Journal of Information Systems and Technology Management – Jistem USP
Vol. 16, 2019, e201916007
ISSN online: 1807-1775
DOI: 10.4301/S1807-1775201916007

# MULTICRITERIA ANALYSIS OF THE COMPLIANCE FOR THE IMPROVEMENT OF INFORMATION SECURITY

**Pedro Solana-González**[1] http://orcid.org/0000-0001-5606-1476
**Adolfo Alberto Vanti**[2] http://orcid.org/0000-0001-5176-2572
**Karen Hackbart Souza Fontana**[3] http://orcid.org/0000-0002-4932-3738

[1]University of Cantabria, Santander, Spain
[2]Universidade Federal de Santa María, Santa Maria, RS, Brazil
[3]Educational Institution São Judas Tadeu, Porto Alegre, RS, Brazil

## ABSTRACT

Information security is a current issue of protection of information assets that considers significant variables of a strategic, organizational and IT governance nature, and that requires to analyze the compliance with international standards that regulate business actions. In this way, the work analyzes institutional compliance to improve information security applying the Analytic Hierarchy Process methodology to the specific practices defined in ISO/IEC 27002:2013. *Expert Choice* has been used as Decision Support Systems that has generated as a result the ranking of priorities of the criteria and alternatives used in the decisional process. It has been later applied in a medium-sized Brazilian industrial company. The results identify that the main security practice is the one related to the independent critical analysis of information security.

**Keywords:** Information security, Compliance, Security practices, Analytic hierarchy process, Decision support system

Manuscript first received: 2018/11/25. Manuscript accepted: 2019/10/10
*Address for correspondence:*
*Pedro Solana-González,* University of Cantabria, Santander, Spain. Email: pedro.solana@unican.es
*Adolfo Alberto Vanti*, Universidade Federal de Santa María, Santa Maria, RS, Brazil. Email: adolfo.vanti@san.uri.br
*Karen Hackbart Souza Fontana*, Educational Institution São Judas Tadeu, Porto Alegre, RS, Brazil. Email: karen.hsfontana@gmail.com

Published by TECSI FEA USP, Brazil – 2019 *www.jistem.fea.usp.br*

## INTRODUCTION

Information security is a dynamic process that facilitates the information protection as the main organizations' asset and reaches a strategic significance (May, 2003; Doherthy & Fulford, 2005; Park & Ruighaver, 2008). This happens in the field of banking, since such type of organizations, which have operational risk, also have its own business risk (Shamala et al., 2015). Therefore, they might lose their ability to properly manage information and their critical processes (customers, suppliers and internal processes) can be affected by even stopping working (OECD 2005; COM, 2006; Pérez-González & Solana-González, 2006) due to the increase in cyber-attacks (Li et al., 2019).

Therefore, information security has become a globally essential element for organizations since it reduces risks and improves the information compliance (Safa, Von Solms & Furnell, 2016). Likewise, in payment cards development and even in the protection of the information security infrastructure in smart cities (Hasbini, Eldab, & Aldallal, 2018) it has become a concern both for scholars and specialized professional, by considering the challenges and practices that help organizations to more accurately and faster detect the breaches and as self-learning for the continuing refinement (McLaughlin & Gogan, 2018).

Information security can be defined, according to Sêmola (2014), as an area of knowledge devoted to the information assets protection against unauthorized access, undue disturbances or its unavailability. Due to Information Technologies (IT) development, information security now covers different topics such as could computing security, the internet of things (IoT) security, user authentication, network security, hardware security, software security, and data encryption (Awad, 2018).

Researches related to cyber security also increasingly consider the strategic, organizational and IT governance variables by analyzing issues related to compliance of information security standards and its certification (Kim, Leem, & Lee, 2005; Kwon et al., 2007; Siponen & Willison, 2009). Such researches also study real cases of information security application in large companies and public bodies (Smith & Jamieson, 2006; Solana-González & Pérez-González, 2011).

In this regard, information security is recognized as a process (Dhillon & Backhouse, 2000; Navarro, 2006) which is developed within an organizational context from which it can't be isolated and which is completely affected. It is a process in which both people and technology actively participate. Thus, since information security is an issue that affects the whole organization, it is needed to deepen its study and broaden the analysis through interdisciplinary approaches which consider organizational and corporate variables by including the compliance analysis to improve its comprehension and implementation by the companies (Melville, Kraemer, & Gurbaxani, 2004; Gordon & Loeb, 2006; Hubbard, 2010).

Within this framework, the research problem is based on the multicriteria analysis of the compliance for the improvement of information security. This requires the multicriteria calculation to define priorities in the compliance variables by using Analytic Hierarchy Process (AHP) and the Expert Choice Decision Support Systems (DSS). Therefore, the research purpose is to analyze the institutional compliance which supports information security by using the AHP method, which is presented by practical support.

## LITERATURE REVIEW

This work's literature review considers the information security strategy, the security practices and the compliance. The research methodology applied is subsequently presented by establishing the type of Decision Support System (DSS) and the AHP multicriteria method used (Saaty, 1980).

### Information security strategy

Information security studied by both scholars and professionals is a relatively modern concept in the management field (Dhillon & Backhouse, 2000; Gordon & Loeb, 2006), which has had an important impact due to the use of the Internet in businesses and the inherent risks of the net. Such impact is also due to the identification of factors that influence the understanding about information security in fee-based mobile services (Gao, Rau, & Zhang, 2018).

However, despite the acknowledgment of its importance, the reports and statistics from international bodies suggest that there is still much to be done regarding information security, especially in small-to-medium enterprises (SME) where the adoption rate of security strategies and policies is lower than 21% (OECD, 2009; Giannakouris & Smihily, 2010), though it is increasing in recent years. Dimopoulos et al. (2004) have also analyzed the security practices and the risk assessment in SME by highlighting that due to their restrictions regarding experience, knowledge and budget, they require a new risk analysis and management methodology approach.

The internationally known standards and models of information security management underscore the need for considering information security in organizations as a process whose development must start from the strategic level of the organization (BS7799-2, 2002; ISO/IEC 27001:2007).

In this sense, this work focuses on security strategy and policy (Ward & Peppard, 2002; Doherty & Fulford, 2006; Von Solms & Von Solms, 2005; Park & Ruighaver, 2008) from a compliance approach for information security to be no longer considered as an exclusively technical matter isolated from the rest of the organization (May, 2003; Luftman, Kempaiah, & Nash, 2006; May & Dhillon, 2010).

It is, therefore, needed to deepen on multicriteria decision models which use variables of the ISO/IEC 27002:2013 standard from a strategic approach that defines the priorities for the organization's security, especially regarding compliance, since this type of analysis is complex and has a multidisciplinary nature. Thus, by also considering the little attention to this matter by security literature in comparison with other more technical approaches (Botha & Gaadingwe, 2006; Park & Ruighaver, 2008), this work is integrated with the decision matter to choose the best way for the managers to provide with effective alternatives for information security control.

### From strategy to security practices

From the reference works analyzed which underlie the topic, it is highlighted that security strategy must be elaborated from a management approach, associated with the corporate strategy rather than from a technical approach, which allows the setting of long-term security policies (May, 2003). Organizations also need to formulate or reformulate strategies to the security of their information and to reduce gaps which consider different knowledge levels in this important subject. They also need to carry out condition analysis to motivate the adoption by taking into account the protection from a more internal protection approach to a more systemic approach regarding resources, capabilities and external environment (Horne, Maynard, & Ahmad, 2017).

