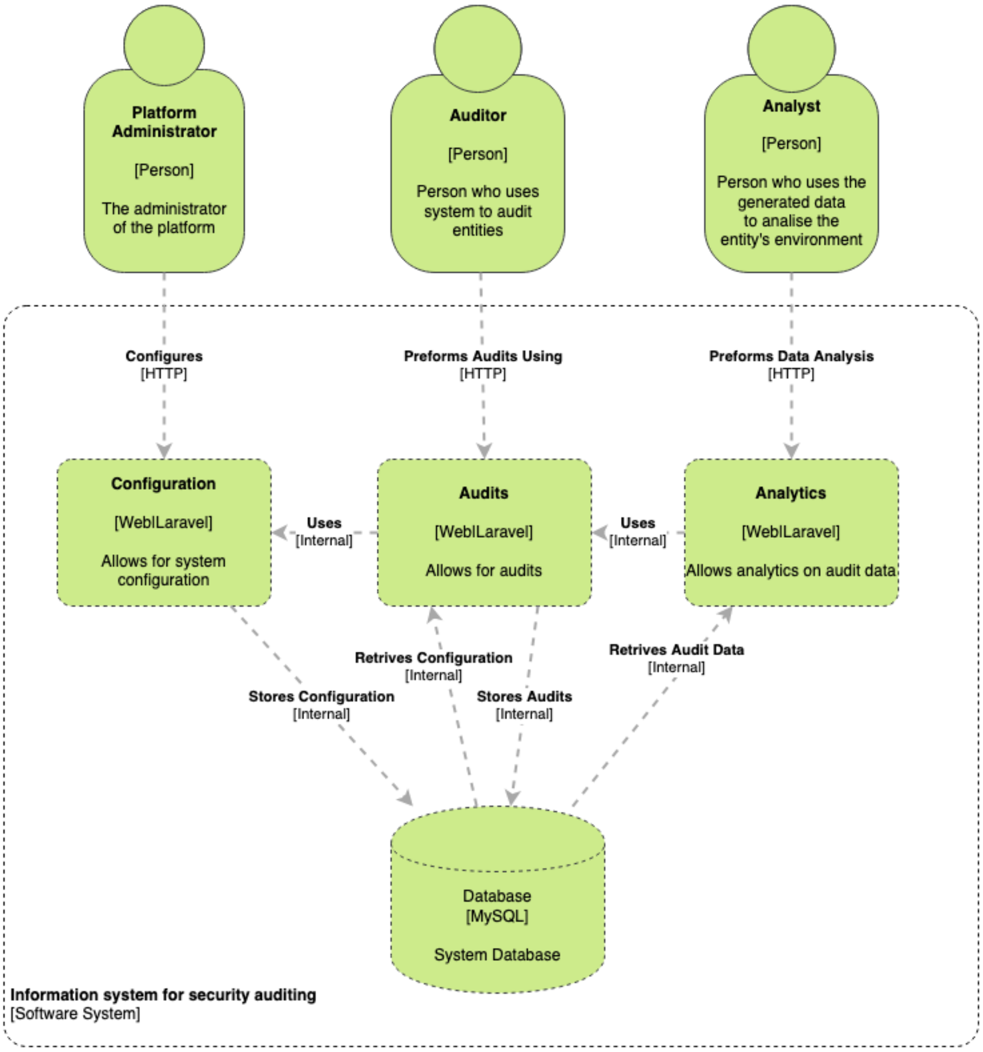


Figure 1. The C4 Level 2 diagram of the application architecture.

The application is organized into three layers: web access through a web browser; an application layer developed in Laravel; and a data layer implemented in a MySQL database (described in Section 3.3). Three major profiles were defined, according to the roles in the auditing process, namely audited enterprise, auditing team, and project manager. In each auditing process, the auditor can carry on multiple interventions. Each intervention is essentially the annotation by the auditor of the results obtained at each visit to the enterprise. Mitigation measures associated with the controls that did not pass are also registered in the application. The report summarizes all the interventions made, the controls that passed and failed, as well as the mitigation actions to be applied to each control, to elevate its compliance level. This report may be generated when needed, therefore allowing the continuous monitoring of the auditing process. Nevertheless, the most common approach is to generate the final report at the end of each intervention (when supported in that scenario) and in the final stage of auditing process to visualize the final results.

3.2. Customization

One of the most exciting features of this application is the ability to easily take a standard, norm, or guideline document and create a way to audit a company, to not only make sure that the standard is met, but also to support the efforts to improve the situation if it is not. To make this process as simple as possible, we created a set of CSV files with the structure we required to populate the auditing system database. The components that are imported to the database are the structure of the standard, the list of controls, the checklist actions, and the mitigation measures that should be applied to each control.

In Figure 2, we can see the overall customization procedure. It starts with: (1) the processing of the standard that we want to apply. In our case study [24] the ISO 27001:2013 standard was used, but the system can support any standard or similar document. The next set (2) is to populate the CSV files with the results of the processing, and in (3), the final step is to import the CSV file into the application.

