International Journal of Business and Technology Management
e-ISSN: 2682-7646 | Vol.6, No. 2, 324-337, 2024
http://myjms.mohe.gov.my/index.php/ijbtm

A Conceptual Model for Promoting Information Security Policy Compliance Behaviour at Workplace

Allen Peter Diman[1*], Titik Khawa Abdul Rahman[1]

[1] School of Graduate Studies, Asia e University, Selangor, Malaysia

*Corresponding Author: C70105150001@aeu.edu.my

Received: 15 May 2024 | Accepted: 18 July 2024 | Published: 31 July 2024

DOI: https://doi.org/10.55057/ijbtm.2024.6.2.29

Abstract: *Securing sensitive and critical information is a significant challenge for many organisations, as leaks can cause financial, reputational, and competitiveness losses. Organisations can implement an Information Security Policy (ISP) that employees must comply with to minimise this risk. However, ensuring compliance with the ISP continues to be a problem. To address this issue, a conceptual model has been proposed that organisations can use to promote ISP compliance behaviour among their employees. The Health Action Process Approach (HAPA) Model is used to derive this model. The model consists of two phases - motivational and volitional which are expected to cover the elements needed to promote behavioural change for ISP compliance. The model's multi-processes approach, covering critical aspects such as risk assessment, self-efficacy, initiation, and maintenance, enables it to serve as a platform for organisations to sustain ISP compliance over the long term. Organisations can conduct employee assessments and provide ISP compliance training and awareness campaigns to implement the model. They can also disseminate cues about information security issues and how the ISP can assist employees in handling them, discourage behaviour that leads to complacency towards ISP compliance, and update the ISP to keep it relevant. The proposed model presents an opportunity for future research to evaluate its applicability in organisational settings.*

Keywords: Information security, Information Security Policy, Health Action Process Approach Model, Self-efficacy, Compliance

1. Introduction

In the modern business world, information is a precious asset for many organisations (Bolek et al., 2023). Therefore, it is crucial to guard and secure the information, especially critical and confidential data (He & Sun, 2022; Naik, 2022). A breach in information security can have catastrophic consequences for a company, including financial losses, reputational damage, and loss of competitive advantage (Cheng et al., 2023; Dong et al., 2023). Recent studies have shown that information security breaches have had severe negative impacts on businesses. According to Reshmi (2021), in 2019, 63% of companies located in the UK and US reported experiencing data security issues. The same author also revealed that the number of data breaches in the UK surged by 160% between 2016 and 2019, impacting 25,575 confidential records in 2019 alone. With over 320,000 new malware and more than 4,000 ransomware attacks happening daily, the number of security incidents is expected to continue to increase (Uddin Sharif & Mohammed, 2022). Separately, a different report revealed that 91% of global data breaches in 2019 were due to phishing emails, resulting in financial losses exceeding USD 11.5 billion (Uddin Sharif & Mohammed, 2022).

Despite the availability of technology to manage these processes, organisations still rely on employee compliance with the Information Security Policy (ISP) as the primary way to reduce the risks associated with information security breaches (Alraja et al., 2023). However, this approach can pose a problem since employees' non-compliance with an organisation's ISP can seriously put critical and confidential information at risk, creating information system vulnerability (Alraja et al., 2023). This is supported by a study conducted by Chen and Tyran (2023), which shows that 37% of employees do not adhere to their organisation's ISP, including copying sensitive data on USB drives, leaving computers unlocked, sharing passwords and misusing the system. Improving employees' compliance with ISPs can enhance information security management in organisations (Bayona-Oré & Ochoa, 2023). Thus, compliance with the ISP is essential to guarantee valuable information and data safety and protect confidentiality, integrity and availability (Bolek et al., 2023). In that sense, ISP compliance behaviour should be integrated into day-to-day business operations and prioritised by organisations (Bolek et al., 2023). Various studies have suggested that adhering to ISP is primarily determined by human behaviour (e.g., Ryutov, 2023; Sulaiman et al., 2022). Researchers have attempted to find solutions using psychological theories, external factors, and theoretical constructs (e.g., Alassaf & Alkhalifah, 2021; Hong & Furnell, 2022). Studies focusing on ISP compliance can generally be categorised into two main dimensions - the intention to comply and to violate. Researchers examine what motivates employees to break the ISP. Some studies analyse compliance-related behaviours with ISPs (e.g., Butler & Brown, 2023), while others explore violation behaviours (e.g., Aggarwal & Dhurkari, 2023; Hengstler et al., 2022). Influential security culture, proper security management, and positive security awareness can improve employee compliance. Conversely, non-compliance may result from psychological or external factors, intentional or accidental.