According to Wang (2005), information security strategy requires a long-term commitment which must be materialized with regard to resources, business demands, and the context of each company (elements that affect the enterprise). Therefore, the strategy is unique for each organization by also considering professional competencies linked to the compliance behavior from the users regarding information security policies (Tsohou & Holtkamp, 2018).

Doherty and Fulford (2005) explain the need of alignment between security policies and the information systems' strategic plan of the organization. Kim & Kim (2017) focus the information security practices based on theory of planned behavior.

According to Park and Ruighaver (2008), information security strategy is the art of deciding how to better use technology and appropriate information security measures and applying them in a coordinated way to defend the organization's information infrastructures against internal and external threats by offering confidentiality, integrity and availability as cost-effectively as possible.

Hone and Ellof (2002) analyze security policy according to the international standards, pointing out that the standards and companies have to work together to define what security policy should be. May (2003) studies the relations among the corporate culture, the security strategy and the BS7799-2 standard and highlights the need of integrating the security strategy as part of the corporate strategy. Nasir and Arshah (2018) lead the approach to the establishment of efforts to foster the information security culture among employees, which is directly related to the security behavior in the workplace. Likewise, (Li et al., 2019) have proved that when employees understand the policy and the company security procedures, they are more competent and skillful in the assessment of cyber threats and in the compliance with this type of protection.

The literature review highlights the need of defining the information security strategy, at the higher organizational level, integrated into the corporate strategy and defined according to the context, goals and business demands. Therefore, once its strategic significance is recognized, the security policy must be developed as a dynamic process which establishes and monitors the compliance of the guidelines, procedures and specific measures according to the information security goals set by the strategy and standards that can be applied.

The information security's goal is to ensure the information protection against unauthorized access, by making it available at the right time in a reliable way. Thus, it is influenced by three main characteristics: confidentiality, integrity and availability of the information (Awad, 2018; Uddin & Preston, 2015, Safa et al., 2015, Sêmola, 2014, Dhillon & Backhouse, 2000). Likewise, it is important to underscore other requirements: (i) compliance – fulfillment of requirements (Buccafurri et al., 2015; Safa, Von Solms, & Furnell, 2016); (ii) responsibility – to take on obligations and new opportunities (Dhillon & Backhouse, 2000); (iii) behavioral trust – accepted and agreed behavioral patterns (Dhillon & Backhouse, 2000); (iv) ethics – informal behavior, moral values (Dhillon & Backhouse, 2000); (v) security policies – employees' statements and responsibility to safeguard the information and resources (Bulgurcu, Cavusoglu, & Benbasat, 2010) and to follow codes of good practices (Bloomfield et al., 2018).

Thanks to these requirements, information security reduces the impact or the probability of security threats and weaknesses at an acceptable level for the organization (Singh & Margam, 2018). Therefore, information security practices related to security technology adoption and to the user behavior (Bulgurcu, Cavusoglu, & Benbasat, 2010; Sêmola, 2014; Parsons et al., 2015; Safa et al., 2015) are used so that the information security goals (Dhillon & Backhouse, 2000; Bulgurcu, Cavusoglu, & Benbasat, 2010; Sêmola, 2014; Uddin & Preston, 2015) can be addressed.

The information security practices might reduce weaknesses, constrain the impacts, and avoid the risks for the business (Sêmola, 2014). In this sense, ISO/IEC 27002:2013 is underlined since it specifically addresses information security practices through an appropriate combination of organizational controls, policies and procedures and hardware and software functions. Thus, it can be considered as the starting point to establish guidelines and targets to manage information security (Rios, Teixeira Filho, & Silva Rios, 2017).

According to Sêmola (2014), the ISO/IEC 27002:2013 standard represents an important instrument that indicates which direction the companies concerned about the business operation, the systems' protection and the cyber security should take. The ISO/IEC 27002:2013 consists of 18 information security categories (the first four ones are introductory ones), where each one meets a control goal (what it is expected to achieve) and the implementation guidelines (detailed information about control support). Thus, these categories converge and contribute to the improvement of different standards, architectures and cyber security patterns (Srinivas, Das, & Kumar, 2019).

This research contemplates the practices related to the section 18 domains – Compliance (Sêmola, 2014). The domains refer to: (D1) Identification of applicable legislation and contractual requirements, (D2) Intellectual property rights, (D3) Protections of records, (D4) Privacy and protection of personally identifiable information, (D5) Regulation of cryptographic controls, (D6) Independent review of information security, (D7) Compliance with security policies and standards and (D8) Technical compliance review.

According to the strategic approach explained and to an orientation to information security practices, the research organizes a decision hierarchic model which integrates strategic variables from the ISO/IEC 27002:2013 standard by aligning the information security policy with particular emphasis on compliance to consider the most feasible way of protection against potential threats (Singh & Margam, 2018). This theoretical-practical model expands the current approaches by establishing a line of research to define the decision priorities by considering the strategic complexities through pairwise comparisons among the different variables involved.

## Compliance with standards and guidelines

Compliance refers to the fulfilment of the regulatory standards both in the internal and external environment of the organization (Ferreira et al., 2014; Mateescu, 2015), which makes a good governance possible since it requires transparency and commitment to the ethical standards, it helps to reduce risks and safeguard the organization's image (Oliveira et al., 2015). Torten, Reaiche, & Boyle (2018) analyze the relation between the awareness of threats from IT professionals and their behaviors of perceived severity, perceived vulnerability, self-efficacy, response efficacy, and response cost.

Hina and Dominic (2018) contemplate compliance as the fulfilment of the information security policies regarding information security culture, awareness, and management. These authors' research revealed that the information security compliance is poor, as well as the dissemination of information security policies to employees. Merhi & Ahluwalia (2019) prove that non-compliance is related to the resistance against information security policies by highlighting that morality and descriptive standards reduce that type of resistance.

It is also noted that some information security incidents have been caused by poor management, rather than by technological weaknesses. Therefore, organizations aim to improve information

security by requiring the security guidelines fulfilment by the employees (Park & Chai, 2018). However, this compliance requirement by means of standards and guidelines can give rise to loss of motivation. According to Cong et al. (2017), users want to participate in an autonomous and active way in the development of safe environments, while information managers and experts want to limit that autonomy. This can lead to a restriction by avoiding the flexibility of administrative activities through a strict control of the procedures.

Griffith et al. (2016), at the symposium organized by *Fordham Journal of Corporate & Financial Law,* addressed compliance as a means to make sure that the employees or other parties are fulfill the standards and the internal and external regulations of the organization. The authors state that compliance makes risk assessment possible, but it can constrict the company's activity.

Knuplesch and Reichert (2017) affirm that the major challenge for companies is to ensure the compliance of their business processes. To that end, organizations use corporate guidelines, better practices and standards. The authors underscore that the compliance standards must be accessible for the specialists to apply and verify them. Likewise, they must avoid ambiguities and have an automated processing.