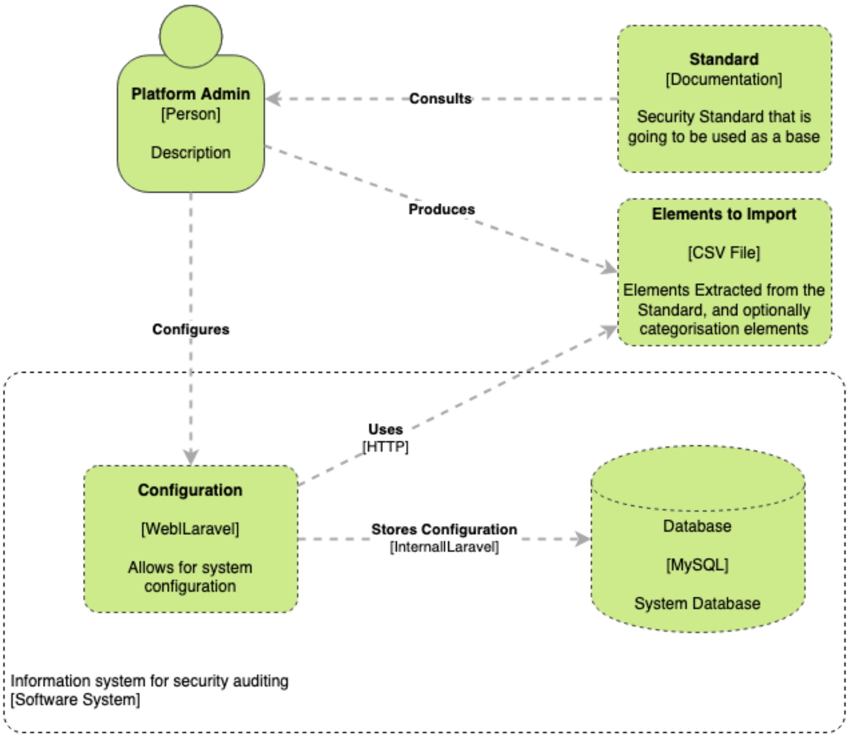


Figure 2. The C4 Level 2 diagram of the customization process.

The more complex part is Step (1). In this step, we need to extract from the standard a set of controls that are usually well defined and add two sets: one for actions and another for mitigation tasks. An action in this context is something that an auditor can validate, for example a specific policy being in place or a technological component being present. A mitigation is a suggestion of measures that should be applied in the case of the control not being fully compliant. These mitigation tasks should either get it to pass or at least improve it in a particular security issue.

Using a standard such as ISO 27001:2013 enabled us to start with a set of well-defined controls, but then, through the creation of the action set for each control, allowed for the possibility of tailoring the process to encompass entities that would otherwise be outside the scope of such a standard. Small companies or businesses that do not have a highly evolved IT infrastructure can still reap benefits from auditing their existing systems in the context of information security or cybersecurity, without the burden of trying to discern for themselves what parts of the standard are relevant to them.

This process is not, nor should it be, a one-time action. In the conducted case study [24], the target was a set of fifty SMEs in the center of Portugal, but if we needed to support the auditing of large enterprises somewhere else, all that would be required is to reevaluate the set of actions and mitigation tasks for that particular scenario; no code changes on the platform are required.

One option set in (1) is to create a set of categories, which allows for aggregation in the final reporting and, for large standards, can be helpful in the analysis of the auditing process.

As can be seen in Figure 3, we could even combine multiple standards and create a sort of meta-auditing framework that could allow companies to audit their processes in a way that encompasses multiple levels of security analysis.