Various factors influence compliance or non-compliance towards ISPs, but evaluating human behaviour can be complex. Several psychological theories have been proposed to cover different aspects of human behaviour. In the information security (IS) context, multiple research models and theories have been suggested by IS researchers to assess individuals' behaviours towards ISPs (e.g., Alanazi et al., 2020; Kuppusamy et al., 2022). However, setting an individual's information security intention can be challenging (Kuppusamy et al., 2022). Although researchers have integrated behavioural theories in the IS context to some extent, several gaps remain open, such as studies conducted by Hengstler et al. (2022) and Kuppusamy et al. (2022), which produced inconsistent results. Therefore, researchers must correctly measure behaviours using these theories' core and full constructs. Similar outcomes can be expected for each behavioural theory used in the IS research. Several popular theories and models are available for assessing human intentions towards information security policies when studying ISP compliance. However, according to Almansoori et al. (2023) and Chiniah and Ghannoo (2023), more standard behavioural process models must be used. Additionally, most theories and models in the extant literature are specific to a particular sector (such as finance or higher education) or various phenomena (Almansoori et al., 2023). Similarly, previous studies have yet to develop a comprehensive process that can exhibit the transformation process from non-compliance to compliance, which is necessary to promote ISP compliance behaviour in organisations. Therefore, it is essential to identify a behavioural transformation process incorporating components that organisations can use to encourage ISP compliance behaviour. This paper aims to fill this gap by proposing the processes required to transform non-ISP compliance behaviours into ISP compliance behaviour through a conceptual model.

2. Literature Review

Numerous studies have explored ISPs' compliance and non-compliance behaviours and proposed several behavioural theories to understand the factors influencing such behaviours. These studies generally provide composite information security compliance frameworks with guidance from past literature (e.g., Alassaf & Alkhalifah, 2021; Sulaiman et al., 2022) or taxonomies of information security behaviours (e.g., Alanazi et al., 2020; Bélanger et al., 2022; Chen & Tyran, 2023). In both circumstances, researchers agreed that compliance and non-compliance behaviours directly or indirectly affect an organisation's information security. Therefore, compliance enhancement studies mainly focus on improving individuals' psychological behaviour towards complying with organisational security policies (e.g., Ali et al., 2020; Chen & Tyran, 2023; Li & Hoffman, 2023) or providing solutions to mitigate individuals' malicious behaviours (e.g., Lee et al., 2023; Nasir et al., 2022; Ryutov, 2023). Information security behaviour consists of many psychological components, and researchers use several psychological theories, such as the theory of planned behaviour (Brooks et al., 2023), the protection motivation theory (Kuppusamy et al., 2022) and the theory of reasoned action (Chiniah & Ghannoo, 2023), to understand such behaviour. Many researchers have presented helpful solutions towards ISP compliance behaviour by examining behavioural activities that vary from culture to culture (Ali et al., 2021; Li & Hoffman, 2023), intrinsic and extrinsic motivations that play a critical role in enhancing employee compliance behaviour, and perceived protection motivations (Kuppusamy et al., 2022; Ogbanufe et al., 2023; Sharma & Aparicio, 2022). In all these studies, researchers agreed that information security culture and awareness are the most influential factors in determining an individual's compliance with organisational policies.

Organisations with a good information security culture are believed to be less prone to security breaches, according to Alraja et al. (2023). Similarly, employee information security awareness contributes to a healthy security culture (Hong & Furnell, 2022). However, it is the responsibility of the organisation's management to enhance employee awareness regarding information security. In most cases, developing a sound culture has proven to be an effective strategy for improving ISP compliance behaviour among employees (Hong & Furnell, 2022). Therefore, it is crucial to evaluate the causes and solutions for non-compliance behaviour by employees. There is ample literature that discusses the reasons behind non-compliance or intent to violate security policies and the solutions to these problems. For example, studies have shown that some employees view information security as an external source of stress and do not feel personally responsible for maintaining security. This leads to security-related conflicts and non-compliance behaviour (Bayona-Oré & Ochoa, 2023; Sulaiman et al., 2022). Heavy security requirements can unintentionally cause employees to violate information security policies due to security-related stress (Aggarwal & Dhurkari, 2023; Chen et al., 2022). In some cases, employees violate organisational policies due to perceived injustice from top management. Corporate injustice causes employees to lose motivation and elicit negative emotions, resulting in non-compliance behaviour (Chen et al., 2022). Researchers have proposed solutions for non-compliance behaviour using criminological theories such as social control theory (Palanisamy et al., 2023) and deterrence theory (Hengstler et al., 2023). In addition, solutions involving deterrence or punishments for insiders have also been proposed in the past (Trang & Nastjuk, 2021; Wang et al., 2022). However, as highlighted by Wang et al. (2022), punishments and deterrence are not always the appropriate way to address non-compliance.

Previously, researchers have presented several ways employees can be encouraged to comply with the organisational ISP. This includes studies by Alexandrou and Chen (2019) and Iriqat et al. (2019), who advocate that employees should evaluate their risk perception concerning non-compliance with the ISP. In that sense, the authors argued that by understanding the risks associated with non-compliance, the employees will be compelled to take the necessary actions to comply with such policy. They can only judge the expected outcomes of such compliance by complying with the ISP (Bayona-Oré & Ochoa, 2023). In addition, employees must also have a sense of self-efficacy to handle compliance with ISP effectively (Hong & Furnell, 2022). Meanwhile, Palanisamy et al. (2023) stated that employees must be conscious of the need to comply with the ISP put forth by their organisation. Only through such action will the employees be less tempted to embark on activities that could lead them to become non-compliant with the ISP. This includes sharing passwords, USB drives and file sharing. Separately, Sulaiman et al. (2022) stated that employees who have the intention to comply with the ISP but are yet to be in the stage of full compliance must plan a series of actions to achieve the stage, and they also must have the plan to cope with the challenges that may arise resulting from ISP compliance. This is supported by Kang et al. (2023), who stated that while employees must plan for their actions and cope with ISP compliance, they must also be able to comply with such requirements. This can be a difficult task for new employees because they may not have the necessary knowledge to plan the required actions and cope with the requirements (Kang et al., 2023).

