Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 196 (2022) 36–43

Procedia
Computer Science

www.elsevier.com/locate/procedia

CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2021

A Customizable Web Platform to Manage Standards Compliance of Information Security and Cybersecurity Auditing

Mário Antunes[a,c,*], Marisa Maximiano[a], Ricardo Gomes[b]

[a]*Computer Science and Communication Research Centre (CIIC), School of Technology and Management, Polytechnic of Leiria; Leiria, Portugal*
[b]*School of Technology and Management, Polytechnic of Leiria; Leiria, Portugal*
[c]*INESC TEC, CRACS, Porto, Portugal*

Abstract

Information security and cybersecurity are key subjects in modern enterprises' management, being ISO-27001:2013, NIST Cybersecurity Framework and ISO-27009 some of the most implemented international frameworks and standards. Their main goal is to globally reduce the risk, by leveraging enterprises' competitiveness in global markets and enhancing business processes and collaborators' cyber awareness. Auditing processes examine and assess a list of predefined controls. For each control, a set of corrective measures could be proposed, to increase its compliance with the standard being used. These processes are time-consuming, involve on-site intervention by specialized consulting teams on the intervened enterprises, and a set of status reports of all the interventions should be elaborated and delivered. The existing auditing information systems are not developed to meet Small and Medium-sized Enterprises (SME) requirements, as they are mostly proprietary and expensive, ground usually on off-the-shelf applications, and are not generic to be used by several standards with different checklists and auditing methodologies. In this paper, a generic and web-integrated cybersecurity auditing information system is described. Its architecture, design, and data model enable it to be used in a wide set of auditing processes, by loading a 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 on an ISO-27001:2013 information security auditing project, which has integrated fifty SMEs. The results obtained during the project are promising and reveal the appropriateness of using this information system in further similar auditing processes.

Keywords: Cybersecurity, Information Security, Auditing, ISO-27001, Small and Medium-sized Enterprises

* Corresponding author.
E-mail address: mario.antunes@ipleiria.pt

10.1016/j.procs.2021.11.070

1. Introduction

Information security and cybersecurity have gained enormous importance by enterprises management boards, as they are becoming aware about the need to protect data and IT infrastructure against cyberattacks [1,2]. Small and Medium-sized Enterprises (SMEs) have fuelled the economy worldwide and represent a large slice of the wealth produced [3]. Their specific characteristics, namely the small dimension, the lack of resident IT staff, and the traditional and familiar business model, put them in a second stage in what information security and cybersecurity auditing and certification concerns is about [4].

Consulting teams, which can be internal or external, bring to themselves the intervention and support in information security, namely by regularly auditing the enterprises according to international standards, like ISO-27001:2013, ISO-27009, and NIST Cybersecurity Framework (NIST-CSF). The auditing process is composed of a checklist to evaluate a list of controls, which is derived from the standard documentation. Consulting teams evaluate the level of compliance achieved by the enterprise in each control being evaluated, and, for each one, a tasks list is delivered to guide the auditor. After assessing all the controls, a global compliance score is calculated and for those that are not fully compliant with the standard, a list of countermeasures and mitigation tasks are proposed, to raise their compliance.

The auditing process can take several weeks or months, and a considerable number of interventions may have to be done, mostly on-site, where physical validation of existing software and hardware take place, as well as identification of assets, and identification of business processes, just to mention a few. During these interventions data are collected and stored for further analysis and reporting. Moreover, after an initial auditing process, a re-evaluation may take place, to assess the enhancements obtained, after applying the countermeasures proposed in the first auditing.

The existing Information Systems (IS) to manage cybersecurity and information security auditing processes are, in general, shallow, mainly due to their inflexibility to serve different standards and to be applied in a heterogeneous set of enterprises. These applications usually fall into two distinct groups: proprietary and oriented to complex auditing processes in big companies; open-source, usually free of charge and mainly composed of spreadsheet-based toolkits delivered by the community. 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. For example, a consulting team running several auditing processes on different companies with distinct standards, has to deal with different toolkits in a decentralized way.

This paper describes an IS to support and manage information security auditing processes. It was designed to load a predefined list of controls to be assessed, and the corresponding checklists and countermeasures tasks. It is supported in a web application, loads and processes checklists of any standards to assess a predefined set of controls. The IS was tested in a cybersecurity auditing project, in which fifty SMEs were audited for the ISO-27001:2013 standard [5].