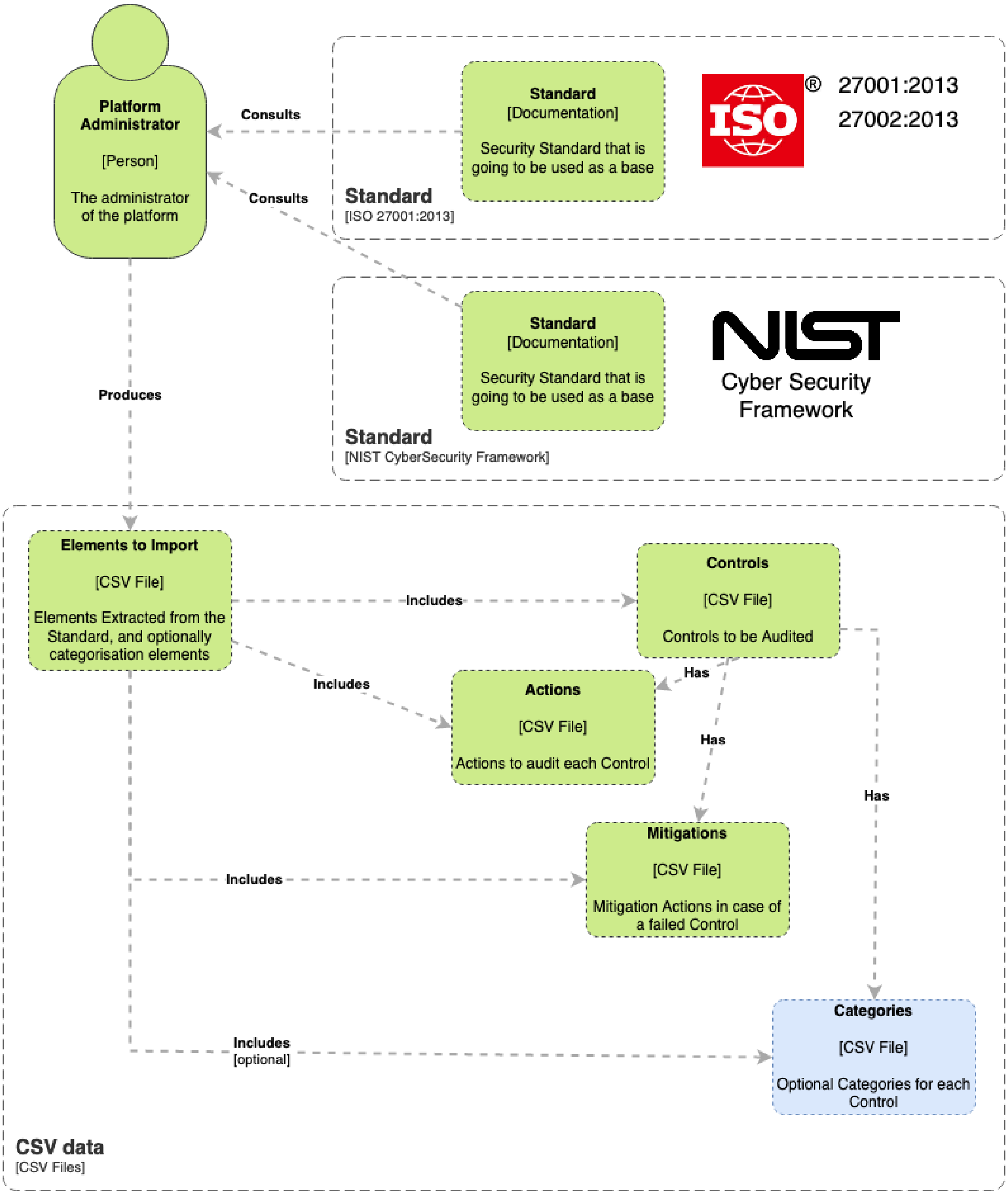


Figure 3. The C4 Level 2 diagram: customization from multiple sources.

3.3. Technologies

The project was developed with two main purposes in mind. First was to have uniformization of the collected data, which is vital for the aim of the project. Second was to allow the automatic generation of reports during the process and, at the end, to assess the outcomes. The IS was implemented in the Laravel framework, since the aim was to have a web application that could be easily accessed by the auditors' teams. Before starting a software implementation, it is important to ensure that all necessary prerequisites have been met or have at least progressed far enough to provide a solid foundation for the requirements that are needed. If the various prerequisites are not satisfied, then the software is likely to be unsatisfactory, even if it is complete. Therefore, the first phase was extremely important during the development phase, as it allowed fully understanding the users' needs and the level of data that was necessary to collect.

The application has three architectural and conceptual layers: a data layer where the data model is defined; a logic layer defining the business processes that are implemented; and finally, a view layer, which implements the data reporting functionalities for the user. The Model–View–Controller (MVC) design pattern integrates well with this architecture and is one of the most used in software engineering. Defined in 1998 [25] in the then-revolutionary Smalltalk programming language, it is still being researched today [26]. This pattern implies the separation of responsibilities of the three architectural layers, by keeping each component easy to evolve, isolated, independent, and highly reusable.

There are several options in today's web development to implement this kind of architecture. Some of them show great promise and interesting features, but this implies the downside of having a great deal of volatility in their ecosystem. PHP is among the most-used web languages, as it is very stable, and it has a few well-established frameworks that fit our architectural needs. PHP's Laravel Framework was chosen for this project because of its strong relationship with the MVC design pattern and the maturity of its codebase [27,28].

3.4. Database Model

The data modeling design included the ISO 27001:2013 standard controls, lists of actions, and mitigation task lists, but not making them explicitly dependent. Therefore, by using this strategy, any other auditing standard can be loaded to the database without additional changes needed to the data model. The data model entities are represented in the database scheme depicted in Figure 4. As can be seen, there is only one direct dependency between the ISO 27001:2013 parts of the data model and the controls' identification. This dependency can be easily assumed to be present in any standard, that is the entities Clauses, Categories, and Controls (upper left of Figure 4) are parts of the standards and are mapped in corresponding data tables of the data model.

The uniformization of the data collection process was initially performed by a "true/false" classification of the controls, which tends to make auditors perform round (and, in some way, binary) calculations during the control's analysis. A better uniformization was performed by applying a "true/false" classification to specific actions (i.e., some specific element to be checked) and grouping a set of actions for each control. This change gave more dynamicity to the calculation of the acceptance criteria, as is inferred from the actions' checklist, instead of the control itself. The mitigation tasks' list related to each control, which should be applied to those that did not fully pass, is provided to the auditors. The application associates this list to the auditing, which enables the possibility to report the mitigation tasks to the management board, for further implementations that may increase the compliance level of the corresponding control.

