Research Article

© 2023 Maurizio Cavallari.
This is an open access article licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (https://creativecommons.org/licenses/by-nc/4.0/)

Received: 15 September 2023 / Accepted: 23 October 2023 / Published: 5 November 2023

# Organizational Determinants and Compliance Behavior to Shape Information Security Plan

**Maurizio Cavallari**

*Universitá Telematica Internazionale UNINETTUNO,*
*Corso Vittorio Emanuele II 39,*
*Roma, Italy*

**DOI: https://doi.org/10.36941/ajis-2023-0151**

***Abstract***

*In the advanced field of Information and Communication Technology (ICT) within modern corporate frameworks, the pressing issue of non-compliance becomes increasingly crucial. Achieving the ideal balance—where one fosters consistent employee commitment without resorting to overly harsh penalties for possible violations—presents a complex problem. Such a nuanced relationship calls for a synchronized coordination among the company's underlying factors, the principles of the Information Security Plan (ISP), and overarching compliance mandates. As companies step into a period where digital environments are in constant flux, the importance of securing information systems rises to a critical level. Against this backdrop, compliance stands out as a vital component, functioning as a stringent safeguard in the ongoing mission to protect precious digital assets—a mission comprehensively detailed within the ISP. This in-depth academic study sets out to rigorously explore and scrutinize the diverse opinions and beliefs of committed employees and insightful management concerning unwavering company alignment with the ISP. This is accomplished by defining a construct that centers on key dimensions: Organizational Culture, Personal Attitudes, Actors, Behavioral Intentions, and Motivational Dynamics. Eleven Hypotheses are outlined and represent the materialisation of the model. This model form a starting point from which future empirical exploration will be able to take place, propelling us towards a deeper understanding of the phenomena under scrutiny.*

***Keywords:*** *compliance, non-compliance, information security policy, ISP, information systems security, theoretical model, empirical investigation*

## 1. Introduction

Compliance serves as a critical cornerstone in the intricate landscape of organizational operations, seamlessly linking the multifarious regulations and policy frameworks that preside over business functionalities as Ali et al. 2021 argued in a systematic literature review to identify the transformation process from noncompliance to compliance with information security behavior and policies (Ali et al., 2021). At its core, Compliance ensures that each minuscule operational element, spanning the gamut from nuanced procedural complexities to critical strategic decisions, is meticulously harmonized with the overarching governing regulations, laws, and corporate policies, as in Sulaiman et al. 2022 in their review on cyber-information security compliance and violation behavior in organizations (Sulaiman et al., 2022). This harmonization is of vital importance in the digital age,

particularly within the domain of Information Systems Security, as in Alraja et al. arguments who explored information security policy compliance from an employee's perspective in a global setting (Alraja et al., 2023). In the present study Compliance takes on the mantle of a sentinel, steadfastly shielding digital infrastructures and assets from the ever-evolving cyber threats.

This paper lays special emphasis on the articulated bond between Compliance and Information Security. Their interrelationship is neither incidental nor superficial; rather, Compliance provides the scaffolding upon which organizations can construct and fortify their digital security foundations (Sulaiman et al., 2022; Alraja et al., 2023). The theoretical framework delineated in this discourse not only introduces this intertwined concept but fervently calls for a deeper, more profound academic exploration. It underscores the urgent need to unravel the mechanisms and strategies through which modern organizations seamlessly weave Compliance into their security narratives, transforming regulatory adherence from a perfunctory task into an intrinsic organizational culture, as pointed out by Hinaet al. who provided theoretical insights into shaping employees 'security compliance behavior in higher education institutions (Hina et al., 2019).

In dissecting the myriad incidents linked to human behavior and multi-layered information systems, a recurrent theme emerges: the crucial role of employee interactions (Qatawneh, 2023). Whether driven by benign neglect, the allure of convenience, or mere oversight, employees sometimes find themselves circumventing established protocols, inadvertently introducing vulnerabilities into the system. Recognizing this, the discourse propose that a robust security framework cannot merely be technocentric, as we find in Huang and Lin who discussed inconsistencies between information security policy compliance and shadow IT usage (Huang and Lin, 2023). Instead, it necessitates a more organizational approach that integrates the often unpredictable human element, prompting organizations to adopt diverse, multi-pronged strategies to address and mitigate these inherent human-centric vulnerabilities (Alraja et al., 2023; Goel et al., 2023; Dwivedi et al., 2023).

