International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 16 (2024) pp. 030-039
© MIR Labs, www.mirlabs.net/ijcisim/index.html

Received: 08 July 2022; Accepted: 05 September 2023; Published: 24 April 2024

Integration of Practices for Information Security Policy Compliance

Norman Fong[1] and Sussy Bayona-Oré[2]
[1] Unidad de Posgrado de la Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos
Calle Germán Amézaga s/n – Lima, Lima-Perú
norman.fong@unmsm.edu.pe

[2] Vicerrectorado de Investigación, Universidad Autónoma del Perú,
Panamericana Sur, Km. 16.3, Villa El Salvador, Lima-Perú
sbayonao@hotmail.com

Abstract: **With the incorporation of Information and Communication Technologies in organizations, Information Security is key to protect the organization's information assets. The purposes and objectives of the organization related to Information Security are set out in the Information Security Policy document, which are mandatory for the employee to comply with. However, despite the efforts made by the organizations to comply with them, this objective is not always achieved. In response, several authors have proposed practices to be followed in order to ensure compliance with Information Security Policies. This article presents a proposal for the integration of the practices identified in the literature review. These practices have been structured in four phases related to: the establishment of the Information Security Committee, considerations in the elaboration of an Information Security Policy, on the communication of information security policies and the evaluation of security performance. Also, a survey was conducted to evaluate the compliance of ISP. A total of 108 security professional participated in the survey. Consideration of good practices supports the deployment and monitoring of Information Security Policy compliance.**

Keywords: information security policies, information security, ISO 27001, ISO 27002, compliance

I. Introduction

Information Security (IS) is one of the most important issues to be addressed in the current information technology landscape [1] [2] since it has been shown that companies and organizations in general, that manage their information assets more efficiently, are the ones that will more easily achieve financial and commercial success. For this reason, multiple actions and measures have been carried out in order to achieve and ensure information security, and one of these actions is the establishment of Information Security Policies (ISP) [1].

ISP is an important security measure in organizations since it establishes the guidelines that all personnel of an organization, without exception, must follow in order to ensure the confidentiality, integrity and availability of the information used in the organizations [3]. However, despite the expectation of employee awareness of and compliance with ISP, in many cases compliance with the policies has been found to be ineffective, resulting in serious breaches of many companies' data.

Several research studies have been conducted in different countries to analyze and determine the set of factors that determine the success or, as a countermeasure, the failure, of compliance with the ISP implemented in a company. There are several researchers that propose models based on theories about the nature of people's behavior and motivation (TPB, TRA, PMT among others) for ISP compliance [4]. Likewise, these researchers propose good practices to achieve the purpose. However, these practices are distributed in the scientific literature related to compliance with ISP. The good practices must be organized and shared to be useful [5].

This article presents a set of practices that contribute to the compliance of ISP as a result of the literature review. The most important steps and decisions to be taken into account are indicated. Also, presents the results of a survey related to compliance of ISP according to the perception of security staff.

The results of this work are a contribution to the body of knowledge of ISP compliance and are aimed at IS professionals responsible for outlining the organization's ISP.

This article has been structured in five sections including the introduction. In Section II on related works, Information Security concepts, Information Security Policies, and security standards extracted from previous research are mentioned. Section III presents the methodology used. Section IV presents the collection of practices in the implementation of ISP. Section V presents the results of a survey to evaluate the compliance of ISP and Section VI presents the Conclusions.

II. Related Work

A. Information Security (IS)

The concept of Information Security (IS) comprises the protection of information against unauthorized access, use, disclosure, interruption, modification or destruction in order to safeguard its confidentiality, integrity, and availability [6]. Then, IS is a "natural aspect of the daily activities of all members of an organization" [7]. Thus, the effective implementation of IS controls is important since it aims to protect an organization's information assets, and by extension, its reputation, legal position, personnel, and other tangible or intangible assets [6]. Current information security standards include the ISO 27000 family of standards.

B. Information Security Policies (ISP)

There is a growing consensus within the literature that the ISP is a business document of increasing importance, which is uniquely positioned to proactively safeguard the availability, confidentiality, and integrity of corporate resources [8]. More specifically, it has been argued that this document should establish the organization's approach to information security management. To this end, a good ISP should specify individual responsibilities, define authorized and unauthorized uses of systems, provide venues for employee reporting of identified and suspected system threats, define penalties for violations, and provide a mechanism for updating the policy [9]

Perhaps the most critical role of the ISP is to explicitly define the specific rights and responsibilities of individual users, and to communicate these successfully to each and every employee, so that a uniform, consistent and effective approach is adopted throughout the organization [9]. Thus, employees should have no excuse for not being able to apply defined security practices in accordance with the established ISP. Consequently, the policy should act as the starting point for employees with respect to all information security issues to achieve successful security management [10].

According to the international standard ISO 27001, the first purpose of an ISP is to convey the objectives that top management intends to achieve with the implementation of the system, while the second purpose of the document is to construct it in a way that is easy for stakeholders to understand [11]. While ISO 27002 states that the ISP is "that document that expresses a general intention and instruction in the way that has been expressed by the company's management" [12]. All of the above, under a framework of Governance of Information and Communications Technologies (GTIC). COBIT 5, in Chapter 2, states the importance of a Governance framework in organizations. "The Board of Directors should mandate the adoption and adaptation of an enterprise IT governance (GEIT) framework, such as COBIT 5, as an integral part of the development of corporate governance [13].

