BJ O&PM Brazilian Journal of Operations & Production Management

ISSN 2237-8960 (Online)

ABEPRO ASSOCIAÇÃO BRASILEIRA DE ENGENHARIA DE PRODUÇÃO

RESEARCH PAPER

Information security governance in the electricity industry

Igor Antônio Magalhães de Oliveira[1], Mirian Picinini Méxas[1], Elaine Mara Marçal Machado[1], Geisa Meirelles Drumond[1]

[1]Fluminense Federal University – UFF, Niterói, RJ, Brazil.

How to cite: Oliveira, I.A.M., Méxas, M.P., Machado, E.M.M. et al. (2022), "Information security governance in the electricity industry", *Brazilian Journal of Operations & Production Management*, Vol. 19, No. 1, e20221228. https://doi.org/10.14488/BJOPM.2021.045

ABSTRACT

Goal: This study aims to assess the importance and use of Information Security (IS) governance in the electricity industry and other segments, in order to propose IS governance guidelines for this industry.

Design / Methodology / Approach: Literature review was made of scientific articles, frameworks and norms that supported the field research applied to managers, coordinators and experts from IS area, totaling 104 respondents from different countries. The data collected were analyzed by comparing the degree of importance with the use, and also by means of cross-analysis.

Results: It was observed that most respondents agree with the importance of the themes approached, however, in practice, these concepts are not always used by the organization. Besides, it was observed that when security is directly responding for the high level of the organization, the maturity level is between optimized and managed. However, where security is subordinated to the technology area, the level appears with higher percentage, as repeatable.

Limitations of the investigation: The sample size is a limiting factor as it was conditioned to questionnaire responses sent to IS experts through electronic means and social networks and it is not possible to generalize as the population size is not known.

Practical implications: To assist the electricity industry in taking measures turned to IS governance, and, with that, increase consumer protection with regard to their classified data and the company's reliability in power supply.

Originality / Value: The present research originality lies in the proposal of 10 IS governance guidelines obtained from the literature review and the field research applied to IS experts, aiming to raise, more and more, its level of maturity.

Keywords: Information Security; Electricity; IS Governance.

INTRODUCTION

Cyber attacks are increasingly more sophisticated and complex, leading companies to financial collapse and degradation of their image. Thus, areas like Information Security (IS) start to play a crucial role in organizations' corporate strategy (Alencar et al., 2018), becoming vital for any industry that wants to protect its data (Cardoso et al., 2019). IS, over the years, could no longer be addressed with a technical view alone, and showed the need of an approach turned to the business and integrated to the strategic management in order to reach the whole organization with well structured norms and policies (Carcary et al., 2016).

Financial support: None.
Conflict of interest: The authors have no conflict of interest to declare.
Corresponding author: gmdrumond@id.uff.br
Received: 2 May 2021.
Approved: 12 Aug 2021.
Editor: Julio Vieira Neto.

It is worth highlighting that vulnerabilities in automation systems have caused social and economic impacts globally. On 12/23/2015, an Ukrainian electricity supply company suffered an attack to the SCADA (Supervisory Control and Data Acquisition), system, leaving over 80 thousand customers without electricity for 3 (three) hours. On 05/07/2021 the Colonial Pipeline System (Texas, USA), the company that operates the largest fuel transfer pipeline on the east coast of the USA, suffered an attack forcing the company to deactivate its operation (Sanger et al., 2021). Another example is a malware that, on 01/25/2003, deactivated the security system from a nuclear company in the United States, Ohio, making impossible the control of temperature measurement sensors' indicators (Rodofile et al., 2019).

According to Nazareth and Choi (2015), Kure et al. (2018), Martins et al. (2019), Kim et al. (2017) and Carcary et al. (2016), companies end up suffering financial losses and degradation of their image due to a low maturity in their Information Security area. It is noticed that, at the peak of the COVID-19 pandemic, companies of large size of the electricity sector had its environment partially paralyzed by cyber-attacks. Numerous publications point out the vulnerability of energy delivery systems. In 2020, the companies Light, Energisa, Raízen, EPE, Enel, CPFL, EDP, and in 2021 the company Copel, all in the Energy segment in Brazil suffered ransomware attacks, paralyzing a large part of the production system. These attacks caused system unavailability, great financial impact and degradation of the company´s image (Nicol, 2021).

However, effective risk management and IS governance help fight and audit eventual cyber crimes. It is worth reminding that such governance comprises a set of norms, policies, awareness tools and trainings in information security (Nazareth and Choi, 2015). These measures reduce risk and mitigate attacks that can come from outside or from inside the organization.

The market currently offers some norms and frameworks turned to IS area, due to its high importance within the organization. However, some methodologies and standards can be too complicated to be adopted in the organizations (Yang et al., 2016). ISO 27001 norm, for example, is the international reference standard for IS management, and has been continuously improved over the years, and results from standard BS7799 (British Standards) (Pardo et al., 2016).

As shown by Schmitz et al. (2021) maturity models are widely used to measure information security, playing a central role in the design of information security governance in organizations. COBIT (Control Objectives for Information and Related Technologies) is a framework used to measure the level of maturity, having a basic structure with best practices, providing control and management (Suryawan and Veronica, 2018).

Therefore, the electricity industry, for dealing with something essential in human life, for containing classified data from customers and offering reliability in electricity supply, must keep a well structured system for IS governance in order to mitigate risks coming from the organization itself or from outside (Martins et al., 2019).

In fact, risks form an endless cycle, that is, they are always back, so, proposals for risk contention must arise in the short and long term, since every day a new method of attack or virus is created (Han et al., 2016; Kalogeraki et al., 2018). Thereby, one can state that information security governance is highly important, and thus, the organization and those responsible for files and locations where information is kept must be prepared for risks and ready for any eventuality, ensuring high level of governance (Mishra, 2015).

The risks faced by the electricity industry due to lack of maturity in IS governance are remarkable and attacks to automation systems, information leaks and financial losses are successful (Kure et al., 2018). Therefore, observing risks and being attentive is always the best option for electricity companies, and is the focus of the present study, since, on the one hand, Information Technology (IT) is growing and seeking to supply the needs of those that seek to protect their information, while, on the other hand, it also grows on the side of those who intend to steal information.

Within this context, the following central research question arises: How can companies in the electricity industry improve the governance of their information security? The general objective of this study is to map the market stakeholders' perception of Information Security Governance in organizations through the analysis of the degree of importance and utilization, as well as cross-analysis of respondents/companies profiles and the level of maturity,

performing a comparative analysis of the results found and the findings of the authors surveyed in the bibliometric research, in order to propose IS governance guidelines to the electricity industry, in order to propose IS governance guidelines to the electricity industry.