For multinational organizations operating on a global scale, the stakes are exponentially heightened. In such sprawling corporate ecosystems, even a minor security breach can set off a ripple effect. Beyond the immediate data loss, the repercussions can erode consumer trust, denting the organization's hard-earned reputation, sometimes irreparably. In this high-stakes game, Compliance ceases to be just a bureaucratic requirement. It morphs into a proactive shield, a bulwark against the potentially catastrophic consequences of security lapses and oversights, as you find comfort of this idea in published research findings (Huang and Lin, 2023; Palanisamy et al., 2023; Xue et al., 2023 and Ifinedo, 2022).

Delving into the semiotics of 'Compliance', one discerns its multifaceted nature. Far from being a static endpoint, Compliance represents a dynamic issue, an ongoing odyssey of alignment with a multitude of regulations, industry benchmarks, and globally accepted best practices. And as this journey unfolds within the complex maze of Information Security, a singular focal point emerges: human behavior (Qatawneh, 2023; Donalds and Barclay, 2022; Dewies et al., 2021). Recognizing this, contemporary organizations are making concerted efforts, channeling resources towards a bevy of strategies, protocols, and training modules, all aimed at inculcating a culture of security awareness and vigilance among their workforce, as Dewies et al. found in their study about the effectiveness of nudging in information security when attitudes are unsupportive (Dewies et al., 2021).

The methodological underpinnings of this study traverse the impervious pathways through which Compliance steers organizations not just towards mere regulatory alignment but towards a broader vision of comprehensive security enhancement. The intent is clear: to demystify the web of interconnections binding Compliance, organizational culture, and pressing security mandates (Alraja et al., 2023; Goel et al., 2023; Dwivedi et al., 2023 and Kim et al., 2020).

In particular Alyami et al. published an investigation that scrutinized academic articles in Information Systems (IS) security to isolate key 'security themes 'beneficial for organizational decision-making. They evaluated 87 scholarly papers featured in the AIS Senior Scholars 'Basket of Journals. Twelve principal "security themes" within the IS landscape were identified. The analysis

underscores that particular themes, such as IS Security Policy, IS Security Behaviour, IS Security Management, and IS Security Awareness, are more heavily researched compared to other areas (Alyami et al., 2020).

In its assessment, we envision an organizational environment where security, far from being a mere check in the box, becomes an ingrained, omnipresent organizational tenet. This transitioning from an obligatory task to an embedded core philosophy, signifies a big paradigm shift, synchronizing seamlessly with both external regulatory edicts and the organization's intrinsic values (Palanisamy et al., 2023; Dewies et al., 2021; Kim et al., 2020 and Alyami et al., 2020).

## 2. Objectives

In prior scholarly investigations, the interplay between Compliance rules (which originate externally) and internal Policies (which emerge from within the organization) has been scrutinized through a fivefold conceptual lens encompassing Organizational Culture, Personal Attitudes, Actors, Intention, and Motivation, as in Cavallari (2011) where is discussed the organizational relationship between compliance and information security finding there is a bi-directional relationship among those and that transformational leadership management action can influence both of them (Cavallari, 2011). In the same sense we find Posey et al. (2011), and Caldwell (2012) who discussed the importance of training in addressing security vulnerabilities (Caldwell, 2012).

This rounded perspective delves into the complex interrelations of how organizations pursue the regulatory norms, molding their internal policies while being influenced by external compliance mandates as in the arguments of Warkentin and Willison (2009) and as in Khan and AlShare (2019), where they studied the distinguishing factors between violators and non-violators of information security measures in organizations (Khan and AlShare, 2019). However, this paper endeavors to transcend the boundaries set by earlier research by not only expanding the existing research model but also delving deeper into the ramifications of compliance-related organizational dynamics on an organization's pre-existing information security policy from a persuasion and cognitive elaboration perspective (Yang et al., 2019).