## METHODOLOGY

The Analytic Hierarchy Process (AHP) is used as Decision Support Systems (DSS) (Sprague & Carlson, 1982; Aversa, Cabantous, & Haefliger, 2018; Keenan & Jankowski, 2019) with its different generator systems. The Multiple Criteria Decision Making (MCDM) is a well-known multicriteria methodological approach for the decision-making process. In addition, it has applications in many areas of scientific and management knowledge, such as the selection of technological solutions, the problems related to location, outsourcing or logistic providers selection (Bianchini, 2018).

The AHP method can be applied to solve problems that require assessment and measurements by establishing weights to the different criteria that take action in setting alternatives, classifying and prioritizing the different decision alternatives. This also happens in the study combined with fuzzy logic applied to providers (Awasthi, Govindan, & Gold, 2018), as well as in Corporate Social Responsibility (CSR) due to the strong influence in the environmental and social issues market (Abdul et al., 2018).

The AHP technique is developed through six key stages SAATY (1980):

1. To define the problem and establish clear goals and the expected results.
2. To deconstruct a complex problem in a hierarch structure of decision elements. At the high level of the hierarchy, the general goals and criteria are divided into particular goals or sub criteria to reach the lowest level where the alternatives are located.
3. To make comparisons among pair-wise decision elements, creating matrices based on the establishment of the relative importance among the factors of each hierarchic level.
4. To check the matrices' consistency properties to ensure that the reasoning made by the decision maker is coherent and consistent.
5. To estimate, according to the previous matrices, the relative weights of the decision elements.
6. Likewise, the way of adjusting or giving importance among the factors is established in accordance with Table 1, which is presented below.

**Table 1.** Weight definition scale in AHP.

| | |
|---|---|
| 1 | Factor i is as important as factor j. |
| 3 | Factor i is slightly more important than factor j. |
| 5 | Factor i is significantly more important than factor j. |
| 7 | Factor i is strongly more important than factor j. |
| 9 | Factor i is extremely more important than factor j. |
| 2,4,6,8 | Intermediate values. |

**Source**: (Saaty, 1980; Cobo, Vanti, & Rocha, 2014).

The AHP method works according to a recommendable psychological judgment of 7 points of difference with 2 variability points related to DSS (Hogue, 1987). It is possible to support the resolution of little or non-structured problems by converging in an increase of links between criteria and alternatives that create a new strategic decisions' scenario, even achieving vague approaches (Nazari et al., 2018) and complementary ones that take into account intangible knowledge derivatives (Ishijaza & Siraj, 2018).

## Data collection and analysis design

The data collection tool has been designed from an early stage to have the total control of the process and the standard comprehension of what is related to compliance. Therefore, it has been possible to understand the hierarchic structure and the processes that make exchanges in the pairwise comparisons. Thus, a series of comparison questions have been established by using the Saaty scale (1-9), and subsequently, the matrices have been organized together with the respondent by using the Expert Choice software. Finally, they have been effectively applied to a medium-sized company in the Brazilian industrial sector with a significant level of investment in R&D.

This has configured what was sought, the resolution of the problem of hierarchical design research for multicriteria decision making that increases the institutional compliance considering information security. Therefore, the hierarchic structure is established in 3 levels:

1 – Main objective: increasing compliance.

2 – Set of related criteria that involve:

- Standards.
- External regulation.
- Internal regulation.
- Risks assessments.

3 – Alternatives to increase the corporate compliance by considering information security:

(D1) Identification of applicable legislation and contractual requirements.

(D2) Intellectual property rights.

(D3) Protections of records.

(D4) Privacy and protection of personally identifiable information.

(D5) Regulation of cryptographic controls.

(D6) Independent review of information security.

(D7) Compliance with security policies and standards.

(D8) Technical compliance review.

Therefore, the hierarchic design has been carried out and the multicriteria decision making process and its respective weights have been characterized. The company's CIO need to understand and validate these decisions by effectively collaborating. Figure 1 shows the hierarchic design implemented in the Expert Choice DSS.

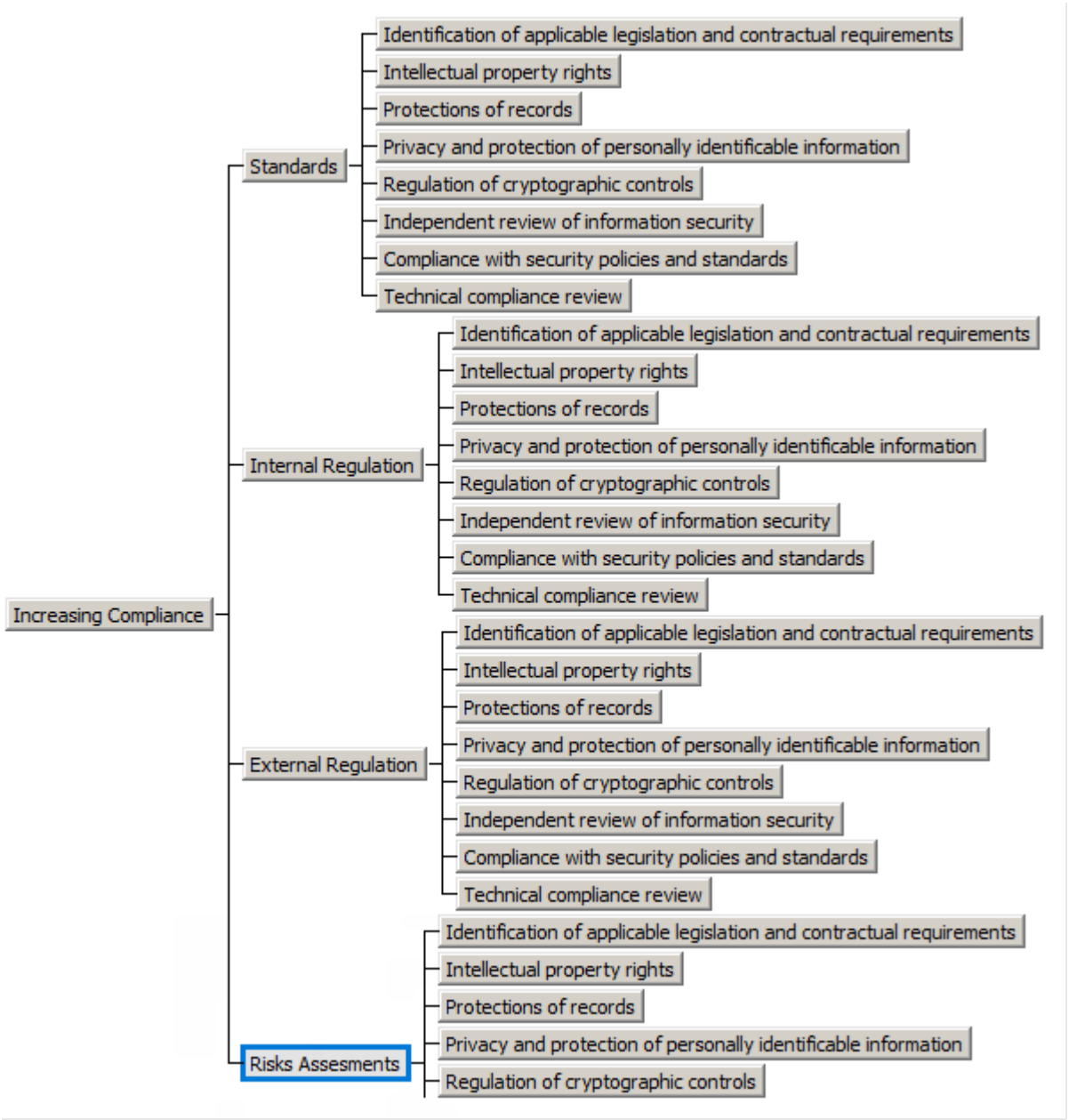


**Figure 1.** Hierarchic design to increase compliance.

Figure 2 plots the structuring of the research's main goal with its respective criteria and alternatives. Thus, the hierarchic model has been designed in an organized, effective and didactic way by means of a user-friendly interface.