The present study was organized in sections; introduction, then section 2 presenting the theoretical framework about Information Security Governance in the electricity industry; section 3 describes the methodological processes; the fourth section presents the analysis of results; and in section 5, IS Governance Guidelines are proposed for the electricity industry; and, finally, the sixth section presents the conclusion and proposals for further research.

INFORMATION SECURITY GOVERNANCE IN THE ELECTRICITY INDUSTRY

In organizational environments, where data interconnections increase every day, information becomes an asset like any other asset of the company, and needs appropriate protection, due to the high exposure to threats and vulnerabilities (Valencia-Duque and Orozco-Alzate, 2017). Thus, Information Security is protection of information from several types of threats to ensure business continuity, minimize risks, and maximize return on investments and business opportunities (Kim et al., 2017).

IS Governance is a tool for specification of rights and decision and responsibility, aiming at encouraging desirable behaviors in the use of information security. Businesses today are increasingly dependent on their information security infrastructures, which makes necessary the implementation of IS governance in companies to ensure business continuity (Yaokumah, 2014).

IS governance main objective is to align this security to the business requirements, considering the guarantee of services continuity and minimization of business exposure to risks. Governance can be motivated by several factors, however, one of the most important factors is transparency in IS administration and availability of this security infrastructure. Providing security and availability of IS infrastructure is currently a challenge for organizations, because these practices ensure the business availability (Georg, 2017).

To avoid and reduce relevant risks, the identification of controls to be implanted requires careful planning and attention to details. IS governance needs, at least, the participation of all employees in the organization, including directors and executives in leadership, organizational structures and processes, which will ensure that the company IS sustains the organization's strategies and goals. The participation of shareholders, suppliers, third parties, customers or other external parties may also be necessary. A specialized external consultancy may also be fundamental (You et al., 2018).

Moreover, IS governance is accountable for controlling, directing and supervising processes required to protect information from an organization in order to guarantee availability, confidentiality, integrity and keep alignment with the business strategic management (Rebollo et al., 2015). This governance is obtained from the implementation of a set of appropriate controls, including policies, processes, procedures, organizational structures and software and hardware functions (Chinyemba and Phiri, 2018).

These controls must be established, implanted, monitored, critically analyzed and improved, where necessary, to ensure that the organization's business goals and security will be met. It should be done jointly with other business management processes (Miloslavskaya and Tolstoy, 2017).

Due to the large impact this area has suffered with internal or external attacks of any nature, companies are seeking high maturity in their IS governance (Carcary et al., 2016). Looking from an organizational perspective, information security governance is part of the corporate governance, playing a strategic role to ensure that goals will be achieved and risks mitigated (Nicho, 2018).

The manager and the team should know the business goals and strategy in order to align information security to these goals. These data can be surveyed through the business' strategic planning documents, meetings with managers, directors and employees (Haqaf and Koyuncu, 2018; Höne and Eloff, 2009; Johnston and Hale, 2009; Moon et al., 2019).

There are discussions, among professionals of the area, on what sphere information security should be within the organizational structure to reach high level of maturity in its governance (Carcary et al., 2016; Cholez and Girard, 2014; Sánchez et al., 2009; You et al., 2018).

It is worth highlighting that there is today in Brazil and across the world a growing demand for electricity to supply the industry, commerce and households. This demand ends up by making companies place themselves in the current market, many times just to build the generation unit and put it into operation, without addressing aspects that can be decisive for the organization business (Machado et al., 2016).

Thus, IS governance is present in the corporate environment of large and medium companies, and this theme is becoming consolidated in the market, but information security focused on operational availability of an electricity generation plant is something really difficult to see nowadays (Krishnan et al., 2017).

IS governance in the utilities industry is a relatively new subject, since this market is increasingly heating. Due to the growing attacks to this environment the theme was given more importance, in order to ensure availability, confidentiality and integrity of information in the electricity industry (Amin and Wollenberg, 2005; Evans et al., 2019; Machado et al., 2016; Kim and Tong, 2013; Rodofile et al., 2019; Thiyagarajan et al., 2015; Woo and Kim, 2018).

The guarantee of availability, confidentiality and integrality of this technology in the electricity industry depends on a structured IS governance (Qassim et al., 2019). Moreover, the risks faced in environments with critical infrastructure, like transport, electricity and telecommunications, have cyber attacks as main threat (Kure et al., 2018).

So, the challenges faced by the electricity sector involving IS are clear. For being something with significant economic and socioenvironmental relevance, on November 22, 2018, in Brazil, the President-in-Office approved Decree N° 9.573, addressing specifically National Policy for Security in Critical Infrastructure, PNSIC. This decree addresses issues about total or partial interruption in critical infrastructure that causes social, economic and environmental impact, preventive and reactive measures destined to critical infrastructure security and resilience capacity after the occurrence of an anomalous situation (Brasil, 2018).

METHODOLOGY

The present study first conducted a literature review with the main focus on ordering concepts of authors and their respective opinion on the subject. The bibliometric research method was adopted, according to Costa (2010) and Ferreira et al. (2019), through access to articles from SCOPUS base. Frameworks and norms involving the theme were also analyzed.

For the bibliometric research, the following keywords were used: a) “information security management” OR “information security governance”, a total of 1424 articles; b) “management strategic” total of 506; c) “information security” AND “energy” total of 507; d) “scada” AND “security”, total of 2207; e) “information technology governance”, total of 245. In all these researches, the following filters were applied: Document Type = Article or Review and Article title, Abstract, Keywords and Source Type = Limit to Journal and Year = Limit to: 2009 to 2019. Thus, the following quantity was found: a) “information security management” OR “information security governance”, a total of 24; b) “management strategic”, total of 7; c) “information security” AND “energy” total of 3, d) “scada” AND “security”, total of 5; e) “information technology governance”, total of 4. Totalizing 43 articles that supported this research (Oliveira et al., 2021).

The bibliometric research result served to ground the survey type field research that was conducted in the ambit of IS governance in some segments of the industry, chiefly the electricity industry, which sought to map opinions of experts in the area.

A survey of key information was made to assist in the preparation of the questionnaire, based on what was found in the literature, shown in Table 1, in order to identify the level of importance and utilization of IS governance, as well as make a cross-analysis of respondents / companies profiles and their level of maturity. The respondents received the link to the questionnaire and, before it was sent, a pre-test was made with three respondents, which validated the issues proposed.