Employees' compliance with the ISP can only be achieved if they take action to initiate and maintain the process or activity. According to Angraini et al. (2021), this is the most challenging part, particularly when maintaining compliance. This is due to constant changes in information security threats, which require employees to stay informed of policy changes to keep critical and confidential information safe. However, if accidental non-compliance occurs and the organisation's data is compromised, Ali et al. (2021) suggested that employees must have the self-efficacy attributes to recover from such a lapse so that similar non-compliance is less likely to occur. Ali et al. (2021) further stated that ISP compliance with such self-efficacy attributes may only be sustainable over the long term. Various researchers have proposed solutions for non-compliance behaviour among employees and recommended ways to encourage compliance. However, the researchers still need to provide a comprehensive process that combines all the causes of non-compliance and solutions that promote compliance behaviour. Based on the above arguments, this article proposes a conceptual model that has all the elements put forth by the above researchers. Through the proposed conceptual model, organisations can plan and take systematic processes that enable their employees to take action to comply with ISP and subsequently sustain such compliance

3. Proposed Model to Promote Information Security Policy Compliance Behaviour

The model proposed in this paper is an adaptation of the Health Action Process Approach (HAPA) Model. Ralf Schwarzer introduced it in the late 1990s as a psychological model to explain and predict changes in health behaviour (Martin et al., 2020). Essentially, the HAPA model combines the elements of the Theory of Planned Behavior (TPB), Bandura's Social Cognitive Theory (SCT), and the Transtheoretical Model (TTM) (Martin et al., 2020). In principle, the model suggests that a person's intention to perform a specific behaviour is influenced by their perception of risk, expectations about outcomes, and self-efficacy, emphasising the importance of motivation and volition in health behaviour change (Martin et al., 2020). The model has been widely used in research involving health psychology and behaviour change to understand better the factors influencing behaviour change and to design interventions that effectively promote health behaviours (van Nes et al., 2023). It acknowledges that people may have good intentions (motivation) but also need the skills and strategies (volition) to translate those intentions into sustained behaviour change.

The HAPA model has been applied to various health-related behaviours, including smoking cessation, physical activity promotion, healthy eating, and medication adherence. For this reason, the model was chosen as the theoretical framework in the proposed model because it has all the elements the organisations can utilise to change employees' behaviour to promote ISP compliance among individuals. Figure 1 illustrates the model presented in this article, which has essentially been derived from the original HAPA model. The key processes have been changed to tailor the methods peculiar to the behavioural changes needed from ISP compliance. Like the original model, the proposed model also consists of motivational and volitional phases.

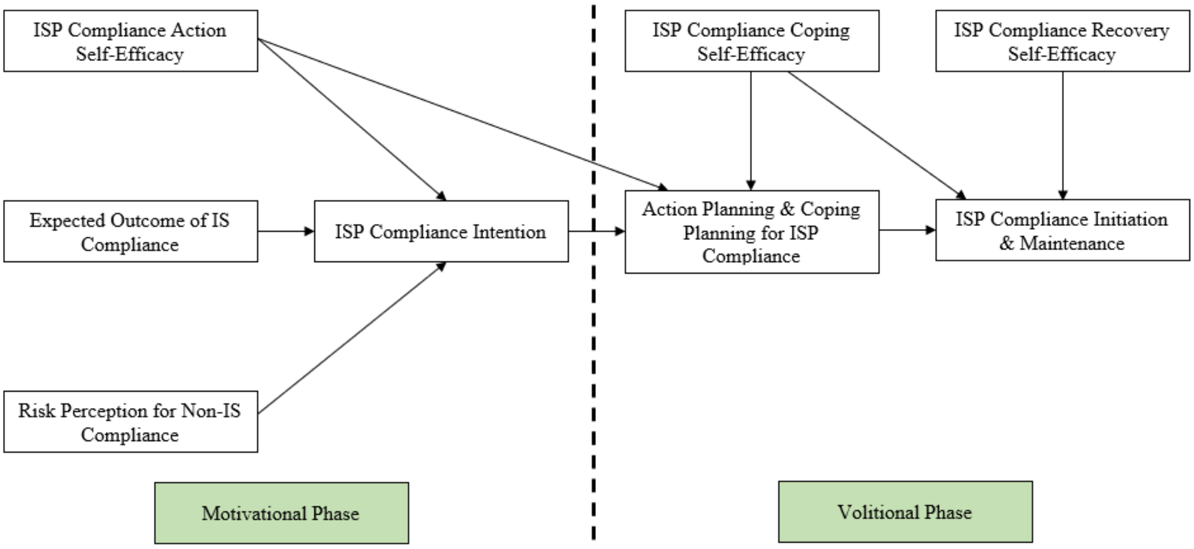
ISP Compliance Action Self-Efficacy
Expected Outcome of IS Compliance
ISP Compliance Intention
Risk Perception for Non-IS Compliance
ISP Compliance Coping Self-Efficacy
ISP Compliance Recovery Self-Efficacy
Action Planning & Coping Planning for ISP Compliance
ISP Compliance Initiation & Maintenance
Motivational Phase
Volitional Phase

Figure 1: The Proposed Model

Based on the proposed conceptual model, the critical processes needed to achieve ISP compliance can be described as follows;

