湖南大学学报（自然科学版）
Journal of Hunan University (Natural Sciences)

第 49 卷 第 12 期
2022 年 12 月

Available online at http://jonuns.com/index.php/journal/index

Vol. 49 No. 12
December 2022

Open Access Article

https://doi.org/10.55463/issn.1674-2974.49.12.28

Identifying Factors of Non-Compliance, Compliance with Information Security Policy, and Behavior Change to Compliance: Literature Review

Ayman Hasan Asfoor[1], Hairoladenan Kasim[2], Aliza Binti Abdul Latif[2], Rina Azlin Razali[2], Zul-Azri Ibrahim[2], Abdelsalam Shanneb[1]

[1] Department of Information Technology, Faculty of Computer Science, Jubail Industrial College, KSA

[2] Department of Informatics, Faculty of Computer and Information Technology, Tanga Nasional Univesity, Selangor, Malaysia

Received: August 16, 2022 / Revised: October 17, 2022 / Accepted: November 10, 2022 / Published: December 30, 2022

Abstract: This paper aims to build a process model that converts employees' non-compliance into compliance. The authors evaluated articles that studied the association between information security behavior and information security policy compliance (ISPC). The authors used grounded theory in this comprehensive literature review. The idea helps researchers study issues in depth and breadth, using the five main approach steps (to define, search, select, analyze, and display). The ISPC analysis placed a greater emphasis on compliance than on non-compliance. Value conflicts, stress due to security issues, and neutralization cause the lack of compliance. This review identified 22 studies that met its criterion for inclusion. Compliance increased for both internal and external causes, as well as for protection. Social circle, management, and company culture motivate employees to be security-aware. Deterrence strategies, managerial practices, culture, and awareness of information security help staff adhere to the rules. Information security is jeopardized when employees do not value ISPC. ISPC studies usually distinguish compliance and non-compliance. The literature lacks a complete grasp of the elements that change employees' Non-compliance to compliance. We conducted a systematic literature review on information security behavior toward ISPC in various settings: research frameworks, research designs, and research methodologies throughout the last decade. This systematic review has implications for information security behavior. This research details a behavior-change technique. The conversion helps security professionals comprehend employee non-compliance and helps them comply. According to research, most security professionals develop information security policies generically, which leads to non-compliance. Most researchers agree that information security policies should be organization-specific. This study explored significant compliance/non-compliance characteristics to help design information security policies.

Keywords: information security policy, information security policy compliance, non-compliance, information security behavior, systematic literature review.

識別不合規因素、遵守信息安全政策和改變合規行為：文獻回顧

摘要：本文旨在構建一個將員工的不合規轉化為合規的流程模型。作者評估了研究信息安全行為與信息安全策略合規性之間關聯的文章。作者在這篇綜合文獻綜述中使用了紮根理論。這個想法幫助研究人員使用五個主要方法步驟（定義、搜索、選擇、分析和顯示）深入和廣度地研究問題。信息安全政策合規性分析更加強調合規性而非不合規性。價值衝突、安

全問題引起的壓力和中和導致缺乏合規性。該評價確定了22項符合其納入標準的研究。由於內部和外部原因以及保護，合規性有所提高。社交圈、管理和公司文化激勵員工具有安全意識。威懾策略、管理實踐、文化和信息安全意識有助於員工遵守規則。當員工不重視信息安全政策合規性時，信息安全就會受到威脅。信息安全政策合規性研究通常會區分依從性和不依從性。文獻缺乏對將員工的不合規轉變為合規的要素的完整把握。我們對過去十年中各種環境下針對信息安全政策合規性的信息安全行為進行了系統的文獻回顧：研究框架、研究設計和研究方法。該系統審查對信息安全行為有影響。這項研究詳細介紹了一種行為改變技術。這種轉換有助於安全專業人員理解員工的違規行為並幫助他們遵守規定。根據研究，大多數安全專業人員普遍制定信息安全策略，這導致不合規。大多數研究人員都同意信息安全策略應該是特定於組織的。本研究探索了重要的合規/不合規特徵，以幫助設計信息安全策略。

关键词：信息安全政策，信息安全政策合規性，不合規性，信息安全行為，系統文獻綜述。

1. Introduction

ISP offers a strategy for protecting information assets and technical knowledge to satisfy the organization's objectives [2]. The ISP secures the organization's information assets and technology by providing a procedure to achieve its goals. Managerial help during ISP installation is crucial.

Companies rely on technology to acquire, store and share data in a hyperconnected world. Such information is in danger of being accessed, disrupted, modified, corrupted, or destroyed by unauthorized parties. Information security secures important data from intruders.

Data breaches may threaten a company's revenue and reputation [3, 4]. 70% of incidents are caused by human irresponsibility, says study (intentional or unintentional). 43% of data breaches occur from employee behavior, according to research [5, 6]. Over 95% of information security incidents occur from employee negligence, according to the 2014 IBM cybersecurity intelligence index [7]. 58% of British company attacks are insider risks, says the study. 33% of these attacks arise from a company's inability to follow ISPs and legislation [8]. Most firms follow NIST's standards (NIST). NIST emphasizes ISP compliance as a key component of information security [9].

However, many firms are worried about implementing employee ISP regulations since they impact the enterprise's general well-being, as employees comprehend security requirements [10]. The human factor is the weakest link in information security, causing breaches.

Many end users are unaware of information management's importance and their firms' accompanying regulations and policies. Moreover, half of the employees admit to breaching their company's ISP [11]. When companies battle internal hazards and ways of inner breaches, organizational employees and researchers should study workers who deliberately breach (ISPs) [12, 13]. More than 75% of organizations surveyed estimate center security repair will cost less than $500,000, according to the "Insider Threat Study." 25% say it will cost more than $500,000, maybe millions [14].

2. Literature Review

Information Security Policy (ISP) describes using a company’s IT resources. Workers must follow the rules, procedures, and technological controls [13]. They may protect an organization’s data [15]. Non-compliance with these standards is widespread. According to a study by Intel, 43% of data breaches are due to violations of IT policy by employees [16]. ENISA reports that 27% of data breaches are due to human error [17]. This is up from 58% last year [18].

Numerous studies have evaluated information security compliance/non-compliance [19, 20]. Behavioral theories affect information security [21, 22]. Another category of study develops composite information security compliance frameworks [23]. Many research created taxonomies for information security behavior [24, 25]. Compliance and non-compliance affect an organization’s information security directly or indirectly. The compliance enhancement study focuses on approaches and practices that may assist employees in acquiring a more positive attitude toward corporate security requirements [13, 26]. Research on Non-compliance provides measures for decreasing harmful behavior [22, 27, 28]. We incorporated studies on enhancing compliance and preventing Non-compliance in

information security policy assessments, ISS texts, and debates.

2.1. Compliance and ISB with ISP

Information security behavior has psychological aspects. Most research conducted to investigate information security behavior relied on psychological theories. These theories included the "protective motive theory" [29], the "planned behavior theory" [30], and the "reasoned action theory" [31]. Information security behavioral research focuses on policy compliance and Non-compliance in organizations. Many scientists helped the ISPC [13, 32]. Researchers who recognized compliance as a behavioral problem said that numerous variables might help ISPs comply with information security rules [32].

Global cultural behavior affects ISB and ISP compliance [33]. Researchers have long argued that intrinsic (self-esteem and achievements) and extrinsic (incentives and recognition) reasons improve employee compliance [34].

Several studies on the influence of information security protection motivations show that a person's compliance with organization norms relies on their perceived protection reasons [35]. The assumption that IS knowledge is the most critical component stems from research suggesting that companies with a robust IS culture are less likely to have data breaches. Information security training adds to a strong workplace culture [36].

Management must increase staff information security expertise. When an organization's leadership develops successful techniques for enhancing ISPC, staff knowledge increases [37].