C. Theories on Attitude Towards ISP Compliance

The main theories identified in studies on attitude towards ISP compliance comprise: Theory of Planned Behavior (TPB), General Deterrence Theory (GDT), Protective Motivation Theory (PMT) [5], Rational Decision Theory (RCT), Habit Theory (HT), and Theory of Reasoned Action (TRA). The Theory of Planned Behavior (TPB) states that attitude toward compliance with ISP is a strong predictor of an individual's intention to engage in such behavior, where such intention is a tendency of compliance action [14] [15] [16]. The General Deterrence Theory (GDT) argues that sanctions should be severe enough to deter employees from violating ISP [1]. Protective Motivation Theory (PMT) argues that, if the benefit of violating a security policy is not comparable to the severity of the penalties, employees will be effectively deterred from violating policies [7]. Rational Decision Theory (RCT) indicates that the perceived degree of punishment or sanction influences employees' decisions about ISP compliance through the balance of costs and benefits [17].

The Habit Theory (HT) argues about habit generated because of a strong safety culture, that many actions occur without a conscious decision to act and are performed because individuals are accustomed to carrying them out, and repeated behavior is often controlled more by situational cues than by conscious decision making [18]. The Theory of Reasoned Action (TRA) argues that "an employee's attitude toward compliance with these policies, combined with social norms, will cause the employee to intend to comply with security policies, leading to actual compliance with policies [19].

III. Methodology

To identify practices, a literature review of scientific articles on Information Security Policy compliance was conducted. The literature review found a number of contributions by authors detailing important activities in the implementation of ISP.

To find articles to review, the following question was posed: “What factors influence the adoption of information security policies?” In addition, the keywords “information security policies” AND “factors” were used. Finally, to exclude the articles of little use for research, it was necessary, by reading them, to determine if the research topics specifically involved information security policies, rather than information security in general.

In total, a review covered 63 articles on research carried out between 2012 and 2020. For each selected article, the most relevant practices related to ISP compliance were identified and organized as a proposal of four phases. This proposal is described in Section IV.

To determine the status of the practices related to compliance with the ISP, a quantitative and cross-sectional investigation was conducted. A questionnaire was designed as an instrument, with questions distributed in three modules. A module to collect sociodemographic information and another module for questions related to practices related to compliance with the ISP. The sample was not probabilistic. A total of 108 security professionals participated in the survey. The result of the survey is described in Section V.

IV. Identified Practices

The practices identified have been organized into four phases. (1) Phase I Establishment of the Information

Security Committee, (2) Phase II Development of Information Security Policies, (3) Phase III Communication of Information Security Policies and (4) Phase IV Security Performance Evaluation. The proposed outline for the integration of ISP practices oriented to the fulfillment of the ISP is presented in Table I.

Each of the Phases is described below. Activities are described for each of the phases. For each activity, tasks are described as a result of practices identified in the literature.

A. Phase I: Establishment of the Information Security Committee

The purpose is to establish a committee of specialists responsible for safeguarding the organization's information security, including among its responsibilities the preparation of the information security policy document. As an input, there is a need for the organization to have Information Security Policies. It is important that the Committee has the support of Senior Management.

The practices identified by activities and/or tasks are as follows.

1) Activity 1.01: Manage and count on the support of Senior Management:

The ISO 27001 standard establishes that senior management must express its total commitment to the security system and its intention to comply with the security requirements of the interested parties.

The following are the practices identified.

Table I. Organization of security practices.

Phases	Description	
Phase I: Establishment of the Information Security Committee	Input	Necessity of Implementing Information Security Policies.
	Activities	Activity 1.01: Manage and count on the support of Senior Management. Activity 1.02: Assess the current information security situation in the organization. Activity 1.03: Evaluate and select security specialists. Activity 1.04: Definition of roles and activities of the members of the Information Security Committee.
	Output	Identification of critical information security points of the organization. List of the members, roles, and activities of the Information Security Committee.
Phase II: Development of the Information Security Policy	Input	Results of Phase I.
	Activities	Activity 2.01: Analysis of critical points of information security. Activity 2.02: Preparation of the preliminary ISP document. Activity 2.03: Review and development of the ISP document. Activity 2.04: Development of the communication and information plan.
	Output	Definition of information security objectives and metrics. Definition of ISP scope. Security Violation Penalty Regulations. Official ISP document.
Phase III: Communication of Information Security Policies	Input	Results of Phase II.
	Activities	Activity 3.01: Execution of the communication plan. Activity 3.02: Publication of the official ISP document. Activity 3.03: Safety training and coaching for individuals in the organization. Activity 3.04: Generation of an organizational safety culture.
	Output	List of trained individuals. Training program report. Security incidents report.
Phase IV: Safety Performance Evaluation	Input	Results of Phase III.
	Activities	Activity 4.01: Evaluation of security metrics. Activity 4.02: ISP document review. Activity 4.03: Review of sanctions for security violations.
	Output	Evaluation report. New version of the official ISP document. New version of the ISP non-compliance sanction regulation.

- Recognize the importance of ongoing coordination activities: such as assessing the risk related to information systems and business process and evaluating the performance and impact of the implemented controls [19].
- Promote support for the establishment and implementation of ISP to increase the effectiveness of Information Management Systems [20].
- Strengthen trust between professionals and their respective sectors: the culture for instilling trust in the organization must be embedded within the organization prior to implementing ISP [21].
- Senior management and other key individuals in the organization must articulate a clear vision for ISP: formulate a clear strategy to achieve effective policy setting and establish clear goals and objectives to generate effective ISP that builds on the requirements of ISP compliance to protect the organization's assets against

security threats [22].

2) Activity 1.02: Assess the current situation of information security in the organization.

According to ISO 27001, the ISP must be adapted to the requirements of the organization, among which is the need to protect the organization's assets. This implies that senior management and those responsible for security must identify the possible risks to these assets and the degree of severity of a security threat resulting from a policy violation, in order to reflect these points in the ISP.

The following practice has been identified.