3.1 Motivational Phase

The first element in the model is a risk perception. Risk perception refers to an individual's vulnerability to a potential threat (Marshall & Curry, 2022). When assessing the employees for ISP compliance, several researchers such as Alanazi et al. (2020), Angraini et al. (2019), and Chen and Tyran (2023) recommend that risk assessment be conducted first to establish the current state and readiness of employees to comply with ISP requirements. In this sense, Chen and Tyran (2023) suggest that risk assessment analysis should include assessing potential threats such as data breaches, financial losses, and reputational damage. While assessing risk perceptions may seem straightforward, according to Alanazi et al. (2020), the process can be complicated as contextual factors influence it. For instance, as looming threats of non-compliance of ISPs become more immediate, risk perceptions tend to become more pessimistic (Alanazi et al., 2020). In addition, risk perceptions also tend to be higher when an information security threat is seen as exceptionally high (Angraini et al., 2019). It is worth noting that contextual factors related to emotions can significantly impact how people perceive risks. In such instances, individuals who experience anger, a high certainty and control emotion tend to have more positive perceptions of risk. In contrast, the opposite will occur for those who experience fear, a low certainty and control emotion as they tend to have more negative risk perceptions (Schwarzer & Hamilton, 2020). This general effect can also influence the formation of risk perceptions. For instance, distressed individuals may perceive risks more severely, and those who are depressed may be more likely to adjust their risk perceptions in response to compliance measures than those who are not depressed. As such, these tendencies may significantly affect forming risk perceptions in the overall context of ISP compliance requirements (Chen & Tyran, 2023). As such, conducting the risk assessment correctly is very important if the organisation is to ensure ISP compliance among its employees as it will help the organisation to gauge the current state of ISP compliance in the organisations and, in addition, help to raise initial awareness among the employees about the significance of information security (Sulaiman et al., 2022). Organisations can communicate the potential risks and consequences of non-compliance with ISPs by having a natural readiness towards ISP compliance.

The next element in the model is the outcome expectancies. Outcome expectancies are anticipated consequences (positive or negative) resulting from engaging in a specific behaviour (van Nes et al., 2022). Hong and Furnell (2022) provide several examples of outcome expectancies for complying and non-complying with the organisation's ISP requirement. Continuing to maintain a good reputation, having highly secure sensitive data, and having no financial losses are the expected outcomes that employees can expect from ISP compliance. In contrast, the opposite is expected for non-ISP compliance. However, as highlighted by Hong and Furnell (2022), one of the main challenges of instilling ISP compliance among employees is the continued negative outcome expectancies due to employees' behaviour. As such, the authors suggested that to overcome this barrier of negative outcome expectancies; organisations must implement the necessary steps to address it effectively. To that effect, Hong and Furnell (2022) encourage organisations to provide employees with clear information about the benefits of information security compliance with activities that promote behaviour change, leading to them being able to protect sensitive data, thereby, in return, leading to them able to maintain complying with the ISP in general. In addition, organisations also need to address any misconceptions or perceived barriers to compliance, such as concerns about productivity loss or inconvenience. Typical activities at the workplace, such as sharing the USB, weak passwords, password sharing and lack of anti-virus protection, will be eliminated once the organisation manages to change the direction of outcome expectancies from negative to positive.

ISP compliance can only be achieved if a person firmly believes they have the knowledge and ability to comply with the organisation's ISP (Chen et al., 2022). This perception is referred to as task self-efficacy. In that respect, task self-efficacy refers to a person's confidence in controlling their behaviour, influencing their environment, and staying motivated to comply with the ISP continuously (Chen et al., 2022). It should be noted that task self-efficacy will also affect an individual’s effort expenditure, choice of activities and persistence. This is because individuals with low task self-efficacy regarding ISP compliance may avoid it, while those who feel capable comply eagerly. As such, individuals who face obstacles to complying with ISP but feel they have the productivity for such compliance ought to work harder to achieve the goal, and it will last longer than those who doubt their abilities (Chiniah & Ghannoo, 2023). According to Chiniah and Ghannoo (2023), individuals acquire information about their task self-efficacy from their performance, observation, effect of persuasion, and physiology. The authors emphasise that one's ability to manage information security can be used to evaluate self-efficacy in complying with ISP. As such, generally, successes in managing information security will raise efficacy in ISP compliance, and failures will lower it.

Based on their risk perception, outcome evaluation and task self-efficacy, individuals will decide whether or not to proceed with ISP compliance, i.e., it will form their intention to comply or vice-versa. They move to the next phase if they perceive the benefits outweigh the costs and are motivated strongly. According to Marshall and Curry (2022), behavioural intention is an affirmed likelihood to engage in certain behaviours. Employees would intend to comply with ISP if they perceived that the risk associated with ISP non-compliance is high, which led them to do whatever is necessary to ensure they remain in compliance with ISP, understand that the adverse expected outcomes for non-compliance with ISP, and finally, they believe they have the required resources to comply with ISP. In contrast, the opposite may likely occur, i.e., intention to not comply with ISP when the above three conditions still need to be met. Understanding the employees' intention to comply with ISP is essential for successful ISP implementation because, in the absence of measures of actual behaviour, Chen et al. (2022) viewed individual behavioural intentions to comply with ISP be used as indicators that signal whether employees will make an effort to comply with ISP or vice-versa. As ISP compliance among the employees in many organisations is still very much a challenge, Chen et al. (2022) advocate that organisations should, therefore, continue to encourage employees to have strong desires to comply with ISP by conducting activities that have a positive impact on risk perception, outcomes expectations and task self-efficacy.