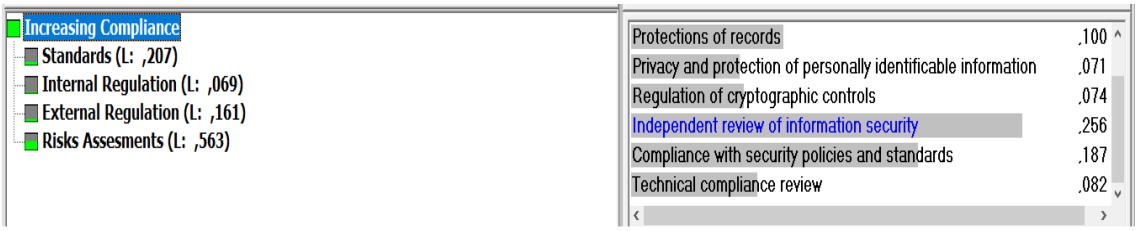


**Figure 2.** Goals, criteria/attributes and alternatives.

The matrices that are presented below for illustrative purposes will subsequently allow to explain the applicability of the model.

Figure 3 represents the beginning of the pairwise comparisons by considering the main goal and the crossing criteria.

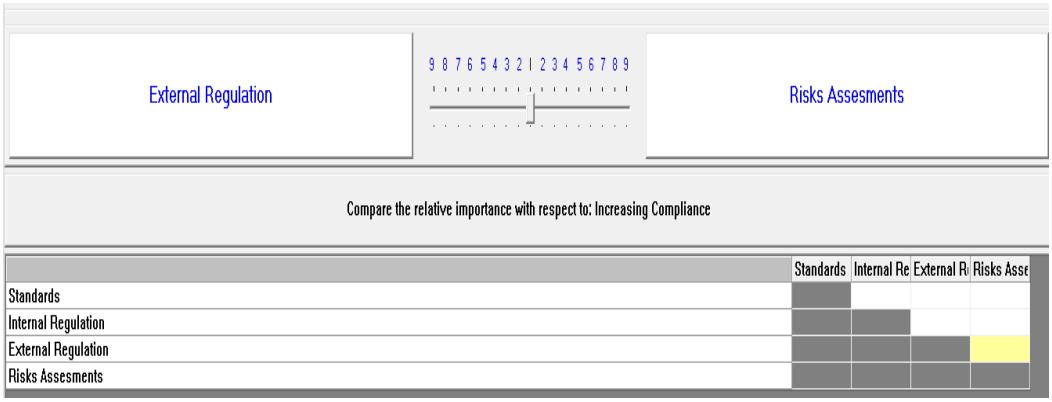


**Figure 3.** External regulation vs Risks assessments to Increasing compliance.

Figure 4 positions the pairwise comparison between the alternatives Identification of applicable legislation and contractual requirements and Intellectual property rights from the standards' point of view.

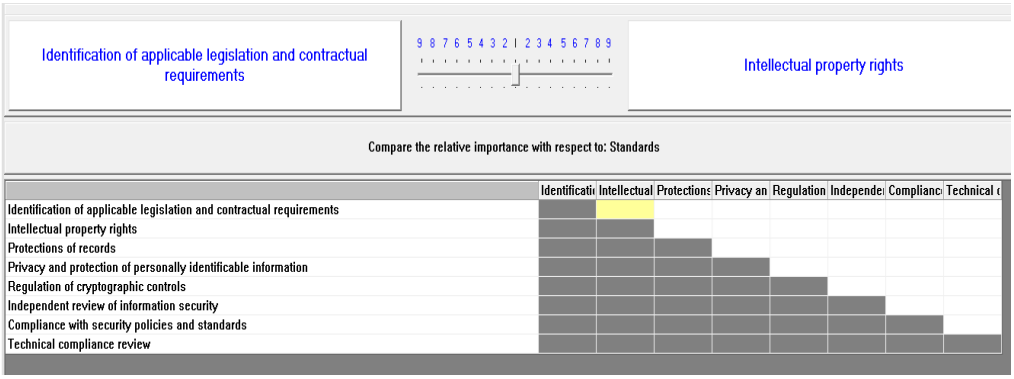


**Figure 4.** Identification of applicable legislation and contractual requirements and Intellectual property rights from the Standards' perspective.

Figure 5 shows the comparison matrix crossing Compliance with security policies and standards with Technical compliance review from the Internal regulation's perspective.

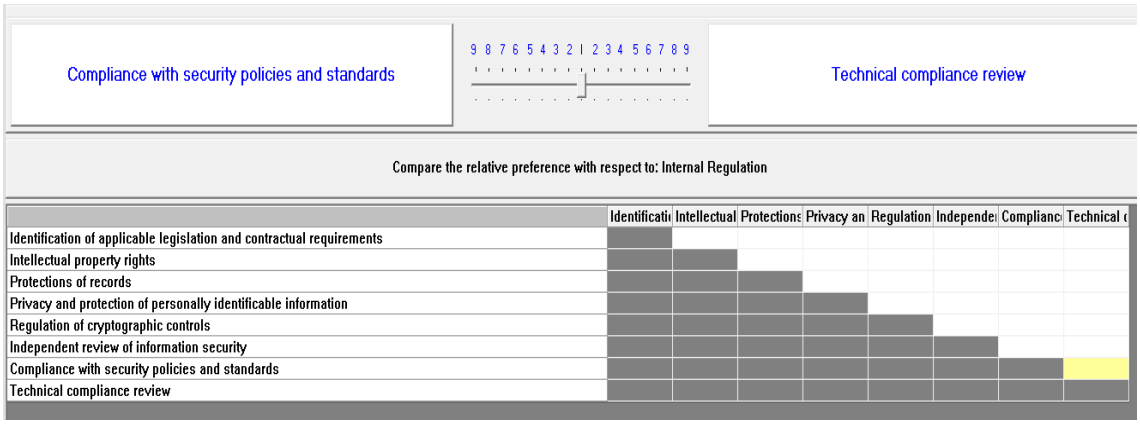


**Figure 5**. Compliance with security policies and standards vs Technical compliance review from the Internal regulation's perspective.

Figure 6 shows the comparison matrix again, crossing the relative importance between Compliance with security policies and standards and the Technical compliance review from the Risks assessments approach.