- Select the tools for diagnosing the current security situation. The Independent Information Security Culture Assessment (ISCA) tool has proven to be effective and practically implementable, yielding results over a period of time related to an information security culture when implementing action plans. This analysis allows: (1) the results to identify specific focus areas such as training and change management that require further development, (2) identify specific groups (e.g., work levels, business units, regions, or generation groups) that require improvement, and (3) achieve continuous improvement of an information security culture [23] [24].

3) *Activity 1.03: Evaluate and select security specialists.*

Although ISO 27001 establishes the need for the total commitment of top management to compliance with security policies, all individuals in the organization are expected to be committed to such compliance. Therefore, in the process of evaluating and selecting security specialists, the organization should take into account, apart from the security expertise required to carry out such responsibilities, that individuals with a strong belief in the organization's information security values and goals will be the most committed to ISP compliance.

The following are the practices identified.

- Determine the positions that make up the Information Security Committee, with the approval of Senior Management: to this end, special departments for ISP should be established and ISP specialists should be recruited [20].
- Carry out the process of calling and evaluating personnel to fill positions on the Information Security Committee: it should be taken into account that the ethical value and practices exhibited by those in positions of power are fundamental in setting the tone and providing employees with a model of acceptable behavior in the organization [25].

4) Activity 1.04: Definition of roles and activities of the members of the Information Security Committee

As part of Senior Management's commitment to information security, the security officers appointed by Senior Management: (1) must be uncompromising and sanction ISP violations, (2) must promote effective communication of ISP scopes so that they constitute a noticeable influence on the norms of individuals in the organization as stakeholders, (3) as well as construct and communicate policies so that they are understandable by all individuals in the organization and (4) implement education, training and security awareness programs.

The following are the practices identified.

- List the key information security activities to be carried out, and assign roles to committee members based on these activities: Organizations should design the roles in such a way that this responsibility is built into them. They can do this by letting the employee know their responsibility for consequences of their ISP-related actions [26].
- Appoint the personnel according to the roles in the positions that make up the Information Security Committee.
- Establish a support team, identifying experts in the area, human resources, and technical support personnel.

The outputs of Phase 1 are: (1) Identification of critical information security points of the organization and (2) List of members, roles, and activities of the Information Security Committee.

B. Phase II: Development of Information Security Policy

The purpose is the construction of the official ISP document by the organization's Information Security Committee. The Input to Phase II is the Output of Phase I. We will mention the practices identified by activities and / or tasks.

1) Activity 2.01: Analysis of critical information security points

According to ISO 27001 and ISO 27002 standards, policies must be built in accordance with the organization's requirements to protect the organization's assets and be communicated efficiently. This implies that senior management and security managers must identify the possible risks to those assets and the degree of severity of a security threat resulting from a policy violation. Once these two aspects have been identified, they must be reflected in the security policies, since they constitute the scope and objectives of the policies.

The following are the practices identified.

- Analyze the impact of security threats on the organization's information assets: In this respect, organizations operating in a global environment need to understand how behaviors and decision making are affected [19].
- Analyze changes in the organizations' information security strategies and practices: Typically, security management strategies and practices place a dominant emphasis on sanctioning and facilitating conditions such as training and providing assistance [25].
- Promote information security culture: organizations require more knowledge in information security than other aspects such as ISP or monitoring to establish an information security culture [27] from the highest level.
- Thinking more strategically and organizationally about security, so that cultures of goal-oriented plans are created for ISP compliance [16].

2) *Activity 2.02: Preparation of the preliminary ISP document*

These should be constructed considering that they should be easy to understand for all individuals in the organization, using simple language, and easy to put into practice [22]. Another element to take into account is the internalization of the policies, which can be achieved by reducing the possible benefits that a violation of security policies can mean for the individual, compared to the severity of the sanctions that such a violation implies. The following practices were considered.

- Collect the data obtained in the analysis of the organization's safety critical points, such as the scope of application, in order to define the objectives of the organization.
- Constructing the first version of the security document, which involves the development of the objectives, scope, principles, responsibilities, key objectives and related policies and use simple language when drafting the ISP: the ISP should be easy to understand so that employees feel confident with the safety guidelines, so that they can be practiced [21-22].
- Pay attention in the drafting of the ISP: according to the results of the ISP assessment and before any anticipated information security problems [20].
- Adapt the ISP in case of evidence of negative attitudinal response, in order to mitigate daily events that impede work, to the contextual aspects of the employees' positions, organization or industry [15].
- Consider having larger organizations adopt a comprehensive ISP framework for developing, implementing and enforcing ISP aimed at systematically and effectively alleviating ISP non-compliance [28].
- Building a better infrastructure around cyber security may decrease the complexity of the task but not at the expense of autonomy and competence, which are the primary motivators of human performance [29].

3) *Activity 2.03: Review and elaboration of the ISP document.*

In case deficiencies such as wording, reading comprehension or clarity are found by the Safety Committee to obtain a version to be approved by management.

The following are the practices identified.

- Review the draft document by senior management and the other members of the safety committee. In addition, the organization must impose written and approved ISP [20].
- Translating best practices that need to be applied means giving meaning to best practices and boundaries in the context of an organization because universal and general best practice procedures are not likely to be directly applicable as such and trying to implement them without a translation is likely to result in practices that employees cannot and therefore will not carry out in their work [30].
- Take organizational practice as the starting point and source of information for translation, so that the valuable advice of IS and other external consultants cannot substitute for local understanding and appreciation of local practices. A policy that is formulated largely or solely by external consultants may be inconsistent with organizational practice. In other words, knowing how employees should work in theory cannot substitute for contextual knowledge of how they work in practice [30].
- Encouraging a participatory approach during the ISP formulation process allows for the identification of possible inconsistencies and requirements that employees may not regularly carry out in their work. Thus, if those who have to comply with the policies cannot actively participate in policy development and if organizational practices are not understood, turning policy into action is, at best, a difficult task [30].
- Train employees after designing ISP to increase their awareness by paying attention to whether employees are more receptive to a deterrence message or a sense of responsibility message: The key implication is that actions taken to increase compliance with ISP should pay attention to the different ways in which employees are inclined or disinclined to comply [31].
- Develop ISP using both top-down and bottom-up approaches, seeking input from all levels in the organization so that all organizational actors take ownership of ISP and foster compliance with ISP [32].
- Support the alignment of personal standards with ISP and overcome discrepancies between policies and personal standards by forming close links between ISP's objectives and the internal values of its employees to encourage compliance [31].