The remainder of this paper is organized as follows. Section 2 describes the most relevant information systems and applications that support information security auditing, especially those related with ISO-27001:2013 standard. Section 3 details the information system, namely its overall architecture, main technological components, and the data model. Section 4 validates the information system being 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. Literature review

This Section describes a subset of tools available to support auditing interventions, mainly those related with ISO-27001:2013 standard. The list of the most relevant tools is enumerated in Table 1 and is divided into two main categories: commercial SaaS applications and community toolkits. The analysis was intended to ascertain if the tools require an existing organizational structure as well as technological maturity of the companies, that is if the applications can be easily applied to both small and large enterprises. The analysis also reflects if the tool support different standards or compliance regulations, other than ISO-27001:2013.

Table 1: ISO-27001 auditing support tools (links accessed on 26 May 2021).

Software Tool	Type	Open Source/ open access	Tech maturity	Other standards
SecuraStar - ISO 27001 Software https://www.securastar.com/iso-27001-software.php	SaaS	No	Yes	No
Advisera - Conformio https://advisera.com/conformio/	SaaS	No	Yes	No
Mango - Limited Mango https://www.mangolive.com/	SaaS	No	Yes	Yes
ISO Manager - ISO Manager https://www.isomanager.com/	SaaS	No	Yes	Yes
Netwrix - ISO IEC Compliance https://www.netwrix.com/ISO_IEC_Compliance.html	SaaS	No	Yes	No
Instant Management Systems B.V. - Instant 27001 https://instant27001.com/	SaaS	No	Yes	Yes
Resolver - IT Compliance https://www.resolver.com/lp/g/it-compliance/	SaaS	No	Yes	Yes
Certikit - ISO 27001 ToolKit https://certikit.com/products/iso-27001-toolkit/	Document Based	No	Yes	No
IT Governance ISO 27001 Documentation Tool Kit https://www.itgovernance.co.uk/iso27001_toolkits	Document Based	No	Yes	No
ISO 27K Forum - ISO 27001 ToolKit https://www.iso27001security.com/html/toolkit.html	Document Based	Yes	No	No
NIST - Cybersecurity Framework Reference Tool https://www.nist.gov/cyberframework/nist-cybersecurity-framework-csf-reference-tool	Standalone application	Yes	No	Yes
Teramind - ISO 27001 Compliance https://www.teramind.co/solutions/compliance/ISO-27001	SaaS	No	Yes	No
OpensourceGRC - ISO 27001 Package https://www.opensourcegrc.org/compliance-requirements?main=3	SaaS and Documents	Yes	No	Yes
Eramba - GRC Software https://www.eramba.org/documentation	SaaS	No	Yes	Yes

As can be seen on Table 1, the available tools are mostly delivered as SaaS cloud applications. According to the scarce documentation available, it is possible to infer that they are less suitable to small companies or those that lack technological maturity. SaaS products rely heavily on features that fit their required organizational structure, like 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. These documents guide the company on using the templates, documents related with policies, and spreadsheets to collect the necessary assets information, normally when an auditing process is being prepared.

Opensource GRC – ISO 27001 package is an interesting solution. It 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 and, for each clause and control of the standard, it provides a set of documentation, like 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.

3. Information System for ISO-27001 auditing

The IS described in this paper was built for ISO-27001:2013 auditing but was designed to support other standard specifications. The customizable approach under the web application was tailored based on the presumptions described as follows. 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 with a “true/false” response and the result allows an auditor to better define an acceptance percentage for each control. 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 to 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 do not allow this kind of flexibility.

In our case study [5] 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 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 ISO-27k family, which contrast 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.

3.1. Proposed Architecture

Figure 1 depicts the auditing process, namely the collection of evidence made by the consulting 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 analyse the aggregated results.

The application is organized into three layers: web access through a web browser; application layer developed in Laravel; a data layer implemented in a MySQL database (described in Section 3.2). 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.