2.2. Non-Compliance and ISB with ISP

Much literature exists on the causes and solutions for Non-compliance. Non-compliance with security requirements has numerous reasons and explanations. Information security may be stressful for employees, according to research. Security-related conflicts lead to Non-compliance since workers do not feel accountable for security [32]. High-security requirements stress staff, breaking ISP [38]. According to research, most employees disobey corporate regulations due to unequal treatment at the top.

Organizational injustice diminishes employee motivation and stress, leading to non-compliance [38]. Research shows that workers have several excuses for inappropriate behavior. "Neutralization," said Gresham Sykes [39]. They used seven deterrents to prevent criminal behavior.

Most research suggested criminological theories as cures for non-compliant behavior [40]. Some research suggested insider penalties or deterrents [41]. Some experts say that punishment and deterrence are not always practicable to minimize non-compliance [42]. According to a longitudinal study, better employee socialization and protective acts may minimize non-compliance [13].

Several scholars have presented solutions for employee non-compliance. None of the studies offered a universal framework for characterizing non-compliance explanations and treatments. If researchers evaluate the literature on Non-compliance with compliance behavior, they will have a realistic schedule.

3. Methodology

This literature review used SLR. An SLR examines the existing literature to discover, appraise, and synthesize research, academic, and practitioner outcomes. Fig. 1 shows the five processes of a literature review (define, search, pick, analyze, and present).

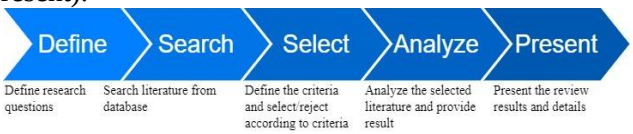

Fig. 1 Methodology for conducting a literature review

A review method and a list of possible follow-ups research questions have been drafted to get started [1].

1. What theories, research methods, and annual publications are used in my study on non-compliance and compliance issues?
2. What behavioral factors have been identified as significant predictors of Non-compliance with information security policies in research?
3. What behavioral characteristics have research revealed to influence information security policy compliance?

Initial searches were limited to computer science, social sciences, information systems, and security journals. The search procedure includes picking a database, specifying words, identifying strings, and executing the algorithm. Table 1 summarizes the study aims that led to Query and keyword creation.

Table 1 Keywords and queries

Keywords	Search
ISB	"Information security behavior and "Information security policy" OR "security policies" OR "policy compliance"
ISPC	"Organizational ICT" OR "IT" and "Information security behavioral compliance"
ISP non-compliance	"Information security behavior" and "Information security policy non-compliance" OR "violations"
ISP violations	"Volitional security behavior or "Information security policy violation" OR "deviance" OR

The database was chosen for its data volume and study area. Digital databases consulted: Using key phrases and keyword combinations improve search results.

The following included articles were studied.

1. Papers in English;

2. Articles focused on information security and policy compliance;
3. Peer-reviewed publication published in 2016–2021.

Articles were rejected if any of the following were true:

1. The articles focused on security behavior, not policy compliance;
2. Non-security-policy-related commentary;
3. Non-compliance;
4. Residential users;
5. Management/awareness/culture articles without behavioral concerns;
6. Articles on cyber security, not information security.
7. Articles that exclude supporting evidence or research methods-based evidence.

Following is the selection of 350 articles; the criteria for including and excluding subjects from the study are presented. Thirty-three articles were removed because they were duplicated, 100 articles were eliminated after the title and abstract screen, and 195 articles were removed after the text screen.

Twenty-two papers were reviewed and considered for inclusion (qualitative, quantitative, and literature review).

4. Results and Discussion

According to this SLR's RQ1, theories that are used in non-compliance and compliance issues, the annual number of publications used in the research, and research techniques

The most commonly used theories of non-compliance are included in Table 2.

Table 2 Most commonly used theories of non-compliance

No.	Theory name
1	Theory of Neutralization (TN)
2	General Deterrence Theory (GDT)
3	Protection Motivation Theory (PMT)
4	Theory of planned behavior (TPB)
5	Rational Choice Theory (RCT)

The most commonly used theories of compliance are included in Table 3.

Table 3 Most commonly used theories of compliance

No.	Theory name
1	Theory of Planned Behavior (TPB)
2	Protection Motivation Theory (PMT)
3	Social Cognitive Theory (SCT)
4	Social Bond Theory (SBT)
5	Social Control Theory (SCT)
6	Rational Choice Theory (RCT)
7	Health Belief Model (HBM)
8	Social Exchange Theory (SET)

The number of articles that are published annually is shown in Fig. 2.

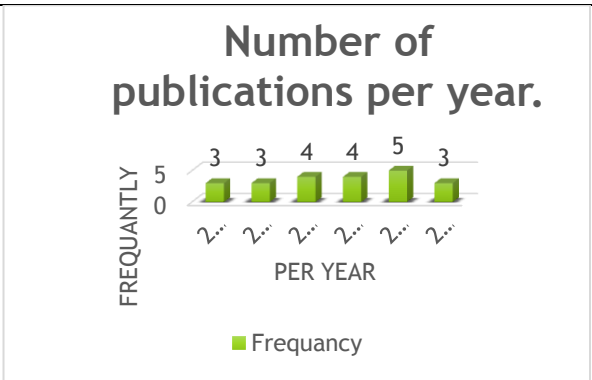

Fig. 2 Articles that are published annually

4.1. Non-Compliance Behavior Is Being Investigated

This SLR's RQ2 reveals the behavioral drivers of information security policy non-compliance. Non-compliance with information security standards can be because of neutralization, security-related stress, value conflicts, and deterrence techniques.

4.1.1. Neutralization, Security-Related Stress (SRS), and Non-Compliance

Research suggests that Security Education, Training, and Awareness (SETA) programs and ISP rules should be easy for personnel to comprehend. Factors of ISP non-compliance were explored [43].

Job impediment, system anxiety, and peer non-compliance impact non-compliance with an ISP. Neutralization and deterrence moderate workers' computer-abusive behavior; [44] analyzed 968 workers for distributive and procedural organizational unfairness (i.e., inequity in compensation and processes). Organizational and individual efforts (such as training and security visibility) are the model's two main components (i.e., peer non-compliance, work impediment, and security system anxiety).

Workers are more likely to participate in abusive behavior if they believe a method is unfair than if they believe that incentives and compensations are unfair. Moreover, workers justify their abusive behavior using neutralization tactics (i.e., denial of the victim, metaphor of the ledger).

Workers' expectations of punishment affect ISP abuse. A framework for ISPC was constructed using 11 topics from the literature [45]. A multilevel research technique was used to construct and evaluate a model for three ISP violation scenarios. Although deterrents, incentives, and social characteristics were not significant predictors of ISP violations, neutralization was.

Reference [38] presents an additional examination of daily SRS implications on ISP compliance. The research says SRS may cause worker unhappiness and fatigue. Employees neutralize tension and fatigue (justification of negative behaviour). Researchers employed ESM (within-individual measures) to examine daily behavior.

Anecdotal data reveal that SRS favorably affects

workers' emotional feelings (such as discontent and weariness) and behavioral desire to comply with the ISP. [46] studied IT professionals' technostress. All technostress-causing elements (overburdening and sophisticated systems) were significant workplace predictors. According to their research, technostress has been linked to anxiety and ISP violation. The theory used, factors, research methodology, sample sizes, and conclusions from various studies analyzing neutralization and non-compliance experiments are in the table in Appendix A1.

4.1.2. Value Conflicts and Non-Compliance

Employees often disobey ISP regulations due to value conflicts with ISP. [28] claimed non-compliant conduct is (i. e., task completion is above ISP compliance). This study found that Non-compliance with ISP is motivated by self-justification and sunk cost (i.e., a refusal to accept loss). Researchers analyzed Brunei's seven focus groups, highlighting the value of knowledge in their study [32]. After conducting 55 in-depth, semi-structured interviews with IT executives and experts, a value-driven information security compliance theory was developed. Research implies that the value of information (i. e., how important it is) influences users' compliance with their ISP

The research investigated an ISP's PMT and IT vision conflict [35]; it studied IT vision conflict mediation's impact on PMT components and ISP non-compliance attitudes. IT vision conflicts occur when IT is separate from the rest of the enterprise, causing a perception gap. Because only the perceived severity of the IT vision conflict is altered, the PMT components majorly affect ISP non-compliance.