Table 1. Theoretical foundation of the questionnaire

Question	Author(s)
1. What is your position in the company? 2. How long have you had experience?	Gray (2012)
3. In an organizational structure, according to your experience, Information Security should answer to whom?	You et al. (2018), Carcary et al. (2016), Cholez and Girard (2014), Sánchez et al. (2009)
4. What is the area of activity of your company? 5. In which country is your company locate?	Gray (2012)
6. In the COBIT maturity scale, what is your company position regarding Information Security?	Carcary et al. (2016), Cholez and Girard (2014), Kure et al. (2018)
7. In your company, to what area does Information Security report?	Georg (2017), Carcary et al. (2016), Nicho (2018)
8. Have a Business Continuity Plan in the organization	Ajayi and Hussin (2018), Kim et al. (2017), Yaokumah (2014), Georg (2017)
9. Have IT governance aligned with corporate governance	El Ghorfi et al. (2018)
10. Have an effective technological resource to mitigate risks related to information	Machado et al. (2016), Krishnan et al. (2017)
11. Information Security Area to be aligned with the company´s Strategic Planning	Georg (2017), You et al. (2018), Carcary et al. (2016), Haqaf and Koyuncu (2018), Alencar et al. (2018)
12. Have a perimeter firewall and a datacenter firewall for a higher level of security in the corporate environment	Vanickis et al. (2018)
13. Raising business and user awareness about information security raises the organization´s maturity level	Höne and Eloff (2009), Nazareth and Choi (2015)
14. Have the Information Security policies and standards signed by senior management	Höne and Eloff (2009), Johnston and Hale (2009)
15. Application and information access control policy in order to prevent unauthorized access	Mishra (2015), Chinyemba and Phiri (2018)
16. In all the creation of new projects, involve the Information Security team so that it is born with controls and standards (Security by Design)	Carcary et al. (2016)
17. Have information security risk management	Kalogeraki et al. (2018), Kure et al. (2018), You et al. (2018), Martins et al. (2019)
18. Employee to have adequate Information Security training when effective in na organization	Höne and Eloff (2009)
19. Have monitoring when a security incident occurs	Nazareth and Choi (2015)
20. Disaster Recovery for effective business continuity	Mishra (2015), Georg (2017), Rebollo et al. (2015)

Source: Authors (2020)

The questionnaire comprised 20 closed-ended and open-ended questions with space for additional comments from respondents. In order to guarantee more intensity in answers, avoiding the use of "yes" and "no" alone, the Likert Scale was used with five points of importance and utilization: (1) Very low; (2) Low; (3) Medium; (4) High; and (5) Very high.

The mailing was sent to IS groups on LinkedIn, WhatsApp and Telegram, and to IS users from several segments of the industry, and a sample of 104 respondents was obtained. There were national and international respondents in order to obtain better understanding in the results. For international respondents, the same questionnaire was used, translated into English.

Next, data collection and tabulation was made based on the questionnaires answered and then the analysis of results, which was separated into four parts: respondents' profile; companies segment and localization; information security governance: utilization x importance; and cross-analysis. The results were analyzed through frequency analysis, comparing the level of importance to utilization. A comparative analysis with literature was also conducted, where we sought to verify whether these were corroborated or not with the findings of the authors surveyed in the bibliometric research.

After analysis of results, guidelines on information security governance were prepared for the electricity industry. The results were analyzed and grounded in the conclusions of this study, as well as for the preparation of future research.

RESULT ANALYSIS

The field research was conducted from 03/05/2020 to 04/26/2020 and included 104 respondents. The analysis of the results is separated into four parts: profile of respondents; profile, segment and localization of companies; information security governance: utilization x importance, and cross-analysis.

Profile of respondents

In order to increase reliability of data collected, the present research mapped the professional profile of respondents and companies (**Question 01**), and found that 26% are IS Managers, 12.5% are IS Coordinators; 40.4% are IS Experts, and others related to IS represent 21.2%.

With regard to the level of experience of respondents (**Question 02),** 43.3% have over 15 years, 22.1% from 10 to 15 years, 20.2% from 5 to 10 years, and 14.4% up to 5 years. The level of respondents with 10 to over 15 years of experience reached 65.4%, showing the research level of confidence.

In order to check strategic issues involving IS governance, a question regarding information security subordination in corporate ambit was made (**Question 03**). Discussion about who information security should report to is controversial among respondents. According to Carcary et al. (2016), Cholez and Girard (2014), this theme must be further addressed and debated. Around 35.6% of respondents suggest that security should directly report to the organization President. For 27.9% of respondents, security should report to the CIO. According to the numbers shown in Table 2, the experts disagree considerably on this theme.

Table 2. Information security subordination according to respondents

In an organizational structure, according to your experience, Information Security should report to whom?	Amount	Percent (%)
Chief Executive Officer (CEO)	37	35.6
Chief Information Officer (CIO)	29	27.9
Risk and Compliance	17	16.3
Chief Technical Officer (CTO)	14	13.5
Chief Financial Officer (CFO)	1	1
Others	6	5.7
Total	104	100%

Source: Authors (2020)

Profile, segment and localization of companies

Companies from the most different sectors were analyzed (**Question 04**), as shown in Table 3, most of them from Information Technology, Information Technology and Energy, totaling 50.9%.

Table 3. Company area of activity

What is the area of activity of your company?	Amount	Percent (%)
Information security	30	28.8
Information technology	23	22.1
Energy	16	15.4
Education	6	5.8
Telecommunications	4	3.8
Other	25	24.0
Total	104	100%

Source: Authors (2020)

Since the theme is highly relevant at global level, the research sought respondents not only in national ambit, but in international ambit as well (**Question 05**). With respondents from several places across the world, the research counted on 19.6% in total, as presented in Figure 1, with 80.4% of Brazilian companies and 73.10% from the Southeast region, the most developed in the country.