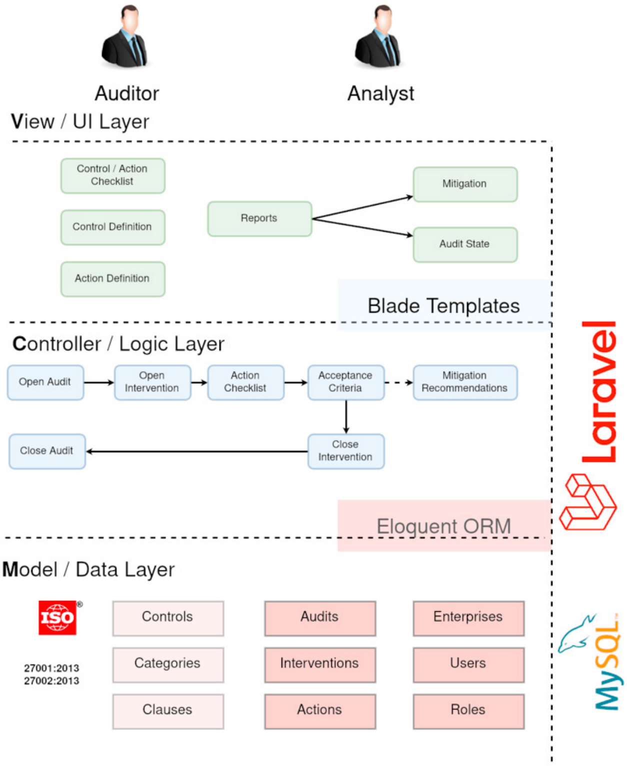

Figure 1. Overall architecture of the developed application.

3.2. Technologies

The project was developed with two main purposes in mind. Firstly, it allows an uniformization of the collected data, which is vital for the aim of the project. Secondly, it allows 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 completed 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 completed. Therefore, the first phase was extremely important during the development phase, as it allowed to fully understand the users' needs and the level of data that was necessary to collect.

The application has three architectural and conceptual layers: a data layer defines the data model; a logic layer defines the business processes that can be performed; and a view layer implements the data reporting functionalities to 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 [6] in the then revolutionary Smalltalk programming language, it is still being researched today [7]. This pattern implies the separation of responsibilities between 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 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 [8] [9].

3.3. Database model

The data modelling design included the ISO-27001:2013 standard controls, lists of actions and mitigation task lists, but not making them an explicit dependency. 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 2. 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 that is present in any standard, that is the entities `Clauses`, `Categories` and `Controls` (upper left of Figure 2) are part of the standards and are mapped in corresponding data tables of the data model.

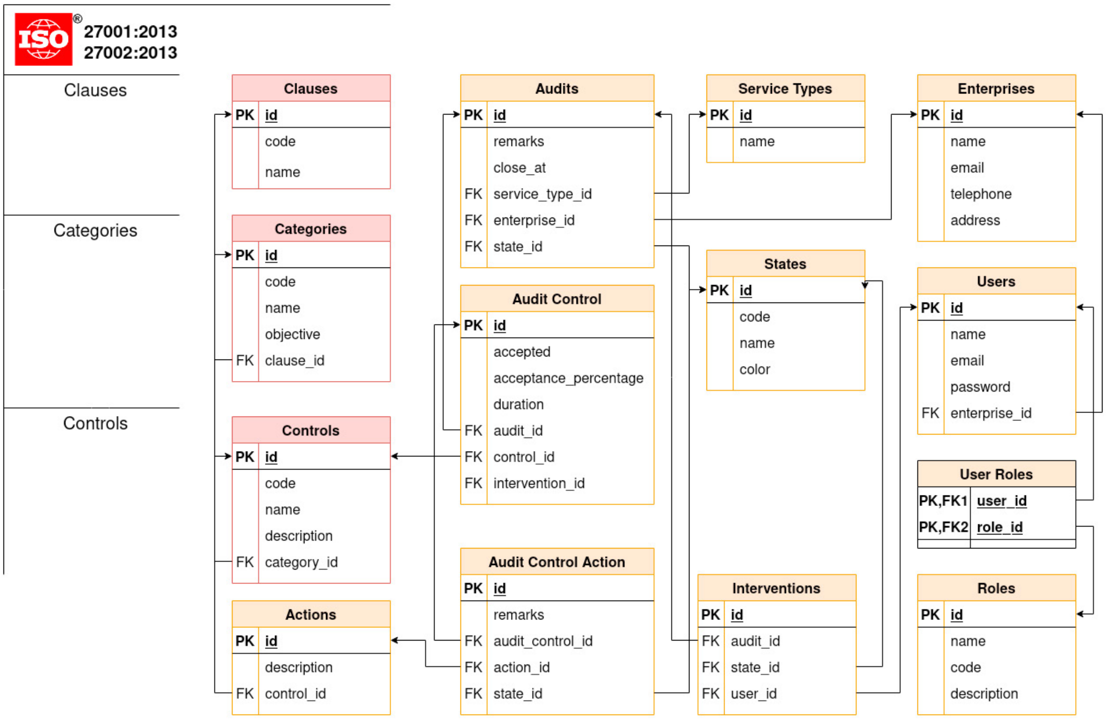
ISO®
27001:2013
27002:2013
Clauses
Categories
Controls
Clauses: PK id, code, name
Categories: PK id, code, name, objective, FK clause_id
Controls: PK id, code, name, description, FK category_id
Actions: PK id, description, FK control_id
Audits: PK id, remarks, close_at, FK service_type_id, FK enterprise_id, FK state_id
Audit Control: PK id, accepted, acceptance_percentage, duration, FK audit_id, FK control_id, FK intervention_id
Audit Control Action: PK id, remarks, FK audit_control_id, FK action_id, FK state_id
Service Types: PK id, name
States: PK id, code, name, color
Interventions: PK id, FK audit_id, FK state_id, FK user_id
Enterprises: PK id, name, email, telephone, address
Users: PK id, name, email, password, FK enterprise_id
User Roles: PK,FK1 user_id, PK,FK2 role_id
Roles: PK id, name, code, description