The database mimics the overall concepts of an information security standard, namely its associated controls, actions' checklists, and mitigation tasks' list. The information system developed organizes the inputs by categories; each one is composed of controls, and each control has clauses. These entities represent the data template that will be presented to the auditors for a specific intervention.

The platform was developed to deliver a customizable way to import the data entities previously described. These automatization and parameterization features allow the automatic importing and ingestion of these data entities from well-known structured formats, such as CSV. This format is easily adjustable to the checklist used by the information standard, and it can be imported automatically and applied in different scenarios.

Therefore, the platform can be set to support different types of standards that follow the same correlation between controls and actions.

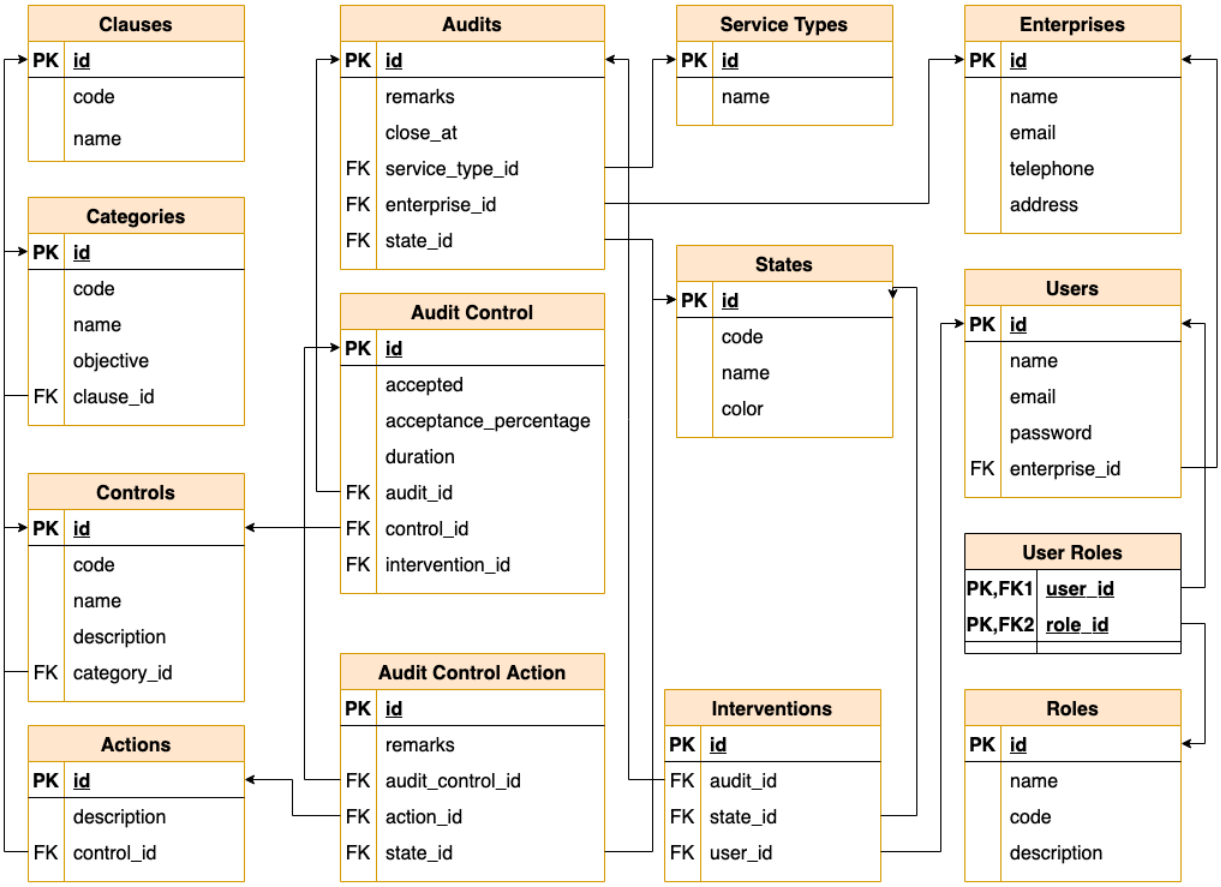


Figure 4. Data model.

Besides the standard entities imported from the CSV file, the data model incorporates other entities and their respective relationships, which are needed to store the auditing activity. As an example, the auditing interventions collect the controls validated by the auditor, which brings an additional management tool to evaluate and control the auditing as a whole. The entity Service Types addresses the two types of audits (Type 1 and Type 2) that were considered in our case study [24] and is described in Section 4.