3.2 Volitional Phase

Action planning is crucial in turning intentions into actions during the volitional phase. It involves creating a detailed plan that specifies when, where, and how to carry out one's intentions (Schwarzer & Hamilton, 2020). By engaging in action planning, an individual can form a mental representation of an appropriate situation and the necessary behavioural actions to achieve their goals. Through action planning, individuals can increase the effectiveness of behavioural change. In this sense, action planning will undoubtedly involve a specific process that comprises detailed planning of the exact steps that must be taken to achieve a particular goal (Schwarzer & Hamilton, 2020). In other words, it involves a person specifying precisely what they will do in the immediate future to work towards their goal. In the case of ISP compliance, the organisation's goal is to eliminate the activities that contribute towards non-ISP compliance, such as the ones mentioned earlier. To help with this, organisations must have a set of precedents to assist employees in setting an action plan that discourages them from performing activities that violate ISP compliance (Sulaiman et al., 2022). In other words, organisations can assist employees in setting specific, achievable goals related to information security compliance, for example, by providing templates or checklists for employees to create personalised action plans for complying with security policies (Sulaiman et al., 2022).

The HAPA Model emphasises the importance of working together with action and coping planning. Coping planning involves anticipating potential barriers or obstacles preventing someone from implementing their intended behaviour (Schwarzer & Hamilton, 2020). It also involves creating a detailed plan for overcoming those challenges. This plan typically includes an if-then statement, where individuals anticipate potential barriers and plan how to cope with those difficulties to execute their desired behaviour (van Nes et al., 2022). This is particularly important in ISP compliance, where the threat landscape constantly evolves and requires employees to adapt constantly (Naik, 2022). Coping planning helps individuals create a mental link between potential barriers and alternative plans to continue their intended behaviour

(Trang & Nastjuk, 2021). When intending to comply with ISP, employees should develop one or more strategies to cope with potential challenges. Similarly, when individuals find themselves in a situation of non-ISP compliance, they should have generated possible solutions to stop non-compliance while still achieving their intended behaviour (Palanisamy et al., 2023).

Effective action and coping planning require a person to evaluate their level of coping self-efficacy. It refers to the optimistic belief in one's ability to face obstacles that arise from a series of planned actions and manage them (van Nes et al., 2022) and having sufficient levels of coping self-efficacy will help one’s judgment about their ability to cope effectively with challenges that may exist during the planning of actions and coping strategies to comply with ISP (Liu et al., 2020). In the example of ISP compliance, one may have put in place the plan of action and coping strategies to comply with ISP but was unable to implement it due to insufficient coping self-efficacy. In other words, the person may be unable to handle the plans as they may not have the proper knowledge and skills to handle the requirements needed to run the ISP. In that sense, part of the ISP may require the person to take the phishing e-mails; however, due to a lack of knowledge of how to identify the phishing e-mails, the individual may be unable to comply with the ISP. This can occur, even though before receiving the phishing e-mails, the person may have the required action and coping planning to deal with such e-mails (Kang et al., 2023). As such, a lack of coping self-efficacy can be a stumbling block towards successfully implementing ISP compliance. Although task self-efficacy is generally essential to ISP compliance, Kang et al. (2023) highlighted that coping self-efficacy plays a unique role in maintaining ISP compliance behaviour. The authors further emphasise that when a person faces potentially non-ISP compliance, having a sense that they can cope with the threat is likely more helpful than having a sense that they can achieve goals.

Once an employee has put the actions and coping plans in place and understands their level of coping self-efficacy, they can initiate the action that led to ISP compliance and subsequently put the maintenance activities in place to maintain such behaviour. In the HAPA Model, initiation actions shift from conscious motivational processes to impulse-driven mechanisms cued by the context (Martin et al., 2020). As this is the final stage of the model, any regulation of actions would become detached from motivational or volitional control (Martin et al., 2020). At this stage, individual habits will also play a role in fostering the actions that will contribute towards habitual behaviour that is triggered spontaneously, and any alternative behavioural responses become less cognitively accessible (Martin et al., 2020). At this stage, positive behaviour promoting ISP compliance can be achieved by implementing planned actions, such as using secure passwords, encrypting data, and following secure communication protocols. Simultaneously, the individuals must have the sense to monitor and track compliance behaviours to identify areas where additional support or training may be needed (Choi et al., 2018). As such, it is essential to maintain the desired behaviour when complying with the ISP regulations. The maintenance aspect is crucial because the constantly changing environmental context influences one's behaviour related to ISP compliance, whether consciously controlled or automatically and habitually. These influences can either support or hinder the maintenance of behaviour change (Angraini et al., 2021). Creating stable contexts can make it easier to sustain behaviours and habits, just as it does for initiating behaviour change. Regarding ISP compliance, organisations can maintain such behaviour by providing regular reminders, updates, and reinforcement of security policies to help employees maintain their commitment to compliance. As a result, if a particular behaviour becomes the dominant response across different contexts, it is likely to be maintained over time.