Figure 2. Data model.

The uniformization of the data collection process was initially made by a "true/false" classification of the controls, which tends to make auditors do round (and, in some way, binary) calculations during the control's analysis. A better uniformization was made, by applying a "true/false" classification to specific actions (i.e., some specific element to be checked) and group a set of actions for each control. This change gave more dynamic to the calculation of the acceptance criteria, as it is inferred from the actions' checklist, instead of the control itself.

The mitigation tasks list related to each control, which should be applied for those who 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 compliant level of the corresponding control.

The database mimics the concepts of the ISO-27001:2013 standard and its associated controls, actions checklists and mitigations task list. Therefore, the IS organizes the inputs by categories that have controls, and each control has clauses. These entities represent the data template that will be presented to the auditors on a specific intervention. The platform was developed to allow a customizable way to import the data entities previously described. These automatization and parameterization features allow the automatic import and ingestion of these data entities from well-known structured formats, such as CSV (entities highlighted in red, in Figure 2). CSV format is similar and easily adjustable to the checklist used by ISO-27001, can be imported automatically and applied in different scenarios. The entity `Service Types` addresses the two types of audits (Type 1 and Type 2) considered in our case study [5], which is described in Section 4.

4. Validation

The IS was successfully applied in a project that aimed to validate the global awareness of fifty SMEs involved, regarding their cybersecurity infrastructure and organizational perspective. The project was leaded by a regional business association and its results are fully described and analysed in [5]. This Section summarizes the results obtained, namely: 1) the ability of the IS to support both types of auditing; 2) the varying number of interventions for each enterprise, which confirms their drastically different organizational and technological structures.