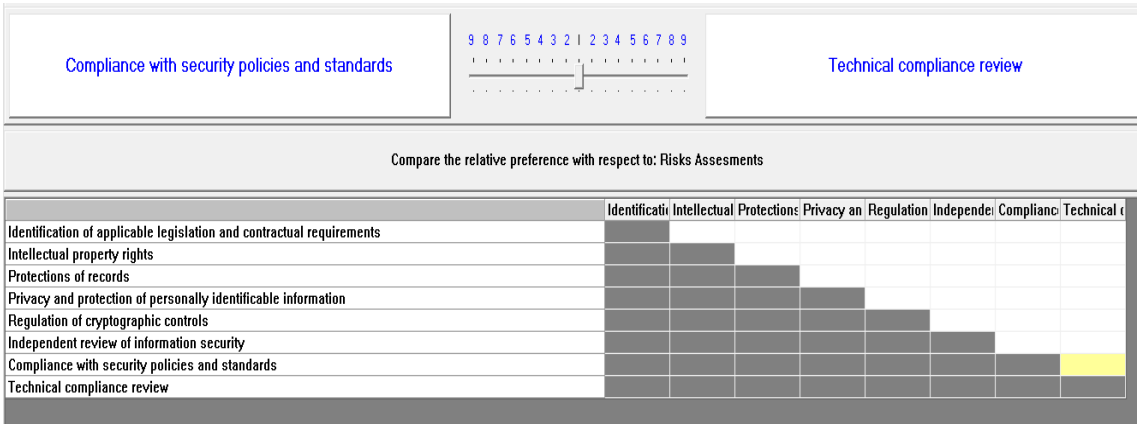


**Figure 6.** Compliance with security policies and standards and the Technical compliance review from the Risks assessments approach.

## Research context

Companies effectively invest in information security because it eliminates or reduces risks and also improves information compliance by keeping a strong infrastructure of protection. Likewise, they are often vulnerable to invasions or to the capture of their systems.

The company which has scientifically cooperated in this research is a medium-sized enterprise who works in the Brazilian industrial sector and strongly invests in information security, advanced technology, and research and development. In addition, it produces with significant differentials in comparison with its competition. However, such company has requested to remain anonymous because it is a sensitive subject and because it collaborated at a specific time.

The research findings are presented below, highlighting that the responses given by the executive (CIO) were used. Such executive was in charge of the information and the information security of the company.

## RESULTS AND DISCUSSION

A practical data collection approach has been used to present the results and to understand the process. First, the matrices have been completed and then there has been an evolution to the display of the results and their respective weights.

Figure 7 presents the results matrix of the relative importance comparative analysis between the decision criteria established at the first level. The results show that Risk assessments is established as the most significant criterion to Increasing compliance regarding the information security improvement. Then, the criterion Standards has the second position. It should also be noted that the matrix shows an inconsistency level at 0.09, which is an acceptable level for generating pairwise results in the AHP method.

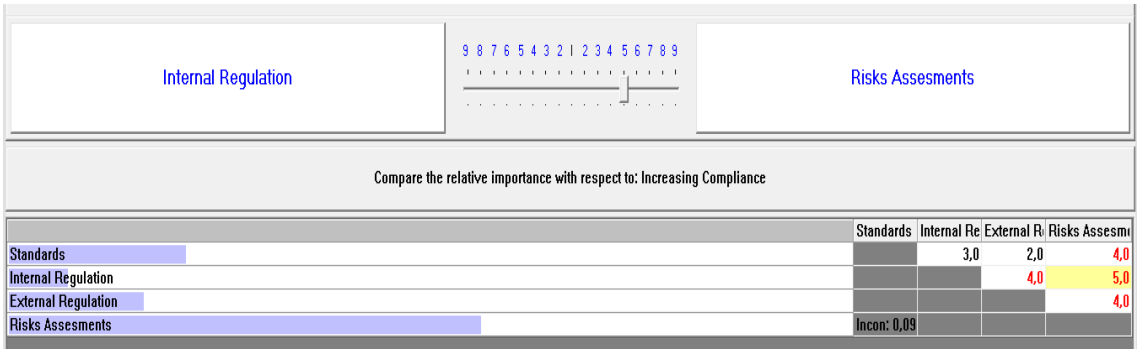


**Figure 7.** Results between Internal regulation and Risks assessments to Increasing compliance.

Figure 8, which is presented below, relates the results between the Identification of applicable legislation and contractual requirements and the Intellectual property rights regarding Risks assessments. With regard to Risks assessments, the primary importance is for the Independent review of information security criterion, followed by the Compliance with security policies and standards criterion in the second position. In the comparison matrix of relative importance, the inconsistency level is exactly at 0.10, which is an acceptable level with the method used.

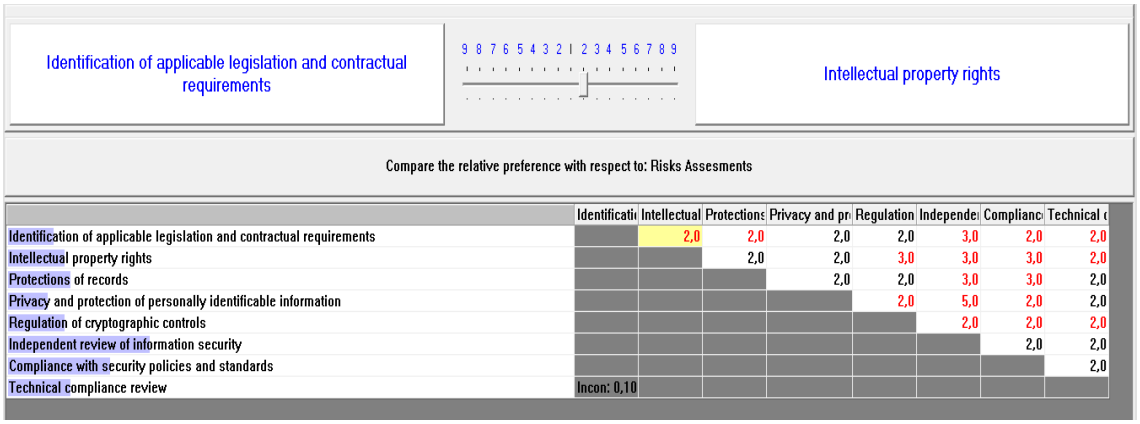


**Figure 8.** Results between Identification of applicable legislation and contractual requirements and Intellectual property rights regarding Risks assessments.

Figure 9 shows the crossing between Identification of applicable legislation and contractual requirements and the Intellectual property rights with regard to the Standards. The comparison matrix of decision alternatives also reveal that the company has to pay attention to information security analysis and to the compliance with security policies and standards. Likewise, the corporate practices that identify the applicable legislation are also important. The results show in the matrix the comparisons among the different decision alternatives regarding Standards.

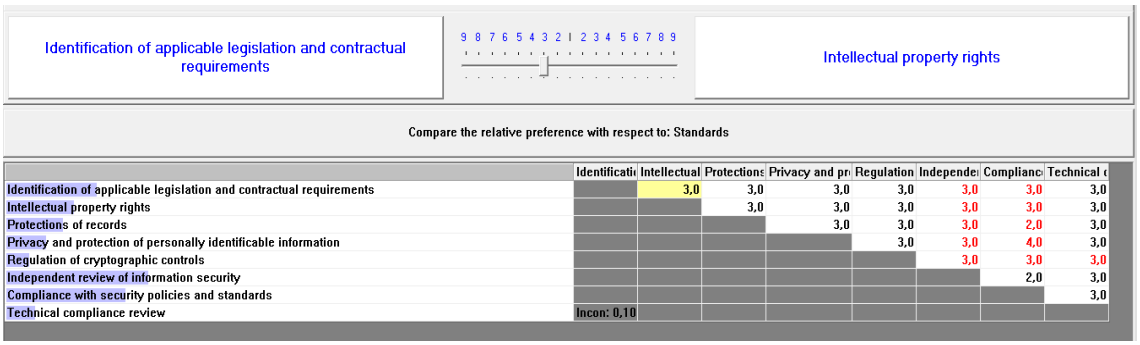


**Figure 9.** Results between Identification of applicable legislation and contractual requirements and Intellectual property rights with regard to Standards.