Irrespective of an organization's current position on the continuum field of compliance, whether aligned with regulatory demands or falling short (Siponen and Vance, 2014), the augmented framework discussed in this paper holds the potential to uncover invaluable insights. One such critical facet is the revelation of the inherent nature of non-compliant employees, as Alskar et al. (2015) suggested about the evolution of information security research on employees' behavior — those who, for various reasons, deviate from the established compliance rules (Alskar et al., 2015). This understanding is fundamental in unraveling the vast mosaic of potential security vulnerabilities within an organization (Boss et al., 2009; Cascavilla et al., 2018 and Kennedy, 2016). By delving into the complexities of non-compliance, this research aspires to cast light on the factors that engender an environment where security is jeopardized.

At its core, this research is dedicated to the formulation and construction of an enriched model, one that reaches beyond the surface and dives into the depths of the knotty relationship between compliance, internal policies, and their intersection with human behavior within organizations. This model, meticulously crafted and poised to encompass a broader spectrum of variables, could serves as a foundation for subsequent empirical explorations. Its purpose transcends mere theoretical discourse; it is geared towards discerning the complex realm of insider threats, be they conscious or inadvertent, that emanate from the human element inherent in organizational dynamics, as clearly argued in past research like in Yoon and Kim (2013) who empirically studied computer security behavioral intention in the workplace (Yoon and Kim, 2013), in Cheng et al. (2013) where they proposed an integrated model based on social control and deterrence theory to understand the violation of IS security policy (Cheng et al., 2013), in Clay Posey et al. (2017) where they categorized and assessed threats to personally identifiable information in organizations (Clay Posey et al., 2017).

The base of this endeavor lies in comprehending how the mosaic of organizational culture,

individual attitudes, key actors within the organizational hierarchy, intentions that underpin actions, and the underlying motivations interplay to shape compliance and its ensuing impact on information security policies as in Herath and Rao (2009a). As these factors converge, a multi-dimensional connections emerge, shedding light on the interwoven dynamics that contribute to the complex spectrum of organizational compliance (Vance et al., 2013). The ultimate aim is not only to decode the nuances of compliance but also to fathom the underlying currents that can potentially cascade into security vulnerabilities—vulnerabilities that often have human actions and decisions at their epicenter.

This paper endeavors to push the boundaries of previous research by proposing an enriched and expanded model that encapsulates the multifaceted relationship between Compliance rules, internal Policies, and the wide spectrum of human behaviors within organizations. By doing so, it seeks to unearth the concealed facets of non-compliance and their implications for information security. As this research unfolds, it strives to transcend theoretical discourse, laying the foundation for empirical investigations that looks into the intricate labyrinth of insider threats—a realm where human motivations and actions intertwine with compliance rules to shape the security posture of organizations (Posey et al., 2011; Vance et al., 2013).

## 3. Previous Research

Scholarly evidence demonstrates that many threats to an organization's information security stem from employees' casual attitudes and behaviors (Cavallari, 2011; Khan and AlShare, 2019; Kennedy, 2016 and Sandhu et al., 2017).

Within the mentioned past research findings were find that Cavallari (2011) discussed the organizational relationship between compliance and information security finding there is a bi-directional relationship among those and that transformational leadership management action can influence both of them (Cavallari, 2011), while Khan and AlShare (2019) studied the distinguishing factors between violators and non-violators of information security measures in organizations (Khan and AlShare, 2019). Kennedy (2016) explored the pathway to security by mitigating user negligence (Kennedy, 2016), as Sandhu et al. identified, on the other hand, the proliferation of malicious edge devices in fog computing environments, finding their ways into organisational disfunctionalities (Sandhu et al., 2017).

Human factors play a vital role in creating vulnerabilities, with complex factors influencing employees' adherence to information security policies (ISP). We find strong evidence of the mention humans factor importance several published research. Ifinedo in 2023 explored personal and environmental factors that can reduce "nonmalicious information security violations". The study pertains unintentional information security violations acted by employees that pose companies at risk. The study aimed at understanding how personal and environmental elements influence the likelihood of such violations among a set of professionals. Results revealed that personal goal setting, organizational commitment, and vicarious learning lessened the intent to commit "nonmalicious information security violations" (Ifinedo, 2023). Dewies et al. (2021) studied the effectiveness of indirect actions in information security when attitudes are unsupportive. They undertook a field experiment and a survey to assess the impact of indirect intervention aimed at influencing people's behavior in a predictable way, without forbidding any options aimed at boosting compliance.