4) *Activity 2.04: Development of the communication and information plan.*

The Safety Committee must establish an ISP communication and information plan aimed at all individuals in the organization. In this way, the Top Management must ensure that employees perceive that complying with ISP is not a purely formal obligation.

The following are the practices identified.

- The change of personal norms related to ISP must be accomplished through a restructuring of social norms related to ISP, as well as the generation of awareness of the consequences and ascription of personal responsibility, as such, instead of appealing directly to the moral obligation of employees, an organization can, through social norms, persuade its employees to behave in a consistent manner [26].
- Conduct regular communications on ISP matters, formal and informal rewards, and recognition of those who perform [33].
- Promote that end users have a clear understanding of their organization's ISP and a high level of confidence in their management's ability to identify security breaches [34].
- Design formal policies and communications to clarify which specific knowledge and skills are important and improve knowledge and attitude sharing in order to increase control of employees' perceived behavior [35].

The outputs of Phase II are: (1) Definition of information security objectives and metrics, (2) Definition of ISP scope, (3) Security violation penalty regulations, and (4) Official ISP document.

C. Phase III: Communication of Information Security Policies.

The purpose of this phase is the effective communication of the ISP to all individuals in the organization in order to ensure its adoption and effective compliance.

The entry is the Result of Phase II. We will mention the practices identified by activities and/or tasks.

1) *Activity 3.01: Execution of the communication plan.*

As established by the ISO 27001 standard, Senior Management must support employees in understanding and complying with the policies, in order to achieve the objectives mentioned in the document and facilitate compliance by all the people in the organization.

The following are the practices identified.

- Establish different communication channels available in the organization [36].
- Proactively communicate to workers about the importance of adhering to information security [37].
- Provide a platform for soliciting end-user feedback on existing security policies and during the drafting of new policies [36].
- Discuss in workshops or seminars the rules and procedures for safeguarding information assets with the objective of ensuring the participation of users [36].
- Allow employees to report challenges with existing ISP and possible solutions to circumvent the challenge while protecting information assets [36].
- Sensitize employees to the effect of non-compliance with the ISP and remind them that severe penalties will be strictly enforced for non-compliance [38].
- Induce a sense of responsibility on the part of employees by emphasizing that an employee has sufficient authority to comply with ISP, and that the organization relies on employee compliance to keep its information assets secure [26].
- To keep ISP non-compliance to a minimum, organizations should take steps to increase employee awareness of the cost of non-compliance [25].
- Effectively communicate rules, policies, codes and professional behaviors with the same rigor as the organization's financial priorities [25].
- Communicate to generate employee awareness of the benefits of ISP compliance emphasizing the moral relevance of compliance with security policies [15].
- Considering the potential value of moral suasion, appealing to shame to improve employees' ISP-violating behavior should be done carefully in practice because of the ethical issues that could arise [39].
- Complying with information security procedures keeps information security breaches down [40].
- Convey that not only employees, but the entire organization could be subject to an information security threat if employees do not comply with ISP [40].
- Understanding employees' perception of injustice enables the definition of mitigation strategies through communication [41].
- Managerial communication, including security awareness training, should be designed to discourage employees from using neutralization techniques that serve to stimulate thoughts of employee retaliation against unfair actions [41].
- Promote familiarity with ISP by communicating key aspects of compliance, such as ISP objectives, the importance of ISP compliance and information security threats [28].

2) *Activity 3.02: Publication of the official ISP document.*

Following the conventions established by ISO 27001, the ISP must be communicated in a way that is understandable to all individuals in the organization.

The following are the practices identified.

- Publish the security policy document on the transparency portal on the organizations official website by the committee responsible for this task. Management should ensure that the ISP is effectively documented and distributed to all employees [21]. Likewise, individuals within the organization should be notified of the publication of the document by the responsible.
- Open ISP referral sources for availability to individuals in the organization by those in charge. In a complementary way the stories of employees who received organizational punishment for non-compliance can be disseminated through blogs, newsletters and emails, so that others become aware of the consequences of non-compliance [42].

3) *Activity 3.03: Security education and training for individuals in the organization.*

A useful way to express senior management's commitment to information security is the implementation of education, training and security awareness programs to train employees to obtain the necessary skills to meet security requirements.

The practices identified are listed below.

- Training in ISP compliance should be adopted and promoted by leaders and should be a required part of the organization's activities [22].
- Develop content related to hazards, their impact and the effectiveness of recommended protective actions to eliminate the hazard, in training programs and minimize resistance [40].
- Developing generic courses that do not attempt to influence attitude and instead simply lecture on policy and procedural knowledge will be much less effective. Instead, training should be contextualized and use case studies to improve both the knowledge of what is expected and also the understanding of why IS is important [43].
- The organization could design intervention programs promoting the doctrine that rules and standards are organizational values, and these values are appreciated and respected by all employees. Such interventions may eventually build the shared perception of employees toward rule-following and, therefore, shape social norms toward compliance with ISP [26].
- Take into account the vulnerability of information security, since, if employees feel that they have no control

over their information infrastructure, together with the perception that such infrastructures are a target and are under daily attack, they will be more likely to comply with the ISP [44].