According to [47], employees spend less time on information security. Procrastination and mental detachment are ways employees evade security tasks (i.e., denial of the necessity of security chores). In workers' eyes, security issues are external (called "perceived externalities"), and their commercial operations are more important than their security obligations (triage). Factors, research methodology, sample sizes, and conclusions from value conflicts and non-compliance are in the table in Appendix A2**.**

4.1.3. Deterrence and Non-Compliance

A previous study suggests that strong social links, peer pressure, and proper controls (i. e., the impression of severity and certainty of penalty) affect employee ISP violation behavior. Safety was evaluated by [48]. Using this paradigm, they defined safe workplace information security.

An employee's information security behaviour can be enhanced if he/she understands the negative repercussions, the seriousness of the threat, and the fear of being found. Another aspect that affects an employee's safe information security behavior is job satisfaction with coworkers. Personality characteristics in behavioral security were postulated by [49]. For the first time, general deterrence was employed to test stability and adaptability. Emotional sturdiness, agreeableness, and conscientiousness define stability and plasticity.

According to the research findings, employees with dominant stability qualities had a lower risk of violating the ISP, whereas employees with high levels of plasticity traits had a higher risk. [27] studied the influence of penalties on information security behavior attitudes. They argue that section threats can boost staff attitudes. Threatening penalties can also alter an employee's attitude toward ISP compliance, which is impacted by the employee's past punishment experience.

[40] found ISP behavioral resistance. According to the authors, punishments and moral standards minimize ISP compliance resistance. One hundred thirty-nine employees from 10 organizations examined the norms-based research model and deterrent (penalty severity and detection certainty).

Deterrence affects norms, which influence ISP resistance, says the research. Meta-analysis of deterrence theory [22].

The meta-major study investigated policy compliance deterrence, cultural impacts, and behavior assessment methods. Thirty-five studies from 2003-2018 examined deterrence theory and ISP compliance. Except for severe punishments, deterrence theory constructs influence compliance. Research methodology, sample sizes, and conclusions from Deterrence and Non-compliance are in the table in Appendix A3.

4.1.4. Reactance, Justice, and Non-Compliance

A negative (i.e., unequal) justice policy occurs when a dispute resolution is unjust, or justice policies are non-distributive, such as when workers feel unfairly rewarded relative to peers of equivalent rank or when incentives are incommensurate with job outputs [51].

According to [52], examining employee IS misuse is key to strengthening corporate information security. According to the study, the perception of strict scrutiny drove employees to abuse IS. This table summarizes studies on these themes. The theory, factors, research technique, sample sizes, and conclusions from several studies studying reactance, justice, and Non-compliance are in the table in Appendix A4.

4.2. Analysis of Compliance Behavior

Here we address the RQ3 of this SLR (What behavioral variables have affected information security policy compliance?). This section evaluated studies on factors related to compliance with information security policies.

In this part, we looked at the research findings on reasons for protection, security awareness, protection

motivations, security culture, awareness behavior compliance, social behavior, and actual behavior with information security requirements.

4.2.1. Protection Motivation Behavior and Compliance

A person's motivation affects how they adjust and maintain information security. Reference found a disconnect between early security adaptation and protective conduct [35]. The PMT-based model suggested and tested with 253 end-users in this study indicated that self-efficacy, perceived threat intensity, and perceived threat susceptibility affect employees' continuance of protective activities, but changes in security policy or procedures made continuation difficult. Hope, optimism, self-efficacy, and resilience were examined in [53] that shows how psychological capital affects employees' risk aversion. Although users perform many security-related behaviors in response to threats, most studies focus on a particular danger or activity.

A study examined IT workers' attitudes and practices toward data protection [54]. This report contends that most previous InfoSec studies entirely ignored IT employees of their target audience of business executives. Prospect theory, deterrence theory, and rational action inform the proposed study framework. Only three of ten hypotheses were supported; therefore, the results were exciting and unexpected. Self-efficacy and perceived impact influence IT professionals' security behavior intentions.

Moral intensity is a multifaceted phenomenon, and researchers in [35] studied its implications on insiders' protection behavior alongside organizational criticality. This was a quantitative study with 216 college staff members and hypothetical settings. Researchers created four scenarios, two with high-criticality protection measures and two with low-criticality.

The findings showed that moral intensity parameters influence moral beliefs and change with organizational criticality. Reference describes a multi-theory approach to evaluating ISPC attitudes and behavior in higher education [16].

Compliance was evaluated using PMT, GDT, TPB, and OT. 206 higher education workers answered correctly. This study indicated that PMT best predicts ISPC in higher education (perceived vulnerability, response efficacy, and response cost). Social punishments, top-down management, and peer pressure are unimportant. The table summarizes research methods, sample size, and conclusions on protection motive and compliance are in the table in Appendix B1.

4.2.2. Security Culture, Awareness Behavior, and Compliance

Reference [55] focuses on ISP early compliance. They suggested that early ISP conformity is better than late or non-conformance. Five hundred thirty-five employees' intentions and attitudes were examined for early ISP compliance using a TPB-based study paradigm. The results demonstrated that awareness positively affects attitude, and attitude impacts early conformity intentions, which later become early ISP conformity.

The reference [20] conducted a thorough literature analysis and identified ISP compliance competencies (knowledge and skills). These researchers suggested that personnel must be competent to comply with ISP. The researchers looked at 32 articles and eight international competence frameworks in this review. Three dimensions (attitude, knowledge, skills) and 11 ISP competency elements were discovered. In this study, an ISP compliance competency model was provided and compared with professional competency frameworks. This study found a mismatch between the literature and professional frameworks. The data showed that most behavioral theories imply ISP compliance requires specific competencies, but professional frameworks cannot present them. The table summarizes the research methods, sample size, and conclusions on security culture, awareness behavior, and compliance in table in Appendix B2.

4.2.3. Social Behavior and Compliance

Information security is multidimensional, but businesses tend to focus on technological solutions (i.e., technical and behavioral) [56], such as establishing a phony online repository and generating an engine for cyber deception.

The reference [57] provided a paradigm for improving organizational behavioral information security based on probabilistic logic graphs. ISP security is a behavioral problem with few technical answers. ISP compliance requires administrative controls (security awareness through social methods, top management support for social behavior).

4.2.4. Actual Behavior and Compliance

TPB, General deterrence theory (GDT) (i.e., severity and certainty), and situational crime prevention theory (SCPT)-based frameworks were provided in [58] to reduce insiders' information security misbehavior.

A total of 444 employees from various organizations participated in the research for this framework. All GDT and Situational crime prevention theory (SCPT) constructs influence employees' negative attitudes about misbehavior, except for lowering provocations and removing excuses; furthermore, all TPB concepts influence employees' real ISB.

5. Conclusion

The main findings of this study provide a blueprint for a thorough behavior modification strategy. The change behavior method assists security practitioners in

identifying employee non-compliance and assisting them in becoming compliant with security regulations. According to a previous study, most security professionals create ISP generic, which leads to non-compliance [35]. Simultaneously, most studies agree that information security policy should be tailored to the organization's requirements [59, 60]. This research covered all important compliance/non-compliance variables to assist practitioners in creating customized information security policies.

The literature research found that workers compromise information security principles while adhering to job deadlines and IT vision. Our study found that experts must address all sorts of disputes while creating information security policies. Employees also fail to comply because of security-related stress. Complicated information security standards lead to anxious employees [38].