The analysis found these actions as ineffective. The study suggests that the action of indirect intervention failed partly due to unaltered attitudes toward the policy and some employee resistance (Dewies et al., 2021; Donalds and Barclay, 2022). Kim et al. (2020) investigated the deterrent effects of punishment and training on insider security threats through a field experiment. The study evaluated the practical effectiveness of information security training and how individual roles within organizations influence its success.

Using a field experiment and simulated phishing attacks, the research measured the deterrent power of both punitive actions and educational interventions. The findings revealed that punishment

successfully stopped individuals from repeating the mistake, while training significantly reduced the likelihood of falling for phishing schemes. Notably, those in higher organizational positions were more vulnerable to phishing, a trend that remained consistent regardless of training or punishment. (Kim et al., 2020). In the same wave other authors have argued about the various effects of the deterrence on employees finding that employees are more prone to adhere to norms and compliance regulations when the recognition for positive behaviors is clear and attractive, rather then the specification of punishment for violations (Alyami et al., 2020; Cavallari, 2011; Posey et al., 2011).

Research also indicates results in the direction of investigating acts that may be intention-based, willful, malicious violation (such as sabotage, data theft, data destruction, etc.) or they may be unintentional or accidental actions (Warkentin and Willison, 2009), while recent studies confirm that the influence of self-efficacy in information security (SEIS) on end user's information security behavior plays a major role (Botong et al., 2023), as also confirmed from other authors (Caldwell, 2012; Ullah Khan et al., 2019; Yang et al., 2019). Other lines of research by Siponen and Vance (2014) argue that there are five crucial aspects to be met while assessing the case of organizations' information policy violations.

Authors state that participants must be made aware that the action under scrutiny contravenes an Information Security Plan (ISP). They explain that this first point is too often overlooked. The second aspect is that researchers targeting intentional breaches of ISPs by employees should gauge concrete instances of such violations. The third suggestion is that scholarly research, when focusing on deliberate infringements of ISPs by employees, should ascertain that the types of violations examined bear practical significance and relevance. The fourth relevance factor in research tools employed (by researchers as well as company managers) to describe ISP violations is what they must be contextually appropriate to the organization under study. Their analysis reveals that the majority of existing works in Information Systems security behavior literature fulfill two or fewer of these mentioned criteria (Siponen and Vance, 2014). Similar ideas are expressed by Alaska et al. (2015) and also expressed by Boss et al. in previous research findings (Boss et al., 2009).

Recent scholarly investigations contend that the integration of comment and user data mining, alongside risk assessment, as well as the utilization of social network visualization techniques for flagging risks, can collectively generate synergistic effects that enhance contributions to cyber-threat intelligence (Cascavilla et al., 2018).

Authors like Kennedy (2016) emphasizes the importance of training and employee education, asserting that through such initiatives, user negligence can be substantially reduced and managed. This, in turn, leads to more effective implementation of the Information Security Plan (ISP) across the entirety of organizations; in the same sense, Yoon and Kim (2013) and Cheng et al. (2013).

On the one other hand researchers has pointed out the importance of identifying major breach types and of providing thorough analysis for each type of breach. They argue also that organisations (in USA) differ regarding their exposure to these breaches, as well as the level of severity, observing that some organizations may succumb to the attacks while others will resist more complex attacks. The researchers propose theoretical insights aimed at enhancing our comprehension of the various kinds of attacks that organizations may encounter. Additionally, they seek to evaluate the underlying factors that account for the variations in the nature of attacks experienced across different organizations (Posey et al., 2017).

With respect to enforcing ISP compliance rules Vance et al. (2013) studied access policy violations and consequent organisational actions. While investigating on the issue of access policy violations, the researchers argue that the implementation of accountability structures significantly curtails the propensity to engage in such violations. These findings recommend practical design interventions that can be seamlessly implemented with limited repercussions on employees within the organization.