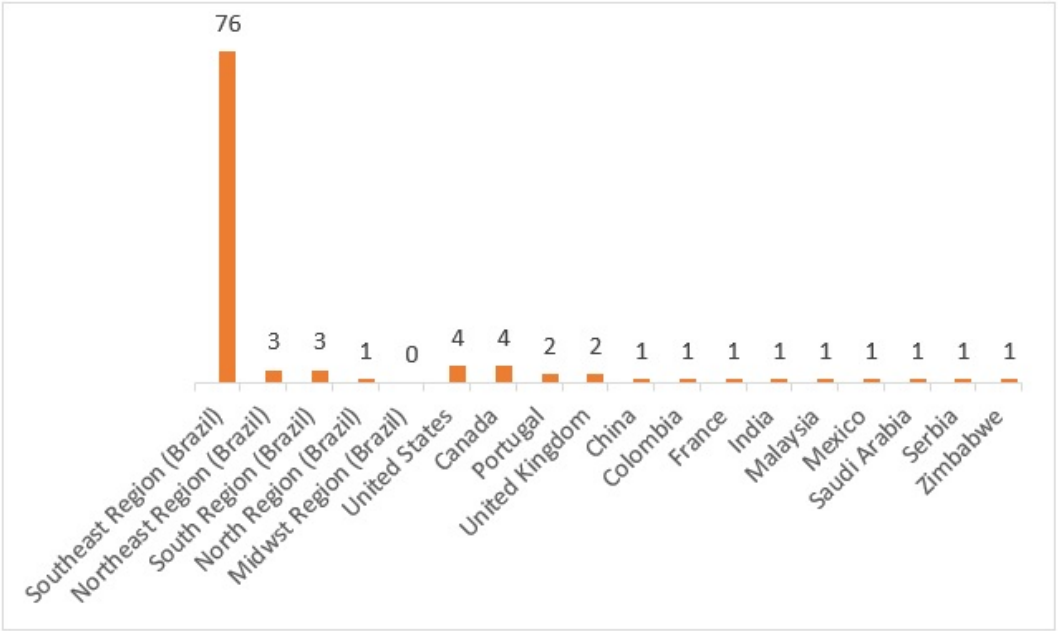

Figure 1. Country where the company operates. Source: Authors (2020)

COBIT is a tool that helps measure the level of maturity of processes. As presented by Schmitz et al. (2021), there are five maturity levels, as follows: 1. Ad-hoc: there are no processes; 2. Repeatable: there is repetition of procedures in a planned, monitored and adjusted way; 3. Defined processes: there is managed control, using process; 4. Managed and measured: controls established, operating within defined limits and 5. Optimized: control is continuously improved to meet targets, and was used to observe the level of maturity of

organizations' information security (**Question 06**). It can be observed, in Table 4, that most companies, 26.9% show level 3 of maturity level, followed by 24% of companies with level 2 of maturity. Corroborating the literature, it is evident the level of maturity of electricity companies (Kure et al., 2018).

Table 4. Level of information security maturity in the organization

In the COBIT maturity scale, what is your company position regarding Information Security?	Amount	Percent (%)
3 – Defined processes	28	26.9
2 - Repeatable	25	24
4 – Managed and measured	21	20.2
5 - Optimized	18	17.3
1 – Ad-hoc	12	11.5
Total	104	100%

Source: Authors (2020)

Aligned to the theme, organizations have different areas where information security can be inserted (**Question 07**), according the Table 5, most of them reports to the CIO (29.8%), CEO (22.1%) and CTO (19.2%), totaling 71.1%.

Table 5. Information security subordination in the organization

In your company, to what area does Information Security report?	Amount	Percent (%)
CIO	31	29.8
CEO	23	22.1
CTO	20	19.2
Risk and Compliance	12	11.5
CFO	2	1.9
Others	16	15.4
Total	104	100%

Source: Authors (2020)

Information Security Governance: Utilization x Importance

The topic information security is discussed from several points of view. In order to have an effective IS governance analysis, the level of importance and utilization of some processes was studied. Many organizations end up by disregarding important processes for being expensive and demanding time.

The objective of this section is to understand the perception of respondents concerning some fundamental aspects found in the literature and understand how their organizations are with regard to each theme proposed. For a better understanding, a table was created unifying 13 questions of the research which are described in the questions from 08 to 20. Both for level of importance and level of utilization, the following abbreviations were used: VL (very low), LO (low), ME (medium), HI (high) and VH (very high), as shown in Table 6. Then a comparative analysis was made of the degree of importance and utilization for each of the 13 questions.

Table 6. Importance x Utilization for the 13 questions

Questions	Importance (%)					Utilization (%)				
	VL	LO	ME	HI	VH	VL	LO	ME	HI	VH
8	2.9	1	3.8	13.5	78.8	8.7	15.4	36.5	19.2	20.2
9	1.9	1.9	9.6	21.2	65.4	6.7	17.3	21.2	30.8	24
10	1.9	0	7.7	14.4	76	4.8	12.5	23.1	23.1	36.5
11	3.8	2.9	5.8	19.2	68.3	10.6	16.3	15.4	26.9	30.8
12	0	1	4.8	18.3	76	3.8	4.8	16.3	21.2	53.8
13	1.9	2.9	1	19.2	75	7.7	13.5	21.2	23.1	34.6
14	1	4.8	9.6	12.5	72.1	8.7	10.6	17.3	20.2	43.3
15	0	3.8	3.8	15.4	76.9	2.9	15.4	16.3	20.2	45.2
16	2.9	3.8	4.8	19.2	69.2	8.8	20	26.9	15.5	28.8
17	1.9	1.9	3.8	22.1	70.2	10.6	16.3	23.1	21.2	28.8
18	3.8	3.8	11.5	14.4	66.3	19.2	13.5	14.4	19.2	33.7
19	1.9	0	4.8	17.3	76	4.8	11.5	24	25	34.6
20	1	3.8	1	18.3	76	16.3	14.4	20.2	18.3	30.8

Source: Authors (2020)

While analyzing the importance and utilization of the Business Continuity Plan (BCP) (**Question 08**), it was observed that high and very high utilization level reached 39.4%. One can notice that few organizations have an effective BCP. When the importance of having a BCP in the organization was analyzed, answers were 92.3% positive (very high and high). This result corroborates the literature, as demonstrated by Georg (2017), Kim et al. (2017), Ajayi and Hussin (2018), Yaokumah (2014). However, 36.5% is observed for medium utilization and 23.8% for low and very low. Therefore, it is important for the company to count on an effective BCP, because it will assist it during a crisis. From this point of v iew, information availability, confidentiality and integrity are also included in this context.

Question 09 addresses IT Governance aligned to Corporate Governance. Since the subject is technology, which involves everything in a company, the importance of keeping alignment with corporate governance, according to respondents, is fundamental for information security, thus corroborating El Ghorfi et al. (2018); and it was mentioned by around 86.6% of respondents as high and very high. On the other hand, 54.8% of companies use IT and Corporate Governance alignment. However, 21.2% for medium utilization and 24% for low and very low were observed, an expressive percent of non utilization.

The perception of the majority of respondents was 90.4% of importance, as presented in **Question 10**, where the theme addressed was efficient technological resources capable of mitigating IS risks. The utilization by organizations also presented a considerable percent, 59.6%. Only 17.3% of respondents answered that the level of utilization was low or very low, leaving a good percent of organizations with high technological resources. Since technology influences performance and particularly information security, in this question, its importance in the literature was identified based on Machado et al. (2016), Krishnan et al. (2017).