This literature study found that practitioners must consider complexity while developing or implementing security policies**.** Security professionals must consider both internal and extrinsic factors. To encourage ISPC, practitioners should urge management to reward the most compliant staff. This review also demonstrated that intrinsic/extrinsic and protective incentives boost social behavior. According to multiple studies, such as [40] and [61], better employee social bonding improve ISPC. Security officials must use this valuable data to improve compliance. For example, organizations should seek out influential individuals who influence employee attitudes toward ISPC.

This research examined the ISB literature concerning ISPC. None of the studies focused on behavior change to the authors' knowledge. This research is the first to focus on employee behavior change. The following part offers suggestions for researchers and management; Fig. 3 shows the change from non-compliance to compliance.

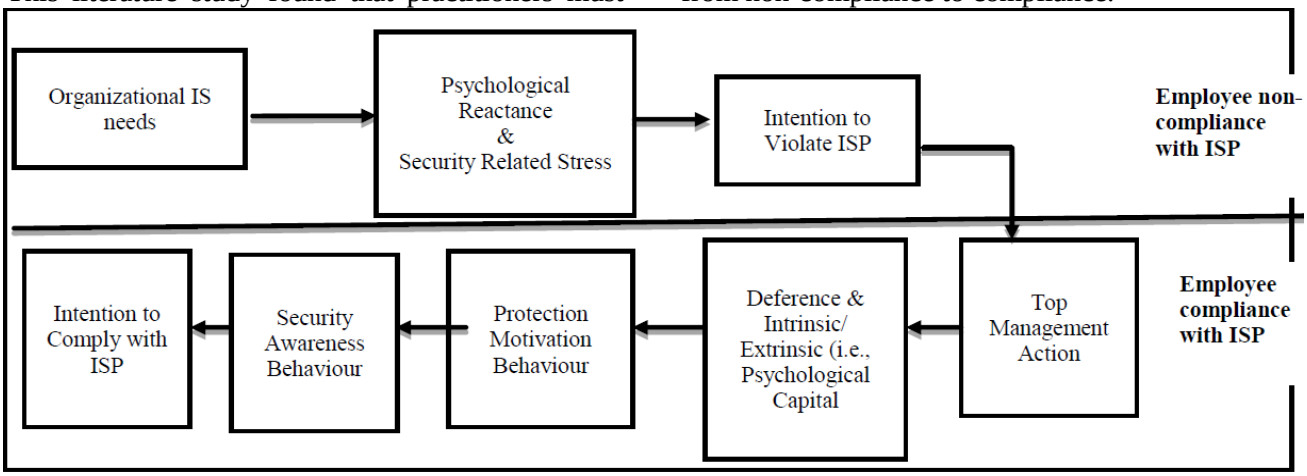

Fig. 3 Behavior changes from non-compliance to ISP compliance

The ISPC literature never discusses the transformation. The researchers reviewed the 2016–2021 literature in two dimensions: (1) Compliance studies, (2) Non-compliance studies.

Literature was organized according to the different aspects of the study, with Appendices A1-A4 focusing on non-compliance types (such as SRS, neutralization, value conflicts, deterrence and reactance, and justice), and Appendices B1 and B2 focusing on compliance types (such as protection motivation behavior and security culture, awareness).

Based on an analysis of the relevant literature, Fig. 3 shows ISB and ISPC activities.

The model contains two lanes: non-compliance and compliance. The following sections cover the combining and transforming actions.

This comprehensive analysis of the relevant literature has resulted in several valuable contributions and implications for behavioral information security research.

This review presented a complete approach to changing behavior.

The transformation process assists security practitioners in gaining an understanding of the factors that contribute to workers' non-compliance and assists them in transforming employees' conduct into compliant behavior.

Previous studies have shown that most security professionals develop ISP generic, which is why employees do not comply with the policy [40].

Concurrently, the vast majority of academics have proposed that an information security policy must be organized by the following requirements and processes of the company.

The results of this study included all of the primary compliance and non-compliance factors, which can assist practitioners in developing information security policies tailored to their organizations' requirements.

This review's study selection was rigorous. Some missing research may improve this literature review's conclusions.

This literature review provides a model for the validation procedure. The research team via query-based analysis will put this process model to the test. The outcomes proved that the procedures currently used to ensure compliance are inadequate. The researchers will use process management tools and approaches to fix the problem.

This research is the first step toward modeling and behavioral information security policy compliance.

Instead of evaluating compliance and Non-compliance, future studies should focus on changing employee behavior.

Non-compliance must be identified and remedied.

Second, there is more research on compliance behavior than on non-compliance; non-compliance behavior need additional theories and causes. Third, design an information security policy. ISP makers do not consider their own company's needs and environment. Researchers should research the organization's needs and then offer ISP improvements.

Fourth, technology-based solutions, such as compliance management systems, are needed. Researchers must use the technology to improve ISPC. Fifth, actual compliance needs more study than intention. This review found few studies on actual compliance.

Acknowledgments

This study was conducted with the assistance of funding provided by UNITEN in the form of a Grant (J510050002/2022034).

References

[1] BOOTH A., SUTTON A., and PAPAIOANNOU D. *Systematic Approaches to a Successful Literature Review*. 2nd ed. SAGE Publications Ltd, London, 2017.

[2] DOHERTY N.F., and FULFORD H. Aligning the information security policy with the strategic information systems plan. *Computers & Security*, 2006, 25(1): 55-63. DOI: 10.1016/j.cose.2005.09.009.

[3] EMAD S., ALI A., LAI F., HASSAN R., and SHAD M.K. The Long-Run Impact of Information Security Breach Announcements on Investors ' Confidence : The Context of Efficient Market Hypothesis sustainability The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context. *Sustainability*, 2021, 13(3): 1066. DOI: 10.3390/su13031066.

[4] AZHAR E., and HASSAN R. Socio-Economic Factors on Sector-Wide Systematic Risk of Information Security Breaches: Conceptual Framework. In: *9th International Economics and Business Management Conference*, 2020. DOI: 10.15405/epsbs.2020.12.05.54.

[5] ALI R.F., DOMINIC P.D.D., and ALI K. Organizational Governance , Social Bonds and Information Security Policy Compliance : A Perspective towards Oil and Gas Employees. *Sustainability*, 2020, (12): 1-27.

[6] CHEN L., ZHEN J., DONG K., and XIE Z. Effects of sanction on the mentality of information security policy compliance. *Argentina Review of Psychological Clinic*, 2020, 29(1): 39-49. DOI: 10.24205/03276716.2020.6.

[7] IBM. *IBM Infographic: Cyber Security Intelligence Index*. IBM, Armonk, NY, USA, 2014.

[8] PWC UK. *Organizations still failing to prepare effectively for cyber attacks*. PwC Cambridge, UK, 2017: 1-3. https://www.pwc.com/m1/en/media-centre/2017/press-releases/documents/organisations-are-failing-to-prepare-effectively-for-cyberattack.pdf

[9] NIST. *NIST Standard Guid.* National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce, Gaithersburg, MD, USA, 2019.

[10] ALOTAIBI M., FURNELL S., and CLARKE N. Information security policies: A review of challenges and influencing factors. In: *2016 11th International Conference for Internet Technology and Secured Transactions*, 2017: 352-358. DOI: 10.1109/ICITST.2016.7856729.

[11] ANTONIOU G.S. *Designing an effective information security policy for exceptional situations in an organization: An experimental study.* Doctoral dissertation. Nova Southeastern University, 2015.

[12] WILLISON R., and WARKENTIN M. Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, 2013, 37(1): 1-20. DOI: 10.25300/MISQ/2013/37.1.01.

[13] D'ARCY J., and LOWRY P.B. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 2019, 29(1): 43-69. DOI: 10.1111/isj.12173.

[14] SANS, HAYSTAX TECHNOLOGY. *Insider Threat Survey*. 2017. https://haystax.com/new-sans-haystax-technology-insider-threat-survey-reveals-malicious-actors-damaging-threat-vector-companies/

[15] HINA S., SELVAM D.P., and LOWRY P.B. Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computer Security*, 2019, 87: 101594. DOI: 10.1016/j.cose.2019.101594.