4. Validation

The IS was successfully applied in a project that aimed to validate the global awareness of the cybersecurity infrastructure and organizational processes targeting the information security concerns of the fifty SMEs involved. The project used the ISO 27001:2013 standard and was led by a regional business association. From the 114 controls that are part of this standard, we may find a comprehensive list of controls that can be used to evaluate the awareness of the enterprise regarding cybersecurity in a particular subject and from a global perspective.

The results were fully described and analyzed in [24]. This section summarizes the results obtained, mainly the overall characterization of the auditing types and the order of magnitude regarding the number of interventions and controls that were analyzed.

Two types of intervention were defined: Type 1, which evaluated 30 out of the 114 controls, in predefined categories of the ISO 27001:2013; Type 2, which corresponds to a full assessment of the 114 controls, and a second validation (intervention) was considered, to assess the improvements attained with the implementation of the controls that did not fully pass in the first auditing. The data were stored in the MySQL database introduced previously (Section 3.4), and the reports can be generated throughout the auditing process. All the massive amount of data that supported the different audits was registered in the developed platform. The fact that the software was fully available to the audit team had great advantages for most of the roles in the project. Primary was the fact that all data were centered in a unique repository, allowing all the different players (roles) to assess the status of the overall process. The simplicity of the user interface, which aimed to facilitate the recording of the gathered data, in conjunction with the ability to monitor the amount of data being assessed is one of the advantages of using this type of technological solution. Its flexibility and the fact that it can be customized to support other needs in terms of different standards are major key points.

Information can be easily registered and retrieved from the web application that support the auditing process. Besides the speed and accuracy of the data gathered in the auditing process, it also allowed retrieving statistical and status data more quickly and with greater confidence in the accuracy. The adopted strategy brought improvements to the auditing productivity of all the people involved in the project. Although the application was designed to meet a specific purpose, its foundations were designed to allow it to be tailored to other standards that follow a similar structure. In the auditing process, from the 50 enterprises, 30 applied the Type 1 (standard) audit, and the remaining 20 enterprises applied the Type 2 (complete) audit, which considers a second intervention. Most enterprises were from the Industry sector (20), followed by Services (16) and Commerce (14).

Figure 5 resumes some of the characteristics of the audited enterprises. The majority of the enterprises (38%) had more than 60 workers, and in terms of age, they were well distributed, with the same number of companies having more than 36 years in business and others that were still young, with less then 17 years.

Regarding the amount of data stored in the database, the following values applied:

- Total amount of controls: 114;
- Total amount of actions: 607;
- Total amount of mitigation tasks: 248;
- Total amount of interventions: 146;
- Total amount of auditing actions: 32,133.

The results from the audit showed the improvements that the enterprises achieved due to the auditing process. Assessing the checklist of all the controls allowed making a diagnosis of the status of the enterprise. Type 1 (see Figure 6) showed the global diagnosis of the controls that were assessed. The major benefits can be seen regarding Type 2 (see Figure 7), since it allowed making a comparison between the initial status and the second interventions.

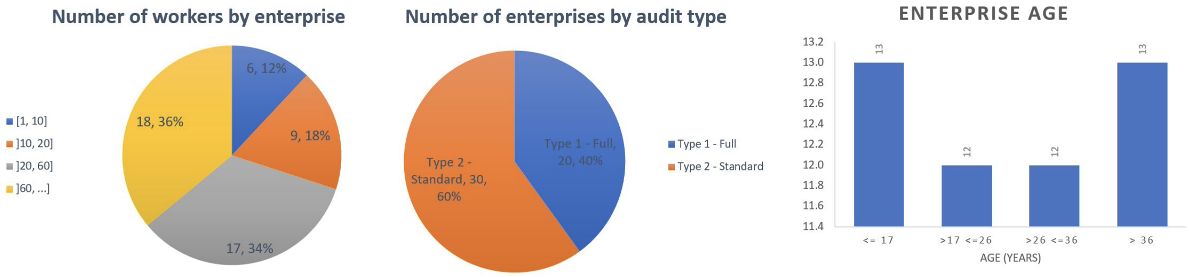


Figure 5. Enterprises' characterization.

In terms of software, the platform allows the auditor to see a list of all the controls considered in the auditing process. In Figure 8 is shown the interface that summarizes the current status if there are two controls (i.e., Control 6.1.1 and Control 5.1.1, from ISO27001:2013). Although the acceptance percentage is suggested by the platform, the auditor can change its value. The amount of visible information can be changed. The user can also drill down the information assessed of each control. It can also see the checklist items that were analyzed by the auditor and that were considered in the audit.