Most respondents agree that Information Security should be aligned to the organization strategic planning (**Question 11**), presenting, between high and very high, 87.5%. However, the level of utilization in companies reached 57.7%. The total of respondents that opted for low and very low is 6.7%. Information Security alignment to strategic planning is fundamental

to obtain high level of maturity, as reported by Georg (2017), You et al. (2018), Carcary et al. (2016), Alencar et al. (2018).

It can be observed that 94.3% of respondents corroborate the theory of having a firewall for perimeter and another for the Datacenter (**Question 12**). The level of utilization is considered by 75% of organizations. Only 8.6% of companies don't present this level of segregation. In the past, information security was more concerned with communications leaving the company to the internet. Over time, it was noticed that lateral movements inside the organization should also be monitored.

Question 13 addresses how the user and the business awareness on information security increase the organization's maturity level. According to Hone and Eloff (2009), Nazareth and Choi (2015), in order to obtain effective information security governance, it is important to raise the user awareness on the theme. According to Table 5, 94.2% of respondents agree with the theme. However, 21.2% of companies do not use this process, while 57% use this process.

About **Question 14**, Security policies and norms signed by the top management, it was observed that around 84.6% agree that norms and policies should be signed by the top management. However, the level of utilization in organizations proved to be very relevant with regard to the theme. Around 63.5% of companies have norms and policies signed by the executive board, while 19.3% do not use policies and norms signed by the board, and 17.3% opted for Medium, informing a transition level in the process. The information security policy is intended to document procedures and guidelines referring to how information should flow inside the organization and outside it, and must be subject to continuous updates. Höne and Eloff (2009), Johnston and Hale (2009) emphasize the creation of policies and norms with the executive board consent. The research revealed agreement of respondents with regard to the theme.

Access controls are described in a policy according to the level of security the information demands (**Question 15**). In this process, rules are defined, as well as each user's responsibility. For Mishra (2015), Chinyemba and Phiri (2018), these controls are necessary in information security governance. In concert with the literature, around 92.3% agree with this opinion. The level of utilization in organizations presents good numbers, around 65.4% of organizations count on access control policies. However, it was observed that 18.3% of organizations do not use the theme addressed in the question, while 16.3% are in transition phase.

Question 16 states that every creation of new projects should involve the information security team for them to include controls and norms (Security by Design), and count on an effective IS governance. The expression 'security by design' indicates that the software, from the beginning, was conceived to present high level of security, that is, it is conceived, first of all, in the security practices and standards. So, the importance of this theme, according to the respondents, reaches 88.4%. However, according to the mentioned research, companies adopt this concept weakly, reaching 44.3%, though the level of importance is high.

The effective risk management (**Question 17)** provides identification of threats, with development of action plan. With the results obtained in risk assessment, the definition of priorities and decision making are put into practice. For Martins et al. (2019), You et al. (2018), Kalogeraki et al. (2018), the risk management involving information security is fundamental for efficient governance. Around 92.3% agree with authors, while 50% of the companies that participated in the study count on this process. However it is worth observing that 26.9% of the organizations do not use the theme addressed and 23.1% marked it as medium, observing the phase of transition.

Providing appropriate training in information security when the employee is admitted in the organization is the theme addressed in **Question 18**. Today, for information security, the user is still the most critical aspect. Raising awareness of the user about information security is critical to avoid simple problems that may cause large financial impacts (Dhillon et al., 2016). According to Höne and Eloff (2009), effective trainings and awareness are still one of the best

ways to help information security governance. Aligned to the authors, 80.7% agree with the theme proposed. However, the level of utilization is below the expected, because 52.9% of the companies use this process in their IS governance and 32.7% do not present low and very low utilization. Also, 14.4% of respondents opted for medium utilization, showing that the process is not yet defined.

An effective monitoring of security incidents (**Question 19**) raises the level of maturity of the governance. It involves, in real time, the monitoring of systemic events that are fundamental to the organization. According to experts, 93.3% agree that it is important to manage incidents in the organization. Companies adopt these measures, reaching 59.6%, while 16.3% do not use the process and 24% are in maturation phase.

Question 20 states that having a DR (Disaster Discovery), in addition to increasing the company's competitiveness and efficiency, provides continuity to the business, keeping information availability. Besides, the quick recovery of the service can avoid financial losses. In this analysis, 94.3% of experts agree with the importance of having a DR to provide continuity to the business. However, because it involves high costs, only 49.1% of organizations use a DR. It was also observed 20.2% of medium utilization and 30.7% of low and very low utilization.

Cross-analyses of Respondents' Profiles x Companies' Profiles x Maturity

In the previous section, the research data were separately assessed, and, in this section, three cross-analyses were made, which provided more assertiveness and understanding of information security governance. The starting point of the cross-analysis was to verify the respondents' understanding with regard to information security subordination, along with the analysis of its organization.

Considering the great discussion the theme has caused in the information security environment, the information crossing generated some points of attention. As presented in Table 7, around 35.6% of respondents informed that information security should be directly subordinated to the President, but, when it was verified in their organizations, only 22.1% of them present this organizational model. Another aspect to be observed is the parity of numbers when security is subordinated to the technology chief. Around 27.9% of respondents informed that security should report to technology and, presenting a very close number, 29.8% of companies count on this organizational structure.

Table 7. Information security subordination according to respondents x security subordination in the organization

In an organizational structure, according to your experience, to whom should Information Security report?	Amount	(%)	In your company, to which area Information Security reports?	Amount	(%)
CEO	37	35.6	CIO	31	29.8
CIO	29	27.9	CEO	23	22.1
Risk and Compliance	17	16.3	CTO	20	19.2
CTO	14	13.5	Risk and Compliance	12	11.5
CFO	1	1	CFO	2	1.9
Others	6	5.8	Others	16	15.4
Total	104	100%	Total	104	100%

Source: Authors (2020)

The level of maturity of organizations with regard to information security varies according to the area subordination. Defined, optimized, managed and measured processes represent

64.4%, according to Table 8. That said, it was observed that the technology area (CIO) presents the highest number, since 29.8% of the companies have security directly linked to technology.