[16] RAJAB M., and EYDGAHI A. Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computer Security*, 2019, 80: 211-223. DOI: 10.1016/j.cose.2018.09.016.

[17] SAXENA N., HAYES E., BERTINO E., OJO P., CHOO K.K.R., and BURNAP P. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, 2020, 9(9): 1460. DOI: 10.3390/electronics9091460.

[18] CYBERSECURITY INSIDERS. *Insider Threat 2018 Report*. 2018: 41. https://www.cybersecurity-insiders.com/

[19] SOMMESTAD T., HALLBERG J., LUNDHOLM K., and BENGTSSON J. Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 2014, 22(1): 42-75. DOI: 10.1108/IMCS-08-2012-0045.

[20] TSOHOU A., and HOLTKAMP P. Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology and People*, 2018, (31): 1047-1068.

[21] D'ARCY J., and HERATH T. A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 2011, 20(6): 643-658. DOI: 10.1057/ejis.2011.23.

[22] TRANG S., and BRENDEL B. A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers*., 2019, 21(6): 1265-1284. DOI: 10.1007/s10796-019-09956-4.

[23] AURIGEMMA S., and PANKO R. A composite framework for behavioral compliance with information security policies. In: *Proceedings of the 2012 45th Hawaii International Conference on System Sciences*, 2013, 3248-

3257. DOI: 10.1109/HICSS.2012.49.
[24] PADAYACHEE K. Taxonomy of compliant information security behavior. *Computer Security*, 2012, 31(5): 673-680. DOI: 10.1016/j.cose.2012.04.004.
[25] POSEY C., ROBERTS T., and LOWRY P. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quaterly*, 2013, 2013-2015.
[26] SIPONEN M., and VANCE A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, 2010, 34(3): 487-502. DOI: 10.2307/25750688.
[27] AURIGEMMA S., and MATTSON T. Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security*, 2017, 25(4): 421-436. DOI: 10.1108/ICS-11-2016-0089.
[28] KOLKOWSKA E., KARLSSON F., and HEDSTRÖM K. Escalation of commitment as an antecedent to non-compliance with information security policy. *Information and Computer Security*, 2017, 26(2): 39-57. DOI: 10.1108/ICS-09-2017-0066.
[29] BOSS S.R., GALLETTA D.F., LOWRY P.B., MOODY G.D., and POLAK P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems*, 2015, 39(4): 837-864. DOI: 10.25300/MISQ/2015/39.4.5.
[30] IFINEDO P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computer Security*, 2012, 31(1): 83-95. DOI: 10.1016/j.cose.2011.10.007.
[31] HSU J.S.C., SHIH S.P., HUNG Y.W., and LOWRY P.B. The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, 2015, 26(2): 282-300. DOI: 10.1287/isre.2015.0569.
[32] DOHERTY N.F., and TAJUDDIN S.T. Towards a user-centric theory of value-driven information security compliance. *Information Technology and People*, 2018, 31(2): 348-367. DOI: 10.1108/ITP-08-2016-0194.
[33] CONNOLLY L.Y., LANG M., and WALL D.S. Information Security Behavior: A Cross-Cultural Comparison of Irish and US Employees. *Information Systems Management*, 36(4): 306-322, 2019. DOI: 10.1080/10580530.2019.1651113.
[34] HERATH T., and RAO H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 2009, 47(2): 154-165. DOI: 10.1016/j.dss.2009.02.005.
[35] LANKTON N.K., STIVASON C., and GURUNG A. Information protection behaviors: morality and organizational criticality. *Information and Computer Security*, 2019, 27(3): 468-488. DOI: 10.1108/ICS-07-2018-0092.
[36] SAFA N.S., SOOKHAK M., VON SOLMS R., FURNELL S., GHANI N.A., and HERAWAN T. Information security conscious care behaviour formation in organizations. *Computer Security*, 2015, 53: 65-78. DOI: 10.1016/j.cose.2015.05.012.
[37] HU Q., DINEV T., HART P., and COOKE D. Managing Employee Compliance with Information Security Policies : The Critical Role of Top Management and Organizational Culture. *Decision Sciences Journal*, 2012, 43: 615-660.
[38] D'ARCY, and TEH P.L. Predicting employee information security J. policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 2019, 56(7). DOI: 10.1016/j.im.2019.02.006.
[39] SYKES G.M., and MATZA D. Techniques of Neutralization : A Theory of Delinquency. *American Sociological Review*, 1957, 22(6): 664-670.
[40] GWEBU K.L., WANG J., and HU M.Y. Information security policy non-compliance: An integrative social influence model. *Information Systems Journal*, 2020, 30(2): 220-269. DOI: 10.1111/isj.12257.
[41] MERHI M.I., and AHLUWALIA P. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, 2019, 92: 37-46. DOI: 10.1016/j.chb.2018.10.031.
[42] ANDERSON C.L., and AGARWAL R. Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quaterly*, 2010, 34(2): 613-643.
[43] HWANG I., KIM, K.T., and KIM S. Why Not Comply with Information Security? An Empirical Approach for the Causes of Non-Compliance. *Online Information Review*, 2017, 41(1): 1-18.
[44] WILLISON R., WARKENTIN M., and JOHNSTON A.C. Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, 2018, 28(2): 266-293. DOI: 10.1111/isj.12129.
[45] MOODY G., SIPONEN M., and PAHNILA S. Toward a unified model of information security policy compliance. *MIS Quaterly*, 2018, 42: 285-302.
[46] SHADBAD F., and BIROS D. Technostress and its influence on employee information security policy compliance. *Information Technology and People*, 2020, 2: 1-23. DOI: 10.1108/ITP-09-2020-0610.
[47] BANSAL G., MUZATKO S., and SHIN S.I. Information system security policy non-compliance: the role of situation-specific ethical orientation. *Information Technology and People*, 2020, 30(1): 1350. DOI: 10.1108/ITP-03-2019-0109.
[48] KLEIN R.H., and LUCIANO E.M. What Influences Information Security Behavior? A Study with Brazilian Users. Journal of Information Systems and Technology Management, 2016, 13(3): 479-496. DOI: 10.4301/s1807-17752016000300007.
[49] JOHNSTON A.C., WARKENTIN M., MCBRIDE M., and CARTER L. Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 2016, 25(3): 231-251. DOI: 10.1057/ejis.2015.15.
[50] MERHI M.I., and AHLUWALIA P. Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, 2019, 92: 37-46. DOI: 10.1016/j.chb.2018.10.031.
[51] TRINKLE B.S., WARKENTIN M., MALIMAGE K., and RADDATZ N. High-risk deviant decisions: Does neutralization still play a role? *Journal of the Association*

for Information Systems, 2021, 22(3): 797-826. DOI: 10.17705/1jais.00680.

[52] XU F., HSU C., LUO X., and WARKENTIN M. Reactions to Abusive Supervision: Neutralization and IS Misuse. *Journal of Computer Information Systems*, 2022, 62(3). DOI: 10.1080/08874417.2021.1887776.

[53] BURNS A.J., POSEY C., ROBERTS T.L., and LOWRY P.B. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, 2017, 68: 190-209. DOI: 10.1016/j.chb.2016.11.018.

[54] HOOPER V., and BLUNT C. Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, 2019, 39(8): 1-13. DOI: 10.1080/0144929X.2019.1623322.

[55] BÉLANGER F., COLLIGNON S., ENGET K., and NEGANGARD E. Determinants of early conformance with information security policies. *Information & Management*, 2017, 54(7): 887-901. DOI: 10.1016/j.im.2017.01.003.

[56] CHAKRABORTY T., JAJODIA S., KATZ J., PICARIELLO A., SPERLI G., and SUBRAHMANIAN V.S. A Fake Online Repository Generation Engine for Cyber Deception. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(2): 518-533. DOI: 10.1109/TDSC.2019.2898661.