The final element in the model is recovery self-efficacy. While employees are expected to maintain the same level of compliance over time, incidents may occasionally lead to a lapse. Sufficient recovery self-efficacy will guide and support employees who may experience such incidents (Huang & Lin, 2023). Moreover, Huang and Lin (2023) reiterate that organisations should play a vital role in encouraging individuals to recommit compliance and apply coping strategies to recover from non-ISP compliance incidents. In this context, Huang and Lin (2023) argued that organisations can provide re-current or refresher training to return employees to the compliance stage. Due to the dynamic nature of information security compliance resulting from new emerging threats, the recovery self-efficacy stage could be one of the most critical stages in the model (Huang & Lin, 2023). This argument is further supported by Jeon et al. (2021) and Liu et al. (2020), who stated that organisations and employees should place greater importance on perceived self-efficacy to recover from a lapse than resistive self-efficacy. They argued that sufficient recovery self-efficacy is necessary for the employees' ability to sustain ISP compliance to be short-lived.

4. Practical Applications and Guidelines for Implementation

An organisation can apply the proposed model through a systematic process that aims to instil the behaviour that exhibits substantial and sustainable ISP compliance among its employees. This paper suggests the following activities be applied for such purpose;

i. The organisation could initiate the program for ISP compliance by conducting a series of assessments on the affected employees. The evaluation shall involve assessing their perception of the potential risks of non-compliance towards the ISP. The other review that is also required is the perception of their self-efficacy in complying with the ISP. Both assessments can be done through questionnaires distributed to them. Subsequently, organisations could conduct training on information security training and processes to comply with the ISP. These training programs can be made as part of employee training programs. In addition, organisations should also conduct information security awareness campaigns in which ISP compliance will be part of the campaigns.

ii. To consistently ensure that employees comply with ISP, organisations could regularly disseminate bulletins or any documentation that provides cues regarding information security issues and how the ISP can assist them with handling the problems. This can be achieved through bulletins or notices placed strategically where it is expected to attract people's attention. As the threats to information security are dynamic and change regularly, the emphasis should be on updating the bulletins or notices monthly. This strategy is essential as it will help create an environment where employees are provided with the latest issues and remove the perception that the organisation's approach to handling ISP compliance is seasonal.

iii. While employees may be continuously being provided with training and information that will enhance their knowledge to keep them updated with the latest techniques and processes needed to maintain proposition towards ISP compliance, organisations must make it clear to their employees that inadequate behavioural action to support such action should be discouraged. This behaviour includes complacency, which can lead them back to practising activities that contradict the ISP requirements. This can be achieved through continuous training programs and the information and cues provided at strategic places such as notice boards. This action will remind them to stay vigilant regarding the requirement, reducing the possibility of ISP compliance lapse.

iv. Finally, organisations must ensure that the ISP will remain relevant considering the dynamics of information security threats. This can be achieved by implementing the policy that the ISP must be updated regularly. Bayona-Oré and Ochoa (2023) recommended that the ISPs be re-visited and updated at least once a year. Through this process, employees will always be ready when faced with new challenges that may arise. The other aspect that organisations must consider is designing an ISP that is attractive to familiar readers; in other words, its contents and format must be able to make the employees understand them. One of the common obstacles to effective ISP implementation is the lack of understanding of the content among its end users. This is often primarily due to the language's complexity and format (Alraja et al., 2023). Therefore, organisations should avoid such circumstances by ensuring their ISP applies to all end users.

ISP compliance is achievable, provided organisations and employees play influential roles in achieving the objectives. Organisations can take cues from the above-suggested activities so that all the procedures laid down in the given conceptual model can be performed effectively and timely.

5. Future Research Opportunities Based on the Model

The proposed conceptual model can provide several opportunities for future research. While, in theory, the proposed model might be able to give valuable insights into what needs to be done to promote ISP compliance among employees in an organisation, the current authors are unable to determine whether all the processes listed in the model are genuinely a reflection of what needs to be done in actual scenario. As such, there is a need to test the model in an organisation to clearly understand the relationships between the variables in the model. This can be done using the quantitative research approach that collects the data using questionnaires. The other important consideration that was not included in the proposed conceptual model is the effect of individual past experiences concerning ISP compliance, their prior knowledge of information security and the differences in personality traits that, based on past studies, influence how individuals would perceive ISP compliance requirement (Alassaf & Alkhalifah, 2021; Hong & Furnell, 2022). Similarly, the organisation's size may also affect the level of ISP compliance, as indicated by a study by Angraini et al. (2021). According to the authors, one of the main reasons behind this circumstance is that more prominent organisations usually have the required resources to ensure compliance with ISP is done satisfactorily. Finally, future studies may use the experiment method to test the participants to gauge their actual response in a simulated scenario. By comparing the results of the experiment and the answers provided in the questionnaires, the researcher will be able to discover whether the answers provided in the questionnaires truly reflect their actual behaviour. This will help to confirm the previous study by Li and Hoffman (2023), who found that individual perceptions based on the answers given in the questionnaires are different than when the respondents are subjected to an experiment.