Figure 10 shows the pairwise evaluation between the Identification of applicable legislation and contractual requirements and the Intellectual property rights regarding Internal regulation. The matrix represents the relative assessments among the different alternatives regarding the Internal regulation criterion.

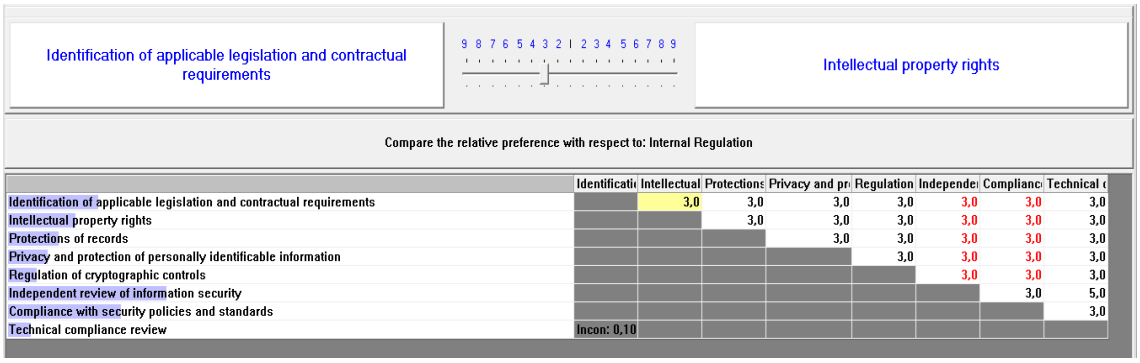


**Figure 10.** Results between Identification of applicable legislation and contractual requirements and Intellectual property rights with regards to Internal regulation.

Figure 11 considers the crossing between Identification of applicable legislation and contractual requirements and Intellectual property rights regarding External regulation. In the matrix, alternatives cross each other at the External regulation hierarchic level, thus proving the primary importance of Independent review of information security, followed by the need of Identification of applicable legislation and contractual requirements, which also presents a high impact to increase compliance with the External regulation applicable to the institution.

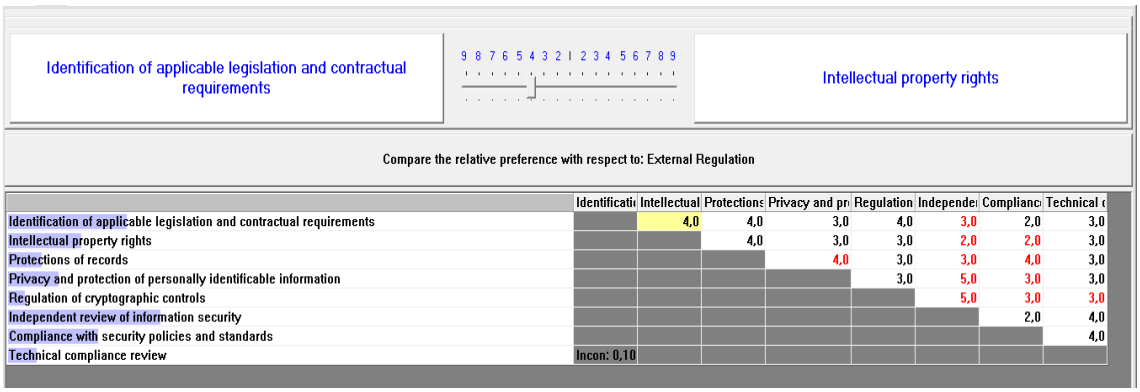


**Figure 11.** Results between Identification of applicable legislation and contractual requirements and Intellectual property rights with regard to External regulation.

Figure 12 presents the alternatives' results considering all the criteria. Therefore, a ranking by priority among each variable applied in the company can be seen.

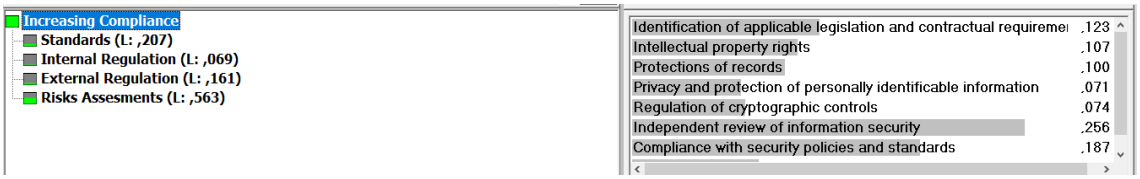


**Figure 12.** Results of the different alternatives considering all the decision criteria.

Figure 13 shows all the results, which point out the path to follow by managers and people in charge of information security to increase the corporate compliance. This figure highlights the importance of the independent reviews of information security, as well as the compliance with security policies and standards. However, the information privacy, the cryptographic controls and the technical requirements play a smaller role in the decision-making process to increase the company's compliance. It should also be noted that the prioritization of alternatives has a general inconsistency level at 0.10, which is highly recommended in the AHP method.

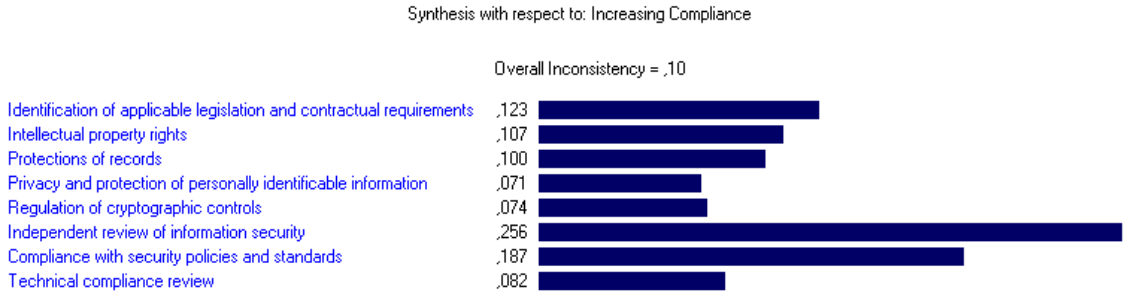


**Figure 13.** Synthesis of the alternatives' prioritization regarding Increasing Compliance.

Figure 14 presents the different graphs available in Expert Choice DSS. One of them is the *sensitivity analysis*, which allows to change every decisional variable and check the results regarding the others in terms of prioritization.