An interesting study direction pursued by many scholars points to the deterrence and the moral level of employees ethics with respect to compliance adherence. Chen et al. (2019) have suggested a model rooted in the awareness-motivation-capability construct, targeting the integration of

determinants that influence an employee's inclination to adhere to an Information Security Plan (ISP). The authors argue that a nuanced strategy for managing ISP compliance among employees can lead to optimal outcomes, "This study is a systematic attempt to integrate various theories to form a broad view of employee security policy compliance" (*supra*).

Alternative perspectives on the same topic draw upon diverse academic fields such as Information Systems (IS) adoption, protection-motivation theory, deterrence theory, and organizational behavior. The study of Herath and Rao (2009a) is underpinned by the foundational belief that the uptake of information security practices and policies is influenced by a confluence of organizational, environmental, and behavioral elements.

Similar conclusions are drawn by recent research on information security behaviour by Ali et al., (2021). The authors point out that the existing body of research on Information Security Plans and compliance predominantly centers on behaviors that align with compliance rather than those that diverge from it. Factors like conflicting values, the emergence of security-related stress, and neutralization strategies contribute meaningful insights into the phenomenon of noncompliance. Simultaneously, internal and external motivators, along with protective incentives, exhibit a notably positive influence on compliant behaviors.

Employees are swayed by internal and external motivators rooted in their own value systems, managerial exemplars, and the overall organizational ethos to adopt practices that are security-conscious. The authors maintain that strategies of deterrence, managerial conduct, cultural elements, and heightened awareness about information security are instrumental in shifting the behavioral patterns of employees from noncompliance to compliance. Lowry et al. in 2017 had already drew the same conclusions, even though starting from a different point. Their research dug deep into the very central role of information security and its core characteristics to determine, among other focuses, the impact of positive action on employees' behaviour (Lowry et al., 2017).

In a similar direction, the academic work of Myyry et al. (2013) investigates the impact of ethical and moral reasoning on adherence to information security protocols. The empirical results from their study support the proposed model, highlighting the significant role that ethical reasoning plays in shaping employee behavior with respect to information security practices.

A different approach is proposed by Niemimaa and Niemimaa (2017) where the authors start from the observation that limited research exists on how organizations effectively transition from idealized best practices in information security to practices that are embedded in their specific contexts. In their study, the authors leverage practice theory, incorporating ideas of canonical and non-canonical practices to dissect this translation mechanism. They discovered that the translation process encountered difficulties such as misaligned practices, limited comprehension of employee activities, and information security managers' detachment from organizational practices. Conversely, they concluded that permitting context-specific practices to influence the information security policy, as well as actively involving employees in reshaping these situated practices, has a favorable impact on the successful translation.

Central to this complexity is personal attitudes, which determine employees' motivation to comply with ISPs as in Ajzen and Fishbein (1980). These attitudes shape individual behaviors and are connected with perceptions, beliefs, and emotions regarding the possible outcomes of actions aligned or misaligned with security protocols as previous research had positively demonstrated (Fishbein and Ajzen, 1975; Ajzen, 1991; Ajzen and Albarracin, 2007).

Attitudes serve as the crucial point in deciding to follow or defy security measures, reflecting a mix of cognitive, emotional, and rational elements (Agarwal and Karahanna, 2000; Fishbein, 2007).

Positive attitudes may come from recognizing the benefits of adherence, while negative ones could arise from viewing the measures as inconvenient or irrelevant as argued in recent research findings from Motaung and Sifolo (2023).

These attitudes are significantly shaped by organizational culture. A culture that sees security as a collective priority often fosters positive attitudes and a compliance-friendly environment as in Kacmar et al. (2009).

Personal attitudes are key within the multifaceted realm of employee behavior concerning ISP compliance as argued by Barron et al. (2016) and by Lyman et al. (2019). Recognizing their power enables organizations to foster a culture where security is essential for both individual and collective well-being, increasing the likelihood of compliance (Bondarouk and Sikkel, 2005; Ni and Sun, 2009; Argote and Miron-Spektor, 2011).

Recent research also highlights the risks from employees' negligence, identifying it as a key channel for security breaches (Hagger et al., 2022). The role of attitudes in shaping this landscape is significant, with empirical studies showing that positive views of ISPs lead to reduced non-compliance, emphasizing the role of individual attitudes in shaping security behaviors as recent research findings suggest (Iniesta, 2023).