Table 8. COBIT Maturity x Information Security subordination in the organization

In COBIT maturity scale, where is your company in Information Security?	Amount	(%)	In your company, to each area is Information Security subordinated?	Amount	(%)
3 – Defined processes	28	26.9	CIO	31	29.8
2 - Repeatable	25	24	CEO	23	22.1
4 – Managed and measured	21	20.2	CTO	20	19.2
5 - Optimized	18	17.3	Risk and Compliance	12	11.5
1 – Ad-hoc	12	11.5	CFO	2	1.9
			Other	16	15.4
Total	104	100%	Total	104	100%

Source: The authors (2020)

However, after further analysis, it was noticed that where security is reporting directly to the organization CEO, the maturity level stays between optimized and managed, as shown in Table 9. However, where security reports to the technology area (CIO), the level that presents higher percent is repeatable.

Table 9. COBIT Maturity x Information Security subordination in the organization separated in areas

Maturity x Organizational structure	CEO	CIO	CTO	Risk and Compliance	CFO
1 – Ad-hoc	2	4	4	1	
2 - Repeatable	2	11	7	1	1
3 - Defined processes	5	9	3	5	1
4 - Managed and measured	7	3	1	4	
5 – Optimized	7	4	5	1	
Total	23	31	20	12	2

Source: Authors (2020)

PROPOSALS OF IS GOVERNANCE GUIDELINES

Based on the analysis of results presented in previous sections, a set of information security governance guidelines was prepared for the electricity industry.

1st Guideline: Information security governance should report directly to the organization CEO.

This guideline discusses information security in the organizational structure. Authors like Carcary *et. al*, (2016) and You *et. al* (2018) debate on the best strategy for subordination of information security governance, and indicate subordination to higher levels of the company. In the present study, most respondents considered subordination to the CEO as the best option, because the maturity level is raised in this scenario.

2nd Guideline: The organization should count on a business continuity plan.

Since this is a strategic item for the organization's continuity, a well prepared plan is required to support IS governance. According to Yaokumah (2014), information security

governance helps ensure the business continuity. This second guideline is proposed to ensure that information security will be considered in the plan.

3rd Guideline: A Disaster Recovery planning aligned to the business continuity plan is essential.

A disaster recovery is necessary to ensure continuity of services and minimization of exposure to risk, according to Georg (2017). Availability is a fundamental aspect for information security.

4th Guideline: Information security alignment with the company's strategic planning.

With this alignment, the top management becomes informed of all security decisions. According to Haqaf and Koyuncu (2018), Nicho (2018), IS governance should be part of corporate governance due to its strategic role, ensuring that the organization objectives will be achieved and risks will be mitigated. That said, this guideline is also corroborated by the study with respondents.

5th Guideline: Awareness of information security to the business and to the user.

It is essential to raise awareness of all on the importance of information security. With it, some risks can be avoided. According to Nazareth and Choi (2015), Höne and Eloff (2009), norms, policies, awareness and training help reduce any type of attack, and minimize risks. With it, governance maturity is also increased.

6th Guideline: Information security policies and norms signed by the executive board.

Well defined information security governance guidelines, policies and norms, with approval of the board, increase the level of maturity, and the documents proposed gain more visibility in the organization. According to Carcary et al. (2016), these policies should reach the whole organization. For Chinyemba and Phiri (2018), IS governance occurs by implementing these policies and controls in the organization. So, this guideline is about acceptance and signature of these policies by the executive board.

7th Guideline: Count on risk management for information security.

Monitoring of risks helps reduce future negative impacts. According to Kure et al. (2018), lack of maturity in information security governance maximized risks in the electricity industry. For Martins et al. (2019), the electricity industry, for being essential to human life, should keep security governance in order to mitigate any type of risks. In this industry, risk management is necessary.

8th Guideline: Train new employees in information security.

With that, the employee becomes aware of information security norms and policies practiced in the company. This movement must be continuous, through training and communication (Cardoso et al., 2019). Training the new employee in guidelines and best information security practices, according to Nazareth and Choi (2015), raises IS governance maturity. It also helps in the effective participation of all inside the organization, according to You et al. (2018). So, training the user in the act of hiring is necessary.

9th Guideline: Monitoring of information security incident.

Such monitoring helps reduce possible negative impacts in case any incident occurs. For Nazareth and Choi (2015), Kure et al. (2018), monitoring tools help avoid attacks, information leaks and financial loss in the organization. So, this guideline of effective monitoring of IS incidents is very important.

10th Guideline: Count on firewall for the datacenter and another for perimeter protection.

This model helps prevent direct attacks to the organization datacenter. In case the perimeter is compromised, actions can be taken with regard to the datacenter. This guideline arises from market experience, where companies do not protect their perimeter, the most valuable portion of the business. Having an effective segmentation in the network, with controlled access helps elevate the level of maturity and reduces the risk of attacks to the productive environment and to the automation environment.

CONCLUSION

The present study, first surveyed the literature on IS governance in corporate ambit, how strategic management directly affected the area and how the electricity industry was positioned about the theme. With this identification, it was possible to ground the composition of this research.

Then, the mapping of the perception of IS managers, coordinators and experts was made with regard to IS governance, by means of the answers obtained with the questionnaire. It was evident, in this stage, that the importance given by the professional to the themes addressed is not always the same in the organization. Moreover, it could be observed that the level of maturity stays between optimized and managed where security reports directly to the organization CEO. On the other hand, if IS is subordinated to more operational areas, such as Information Technology, the maturity level is much lower, reaching a repeatable level.

Since the financial aspect and the organization image are highly affected when some anomaly occurs in the cybercrime environment, some companies, for presenting high maturity level in their processes, seek to follow good practices not to face a financial collapse or tarnish their image.

Based on the research results, 10 guidelines were suggested as best practices for the electricity industry, aiming to answer the central question of the research. It is worth highlighting the following guidelines: information security should report to the CEO; there should be internal segmentation of the environment allowing actions of authorized persons only; there should be efficient monitoring of information security incidents in order to control anything that occurs in the network.

All guidelines help form an effective IS governance with methods, training, awareness, and well defined norms. It is worth mentioning that this is a continuous movement, always seeking the evolution of processes and increasing their maturity.

However, the proposed guidelines may not be generalized and further studies should be conducted to adapt new IS governance guidelines in other industries, because there is a limitation in the size of the sample used, which was conditioned to the 104 respondents of the questionnaire, making it impossible to generalize as the size of the population is not known.

With the analysis of this research and answers obtained in this study, we hope that companies will adopt information security governance, or, for those that already count on well structured processes, that they will increasingly raise their level of maturity. IS must reach the whole organization with its processes and norms, rather than being just a technological information security.

While seeking the theme evolution in organizations, due to the importance of the subject, it is suggested, as future work, the creation of new IS governance guidelines to contribute to the improvement in the organizational maturity level. A research turned to the safe development in organizations and the maturity of the teams, factors that influence IS maturity and respective subordination to the organization hierarchical level. An analysis of the data from the respective research, using multivariate analysis or MCDM method, - Multiple criteria decision making, is also proposed, since the General Data Protection Law in Brazil is focused on personal data leaks and this development team will play a key role in this protection.