- Encourage employees to share knowledge, as well as to collaborate in projects related to information security and the exchange of skills and experiences [35].
- Execute training programs and demonstrate the importance of data protection to the organization's existence and, therefore, its job security, along with proving that these policies also serve to protect employees' personal data. Additionally, organizations can use ethics training to increase employee morale levels [31].
- Implement security education, training and awareness programs, emphasizing the negative effects of ISP violations on employees, the organization and society as a whole [15].
- Organizations should provide employees with the knowledge and technical skills necessary to comply with ISP, effectively enriching their self-efficacy in this domain [15].
- Consider that expert, reward and legitimate power positively influence the relationship between SETA programs and ISP compliance intentions, while coercive power and referral power do not [45].
- Increasing security awareness outside the workplace allows high levels of interest in information security and significantly reduces the effort and time spent on training activities [46].

4) Activity 3.04: Generating an organizational safety culture.

According to the literature, there are many angles to be addressed in order to generate a strong safety culture. Many of these approaches relate to Phase I, II and III activities. The following are the practices identified.

- Encourage compliance by all personnel in the organization by identifying and assigning tasks to all managers or department heads in order to demonstrate ISP-compliant behavioral intentions and thus motivate their colleagues [36].
- Compliance with ISP must be integrated into the organizational culture of the organization's Senior Management: Such leaders must promote the organizational culture through influence, empowerment, motivation and effective communication [22].
- Provide an environment where people can learn the values and importance of such policies through socialization with co-workers. Thus, managers could proactively promote the development of collaborative attributes among workers, especially those who are focused on information security issues [32].
- Fostering climates where employee commitment to ISP is linked to some form of motivation, whether intrinsic or extrinsic [32].
- Leverage social bonding information to foster compliance intentions. For example, influential personalities in organizations capable of motivating or shaping the opinions of others in their work groups or units could be tasked with "championing" the cause of ISP compliance in their context [32].
- Recognize that setting quality expectations for information security would make employees less motivated to consider noncompliance with the ISP [47].
- Effectively controlling or managing employee behavior, to some extent, would contribute significantly to solving the human vulnerability problem experienced, as employees will be equipped with the necessary behavioral attributes to defend against social engineering attacks [48].
- Determine whether, in general terms, people's anticipated regret and threat assessment are important to their behavioral intentions. Such consideration should be made when compliance with the ISP is explained or influenced [49].
- Identify, with a multilevel analysis, that groups influence opinions on the variables that determine ISP compliance intentions. Thus, if culture is viewed as more than a shared understanding of context, information security culture is formed and maintained primarily among employees in the same worksite [50].
- Measure homogeneity in beliefs, opinions and values that can be expressed in a survey; in fact, the norms that people perceive and can articulate in a questionnaire are much better predictors of intentions than the classification of the work-related groups to which they belong [50].
- Supporting end-users to truly understand the benefits of ISP compliance rather than educating them on security duties [51].
- Continuously reinforce employees' safety attitude and accountability. Regarding the mechanisms for sharing safety tips, which can take place as a result of work and trust relationships, there are different options [51].
- Consider implementing job rotation, mentoring or team building to increase the sharing of work tips and the development of a relationship between employees, which may subsequently lead to increased sharing of safety tips [51].
- Compliance should not be enforced solely from the top down through formal sanctions, but rather modeled on a daily basis by employees at all levels, including supervisors and the IT department [31].

Phase III outputs are: (1) List of trained individuals, (2) Training program report, and (3) Security incidents report.

D. Phase IV: Safety performance evaluation.

The purpose of this phase is to evaluate the results of the ISP implementation with respect to its metrics, in order to determine the necessary actions and corrections to be taken.

The input is the result of Phase III. We will mention the practices identified by activities and/or tasks.

1) *Activity 4.01: Evaluation of security metrics.*

As stated in ISO 27001, the first purpose of an ISP is to convey the objectives that senior management intends to achieve with the implementation of policies, while the second purpose is to construct the document in such a way that it is easy to understand for stakeholders. Therefore, the

Information Security Committee must periodically evaluate whether the metrics and objectives established in the ISP document have been fully or partially met, in order to take the necessary actions if the latter is the case.

The following are the practices identified.

- Execute the evaluation by the Information Security Committee. In order to carry out the measurement of metrics, it is possible to use the instrument generated in the research of Hanus et al [46]. The study proposed and developed a comprehensive instrument that allows a quick assessment of security awareness in individuals. The instrument was also designed to facilitate the construction of an effective training program [46].
- Adjust the instrument to obtain a customized approach and levels of granularity [46], since it allows for a quick identification of potential weaknesses in information security awareness and, therefore, will facilitate the design of a reinforcement activity or training program to address such deficiencies.

2) Activity 4.02: ISP document review.
According to ISO 27001 and ISO 27002, policies should be elaborated according to the requirements of the organization, communicated efficiently, and if poor security performance occurs in the organization, these policies should be revised, as well as redefining and clarifying the responsibilities of certain individuals in certain aspects of the policies.

The following are the practices identified.

- Review and approve the new version of the security document by the Information Security Committee and Senior Management. This review can be carried out under other important criteria [20].
- Continuously and periodically improve policies to anticipate the dangers and threats that may be encountered in relation to the organization's information and data, thus facilitating the taking of measures when necessary [20].
- From the ISP decisions of the organization's personnel, management can determine the type of security policy that intensifies the intent to breach ISP [28], and thus, should prioritize the most frequently chosen policies, and subsequently, review those policies to increase their usability and effectiveness.
- Management should regularly discuss with users to understand their perceptions of ISP, working together to address ISP-related problems [28].