[57] HAN Q., MOLINARO C., PICARIELLO A., SPERLI G., SUBRAHMANIAN V.S., and XIONG Y. Generating Fake Documents using Probabilistic Logic Graphs. *IEEE Transactions on Dependable and Secure Computing.*, 2021, 5971(c): 1-14. DOI: 10.1109/TDSC.2021.3058994.

[58] SAFA N.S., MAPLE C., FURNELL S., AZAD M.A., PERERA C., DABBAGH M., and SOOKHAK M. Deterrence and prevention-based model to mitigate information security insider threats in organizations. *Future Generation Computer Systems*, 2019, 97: 587-597.

[59] KIM H.L., and HAN J. Do employees in a 'good' company comply better with information security policy? A corporate social responsibility perspective. *Information Technology and People*, 2018, 32(4): 858-875. DOI: 10.1108/ITP-09-2017-0298.

[60] YAZDANMEHR A., and WANG J. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 2016, 92: 36-46. DOI: 10.1016/j.dss.2016.09.009.

[61] AURIGEMMA S., and MATTSON T. Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computer Security*, 2017, 66: 218-234. DOI: 10.1016/j.cose.2017.02.006.

[62] MERRILL W., and ALLEN C. Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 2016, 92: 25-35. DOI: 10.1016/j.dss.2016.09.013.

[63] TSOHOU A., and HOLTKAMP P. Are users competent to comply with information security policies? An analysis of professional competence models. *Information Technology and People*, 2018, 28(1): 163-194.

参考文:

[1] BOOTH A.、SUTTON A. 和 PAPAIOANNOU D. 成功文獻綜述的系統方法。第二版。智者出版有限公司，倫敦，2017年。

[2] DOHERTY N.F. 和 FULFORD H. 使信息安全政策與戰略信息系統計劃保持一致。計算機與安全，2006年，25(1)：55-63。DOI：10.1016/j.cose.2005.09.009。

[3] EMAD S.、ALI A.、LAI F.、HASSAN R. 和 SHAD M.K. 信息安全違規公告對投資者信心的長期影響：有效市場假設可持續性的背景信息安全違規公告對投資者信心的長期影響：背景。可持續性，2021年，13(3)：1066。DOI：10.3390/su13031066。

[4] AZHAR E. 和 HASSAN R. 信息安全漏洞的全行業系統性風險的社會經濟因素：概念框架。在：第9屆國際經濟與企業管理會議，2020年。DOI：10.15405/epsbs.2020.12.05.54。

[5] ALI R.F.、DOMINIC P.D.D. 和 ALI K. 組織治理、社會債券和信息安全政策合規性：對石油和天然氣員工的看法。可持續性, 2020, (12): 1-27.

[6] CHEN L., ZHEN J., DONG K. 和 XIE Z. 制裁對信息安全政策遵從心態的影響。阿根廷心理診所評論，2020，29(1)：39-49。DOI：10.24205/03276716.2020.6。

[7]國際商業機器公司。國際商業機器公司信息圖：網絡安全情報索引。國際商業機器公司，美國紐約州阿蒙克，2014年。

[8]英國普華永道。組織仍然未能有效地為網絡攻擊做好準備。普華永道英國劍橋，2017年：1-3。https://www.pwc.com/m1/en/media-centre/2017/press-releases/documents/organisations-are-failing-to-prepare-effectively-for-cyberattack.pdf

[9]美國國家標準技術研究院。美國國家標準技術研究院標準指南。美國商務部國家標準與技術研究院，美國馬里蘭州蓋瑟斯堡，2019年。

[10] ALOTAIBI M.、FURNELL S. 和 CLARKE N. 信息安全政策：挑戰和影響因素回顧。載於：2016年第11屆互聯網技術與安全交易國際會議，2017：352-358。DOI：10.1109/ICITST.2016.7856729。

[11] ANTONIOU G.S. 為組織中的特殊情況設計有效的信息安全策略：一項實驗研究。博士論文。諾瓦東南大學, 2015.

[12] WILLISON R. 和 WARKENTIN M. 超越威懾：員工計算機濫用的擴展視圖。管理信息系統季刊, 2013, 37(1): 1-20. DOI：10.25300/MISQ/2013/37.1.01。

[13] D'ARCY J. 和 LOWRY P.B. 員工日常遵守信息安全政策的認知-情感驅動因素：多層次、縱向研究。信息系統雜誌, 2019, 29(1): 43-69. DOI：10.1111/isj.12173。

[14]系統管理員、審計、網絡和安全，乾草技術。內部威脅調查。2017. https://haystax.com/new-sans-haystax-technology-insider-threat-survey-reveals-malicious-actors-damaging-threat-vector-companies/

[15] HINA S.、SELVAM D.P. 和 LOWRY P.B. 機構治理和保護動機：對發展中國家高等教育機構員工安全合規行為塑造的理論見解。計算機安全, 2019, 87: 101594. DOI: 10.1016/j.cose.2019.101594.

[16] RAJAB M. 和 EYDGAHI A.

評估理論框架對遵守高等教育信息安全政策意圖的解釋力。計算機安全，2019，80：211-223。DOI：10.1016/j.cose.2018.09.016。

[17] SAXENA N.、HAYES E.、BERTINO E.、OJO P.、CHOO K.K.R. 和 BURNAP P. 內部威脅對組織和關鍵業務的影響和主要挑戰。電子學, 2020, 9(9): 1460. DOI: 10.3390/electronics9091460.

[18]網絡安全內部人士。2018年內部威脅報告。2018年：41。https://www.cybersecurity-insiders.com/

[19] SOMMESTAD T.、HALLBERG J.、LUNDHOLM K. 和 BENGTSSON J. 影響信息安全策略合規性的變量：定量研究的系統回顧。信息管理與計算機安全, 2014, 22(1): 42-75. DOI：10.1108/IMCS-08-2012-0045。

[20] TSOHOU A. 和 HOLTKAMP P. 用戶是否有能力遵守信息安全政策？專業能力模型分析。信息技術與人, 2018, (31): 1047-1068.

[21] D'ARCY J. 和 HERATH T. 對是安全文獻中威懾理論的回顧和分析：理解不同的發現。歐洲信息系統雜誌，2011年，20(6)：643-658。DOI：10.1057/ejis.2011.23。

[22] TRANG S. 和 BRENDEL B. 信息安全政策合規研究中威懾理論的薈萃分析。信息系統前沿, 2019, 21(6): 1265-1284. DOI：10.1007/s10796-019-09956-4。

[23] AURIGEMMA S. 和 PANKO R. 信息安全策略行為合規性的複合框架。在：2012年第45屆夏威夷國際系統科學會議論文集，2013年，3248-3257。DOI：10.1109/HICSS.2012.49。

[24] PADAYACHEE K. 合規信息安全行為分類學。計算機安全, 2012, 31(5): 673-680. DOI：10.1016/j.cose.2012.04.004。

[25] POSEY C.、ROBERTS T. 和 LOWRY P. 內部人員對組織信息資產的保護：基於系統學的分類學和保護動機行為多樣性理論的發展。管理信息系統季刊，2013年，2013-2015年。

[26] SIPONEN M. 和 VANCE A. 中和：對員工信息系統安全策略違規問題的新見解。管理信息系統 季刊：管理信息系統，2010年，34(3)：487-502。DOI：10.2307/25750688。

[27] AURIGEMMA S. 和 MATTSON T. 威懾和懲罰經驗對信息安全政策合規態度的影響。信息與計算機安全, 2017, 25(4): 421-436. DOI：10.1108/ICS-11-2016-0089。

[28] KOLKOWSKA E.、KARLSSON F. 和 HEDSTRÖM K. 承諾升級作為不遵守信息安全政策的前提。信息與計算機安全, 2017, 26(2): 39-57. DOI：10.1108/ICS-09-2017-0066。