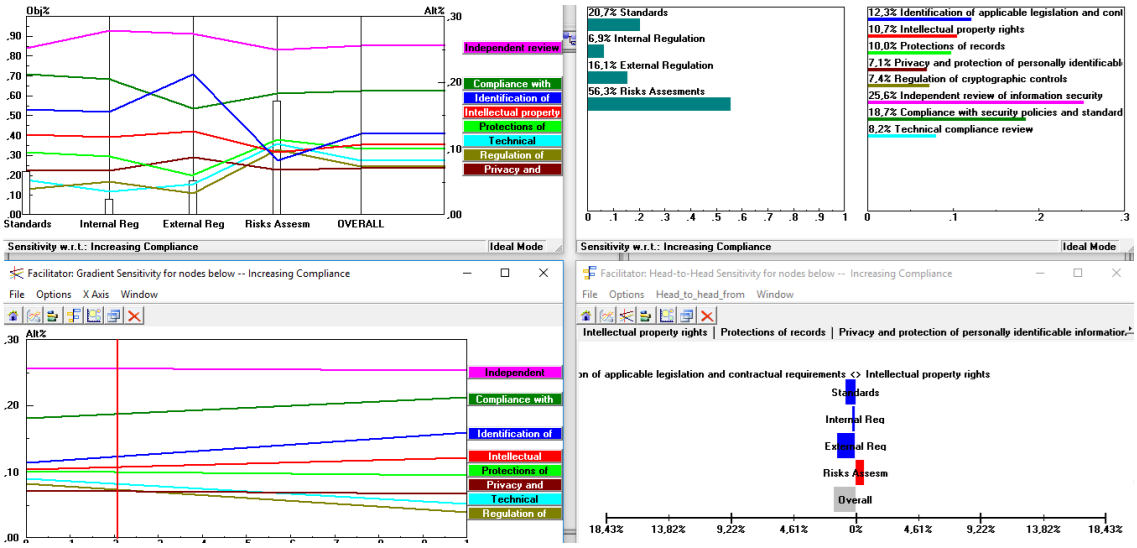


**Figure 14.** Results with sensitivity analysis.

All the results have been validated by the company's CIO. The executive has confirmed the results but didn't authorized to disclose the name of the company because their scientific contribution is based on the own company's culture, policies and management of the standards and information security. The important aspect is that the decision theory and the compliance with the information security practices have been linked, validating this connection in a real industrial environment and in a non-profit work. Therefore, the problem of information security in the business world has been approached to the scientific research field in order to bring approaches and solutions closer that can guide the compliance and security policy in companies.

## CONCLUSIONS

Information security involves the protection of information assets, which requires a significant consideration of the strategic, organizational and IT governance variables, and the analysis of the different issues related to the compliance with international standards that regulate business actions. By taking into account this need and the lack of current studies that address these issues, the compliance analysis research problem has been addressed to support and improve information security by using different variables from the ISO/IEC 27002:2013 standard.

The work has focused on the application of the Analytic Hierarchy Process method and on the Decision Support Systems by using the Prof. Saaty's Expert Choice DSS. This has allowed the structuring and the practical processing of the hierarchic design created from the decisional analysis.

The research has been developed in an industrial company, emphasizing that this is a non-profit work. This company, which stands out at a national level because it intensely invests in technology and information security, has cooperated by means of its CIO, who has answered to the questions raised by reflecting on every process of the ISO/IEC 27002:2013 standard - compliance practices turned into criteria-.

The generated prioritization results have been considered as coherent, regarding the daily activity of the company, by the CIO in charge of the information security. By taking into account the standard

control goals and the information security revisions needed, the main control practice to improve the corporate compliance is the D6 "Independent review of information security", followed by the D7 "Compliance with security policies and standards". Likewise, in the legislation and contractual requirements compliance framework is confirmed that the D1 practice: "Identification of applicable legislation and contractual requirements" also contributes to improving the institutional compliance for a greater control of information security.

Therefore, it is proved that the multicriteria decision without a specific method that achieves the 7 variability psychological judgements, which cannot be calculated by humans, are often compensated by the managers according to the company's daily experiences at its different organizational levels – strategic, tactical and operational –. Thus, the executives can take part of a complex decision process by continuously interacting in situ with all the corporate activities or processes that coexist on a daily basis.

As a work limitation, it has been identified that many times the security standards, because they are very technical, generate doubts when they are crossed to establish their relative importance. This is why they have been checked several times: the daily activity does not imply knowing their definitions for each process.

In future works it is needed to research to obtain a greater integration between the security standards and the control of management approaches. This integration can be addressed through the adaptation of the standard to different organizational and cultural environments.

## REFERENCES

Abdul, M., Towfique, R., Charbel, J., Syed, M., & Golam, K. (2018). Prioritization of drivers of corporate social responsibility in the footwear industry in an emerging economy: A fuzzy AHP approach. *Journal of Cleaner Production*, 201, 369-381.

Aversa, P., Cabantous, L., & Haefliger, S. (2018). When decision support systems fail: Insights for strategic information systems from Formula 1. *Journal of Strategic Information Systems*, *27*(3), 221-236.

Awad, A. I. (2018). Introduction to information security foundations and applications. In: *Information Security: Foundations, Technologies and Applications*, pp. 3-11. The Institution of Engineering and Technology (IET).

Awasthi, A., Govindan, K., & Gold, S. (2018). Multi-tier sustainable global supplier selection using a fuzzy AHP-VIKOR based approach. *International Journal of Production Economics*, 195, 106-117.

Bianchini, A. (2018). 3PL provider selection by AHP and TOPSIS methodology. *Benchmarking: An International Journal*, *25*(1), 235-252.

Bloomfield, R., Bishop, P., Butler, E., & Stroud, R. (2018). Security-informed safety: Supporting stakeholders with codes of practice. *Computer*, *51*(8), 60-65.

Botha, R. A., & Gaadingwe, T. G. (2006). Reflecting on 20 SEC conferences. *Computers & Security*, *25*(4).

BS7799-2 (2002). *Specification for information security management systems*. London, UK: British Standard Institute.

Buccafurri, F., Fotia, L., Furfaro, A., Garro, A., Giacalone, M., & Tundis, A. (2015). An analytical processing approach to supporting cyber security compliance assessment. In: *Proceedings of the 8th International Conference on Security of Information and Networks*, pp. 46-53. ACM.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

Cobo, A., Vanti, A., & Rocha, R. (2014). A fuzzy multicriteria approach for it governance evaluation. *Journal of Information Systems and Technology Management*, *11*(2), 257-276, doi.org/10.4301/S1807-17752014000200003.

COM (2006). *The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society*. Commission of the European Communities.

Cong, H., Dang, D., Brennan, L., & Richardson, J. (2017). Information security and people: A conundrum for compliance. *Australasian Journal of Information Systems*, 21, 1-16.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Dimopoulos, V., Furnell, S. M., Jennex, M., & Kritharas, I. (2004). Approaches to IT security in small and medium enterprises. In: *Proceedings of the 2nd Australian Information Security Management Conference 2004*, Perth, Australia.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security*, *25*(1), 55-63.

Ferreira, E., Matos, F., Matos, D., Bugarim, M. C., & Machado, D. (2014). Governança corporativa na saúde suplementar: estudo de caso em uma operadora de plano de saúde. Pensamento & Realidade. *Revista do Programa de Estudos Pós-Graduados em Administração-FEA*, *29*(3), 19-39.

Gao, F., Rau, P. L. P., & Zhang, Y. (2018). Perceived Mobile Information Security and Adoption of Mobile Payment Services in China. In *Mobile Commerce: Concepts, Methodologies, Tools, and Applications*, pp. 1179-1198. IGI Global.