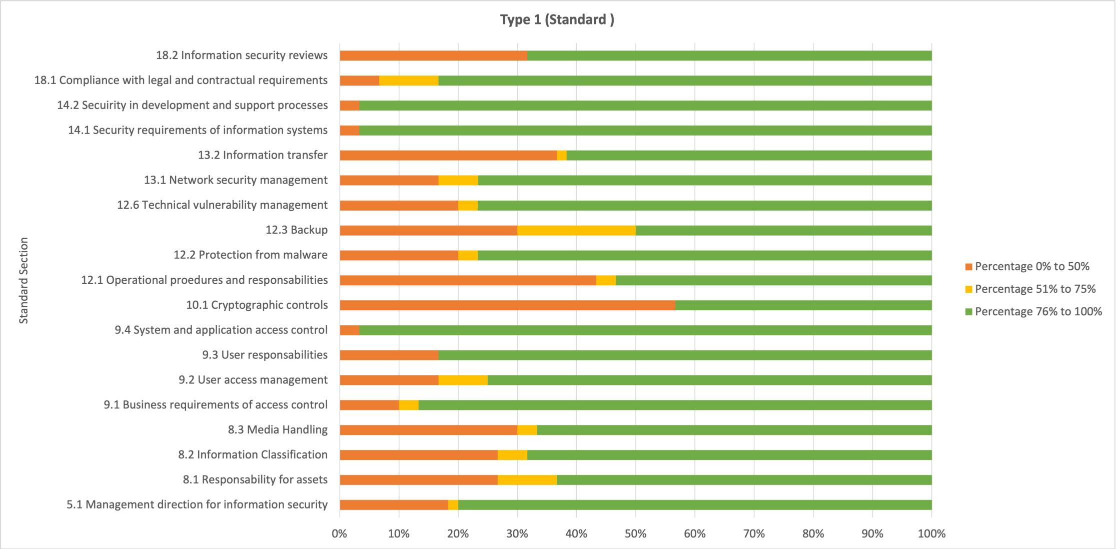


Figure 6. Type 1 results summarizing all the controls assessed in the audit.

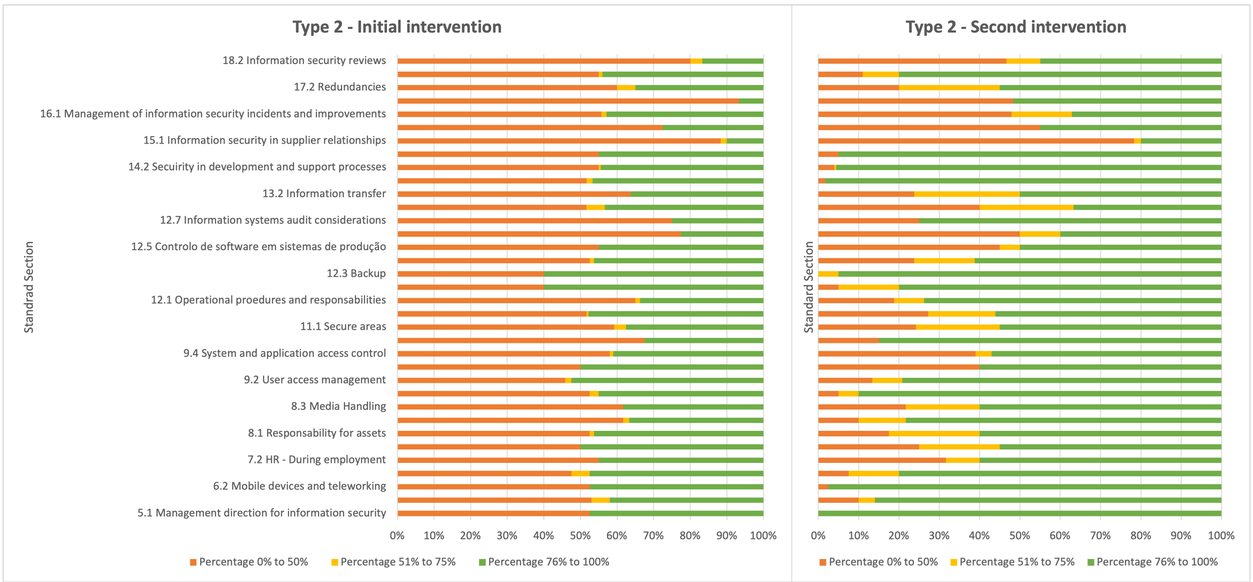
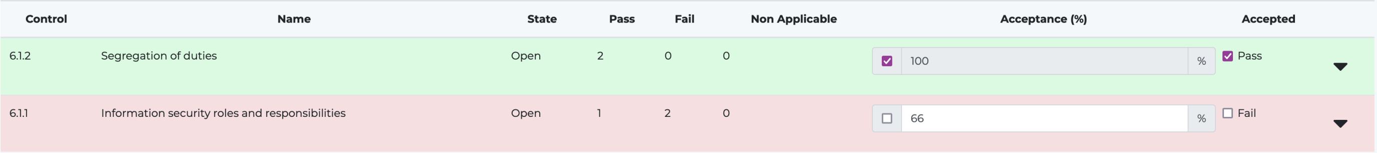