3) Activity 4.03: Review of sanctions for security violations.
Given that the ISO 27001 standard mentions among the critical success factors of the implementation of the ISP, the aligned objectives and activities and an effective SETA program where employees and other interested parties are informed of their obligations mentioned in the ISP and security standards, the new sanctions to be applied in the event of a violation of the ISP should be considered based on these factors and as part of the continuous improvement process, as part of the review of the policy document.

The most important tasks to be performed are:

- Evaluate the impact of the current sanctions for information security violations with respect to the metrics established in the security document.
- Review the sanctions for security violations with respect to the results of the evaluation by the committee, and their approval by Senior Management. It should be taken into account that increasing effort, risk and reducing rewards significantly influences employees' attitudes towards the prevention of information security misbehaviour [52].
- Publish the sanctions regulations in official and reference sources available to staff.
- Foster a climate in which appropriate sanctions and penalties are instituted, in the sense that any sanctions imposed on offending employees must be measured, since recent research has shown that the application of sanctions without such considerations can lead to counterproductive results [37].

The outputs of Phase IV are: (1) Evaluation report, (2) New version of the official ISP document and (3) New version of the ISP non-compliance sanction regulation.

V. Practices and ISP compliance

The practices related to Organizational commitment, Attitude towards ISP, ISP Awareness, Security Education Training and Awareness Program (SETA), and Organizational security culture were evaluated. Next, the results of practices related to ISP compliance [53].

- *Organizational commitment:* The commitment of individuals to the organization implies adopting and complying with the ISP used in it to save the well-being of its organizational assets and its stability. The average answers to the questions of the Organizational Commitment factor were: 92% answered between “Always” and “Almost Always”, 6% answered “Sometimes” and 2% answered “Almost Never”.
- *Attitude towards ISP*: The attitude towards ISP allows employees to feel more inclined to adopt and comply with the policies. The average answers to the questions of the Attitude factor towards ISP were: 68% answered "Almost Always", 26% answered "Sometimes" and 6% "Almost Never".
- *ISP Awareness:* Information security awareness in ISP compliance plays a vital role in mitigating the risk of IS breaches. The average answers to the questions of the ISP Awareness factor were: 90% answered between “Always” and “Almost Always”, while 10% answered “Sometimes”.
- *Security Education and Training Awareness (SETA)*
  The SETA program is important for training employees and has shown consistent effects on the perceived benefits of ISP compliance. The average answers to the questions of the Education Program factor were: 67% answered between “Always” and “Almost Always”, 26% answered “Sometimes” and 7% answered “Almost Never”.
- *Organizational security culture:* The organizational security culture in compliance with the ISP must be promoted by supporting the IT staff, providing the necessary IT resources and information. The average

answers to the questions of the Organizational Safety Culture factor were: 73% answered between "Always" and "Almost Always", 20% answered "Sometimes" and 7% answered between "Almost Never" and " Never".

The results of this study show the importance of promoting practices related to ISP compliance. The prime concern in the digital world are the security measures []. to ensure the data integrity, data safety, and security of the digital infrastructure.

VI. Conclusions

The scientific literature on ISP compliance is extensive and presents different proposals based on different theories with the purpose of determining the most common causes of poor ISP compliance. Most of the theories are related to the human factor, which despite the efforts made by organizations has not achieved its objectives. A set of practices resulting from the literature review have been integrated into the four-phase proposal presented in this article. The practices involve supporting the process of deployment and monitoring of ISP compliance by the organizations' personnel, since employees are the target audience of the organizations, so it is necessary to understand the human aspect of information security. At the same time, the top management of the organizations must be the main architect of the improvement of the ISP compliance culture since they must make the relevant decisions to ensure the transition to an optimal information security culture. To evaluate the practices related to ISP compliance a survey was conducted with the participation of 108 security professionals. The results show that it is important to develop strategies to improve the security culture, training activities, improve la culture of security and the attitude.

References

[1] X. Chen, D. Wu, L. Chen, and J. K. Teng, “Sanction Severity and Employees’ Information Security Policy Compliance: Investigating mediating, moderating, and control Variable,” *Information Management* vol. 55, no. 8: pp. 1049-1060, 2018, https://doi.org/10.1016/j.im.2018.05.011

[2] B. Sussy, C. Wilber, L. Milagros and M. Carlos, "ISO/IEC 27001 implementation in public organizations: A case study," *In Proceedings on 2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1-6, 2015, doi: 10.1109/CISTI.2015.7170355.

[3] J. Weidman, and J. Grossklags, “Assessing the current state of information security policies in academic organizations.” *Inf. Comput. Secur.*, vol. 28, pp. 423-444, 2020, https://doi.org/10.1108/ICS-12-2018-0142

[4] J., Yupanqui, and S. Bayona, “Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento,” *Revista Ibérica de Sistemas e Tecnologias de Informação,* vol. 25, pp. 112-134, 2017.

[5] B. Sussy, C. Antonio, C. Gonzalo, C., S. Tomás, F., and S. Angel, Process deployment in a multi-site CMMI level 3 organization: A case study. Computer and Information Science, 147-156, 2008.