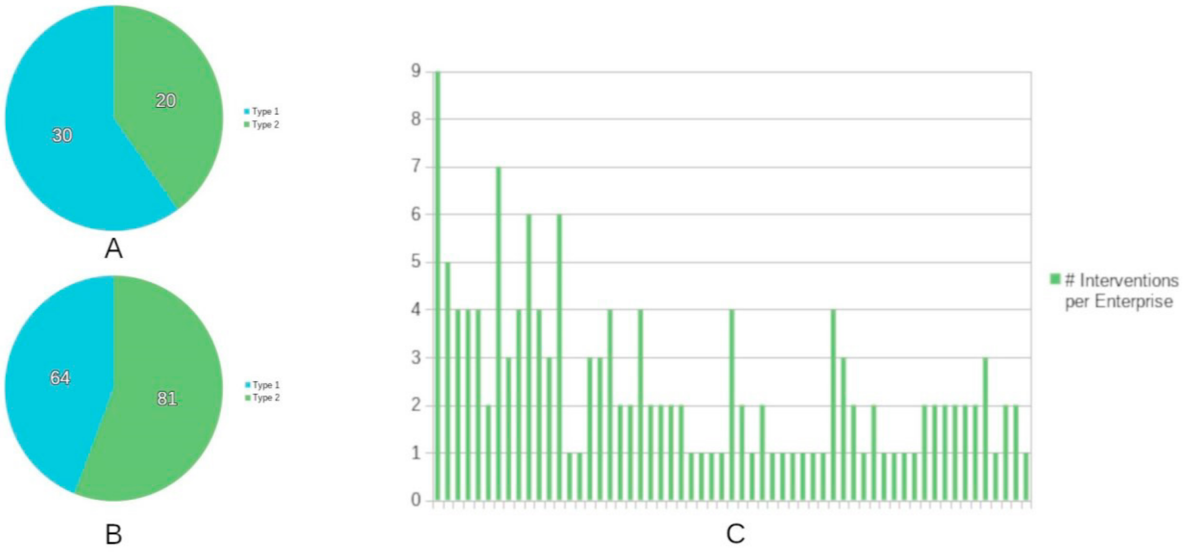

Figure 3. A) Enterprises per type; B) Interventions per type; C) Interventions per enterprise.

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 pass in the first auditing. The data is fully stored in the MySQL database introduced previously (Section 3.3), and the reports can be generated throughout the auditing process.

Figure 3(A) indicates the number of enterprises that participated in the case study, namely 30 enterprises have been intervened in the Type 1, while 20 have chosen Type 2. In Type 2, since it considers a second assessment of the actions that have failed in the first auditing, a higher number of interventions have been done. The amount of data generated by this process can be seen in Figure 3(B), where it is possible to identify the number of interventions by type, registered in the platform. Figure 3(C) depicts the number of interventions by enterprises.

Figures 3(B) and 3(C) illustrates a key benefit of using the proposed IS, namely its flexibility in allowing for different audit types, which could be easily extended to different standards. Multiple physical interventions are also allowed for enterprises of distinct complexity whilst creating a homogeneous set of reports [5].

5. Conclusions and future work

This paper presented a generic, open source, and web integrated information security auditing IS. The architecture and the data model are summarized. The implementation in an information security and cybersecurity project was described, as well as the performance results achieve, is summarized. Besides the case study was related with an ISO-27001:2013 auditing, and only the predefined checklist was loaded in the platform, the data model is flexible and accommodates agnostically checklists that could have been based on other standards, such as NIST-CSF or ISO-27009.

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 favourite target to use this type of IS to record the auditing activities, mainly due to their intrinsic characteristics. Besides the IS can be 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.

Besides the adoption of the IS in auditing projects, additional features are being put forward. A dashboard for easy overview of the ongoing processes, and a statistical analysis module to allow auditors to extract knowledge from the acquired datasets.

Acknowledgements

The authors acknowledge NERLEI business association project team by the support given along the implementation of the project. This project was funded by “POCI—Programa Operacional para a Competitividade e Internacionalização” grant number POCI-02-0853-FEDER-026352. This publication and the research was funded by FCT—Fundação para a Ciência e Tecnologia, I.P., under the project UIDB/04524/2020.

References

[1] Al-Sartawi, A. M. M. (2020). Information technology governance and cybersecurity at the board level. International Journal of Critical Infrastructures, 16(2), 150-161.

[2] ENISA Threat Landscape (2020), available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/, accessed on 8, May, 2021.

[3] Nistotskaya, M., Charron, N., & Lapuente, V. (2015). The wealth of regions: quality of government and SMEs in 172 European regions. Environment and Planning C: Government and Policy, 33(5), 1125-1155.

[4] Ozkan, B. Y., & Spruit, M. (2021). Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1252-1278). IGI Global.

[5] Antunes, M.; Maximiano, M.; Gomes, R.; Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. J. Cybersecur. Priv. 2021, 1, 219-238. doi: 10.3390/jcp1020012

[6] G. E. Krasner and S. T. Pope, “A Description of the Model-View-Controller User Interface Paradigm in the Smalltalk-80 System,” Journal of Object-Oriented Programming, vol. 1, no. 3, p. 35, Aug. 1988.

[7] D. Guamán, S. Delgado, and J. Pérez, “Classifying Model-View-Controller Software Applications Using Self-Organizing Maps,” IEEE Access, vol. 9, pp. 45201–45229, 2021, doi: 10/gj3fhb.

[8] R. Valarezo and T. Guarda, “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 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Jun. 2018, pp. 1–6. doi: 10/gj3d64.

[9] M. Laaziri, K. Benmoussa, S. Khoulji, K. Mohamed Larbi, and A. E. Yamami, “A comparative study of laravel and symfony PHP frameworks,” IJECE, vol. 9, no. 1, p. 704, Feb. 2019, doi: 10/gj3d4x.