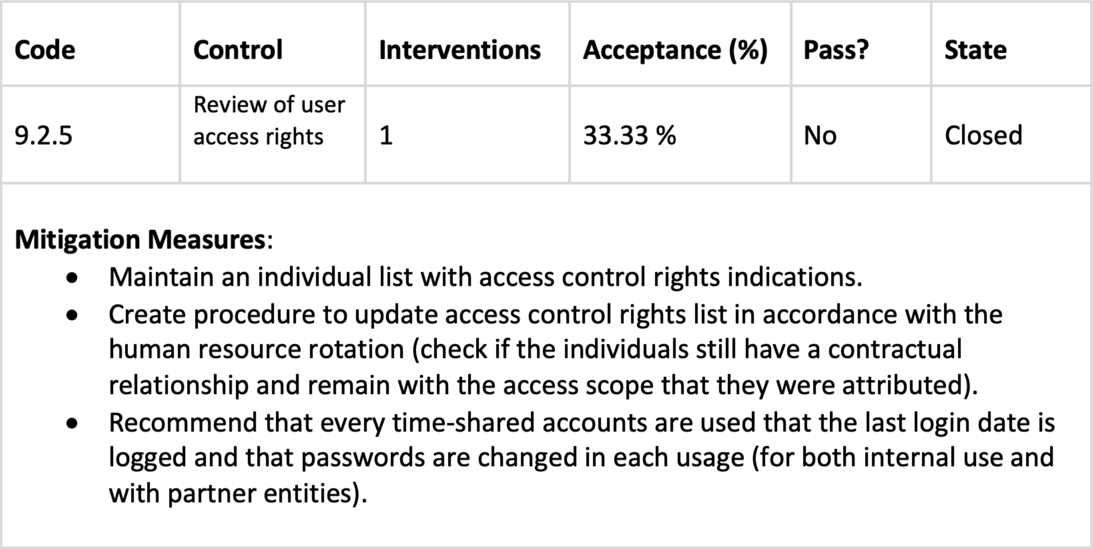
Figure 7. Results from the Type 2 audit, showing both interventions (the first and the second one).



Control	Name	State	Pass	Fail	Non Applicable	Acceptance (%)	Accepted
6.1.2	Segregation of duties	Open	2	0	0	☑ 100 %	☑ Pass
6.1.1	Information security roles and responsibilities	Open	1	2	0	□ 66 %	□ Fail

Figure 8. An example of the user interface and the level of information available.

Figure 9 shows how it is possible to generate the report that summarizes the overall auditing process. The example shows a detailed description of all data stored for Control 9.2.5 (ISO27001:2013). The reports are generated in PDF format, allowing full support with all systems known today. For each control considered in the auditing process, the report includes a summary of the name of the control, the interventions it refers to, the acceptance percentage, a true/false clause stating if it has passed or failed in the auditing process, and a state control verification setting if the control is considered close or not. For each control, the generated report also includes a list of suggested mitigation procedures that can be addressed to mitigate the vulnerability.



Code	Control	Interventions	Acceptance (%)	Pass?	State
9.2.5	Review of user access rights	1	33.33 %	No	Closed

Mitigation Measures:

- Maintain an individual list with access control rights indications.
- Create procedure to update access control rights list in accordance with the human resource rotation (check if the individuals still have a contractual relationship and remain with the access scope that they were attributed).
- Recommend that every time-shared accounts are used that the last login date is logged and that passwords are changed in each usage (for both internal use and with partner entities).

Figure 9. Example of the report generated for Control 9.2.5.

The major advantage of the platform is the ability to generate a full report about each intervention, when needed. All the data can also be exported, and since it follows the same layout in all the auditing processes, in the future, it can be used to generate richer reports/dashboards about the auditing process. These reports are also pivotal for the management board, as they give strict directions about the cybersecurity level and the measures that should be taken to reduce the risk.

5. Conclusions

This paper presented a generic, open-source, and web-integrated information security auditing information system. The architecture of the IS and the data model were described. The implementation in an information security and cybersecurity project was summarized, as well as the results achieved and the corresponding analysis were given. Besides, the case study was related to the implementation of an ISO 27001:2013 audit, and only the predefined checklist and mitigation actions were loaded in the platform. The data model is flexible and accommodates agnostic checklists and mitigation lists, which could be based on other standards, such as NIST-CSF, ISO 27009, or ISO 22301:2012. The strength of this IS is the fact that distinct and radically different information security and cybersecurity standards can be used and their corresponding actions and mitigation lists can be uploaded.

In the case study used to validate the IS, the participating enterprises were solely SMEs, intervened by a consulting team. The auditing management was centralized, and the consulting team was able to track the auditors' activities, the status of each auditing process, and the scoreboard with the global results. SMEs are a favorite target to use this type of IS to record the auditing activities, mainly due the fact that different standards can be adopted and benchmarked. Besides the IS possibly being a useful tool to the auditing teams, it could be also relevant to SMEs (and other types of enterprises) in cybersecurity self-assessment and self-auditing activities.

Additional features are being put forward in the IS, namely the development of a dashboard for an easy overview of the ongoing processes and a statistical analysis module to allow auditors to extract knowledge from the acquired datasets.