6. Conclusion

This paper proposes a model organisations can use to encourage employees to comply with information security policies (ISPs). The model is based on the Health Action Process Approach (HAPA) Model, which was chosen because organisations face constantly changing challenges regarding information security lapses. The proposed model consists of two phases: the motivational phase and the volitional phase. The motivational phase includes risk perception, the expected outcome, self-efficacy to take action, and the intention to comply with ISP. The second phase of the model focuses on action planning and coping planning, self-efficacy, initiation and maintenance, and self-efficacy to recover from non-compliance with ISP. By incorporating both phases, organisations can promote a culture of security awareness and responsible behaviour among employees. However, the current authors anticipate several limitations with the proposed model, including a need for explicitly considering non-conscious processes. People often act on emotional impulses, and social-cognitive approaches to behaviour change may be ineffective. Despite the limitations, the proposed model can still help organisations promote ISP compliance behaviour among their employees. Cumulative evidence suggests that shifting from static motivational and attitude variables to dynamic self-regulatory variables like coping planning, maintenance self-efficacy, and action control is a promising step towards better compliance with ISP. The model's strength is also rooted in its emphasis on mediating mechanisms involving several volitional constructs. Therefore, by applying the HAPA model to ISP compliance, organisations can create a structured approach that combines motivation and volition to foster a culture of security awareness and responsible behaviour among employees. As a result, this can improve information security and reduce the risks of data breaches and security incidents.

Acknowledgement
The authors would like to thank the School of Graduate Studies, Asia e University (AeU), for supporting the publication of this concept paper.

.

References

Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy non-compliance behaviour: A meta-analysis. *Computers and Security*, *124*. https://doi.org/10.1016/j.cose.2022.102991

Alanazi, S. T., Anbar, M., Ebad, S. A., Karuppayah, S., & Al-Ani, H. A. (2020). Theory-based model and prediction analysis of information security compliance behaviour in the Saudi healthcare sector. *Symmetry*, *12*(9). https://doi.org/10.3390/SYM12091544

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. In *IEEE Access* (Vol. 9). https://doi.org/10.1109/ACCESS.2021.3132574

Alexandrou, A., & Chen, L.-C. (2019). A security risk perception model for the adoption of mobile devices in the healthcare industry. *Security Journal*, *32*(4), 410–434. https://doi.org/10.1057/s41284-019-00170-0

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability*, *12*(20), 8576. https://doi.org/10.3390/su12208576

Ali, R. F., Dominic, P. D., Ali, S. E., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383. https://doi.org/10.3390/app11083383

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. In *Applied Sciences (Switzerland), 13*(9). https://doi.org/10.3390/app13095700

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers &amp; Security*, *129*, 103208. https://doi.org/10.1016/j.cose.2023.103208

Angraini, C., Alias, R. A., & Okfalisa, A. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

Bayona-Oré, S., & Ochoa, N. F. (2023). Information security policy compliance: Usefulness and ease of use. *Proceedings of Eighth International Congress on Information and*

Communication Technology, 413–419. https://doi.org/10.1007/978-981-99-3236-8_32

Bélanger, F., Maier, J., & Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. *Computers &amp; Security*, *116*, 102641. https://doi.org/10.1016/j.cose.2022.102641

Bolek, V., Romanová, A., & Korcek, F. (2023). The information security management systems in e-business. *Journal of Global Information Management*, *31*(1), 1–29. https://doi.org/http://dx.doi.org/10.4018/JGIM.316833

Brooks, R. R., Williams, K. J., & Lee, S.-Y. (2023). Personal and contextual predictors of information security policy compliance: Evidence from a low-fidelity simulation. *Journal of Business and Psychology*. https://doi.org/10.1007/s10869-023-09878-8

Butler, K. J., & Brown, I. (2023). COVID-19 pandemic-induced organisational cultural shifts and employee information security compliance behaviour: A South African case study. *Information and Computer Security*, *31*(2). https://doi.org/10.1108/ICS-09-2022-0152

Chen, H., Liu, M., & Lyu, T. (2022). Understanding employees' information security-related stress and policy compliance intention: The roles of information security fatigue and psychological capital. *Information & amp; Computer Security*, *30*(5), 751–770. https://doi.org/10.1108/ics-03-2022-0047

Chen, X., & Tyran, C. K. (2023). A framework for analysing and improving ISP compliance. *Journal of Computer Information Systems*, *63*(6), 1408–1423. https://doi.org/10.1080/08874417.2022.2161024

Cheng, Y., Mei, S., Zhong, W., & Gao, X. (2021). Managing consumer privacy risk: The effects of privacy breach insurance. *Electronic Commerce Research*, *23*(2), 807–841. https://doi.org/10.1007/s10660-021-09492-x

Chiniah, A., & Ghannoo, F. (2023). A multi-theory model to evaluate new factors influencing information security compliance. *International Journal of Security and Networks*, *18*(1). https://doi.org/10.1504/IJSN.2023.129949

Choi, Y., Yang, S. J., & Song, H. Y. (2018). Effects of the variables related to the health action process approach model on physical activity: A systematic literature review and meta-analysis. *Journal of Korean Academy of Community Health Nursing*, *29*(3), 359. https://doi.org/10.12799/jkachn.2018.29.3.359

Dong, T., Zhu, S., Oliveira, M., & Luo, X. (Robert). (2022). Making better IS security investment decisions: Discovering the cost of data breach announcements during the COVID-19 pandemic. *Industrial Management &amp; Data Systems*, *123*(2), 630–652. https://doi.org/10.1108/imds-06-2022-0376

He, J., & Sun, Y. (2022). Information security countermeasures for big data platforms based on cloud computing. *Mobile Information Systems*, *2022*, 1–11. https://doi.org/10.1155/2022/3981775

Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I., & Trang, S. (2023). Should I really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior. *Computers &amp; Security*, *133*, 103370. https://doi.org/10.1016/j.cose.2023.103370