[29] BOSS S.R.、GALLETTA D.F.、LOWRY P.B.、MOODY G.D. 和 POLAK P. 系統用戶必須擔心什麼？使用恐懼訴求來產生威脅和恐懼，從而激發保護性安全行為。管理信息系統季刊：管理信息系統, 2015, 39(4): 837-864. DOI：10.25300/MISQ/2015/39.4.5。

[30] IFINEDO P. 了解信息系統安全策略合規性：計劃行為理論和保護動機理論的整合。計算機安全, 2012, 31(1): 83-95. DOI：10.1016/j.cose.2011.10.007。

[31] HSU J.S.C.、SHIH S.P.、HUNG Y.W. 和 LOWRY P.B. 角色外行為和社會控制在信息安全政策有效性中的作用。信息系統研究, 2015, 26(2): 282-300. DOI：10.1287/isre.2015.0569。

[32] DOHERTY N.F. 和 TAJUDDIN S.T. 邁向以用戶為中心的價值驅動信息安全合規理論。信息技術與人, 2018, 31(2): 348-367. DOI：10.1108/ITP-08-2016-0194。

[33] CONNOLLY L.Y.、LANG M. 和 WALL D.S. 信息安全行為：愛爾蘭和美國員工的跨文化比較。信息系統管理, 36(4): 306-322, 2019. DOI: 10.1080/10580530.2019.1651113.

[34] HERATH T. 和 RAO H.R. 鼓勵組織中的信息安全行為：懲罰、壓力和感知有效性的作用。決策支持系統，2009，47（2）：154-165。DOI：10.1016/j.dss.2009.02.005。

[35] LANKTON N.K.、STIVASON C. 和 GURUNG A. 信息保護行為：道德和組織重要性。信息與計算機安全, 2019, 27(3): 468-488. DOI：10.1108/ICS-07-2018-0092。

[36] SAFA N.S.、SOOKHAK M.、VON SOLMS R.、FURNELL S.、GHANI N.A. 和 HERAWAN T. 組織中信息安全意識關懷行為的形成。計算機安全, 2015, 53: 65-78. DOI：10.1016/j.cose.2015.05.012。

[37] HU Q.、DINEV T.、HART P. 和 COOKE D. 管理員工遵守信息安全政策：最高管理層和組織文化的關鍵作用。決策科學雜誌，2012年，43：615-660。

[38] D'ARCY 和 TEH P.L. 每天預測員工信息安全 J. 政策合規性：與安全相關的壓力、情緒和中和的相互作用。信息與管理, 2019, 56(7). DOI：10.1016/j.im.2019.02.006。

[39] SYKES G.M. 和 MATZA D. 中和技術：犯罪理論。美國社會學評論，1957年，22(6)：664-670。

[40] GWEBU K.L., WANG J. 和 HU M.Y. 信息安全政策不合規：綜合社會影響模型。信息系統雜誌, 2020, 30(2): 220-269. DOI：10.1111/isj.12257。

[41] MERHI M.I. 和 AHLUWALIA P. 檢查威懾因素和規範對信息系統安全阻力的影響。人類行為中的計算機，2019，92：37-46。DOI：10.1016/j.chb.2018.10.031。

[42] ANDERSON C.L. 和 AGARWAL R. 實踐安全計算：家庭計算機用戶安全行為意圖的多媒體實證檢驗。管理信息系統季刊，2010年，34(2)：613-643。

[43] HWANG I.、KIM、K.T. 和 KIM S. 為什麼不遵守信息安全？不合規原因的實證方法。網絡信息評論, 2017, 41(1): 1-18.

[44] WILLISON R.、WARKENTIN M. 和 JOHNSTON A.C. 檢查員工計算機濫用意圖：來自正義、威懾和中和觀點的見解。信息系統雜誌, 2018, 28(2): 266-293. DOI：10.1111/isj.12129。

[45] MOODY G.、SIPONEN M. 和 PAHNILA S. 邁向信息安全政策合規的統一模型。管理信息系統季刊

，2018年，42：285-302。
[46] SHADBAD F. 和 BIROS D. 技術壓力及其對員工信息安全策略合規性的影響。信息技術與人，2020，2：1-23. DOI：10.1108/ITP-09-2020-0610。
[47] BANSAL G.、MUZATKO S. 和 SHIN S.I. 信息系統安全政策不合規：特定情況下道德取向的作用。信息技術與人, 2020, 30(1): 1350. DOI: 10.1108/ITP-03-2019-0109.
[48] KLEIN R.H. 和 LUCIANO E.M. 什麼影響信息安全行為？對巴西用戶的研究。信息系統與技術管理學報，2016，13(3)：479-496. DOI：10.4301/s1807-17752016000300007。
[49] JOHNSTON A.C.、WARKENTIN M.、MCBRIDE M. 和 CARTER L. 性格和情境因素：對違反信息安全政策的影響。歐洲信息系統雜誌，2016年，25(3)：231-251。DOI：10.1057/ejis.2015.15。
[50] MERHI M.I. 和 AHLUWALIA P. 檢查威懾因素和規範對信息系統安全阻力的影響。人類行為中的計算機，2019，92：37-46。DOI：10.1016/j.chb.2018.10.031。
[51] TRINKLE B.S.、WARKENTIN M.、MALIMAGE K. 和 RADDATZ N. 高風險偏差決策：中和仍然起作用嗎？信息系統協會雜誌，2021年，22(3)：797-826。DOI：10.17705/1jais.00680。
[52] XU F.、HSU C.、LUO X. 和 WARKENTIN M. 對濫用監督的反應：中和和信息系統濫用。計算機信息系統學報，2022，62(3). DOI：10.1080/08874417.2021.1887776。
[53] BURNS A.J.、POSEY C.、ROBERTS T.L. 和 LOWRY P.B. 檢查組織內部人員的心理資本與信息安全威脅和應對評估的關係。人類行為中的計算機，2017年，68：190-209。DOI：10.1016/j.chb.2016.11.018。
[54] HOOPER V. 和 BLUNT C. 影響它員工信息安全行為的因素。行為與信息技術，2019，39(8)：1-13. DOI：10.1080/0144929X.2019.1623322。
[55] BÉLANGER F.、COLLIGNON S.、ENGET K. 和 NEGANGARD E. 早期遵守信息安全政策的決定因素。信息與管理，2017，54(7): 887-901. DOI：10.1016/j.im.2017.01.003。
[56] CHAKRABORTY T.、JAJODIA S.、KATZ J.、PICARIELLO A.、SPERLI G. 和 SUBRAHMANIAN V.S. 用於網絡欺騙的虛假在線存儲庫生成引擎。電氣和電子工程師協會可靠和安全計算交易，2021，18(2)：518-533。DOI：10.1109/TDSC.2019.2898661。
[57] HAN Q.、MOLINARO C.、PICARIELLO A.、SPERLI G.、SUBRAHMANIAN V.S. 和 XIONG Y. 使用概率邏輯圖生成假文檔。電氣和電子工程師協會可靠和安全計算交易。，2021，5971(c)：1-14。DOI：10.1109/TDSC.2021.3058994。
[58] SAFA N.S.、MAPLE C.、FURNELL S.、AZAD M.A.、PERERA C.、DABBAGH M. 和 SOOKHAK M. 基於威懾和預防的模型，以減輕組織中的信息安全內部威脅。下一代計算機系統, 2019, 97: 587-597.
[59] KIM H.L. 和 HAN J. “好”公司的員工是否更好地遵守信息安全政策？企業社會責任視角。信息技術與人，2018，32(4)：858-875. DOI：10.1108/ITP-09-2017-0298。
[60] YAZDANMEHR A. 和 WANG J. 員工信息安全政策合規性：規範激活視角。決策支持系統, 2016, 92: 36-46. DOI：10.1016/j.dss.2016.09.009。
[61] AURIGEMMA S. 和 MATTSON T. 特權或程序：評估員工身份對遵守社交互動信息安全威脅和控制的意圖的影響。計算機安全，2017年，66：218-234。DOI：10.1016/j.cose.2017.02.006。
[62] MERRILL W. 和 ALLEN C. 保護性安全行為的延續：一項縱向研究。決策支持系統，2016年，92：25-35。DOI：10.1016/j.dss.2016.09.013。
[63] TSOHOU A. 和 HOLTKAMP P. 用戶是否有能力遵守信息安全政策？專業能力模型分析。信息技術與人, 2018, 28(1): 163-194.