[6] Nieles, K. Dempsey, and V. Y. Pillitteri, “An Introduction to Information Security,” *NIST Special Publication*, pp. 1-91, 2017, https://doi.org/10.6028/NIST.SP.800-12R1

[7] K. Alshare, P. Lane, and M. Lane, “Information security policy compliance: a higher education case study,” *Information & Computer Security vol.* 26, no. 1, pp. 91-108, 2018, https://doi.org/10.1108/ICS-09-2016-0073

[8] E. Niemimaa, “Crafting Organizational Information Security Policies,” *Tampere University of Technology. Publication*; vol. 1507, 2017

[9] H. Paananen, M. Lapke, and M. Siponen, “State of the art in information security policy development,” *Computers & Security* vol. 88, pp.101608, 2020, https://doi.org/10.1016/j.cose.2019.101608

[10] A. Ghazvini, Z. Shukur, and Z. Hood, “Review of information security policy based on content coverage and online presentation in higher education,” *International Journal of Advanced Computer Science and Applications*, vol. 9, pp. 410-423, 2018, https://doi.org/10.14569/ijacsa.2018.090853

[11] ISOTools Excellence, “Qué debe incluir la Política security de la Información según ISO 27001,” *Blog Calidad y Excelencia*. 2017. Translated from https://www.isotools.org/2017/04/09/incluir-la-politica-seguridad-la-informacion-segun-iso-27001/

[12] Pmg-ssi.com, “Norma ISO 27002: El dominio política de seguridad,” August 3, 2017, https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/.

[13] ISACA, “Chapter 2: Positioning Enterprise Governance of I%T” *COBIT 2019 Implementation Guide*, Schaumburg IL, Illinois, USA, pp. 19-20, 2012.

[14] T. Sommestad, H. Karlzén, and J. Hallberg, “The Theory of Planned Behavior and Information Security Policy Compliance,” *Journal of Computer Information Systems* vol. 59, no. 4, pp. 344-353, 2019, http://dx.doi.org/10.1080/08874417.2017.1368421

[15] J. D'Arcy, and P.B. Lowry, “Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study,” *Information Systems Journal*, vol. 29, no. 1, pp. 43-69, 2019, https://doi.org/10.1111/isj.12173

[16] Hina, P. Dominic, and P.B. Lowry, “Institutional governance and protection motivation: Theoretical insights into shaping employees’ security compliance behavior in higher education institutions in the developing world,” *Computers & Security* vol. 87, pp. 101594, 2019, https://doi.org/10.1016/j.cose.2019.101594

[17] J. Han, Y. Kim, and H. Kim, “An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective,” *Computers & Security* 66: 52-65, 2017, http://dx.doi.org/doi: 10.1016/j.cose.2016.12.016

[18] A. Vance, M. Siponen, and S. Pahnila, “Motivating IS security compliance: Insights from Habit and Protection Motivation Theory,” *Information & Management* vol. 49, no. 3-4, pp. 190-198, 2012, https://doi.org/10.1016/j.im.2012.04.002

[19] W. Flores, E. Antonsen, and M. Ekstedt, “Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture,” *Computers & Security*, vol. 43, pp. 90-110, 2014, http://dx.doi.org/10.1016/j.cose.2014.03.004

[20] A. Abdelwahed, A. Mahmoud, and R. Bdair, “Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip,” *International Journal of Information Science and Management, vol.* 15, pp. 1-26, 2016.

[21] N. Humaidi, and V. Balakrishnan, “Indirect effect of management support on users’ compliance behaviour towards information security policies,” *Health Information Management Journal, vol.* 47, no. 1: pp. 17-27, 2018, https://doi.org/10.1177/1833358317700255

[22] A. Koohang, A. Nowak, J. Paliszkiewicz, and J. Nord, “Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness,” *Computer Information Systems*, vol. 60, no. 1, pp. 1-8, 2020, https://doi.org/10.1080/08874417.2019.1668738

[23] A. Veiga, and N. Martins, “Improving the information security culture through monitoring and implementation actions illustrated through a case study,” *Computers & Security*, vol. 49, pp. 162-176, 2015, http://dx.doi.org/10.1016/j.cose.2014.12.006

[24] A. Veiga, and N. Martins, “Information security culture and information protection culture: A validated assessment instrument,” *Computer Law & Security Review*, vol. 31, pp. 243-256, 2015, http://dx.doi.org/10.1016/j.clsr.2015.01.005

[25] K. Gwebu, J. Wang, and M. Hu, “Information security policy noncompliance: An integrative social influence model,” *Information Systems Journal*, vol. 30, pp. 220-269, 2020, https://doi.org/10.1111/isj.12257

[26] A. Yazdanmehr, and J. Wang, “Employees' information security policy compliance: A norm activation perspective,” *Decision Support Systems* vol. 92, pp. 36-46, 2016, http://dx.doi.org/10.1016/j.dss.2016.09.009

[27] A. Nasir, R. Arshah, and M. Hamid, “A dimension-based information security culture model and its relationship with employees’ security

behavior: A case study in Malaysian higher educational institutions," *Information Security Journal: A Global Perspective*, vol. 28, no. 3: pp. 55-80, 2019, https://doi.org/10.1080/19393555.2019.1643956

[28] K. Chang, and Y. Seow, "Protective Measures and Security Policy Non-Compliance Intention: IT Vision Conflict as a Moderator," *Journal of Organizational and End User Computing, vol.* 31, no. 1, pp. 1-21, 2019, https://dx.doi.org/10.4018/JOEUC.2019010101

[29] H. Pham, "Information security burnout: Identification of sources and mitigating factors from security demands and resources," *Journal of Information Security and Applications* vol. 46, pp. 96-107, 2019, https://doi.org/10.1016/j.jisa.2019.03.012

[30] E. Niemimaa, and M. Niemimaa, "Information systems security policy implementation in practice: from best practices to situated practices," *European Journal of Information Systems, vol. 26, pp. 1–20,* 2017, https://doi.org/10.1057/s41303-016-0025-y

[31] L. Jaeger, A. Eckhardt, and J. Kroenung, "The role of deterrability for the effect of multi-level sanctions on information security policy compliance: results of a multigroup analysis," *Information & Management,* vol 58, no. 3, 103318, 2020, https://doi.org/10.1016/j.im.2020.103318