REFERENCES

Ajayi, B.A. and Hussin, H. (2018), "Conceptualizing information technology governance model for higher education: an absorptive capacity approach", *Bulletin of Electrical Engineering and Informatics*, Vol. 7, No. 1, pp. 117-24. http://dx.doi.org/10.11591/eei.v7i1.898.

Alencar, G.D., Moura, H.P., Farias Júnior, I.H. et al. (2018), "An adaptable maturity strategy for information security", *Journal of Convergence Information Technology*, Vol. 13, No. 2, pp. 1-12.

Amin, S.M. and Wollenberg, B.F. (2005), "Toward a smart grid: power delivery for the 21st century", *IEEE Power & Energy Magazine*, Vol. 3, No. 5, pp. 34-41. http://dx.doi.org/10.1109/MPAE.2005.1507024.

Brasil (2018), *Decreto n° 9.573, que trata especificamente em Política Nacional de Segurança em Infraestrutura Crítica, PNSIC*. Brasília.

Carcary, M., Renaud, K., McLaughlin, S. et al. (2016), "A framework for information security governance and management", *IT Professional*, Vol. 18, No. 2, pp. 22-30. http://dx.doi.org/10.1109/MITP.2016.27.

Cardoso, J.A.A., Ishizu, F.T., Lima, J.T. et al. (2019), "Blockchain Based MFA Solution: the use of hydro raindrop MFA for information security on WordPress websites", *Brazilian Journal of Operations & Production Management*, Vol. 16, No. 2, pp. 281-93. http://dx.doi.org/10.14488/BJOPM.2019.v16.n2.a9.

Chinyemba, M.K. and Phiri, J. (2018), "An investigation into information security threats from insiders and how to mitigate them: a case study of Zambian public sector", *Journal of Computational Science*, Vol. 14, No. 10, pp. 1389-400. http://dx.doi.org/10.3844/jcssp.2018.1389.1400.

Cholez, H. and Girard, F. (2014), ""Maturity assessment and process improvement for information security management in small and medium enterprises", *Journal of Software: Ecological Processes*, Vol. 26, No. 5, pp. 496-503. http://dx.doi.org/10.1002/smr.1609.

Costa, H. (2010), "Modelo para webibliomining: proposta e caso de aplicação", *Revista da FAE*, Vol. 13, pp. 115-26.

Dhillon, G., Syed, R. and Pedron, C. (2016), "Interpreting information security culture: An organizational transformation case study", *Computers & Security*, Vol. 56, pp. 63-9. http://dx.doi.org/10.1016/j.cose.2015.10.001.

El Ghorfi, R., El Aroussi, M., Ouadou, M. et al. (2018), "Valuating IT governance strategies with real options in a decision making framework", *International Journal of Information Systems in the Service Sector*, Vol. 10, No. 4, pp. 42-58. http://dx.doi.org/10.4018/IJISSS.2018100103.

Evans, M., He, Y., Maglaras, L. et al. (2019), "HEART-IS: a novel technique for evaluating human error-related information security incidents", *Computers & Security*, Vol. 80, pp. 74-89. http://dx.doi.org/10.1016/j.cose.2018.09.002.

Ferreira, S.A., Vieira Neto, J. and Batista, H.M.C.S. (2019), "Critical success factors on project and process management in competitive strategy implementation", *Brazilian Journal of Operations & Production Management*, Vol. 16, No. 4, pp. 605-16. http://dx.doi.org/10.14488/BJOPM.2019.v16.n4.a6.

Georg, L. (2017), "Information security governance: pending legal responsibilities of non-executive boards", *The Journal of Management and Governance*, Vol. 21, No. 4, pp. 793-814. http://dx.doi.org/10.1007/s10997-016-9358-0.

Gray, D.E. (2012), *Pesquisa no Mundo Real*, Penso, Porto Alegre.

Han, Z., Huang, S., Li, H. et al. (2016), "Risk assessment of digital library information security: a case study", *The Electronic Library*, Vol. 34, No. 3, pp. 471-87. http://dx.doi.org/10.1108/EL-09-2014-0158.

Haqaf, H. and Koyuncu, M. (2018), "Understanding key skills for information security managers", *International Journal of Information Management*, Vol. 43, pp. 165-72. http://dx.doi.org/10.1016/j.ijinfomgt.2018.07.013.

Höne, K. and Eloff, J.H.P. (2009), "Information security governance: Business requirements and research directions", *Corporate Ownership and Control*, Vol. 7, No. 1, pp. 309-17. http://dx.doi.org/10.22495/cocv7i1c2p6.

Johnston, A.C. and Hale, R. (2009), "Improved security through information security governance", *Communications of the ACM*, Vol. 52, No. 1, pp. 126-9. http://dx.doi.org/10.1145/1435417.1435446.

Kalogeraki, E.-M., Papastergiou, S.N., Mouratidis, H. et al. (2018), "A novel risk assessment methodology for SCADA maritime logistics environments", *Applied Sciences*, Vol. 8, No. 9, pp. 1477. http://dx.doi.org/10.3390/app8091477.

Kim, H., Lee, K. and Lim, J. (2017), "A study on the impact analysis of security flaws between security controls: An empirical analysis of K-ISMS using case-control study", *Transactions on Internet and Information Systems*, Vol. 11, No. 9, pp. 4588-608. http://dx.doi.org/10.3837/tiis.2017.09.022.

Kim, J. and Tong, L. (2013), "On topology attack of a smart grid: Undetectable attacks and countermeasures", *IEEE Journal on Selected Areas in Communications*, Vol. 31, No. 7, pp. 1294-305. http://dx.doi.org/10.1109/JSAC.2013.130712.

Krishnan, R.B., Thandra, P.K., Murty, S.A.V.S. et al. (2017), "Font Attributes based Text Steganographic algorithm (FATS) for communicating images: a nuclear power plant perspective", *Kerntechnik*, Vol. 82, No. 1, pp. 98-111. http://dx.doi.org/10.3139/124.110651.

Kure, H.I., Islam, S. and Razzaque, M.A. (2018), "An integrated cyber security risk management approach for a cyber-physical system", *Applied Sciences*, Vol. 8, No. 6, pp. 898. http://dx.doi.org/10.3390/app8060898.

Machado, T.G., Mota, A.A., Mota, L.T.M. et al. (2016), "Methodology for Identifying the Cybersecurity Maturity Level of Smart Grids", *IEEE Latin America Transactions*, Vol. 14, No. 11, pp. 4512-9. http://dx.doi.org/10.1109/TLA.2016.7795822.