Appendices

Appendix A1 Studies on SRS, neutralization, and non-compliance

No.	Authors	Theories used	Factors	Research Method	Sample Size	Findings
1	[43]	PMT and the Health Belief Model	Security systems, security education, security visibility	The quantitative research approach was used. SEM is used to test hypotheses and models.	From manufacturing and service companies, 415 usable replies were gathered.	Peer non-compliance, work constraints, and security system anxiety cause non-compliance with ISP.
2	[44]	Theory of neutralization, Deterrence	Organizational injustice (procedural and distributive)	A quantitative analysis based on scenarios. SPSS and PROC MIXED were used to test the hypotheses and data.	968 complete responses collected	Procedural and organizational unfairness causes computer abuse behavior; punishment certainty minimizes the effect of injustice and the desire to misuse ISP.
3	[45]	Neutralization techniques,	Social factors,	Design of a mixed-	924 participants	Neutralization was

		Theory of self-regulation, Health belief model, Theory of reasoned action, Protection motivation theory, Theory of interpersonal behavior, Deterrence theory, Extended protection motivation theory	punishment, Rewards/Costs, Habit, Neutralization, Response efficacy, Facilitating conditions, Reactance, Intention	method study	from the Finnish workplace took part.	found to be an excellent predictor of ISPC reactance.
4	[38]	Theory of neutralization	SRS fatigue, and frustration	The experience sampling approach was used. For results analyzes, hierarchical linear modeling is used.	It was determined that 138 of the responses were correct.	Stress-related security requirements result in exhaustion and dissatisfaction, eventually leading to neutralization. Additionally, neutralization has a damaging behavioral impact on ISP compliance.
5	[46]			Design of quantitative research	A total of 356 IT professionals took part in the survey.	Technostress has a favorable (direct and indirect) relationship with perceived strain and the propensity to breach ISP.

Appendix A2 Studies on value conflicts and non-compliance

No.	Authors	Theories used	Factors	Research Method	Sample Size	Findings
1	[28]	Prospect theory, RCT, self-justification theory, approach avoidance theory	Sunk cost, self-justification, and risk perception	Quantitative research methods including pre- and post-testing. For findings and analysis, SEM was employed.	Total of 500 people from various companies participated.	Impediments to task completion have a substantial impact on employees' non-compliance with ISP.
2	[32]	Grounded theory	Value assignment, perception of information value	NVivo 11 was used to construct the qualitative research and analyze the outcomes.	We conducted 55 semi-structured interviews.	The worth of information influences users' compliance behavior.
3	[35]	PMT	IT vision conflict	The quantitative research approach employed, as well as the PLS used for findings and analysis	We got 275 correct answers.	IT vision conflict influence the perceived severity and attitude regarding ISP non-compliance behavior.
4	[47]	Deterrence theory and RCT	Punishment LaHood, Reward likelihood, Moral Beliefs, Control variables, Neutralization Scenarios	Design of quantitative research	A total of 120 females and 101 males took part in the research	Procedural and organizational unfairness causei computer abuse behavior; punishment certainty minimizes the effect of injustice and the desire to misuse ISP.

Appendix A3 Studies on deterrence and non-compliance

No.	Authors	Theories used	Factors	Research Method	Sample Size	Findings
1	[48]	Deterrence theory	Satisfaction and safe behavior	Pre- and post-test quantitative research approaches were employed for instrument validation, whereas PLS was used for hypotheses and data analysis.	185 workers were tested.	Deterrence, social connections, and societal pressures all play important roles in avoiding ISSP violations.
2	[49]	PMT and GDT	Human personality traits (stability and plasticity)	The quantitative research approach used	112 correct responses collected	To keep ISB secure, it's important to consider factors such as susceptibility, severity, certainty of detection, penalties, and satisfaction.
3	[27]	TPB, PMT, GDT	Previous punishment experience	The quantitative research approach was used. SEM based on covariants is used	239 workers from the United States Department of	The rational use of punishments results in attitude-dependent ISB. The attitude formed because of

				for research model testing.	Defense took part in the exercise.	disciplinary past punishment experience influences threats.
4	[41]	TPB, GDT	Descriptive norms, moral norms	The design of quantitative research. PLS is used in model testing.	139 employees from ten different companies took part.	Deterrence variables shape employee norms, which impact behavioral resistance to ISP compliance.
5	[22]	Deterrence theory	Formal sanction, Informal sanction	A meta-analysis was performed (literature review)	A total of 35 studies were studied.	1) Deterrence theory influences ISP compliance behavior (save for punishment speed). (2) Distinct cultures have different deterrent effects

Appendix A4 Reactance, justice and non-compliance

No.	Authors	Theory Used	Factors	Research Method	Sample Size	Findings
1	[51]	Deterrence theory, Theory of neutralization	Sanction Severity, Sanction Certainty, Intention to violate, Technique of Neutralization	The quantitative research design used	121 graduate and undergraduate (senior-level) accounting students from a prominent institution in the southeast US.	Workers may attempt to rationalize their unethical behavior by denying responsibility for their actions, for example, by claiming that their supervisors pressured them into performing the violations; additionally, awareness and perceptions of the certainty and severity of organizational punishment are likely to attenuate such deviant behavior
2	[52]	Neutralization	Abusive supervision, organization-directed IS misuse, metaphor of the ledger, Tenure with supervisor	The quantitative research design used	203 responses	Demonstrated that when individuals felt abusive supervision, they were more likely to use the ledger metaphor as a neutralizing tactic to justify their participation in IS abuse..

Appendix B1 Protection motivation behavior and compliance

No.	Authors	Factors	Theory used	Research Method	Sample Size	Findings
1	[62]	Continues intention, perceived extraneous circumstances	PMT	For this study, we opted for a longitudinal approach. Data and models can be tested with PLS's help.	We obtained 253 legitimate replies.	Employees' perceptions of self-efficacy, threat intensity, and vulnerability highly influence their propensity to engage in continuing preventive behavior.
2	[53]	Hope, optimism, self-efficacy, resilience, fear, and protection motivation	PMT	Methods used in quantitative studies concept and adoption of the Structural Equation modeling The validation of Hypotheses	We obtained 377 relevant answers from government and non-government agencies.	Having a high level of psychological capital is beneficial for employees' self-preservation**.**
3	[54]	Self-efficacy and impact	PMT, Health Belief Model, DT, TRA Self-efficacy and impact Ethical Decision-Making Model, and Value	Statistical analysis by using the structural equation model (SEM) was employed in this quantitative study.	New Zealand-based IT professionals, 70 strong.	The likelihood that a person will engage in information security practices is influenced favorably by their perception of the impact such practices will have and by their belief in their own abilities to implement such practices.
4	[35]	Moral beliefs	Congruence Theory	A quantitative research layout is based on potential outcomes. Evaluation of models with partial least squares		

Appendix B2 Security culture, awareness behavior and compliance

No.	Authors	Factors	Theory used	Research Method	Sample Size	Findings
1	[55]	Security awareness, intention to confirm early	TPB	The model was evaluated using PLS using the quantitative research approach, and the results were analyzed.	A university received 535 suitable replies, all of which were useful.	Attitudes and intentions strongly influence early ISP compliance behavior.

Continuation of Appendix B2

2	[63]	N/A	N/A	Systematic literature review	32 papers and eight professional frameworks were reviewed to determine if users have the necessary competence to ensure ISP compliance.	ISP compliance capabilities are excluded in professional frameworks.