Hengstler, S., Nickerson, R. C., & Trang, S. (2022). Towards a taxonomy of information security policy non-compliance behavior. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2022-January*. https://doi.org/10.24251/hicss.2022.588

Hong, Y., & Furnell, S. (2022). Motivating information security policy compliance: Insights from perceived organizational formalization. *Journal of Computer Information Systems*, *62*(1). https://doi.org/10.1080/08874417.2019.1683781

Huang, H.-H., & Lin, J.-W. (2023). Inconsistencies between information security policy compliance and shadow IT USAGE. *Journal of Computer Information Systems*, 1–11. https://doi.org/10.1080/08874417.2023.2234318

Iriqat, Y. M., Ahlan, A. R., & Molok, N. N. (2019). Information security policy perceived compliance among staff in Palestine universities: An empirical pilot study. *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*. https://doi.org/10.1109/jeeit.2019.8717438

Jeon, S., Son, I., & Han, J. (2020). Exploring the role of intrinsic motivation in ISSP compliance: Enterprise digital rights management system case. *Information Technology &amp; People*, *34*(2), 599–616. https://doi.org/10.1108/itp-05-2018-0256

Kang, P., Kang, J., & Monsen, K. A. (2023). Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. *CIN - Computers Informatics Nursing*, *41*(8). https://doi.org/10.1097/CIN.0000000000000981

Kuppusamy, P., Samy, G. N., Maarop, N., Shanmugam, B., & Perumal, S. (2022). Information security policy compliance behaviour models, theories, and influencing factors: A systematic literature review. *The Journal of Theoretical and Applied Information Technology*, *100*(5).

Lee, D., Lallie, H. S., & Michaelides, N. (2023). The impact of an employee's psychological contract breach on compliance with information security policies: Intrinsic and extrinsic motivation. *Cognition, Technology &amp; Work*, *25*(2–3), 273–289. https://doi.org/10.1007/s10111-023-00727-5

Li, Y. J., & Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment. *Journal of Economic Behavior &amp; Organization*, *212*, 138–159. https://doi.org/10.1016/j.jebo.2023.05.033

Liu, C., Wang, N., & Liang, H. (2020). Motivating information security policy compliance: The critical role of supervisor-subordinate Guanxi and organizational commitment. *International Journal of Information Management*, *54*, 102152. https://doi.org/10.1016/j.ijinfomgt.2020.102152

Marshall, B., Curry, M., Crossler, R. E., & Correia, J. (2021). Machine learning and survey-based predictors of Infosec Non-Compliance. *ACM Transactions on Management Information Systems*, *13*(2), 1–20. https://doi.org/10.1145/3466689

Martin, J. J., Snapp, E., & Ketcheson, L. (2020). Motivational theories. *Routledge Handbook of Adapted Physical Education*, 347–362. https://doi.org/10.4324/9780429052675-26

Naik, L. B. (2022). Cyber security challenges and its emerging trends on the latest technologies. *International Journal of Scientific Research in Engineering and Management*, *06*(06). https://doi.org/10.55041/ijsrem14488

Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2022). Information security culture concept towards information security compliance: A comparison between it and Non-IT Professionals. *International Journal of Integrated Engineering*, *14*(3). https://doi.org/10.30880/ijie.2022.14.03.017

Ogbanufe, O., Crossler, R. E., & Biros, D. (2023). The valued coexistence of protection motivation and stewardship in information security behaviors. *Computers &amp; Security*, *124*, 102960. https://doi.org/10.1016/j.cose.2022.102960

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2023). Employees' BYOD security policy compliance in the public sector. *Journal of Computer Information Systems*, *64*(1), 62–77. https://doi.org/10.1080/08874417.2023.2178038

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - A systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Ryutov, T. (2023). An empirical investigation of psychological factors affecting compliance with information security organizational policies. In *Cybersecurity for Decision Makers*. https://doi.org/10.1201/9781003319887_15

Schwarzer, R., & Hamilton, K. (2020). Changing behaviour using the Health Action Process Approach. *The Handbook of Behavior Change*, 89–103. https://doi.org/10.1017/9781108677318.007

Sharma, S., & Aparicio, E. (2022). Organizational and team culture as antecedents of protection motivation among its employees. *Computers &amp; Security*, *120*, 102774. https://doi.org/10.1016/j.cose.2022.102774

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber-information security compliance and violation behaviour in organisations: A systematic review. In *Social Sciences* (Vol. 11, Issue 9). https://doi.org/10.3390/socsci11090386

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers &amp; Security*, *104*, 102222. https://doi.org/10.1016/j.cose.2021.102222

Uddin Sharif, M. H., & Mohammed, M. A. (2022). A literature review of financial losses statistics for cybersecurity and future trends. *World Journal of Advanced Research and Reviews*, *15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

van Nes, K. A., van Loveren, C., Luteijn, M. F., & Slot, D. E. (2022). Health Action Process Approach in oral health behaviour: Target interventions, constructs and groups—a systematic review. *International Journal of Dental Hygiene*, *21*(1), 59–76. https://doi.org/10.1111/idh.12628

Wang, X., Wang, C., Yi, T., & Li, W. (2024). Understanding the deterrence effect of punishment for marine information security policies non-compliance. *Journal of Ocean Engineering and Science*, *9*(1), 9–12. https://doi.org/10.1016/j.joes.2022.06.001