Expanding the discourse, another layer of importance surfaces, focusing on the efficacy of policies formulated to guide organizational behavior. Policies rendered ineffective, often remaining confined to the realm of theoretical documentation without translating into actionable strategies, introduce a critical component that contributes to the discord between policy intention and operational reality (Devi al., 2023). This discord frequently paves the way for employee apathy towards security norms (Hagger et al., 2022). Within this context, instances of employee negligence manifest, further exacerbated by unreported breaches in compliance. This cyclic pattern underscores the interaction between inadequately enforced policies, lackluster implementation, and employee actions, culminating in an ecosystem where security measures remain ineffective and instances of non-compliance go unnoticed (Alshwayat et al., 2021).

The essence of the issue lies within the complex network of relationships that form the foundation of security compliance within organizational structures. Employee attitudes, shaped by their views on ISP as facilitators or hindrances to operational efficiency, stand out as a crucial factor impacting the dynamics of security behavior as clearly stated by Argote and Miron-Spektor (2011). Recognizing that a positive stance toward security protocols can restrict non-compliance emphasizes the need to cultivate an atmosphere where security is deeply embedded in the organizational culture (Büschgens et al., 2013).

Simultaneously, the disconnection between policy conceptualization and practical implementation assumes critical importance, serving as a notable source of non-compliance. Policies relegated to mere theoretical constructs, bereft of comprehensive implementation strategies, lack the potency to command the requisite attention and adherence. This disconnection fosters an environment where employees tend to disregard security protocols, cultivating a sense of complacency that fuels non-compliant behaviors (Ali et al., 2021). Recognizing that this dissonance not only compromises security protocols but also contributes to breaches underscores the urgency of bridging the divide between policy design and execution (Costa et al., 2013; Donner, 2023).

The discussion pertyaining non-compliant actions in the context of organizational information security calls for careful examination (Tejay and Mohammed, 2023). Employee negligence surfaces as a pertinent concern, with attitudes significantly influencing the prevalence of non-compliance incidents (*supra*).

Additionally, the gap between policy creation and its real-world implementation highlights a crucial point at which policy shortcomings contribute to non-compliance. A comprehensive approach to these issues is essential for organizations aiming to construct a solid security infrastructure. This not only involves crafting policies that garner adequate respect but also demands a steadfast dedication to their successful implementation, thereby reducing the probability of security lapses and associated risks, as suggested by Alhogail (2015).

In academic discussions, there's a belief that many organizations face difficulties in consistently enforcing security compliance due to the complex nature of related rules and policies (Büschgens et al., 2013; Siponen and Vance, 2014; Malte Dewies et al., 2021). These vital components, intended to protect information systems, often seem too complex for employees (*supra*).

This complexity leads to implementation challenges. Organizations often fail to consistently enforce security measures, revealing leniency in managing and governing these policies as in Donner

(2023). As a result, employees may become lax in adherence, knowing the rules aren't rigorously enforced. Furthermore, employees might attempt to sidestep penalties due to these perceived policy leniencies. Such a situation creates a paradox where policies designed for security inadvertently allow non-compliance (Alhogail, 2015; Tejay and Mohammed, 2023).

The dynamics highlight the challenges posed by the nuanced nature of security regulations, their enforcement, and their impact on organizational efficiency. The detailed security guidelines, combined with lenient enforcement, allow for potential employee negligence, diminishing the policies' effectiveness (Chang and Lin, 2007; Xue et al., 2023).

It's essential for organizations to ensure policies are both understandable and strictly enforced. Clear communication of security guidelines and stronger commitment to their enforcement can lead to a collective effort in compliance. Addressing these challenges will help organizations maintain a robust security posture that's comprehensible and consistently followed (Chen et al., 2015).

In academic literature, it's also argued that many employees are unaware of their organizations' security and compliance policies, indicating a widespread knowledge gap (Chang and Lin, 2007; Alshwayat et al., 2021). These policies, so important for information protection and regulation adherence, lose effectiveness if employees are uninformed (*supra*; Da Veiga and Martins, 2015).