[32] P. Ifinedo, "Roles of Organizational Climate, Social Bonds, and Perceptions of Security Threats on IS Security Policy Compliance Intentions," *Information Resources Management Journal,* vol. 31, pp. 52-83, 2018, http://dx.doi.org/ 10.4018/IRMJ.2018010103

[33] X. Chen, D. Wu, L. Chen, and J.K. Teng, **"**Sanction Severity and Employees' Information Security Policy Compliance: Investigating mediating, moderating, and control Variables," *Information & Management,* vol. 55, pp. 1049-1060, 2018, https://doi.org/10.1016/j.im.2018.05.011

[34] H. Khan, and K.A. Alshare, "Violators versus non-violators of information security measures in organizations—A study of distinguishing factors," *Journal of Organizational Computing and Electronic Commerce* vol. 29, no. 1, pp. 4-23, 2019, https://doi.org/10.1080/10919392.2019.1552743

[35] Y. Hong, and S. Furnell, "Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization," *Journal of Computer Information Systems,* pp. 1-10, 2019, https://doi.org/10.1080/08874417.2019.1683781

[36] E. Amankwa, M. Loock, and E. Kritzinger, "Establishing information security policy compliance culture in organizations," *Information & Computer Security,* vol. 26, pp. 420-426, 2018, https://doi.org/10.1108/ICS-09-2017-0063

[37] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?," *Information Systems Management,* vol. 33, pp. 30-41, 2016, http://dx.doi.org/10.1080/10580530.2015.1117868

[38] J. Addae, G. Simpson, and, G. Ampong, "Factors Influencing Information Security Policy Compliance Behavior,"*In the proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT):* pp. 43-47, 2019, https://doi.org/10.1109/ICSIoT47925.2019.00015

[39] A. Vance, M. Siponen, and D. Straub, "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures," *Information & Management* vol. 57, no. 4, 103212, 2020, https://doi.org/10.1016/j.im.2019.103212

[40] G. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly*, vol. 42, pp. 285-311, 2018, https://dx.doi.org/10.25300/MISQ/2018/13853

[41] R. Willison, M. Warkentin, and A. Johnston, "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives," *Information Systems Journal*, vol. 28, pp. 266-293, 2018, https://dx.doi.org/ 10.1111/isj.12129

[42] M. Merhi, and P. Ahluwalia, "Examining the impact of deterrence factors and norms on resistance to Information Systems Security," *Computers in Human Behavior,* vol. 92, pp. 37-46, 2019, https://doi.org/10.1016/j.chb.2018.10.031

[43] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q).,"*Computers & Security,* vol. 42, pp. 165-176, 2014, http://dx.doi.org/10.1016/j.cose.2013.12.003

[44] M. Rajab, and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Computers & Security, vol. 80*, 211-233, 2019, https://doi.org/10.1016/j.cose.2018.09.016

[45] H. Kim, H. Choi, and J. Han, "Leader power and employees' information security policy compliance," *Security Journal,* vol. 32: pp. 391-409, 2019, https://doi.org/10.1057/s41284-019-00168-8

[46] B. Hanus, J.C. Windsor, and Y. Wu, "Definition and Multidimensionality of Security Awareness: Close Encounters of the Second Order," *The DATA BASE for Advances in Information Systems,* vol. 49, pp. 103-133, 2018, https://dx.doi.org/10.1145/3210530.3210538

[47] M. Kajtazi, H. Cavusoglu, I. Benbasat, and D. Haftor, "Escalation of commitment as an antecedent to noncompliance with information security policy," *Information & Computer Security,* vol. 26, pp. 171-193, 2018, https://doi.org/10.1108/ICS-09-2017-0066

[48] I. van Vuuren, E. Kritzinger, and C. Mueller, "Identifying Gaps in IT Retail Information Security Policy Implementation Processes: Towards developing a secure IT enterprise built on trust," *In proceedings of the 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), 2015,* https://doi.org/10.1109/InfoSec.2015.7435517

[49] T. Sommestad, H. Karlzén, and J. Hallberg, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," *Information & Computer Security*, vol. 23, pp. 200-217, 2015, http://dx.doi.org/10.1108/ICS-04-2014-0025

[50] T. Sommestad, "Work-related groups and information security policy compliance" *Information and Computer Security*, vol. 26, pp. 533-550, 2018, https://doi.org/10.1108/ICS-08-2017-0054

[51] D. Dang-Pham, S. Pittayachawan, and V Bruno, "Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace.," *Computers in Human Behavior,* vol. 67, pp. 196-206, 2017, http://dx.doi.org/10.1016/j.chb.2016.10.025

[52] N. Safa, C. Maple, S. Furnell, M. Azad, C. Perera, M. Dabbagh, and M. Sookhak, "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Future Generation Computer Systems,* vol. 97, pp. 587-597, 2019.

[53] S. Bayona-Oré, and N. Ochoa, Políticas de Seguridad de la Información y los Factores Relacionados con su Cumplimiento. Revista Ibérica de Sistemas e Tecnologias de Informação, vol. E51, pp. 540-548, 2022.

[54] G. Datt, G. and N. Tewari, N., "A Study of Computer Users' Attitude and Awareness towards Cyber Security," *International Journal of Computer Information Systems & Industrial Management Applications*, vol. 13, no. (2021), pp. 300-307, 2021.

Author Biographies

NORMAN FONG OCHOA is Systems Engineer with master's degree in Governance of Information Technology at Universidad Nacional Mayor de San Marcos. He has managed technology projects for more than two years. Her current research interests include security information.

SUSSY BAYONA ORÉ is a professor and researcher at the Universidad Autónoma del Perú and Universidad Nacional Mayor de San Marcos, Peru. She received her Ph.D. in software engineering from Universidad Politécnica de Madrid, Spain. Her field of expertise focuses on software development projects, process improvement, security information and e-government. She has more than 25 years of experience in technology areas.