Giannakouris, K., & Smihily, M. (2010). *ICT security in enterprices, 2010*. Eurostat, European Commision.

Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: an emerging field of research. *Information Systems Frontiers*, *8*(5), 335-337.

Griffith, S. J., Thel, S., Baer, M., Miller, G. P., Manwah, G., Breslow, S., ... & Baxter Jr, T. C. (2016). The changing face of corporate compliance and corporate governance. *Fordham Journal of Corporate & Financial Law*, *21*(1), 1-69.

Hasbini, M. A., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development*, *14*(1), 86-98.

Hina, S., & Dominic, P. D. D. (2018). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, 1-11, doi.org/10.1080/08874417.2018.1432996.

Hogue, J. T. (1987). A Framework for the examination of management involvement in decision support systems. *Journal of Management Information Systems*, *4*(1), 96-110.

Hone, K., & Eloff, J. H. P. (2002). Information security policy – what do international security standards say? *Computers & Security*, *21*(5), 402-409.

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational information security strategy: Review, discussion and future research. *Australasian Journal of Information Systems*, 21, art. no. 1427, doi.org/10.3127/ajis.v21i0.1427.

Hubbard, D. W. (2010). *How to measure anything: finding the value of intangibles in business*. 2nd Edition. New York: John Wiley & Sons.

Ishijaza, A., & Siraj, S. (2018). Are multi-criteria decision-making tools useful? An experimental comparative study of three methods. *European Journal of Operational Research*, *264*(2), 462-471.

ISO/IEC 27001:2007. *Information technology, security techniques, information security management systems: requirements*. International Standard Organization.

ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls*. International Standard Organization.

Keenan, P., & Jankowski, P. (2019). Spatial decision support systems: Three decades on. *Decision Support Systems*, 116, 64-76.

Kim, K., & Kim, J. (2017). An exploratory research about identifying security practices based on theory of planned behavior. *Far East Journal of Electronics and Communications, 17*(3), 531-538.

Kim, S., Leem, C. S., & Lee, H. J. (2005). An evaluation methodology of enterprise security management systems. *International Journal of Operations and Quantitative Management*, *11*(4), 303-312.

Knuplesch, D., & Reichert, M. (2017). A visual language for modeling multiple perspectives of business process compliance rules. *Software & Systems Modeling*, *16*(3), 715-736.

Kwon, S., Jang, S., Lee, J., & Kim, S. (2007). Common defects in information security management system of Korean companies. *Journal of Systems and Software*, *80*(10), 1631-1638.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24.

Luftman, J., Kempaiah, R., & Nash, E. (2006). Key issues for IT executives. *MIS Quarterly Executive*, *5*(2), 81-99.

Mateescu, R. A. (2015). Corporate governance disclosure practices and their determinant factors in European emerging countries. *Accounting and Management Information Systems*, *14*(1), 170-192.

May, C. (2003). Dynamic corporate culture lies at the heart of effective security strategy, *Computer Fraud & Security*, *2003*(5), 10-13.

May, J., & Dhillon, G. (2010). A holistic approach for enriching information security analysis and security policy formation. In: *ECIS 2010 Proceedings,* Paper 146. http://aisel.aisnet.org/ecis2010/146

McLaughlin, M. D., & Gogan (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, *17*(3), 237-262.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: information technology and organizational performance: an integrative model of IT business value. *MIS Quarterly, 28*(2), 283-322.

Merhi, M., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, 92, 37-46.

Nasir, A., & Arshah, R. A. (2018). Information security culture dimensions in information security policy compliance study: A review. *Advanced Science Letters*, *24*(2), 943-946.

Navarro, M. (2006). Security evolves towards maturity. *Universia Business Review*, 2nd quarter, 10, 96-103.

Nazari, S., Fallah, M., Kazemipoor, H., & Salehipour, A. (2018). A fuzzy inference- fuzzy analytic hierarchy process-based clinical decision support system for diagnosis of heart diseases. *Expert Systems with Applications*, *95*(1), 261-271.

Ngo, L., & Zhou, W. (2005). The Multifaceted and Ever-Changing Directions of Information Security – Australia Get Ready! In: *3rd International Conference on Information Technology and Applications (ICITA 2005)*, Sydney, Australia: IEEE Press.

OECD (2005). *The promotion of a culture of security for information systems and networks in OECD countries*. Organisation for Economic Cooperation and Development.

OECD (2009). *The impact of the global crisis on SME and entrepreneurship financing and policy responses*. Organisation for Economic Cooperation and Development.

Oliveira, D., Silva, M. P., Lima, T. A., & Souza, M. M. (2015). Um estudo exploratório da gestão de pessoas na integração e disseminação da governança corporativa. *Augusto Guzzo Revista Acadêmica*, *2*(16), 241-268.

Park, M., & Chai, S. (2018). Internalization of information security policy and information security practice: A comparison with compliance. In: *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 4723-4731.

Park, S., & Ruighaver, T. (2008). Strategic approach to information security in organizations. In: *Proceedings of the 2008 International Conference on Information Science and Security,* Seoul, South Korea: IEEE Press.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.

Pérez-González, D., & Solana-González, P. (2006). Intranets: medición y valoración de sus beneficios en las organizaciones. *El Profesional de la Información*, *15*(5), 331-341.

Rios, O. K. L., de Almeida Teixeira Filho, J. G., & da Silva Rios, V. P. (2017). Melhores práticas do COBIT, ITIL e ISO/IEC 27002 para implantação de política de segurança da informação em Instituições Federais do Ensino Superior. *Revista Gestão & Tecnologia*, *17*(1), 130-154.

Saaty, T. L. (1980). *The analytical hierarchy process: Planning, priority setting, resource allocation*. New York: Mc Graw-Hill.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Sêmola, M. (2014). Gestão da segurança da informação: uma visão executiva. 2ª edição, Brasil: Elsevier.

Shamala, P., Ahmad, R., Zolait, A. H., & bin Sahib, S. (2015). Collective information structure model for Information Security Risk Assessment (ISRA). *Journal of Systems and Information Technology*, *17*(2), 193-219.

Singh, V., & Margam, M. (2018). Information security measures of libraries of Central Universities of Delhi: A study. *DESIDOC Journal of Library & Information Technology*, *38*(2), 102-109.

Siponen, M., & Willison, R. (2009). Information security management standards: problems and solutions. *Information & Management*, *46*(5), 267-270.

Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information system security. *Information Systems Management*, *23*(2), 23-32.

Solana-González, P., & Pérez-González, D. (2011). Security model applied to electronic records management: experiences and results in the nuclear sector. *International Journal of Technology Management*, *54*(2/3), 204-228.

Sprague, R., & Carlson, E. (1982). *Building effective decision support systems.* Englewood Cliff: Prentice Hall.

Srinivas, J., Das, A., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92, 178-188.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers and Security*, 79, 68-79.

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology and People*, *31*(5), 1047-1068.

Uddin, M., & Preston, D. (2015). Systematic Review of Identity Access Management in Information Security. *Journal of Advances in Computer Networks*, *3*(2), 150-156.

Von Solms, B., & Von Solms, R. (2005). From information security to…business security? *Computers & Security*, *24*(4), 271-273.

Ward, J. L., & Peppard, J. (2002). *Strategic Planning for Information Systems*. Chichester, England: John Wiley & Sons.