Author Contributions: Conceptualization, M.A., M.M. and R.G.; data curation, R.G.; formal analysis, M.A., M.M. and R.G.; funding acquisition, M.A. and M.M.; investigation, M.A., M.M. and R.G.; methodology, M.A., M.M. and R.G.; software, M.M. and R.G.; supervision, M.A., M.M. and R.G.; validation, M.A. and M.M.; visualization, R.G.; writing—original draft: M.A., M.M. and R.G.; writing—review and editing; M.A., M.M. and R.G.; 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available upon request from the corresponding author. The data are not publicly available due to privacy concerns and the need to be made anonymous upon 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
CSV	Comma-Separated Values
HR	Human Resources
ISMS	Information Security Management System
ISO	International Organization for Standardization
IS	Information System
IT	Information Technology
MVC	Model–View–Controller
NERLEI	Núcleo Empresarial da Região de Leiria
NIST	National Institute of Standards and Technology
NIST-CSF	NIST Cybersecurity Framework
SaaS	Software-as-a-Service
SBS	Small Business Standards
SME	Small and Medium-sized Enterprise

References

1. Al-Sartawi, A.M.M. Information technology governance and cybersecurity at the board level. *Int. J. Crit. Infrastruct.* **2020**, *16*, 150–161. [CrossRef]
2. ENISA Threat Landscape—2020. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ (accessed on 29 March 2022).
3. Nistotskaya, M.; Charron, N.; Lapuente, V. The wealth of regions: Quality of government and SMEs in 172 European regions. *Environ. Plan. C Gov. Policy* **2015**, *33*, 1125–1155. [CrossRef]
4. Street, D.; Albu, C.; Albu, N.W.; Webber, S.S. *The SMP of the Future in a Changing World*; Edinburgh Group: London, UK, 2019.
5. SME Definition. Available online: https://ec.europa.eu/growth/smes/sme-definition_en (accessed on 29 March 2022).
6. 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.
7. ISO 27K Forum—ISO 27001 ToolKit. Available online: https://www.iso27001security.com/html/toolkit.html (accessed on 29 March 2022).
8. NIST—Cybersecurity Framework Reference Tool. Available online: https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool (accessed on 29 March 2022).
9. ISO 22301:2012 Societal Security—Business Continuity Management Systems. Available online: https://www.iso.org/standard/50038.html (accessed on 29 March 2022).
10. Health Insurance Portability and Accountability Act of 1996. Available online: https://www.cdc.gov/phlp/publications/topic/hipaa.html (accessed on 29 March 2022).

11. 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 18 April 2021).
12. Mango—Limited Mango. Available online: https://www.mangolive.com/ (accessed on 29 March 2022).
13. ISO Manager—ISO Manager. Available online: https://www.isomanager.com/ (accessed on 29 March 2022).
14. Instant Management Systems B.V.—Instant 27001. Available online: https://instant27001.com/ (accessed on 29 March 2022).
15. Resolver—IT Compliance. Available online: https://www.resolver.com/lp/g/it-compliance/ (accessed on 29 March 2022).
16. OpensourceGRC—ISO 27001 Package. Available online: https://www.opensourcegrc.org/compliance-requirements?main=3 (accessed on 29 March 2022).
17. Eramba—GRC Software. Available online: https://www.eramba.org/documentation (accessed on 29 March 2022).
18. SecuraStar—ISO 27001 Software. Available online: https://www.securastar.com/iso-27001-software.php (accessed on 29 March 2022).
19. Advisera—Conformio. Available online: https://advisera.com/conformio/ (accessed on 29 March 2022).
20. Netwrix—ISO IEC Compliance. Available online: https://www.netwrix.com/ISO_IEC_Compliance.html (accessed on 29 March 2022).
21. Certikit—ISO 27001 ToolKit. Available online: https://certikit.com/products/iso-27001-toolkit/ (accessed on 29 March 2022).
22. IT Governance ISO 27001 Documentation Tool Kit. Available online: https://www.itgovernance.co.uk/iso27001_toolkits (accessed on 29 March 2022).
23. Teramind—ISO 27001 Compliance. Available online: https://www.teramind.co/solutions/compliance/ISO27001 (accessed on 29 March 2022).
24. 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. [CrossRef]
25. Krasner, G.E.; Pope, S.T. A description of the model-view-controller user interface paradigm in the smalltalk-80 system. *J. Object Oriented Program.* **1988**, *1*, 26–49.
26. Guamán, D.; Delgado, S.; Pérez, J. Classifying Model-View-Controller Software Applications Using Self-Organizing Maps. *IEEE Access* **2021**, *9*, 45201–45229. [CrossRef]
27. Valarezo, R.; Guarda, T. Comparative analysis of the laravel and codeigniter frameworks: For the implementation of the management system of merit and opposition competitions in the State University Península de Santa Elena. In Proceedings of the 2018 13th IEEE Iberian Conference on Information Systems and Technologies (CISTI), Caceres, Spain, 13–16 June 2018; pp. 1–6.
28. Laaziri, M.; Benmoussa, K.; Khoulji, S.; Larbi, K.M.; El Yamami, A. A comparative study of laravel and symfony PHP frameworks. *Int. J. Electr. Comput. Eng.* **2019**, *9*, 704. [CrossRef]