Several factors exacerbate this problem. Poor communication might leave policies unnoticed. Insufficient training sessions can leave employees unprepared to follow intricate security protocols. Additionally, the sheer number of policies can confuse employees about which ones are relevant to their roles, Vroom and Von Solms (2004), Cavallari (2010), Knapp et al. (2006), Alhogail and Mirza (2014).

Academic debates also suggest that many organizations struggle to enforce security compliance consistently due to the complexity of related rules and policies. Despite being essential for protecting information systems, these policies often overwhelm employees. Organizations' lenient enforcement causes employees to be relaxed in adherence, creating a paradox where security guidelines may unintentionally foster non-compliance. These nuances underscore the tension between security regulations and organizational efficiency. It's crucial that organizations communicate these policies clearly and enforce them rigorously to foster a culture of compliance (*supra*). Furthermore, a prevalent issue is that many employees remain unaware of their organization's security policies (Martins and Eloff, 2002; Nwankpa and Datta, 2023). This knowledge gap, often exacerbated by inadequate communication and training, reduces the efficacy of essential security measures, leaving room for potential vulnerabilities (Mady et al., 2023; Dornheim and Zarnekow, 2023).

## 4. The Research Questions

Interesting revelations concerning Compliance and ISP underscore the leading meaning attributed to the "sense of security" perception, as in Rocha Flores and Ekstedt (2016). This intriguing assertion posits that the multifaceted interplay between subjective perception and personal contemplation supersedes the tangible benchmarks of technical implementation Alhogail (2015) and Chang and Lin (2007). This realisation underscores the profound impact of cognitive and perceptual dimensions on the landscape of compliance within organizations Ifinedo (2014).

Aligned with these assertions, the research focuses from the conventional emphasis on technical complexity to the realm of Compliance behaviour Yoon and Kim (2013), Bosnjak et al. (2020). The aim is to delve into the multifaceted facets associated with employees' perceptions of security and ISP, recognising their substantial implications for compliance dynamics and the broader organisational alignment with security protocols Niemimaa and Niemimaa (2017), Dornheim and Zarnekow (2023).

The present research endeavour is dedicated to unearthing concealed and less evident dimensions encapsulated within the domain of Compliance and ISP. This quest is steered by a suite of five Research Questions (R.Q.), serving as foundational guideposts directing the trajectory of the subsequent scholarly argumentation:

R.Q.1 Does Compliance function as an intrinsic component of the organisational culture?

This inquiry probes the role of Compliance within the cultural fabric of an organisation. It seeks to unravel whether Compliance is perceived as a deeply ingrained value or merely a superficial policy.

R.Q.2 To what extent does personal attitude influence the attainment of Compliance?

This question explores the intricate nexus between individual attitudes and the pursuit of Compliance. It investigates whether personal dispositions play a defining role in motivating employees to adhere to security protocols.

R.Q.3 How is the perception shaped regarding the actors responsible for enforcing Compliance with ISP?

This query delves into the perceptions surrounding the key players tasked with enforcing Compliance with Information Security Policies. It examines whether employees associate enforcement with specific organisational roles.

R.Q.4 Is there a discernible disparity in viewpoints between employees and managers concerning Compliance and ISP?

This question explores potential variations in perspectives between employees and managerial echelons. It aims to uncover whether divergent viewpoints exist, shedding light on potential gaps in organisational understanding.

R.Q.5 What underpins the foundational motivation for compliant behaviour?

This inquiry delves into the core motivations that drive individuals to exhibit compliant behaviour. It seeks to elucidate the underlying factors influencing the conscious alignment with security protocols.

To unravel these R.Q.s, the research adopts an approach that factors in the perceptions of both employees and managers regarding Compliance and ISP [64-66]. Additionally, it takes into account personal conceptions about the essence of Compliance and the paramount roles vested with enforcing Compliance and ISP, Bosnjak et al. (2020), Alshwayat et al. (2021), Mady et al. (2023).

This strategic selection of Research Questions is congruent with the findings derived from existing literature and robust theoretical formulations Herath and Rao (2009a), Herath and Rao (2009b), Cavallari (2011), Vance et al. (2013), Khan and AlShare (2019), Costa et al. (2013), Dornheim and Zarnekow (2023), Mady et al. (2023).