Martins, R.J., Knob, L.A.D., Silva, E.G. et al. (2019), "Specialized CSIRT for Incident Response Management in Smart Grids", *Journal of Network and Systems Management*, Vol. 27, No. 1, pp. 269-85. http://dx.doi.org/10.1007/s10922-018-9458-z.

Miloslavskaya, N.G. and Tolstoy, A.I. (2017), "Visualization of information security management processes", *Scientific Visualization*, Vol. 9, No. 5, pp. 117-36. http://dx.doi.org/10.26583/sv.9.5.10.

Mishra, S. (2015), "Organizational objectives for information security governance: a value focused assessment", *Information and Computer Security*, Vol. 23, No. 2, pp. 122-42. http://dx.doi.org/10.1108/ICS-02-2014-0016.

Moon, T.W., Hur, W.-M. and Choi, Y.J. (2019), "How leaders' perceived emotional labor leads to followers' job performance: a serial mediation model", *Journal of Service Theory and Practice*, Vol. 29, No. 1, pp. 22-44. http://dx.doi.org/10.1108/JSTP-11-2017-0201.

Nazareth, D.L. and Choi, J. (2015), "A system dynamics model for information security management", *Information & Management*, Vol. 52, No. 1, pp. 123-34. http://dx.doi.org/10.1016/j.im.2014.10.009.

Nicho, M. (2018), "A process model for implementing information systems security governance", *Information and Computer Security*, Vol. 26, No. 1, pp. 10-38. http://dx.doi.org/10.1108/ICS-07-2016-0061.

Nicol, D.M. (2021), "The ransomware threat to energy-delivery systems", *IEEE Security and Privacy*, Vol. 19, No. 3, pp. 24-32. http://dx.doi.org/10.1109/MSEC.2021.3063678.

Oliveira, I.A.M., Drumond, G.M. and Méxas, M.P. (2021), "Governança de Segurança da Informação na Indústria de Energia Elétrica: Revisão Bibliográfica", *Revista Científica Multidisciplinar Núcleo do Conhecimento*, Vol. 15, pp. 64-88. http://dx.doi.org/10.32749/nucleodoconhecimento.com.br/tecnologia/governanca-de-seguranca.

Pardo, C., Pino, F.J. and García, F. (2016), "Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards", *International Journal of Software Engineering and Its Applications*, Vol. 10, No. 9, pp. 217-30. http://dx.doi.org/10.14257/ijseia.2016.10.9.18.

Qassim, Q.S., Jamil, N., Daud, M. et al. (2019), "A review of security assessment methodologies in industrial control systems", *Information and Computer Security*, Vol. 27, No. 1, pp. 47-61. http://dx.doi.org/10.1108/ICS-04-2018-0048.

Rebollo, O., Mellado, D., Fernández-Medina, E. et al. (2015), "Empirical evaluation of a cloud computing information security governance framework", *Information and Software Technology*, Vol. 58, pp. 44-57. http://dx.doi.org/10.1016/j.infsof.2014.10.003.

Rodofile, N.R., Radke, K. and Foo, E. (2019), "Extending the cyber-attack landscape for SCADA-based critical infrastructure", *International Journal of Critical Infrastructure Protection*, Vol. 25, pp. 4-35. http://dx.doi.org/10.1016/j.ijcip.2019.01.002.

Sánchez, L.E., Parra, A.S.O., Rosado, D.G. et al. (2009), "Managing security and its maturity in small and medium-sized enterprises", *Journal of Universal Computer Science*, Vol. 15, No. 15, pp. 3038-58. http://dx.doi.org/10.3217/jucs-015-15-3038.

Sanger, D.E., Krauss, C. and Perlroth, N. (2021), *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*. The New York Times, 8 maio.

Schmitz, C., Schmid, M., Harborth, D. et al. (2021), "Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities", *Computers & Security*, Vol. 108, pp. 102306. http://dx.doi.org/10.1016/j.cose.2021.102306.

Suryawan, A.D. and Veronica. (2018), "Information technology service performance management using COBIT and ITIL frameworks : a case study", in *International Conference on Information Management and Technology (ICIMTech) 2018*. IEEE, Jakarta. http://dx.doi.org/10.1109/ICIMTech.2018.8528197

Thiyagarajan, P., Thandra, P.K., Rajan, J. et al. (2015), "Shamir secret sharing scheme with dynamic access structure (SSSDAS): Case study on nuclear power plant", *Kerntechnik*, Vol. 80, No. 2, pp. 150-60. http://dx.doi.org/10.3139/124.110489.

Valencia-Duque, F.J. and Orozco-Alzate, M. (2017), “A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards”, *RISTI - Revista Iberica de Sistemas e Tecnologias de Informação*, No. 22, pp. 73-88. https://doi.org/10.17013/risti.22.73-88

Vanickis, R., Jacob, P., Dehghanzadeh, S. et al. (2018), “Access control policy enforcement for zero-trust-networking”, in *29th Irish Signals and Systems Conference (ISSC) 2018*, New York, IEEE.

Woo, P.S. and Kim, B.H. (2018), "Establishment of cyber security countermeasures amenable to the structure of power monitoring & control systems", *Transactions of the Korean Institute of Electrical Engineers*, Vol. 67, No. 12, pp. 1577-86. http://dx.doi.org/10.5370/KIEE.2018.67.12.1577.

Yang, T.-H., Ku, C.-Y. and Liu, M.-N. (2016), "An integrated system for information security management with the unified framework", *Journal of Risk Research*, Vol. 19, No. 1, pp. 21-41. http://dx.doi.org/10.1080/13669877.2014.940593.

Yaokumah, W. (2014), "Information security governance implementation within Ghanaian industry sectors an empirical study", *Information Management & Computer Security*, Vol. 22, No. 3, pp. 235-50. http://dx.doi.org/10.1108/IMCS-06-2013-0044.

You, Y., Oh, J., Kim, S. et al. (2018), "Advanced approach to information security management system utilizing maturity models in critical infrastructure", *Transactions on Internet and Information Systems*, Vol. 12, No. 10, pp. 4995-5014. http://dx.doi.org/10.3837/tiis.2018.10.020.

Author contributions: I.A.M.O. - Conceptualization, Writing - Original Draft, Data Collection & Analysis; M.P.M. – Conceptualization, Writing - Review & Editing, Project Administration; E.M.M.M. - Conceptualization, Writing - Review & Editing; G.M.D. - Writing - Review & Editing; All authors read and approved the final manuscript.