By aligning with these established findings, the research seeks to contribute to the ongoing scholarly discourse by extending the scope of understanding surrounding the complicated interlink between Compliance, ISP, and the elaborated and often subtle interplay of perceptions and motivations within organisational contexts.

## 5. The Model and the Hypotheses

The research model proposed in this study, serving as its fundamental underpinning, arises from the synthesis of diverse existing formulations, Bosnjak et al. (2020), Niemimaa and Niemimaa (2017), Knapp et al., 2006. This amalgamation draws upon a rich field of scholarly insights derived from a variety of academic contributions. It is imperative to acknowledge that the construction of this research model does not occur in isolation but rather serves as a continuation of the ongoing academic discourse concerning the detailed contours of Compliance with ISP.

By harmonising with established formulations, the present research model signifies a cohesive amalgamation of insights culled from various scholarly investigations. This integration of perspectives seeks to offer a integrated framework through which the intricate dimensions of culture, attitudes, actors, intention, and motivation can be comprehensively grasped within the context of Compliance with ISP.

To address the R.Q.s above, five constructs were identified as instruments to guide the analytical results of the envisaged, successive, empirical investigation: Organizational Culture (ORC); Personal Attitude (ATT); Actors (ACT); Intention (INT); Motivation (MOT).

### *5.1 Construct ORC.*

In the context of this study, the construct of Organizational Culture (abbreviated as ORC) serves as a critical area of inquiry and is examined through a socio-technical perspective, as noted by Van Thuan and Hai in their 2024 research. The framework investigates the intricate dimensions of organizational culture, specifically focusing on how employees' belief systems influence their attitudes towards the value of information security and the crucial role that compliance plays in strengthening security measures—insights that are supported by the works of Alhogail and Mirza (2014), as well as Chang and Lin (2007).

The ORC construct conducts a nuanced examination of several key elements that directly impact both information security and compliance within organizational settings. One such element is the emphasis on the conviction among employees regarding the indispensability of information security for the overall well-being of the organization. This sense of collective conviction nurtures a culture of shared responsibility, a point articulated by Rocha Flores and Ekstedt in 2016. Additionally, the ORC construct accentuates the perspective that mechanisms of compliance serve as effective tools for the enforcement of security protocols. This viewpoint incorporates the notion that the prospect of repercussions for non-compliance buttresses the significance of adhering to instituted security measures, an idea supported by King et al. in their 2023 study.

Furthermore, the ORC framework integrates considerations about the general awareness of Information Security (IS) threats. Such awareness is posited to encourage a more proactive approach to compliance, as suggested by Myyry et al. (2013) and Xue et al. (2023). It also assesses whether compliance is perceived as a rewarding endeavor, thereby motivating active employee engagement. Moreover, the construct probes the extent to which compliance is considered a foundational principle, permeating various departments and roles within the organization, thereby amplifying its significance as a collective enterprise.

At its core, the ORC construct is rooted in scholarly literature that delineates the linkages between individual beliefs and the behaviors that ensue from them. Therefore, the ORC serves as an encompassing framework that encapsulates various employee beliefs and behaviors relating to information security and compliance. In doing so, it enriches the larger academic conversation about the interplay between organizational culture, individual perceptions, and behavioral outcomes in the realm of compliance. This is supported by further academic contributions from researchers such as Ifinedo (2014) and Bosnjak (2020).

### *5.2 Construct ATT.*

The further examination of employees' Personal Attitudes (abbreviated as ATT) situates itself within the esteemed theoretical bounds of the Theory of Planned Behavior. This foundational construct, first delineated by leading scholars such as Ajzen and Fishbein (1980), Fishbein and Ajzen (1975), and subsequently refined by Ajzen (1991), Ajzen and Albarracin (2007), and Fishbein (2007), serves as the intellectual scaffold for the study. Within this theoretical base, attitudes are not treated as a monolithic entity; rather, they are disentangled into two fundamental categories: technological drivers and behavioral motivators. This nuanced classification provides fertile ground for understanding the complex dialectic between contextually shaped attitudes and deep-seated psychological dispositions, as elaborated by Barbera and Ajzen (2020).

Serving as an architectural cornerstone of this theoretical paradigm is the influence of Information Technology (IT) Leadership. This becomes especially discernible when the organization's strategic initiatives find an inadvertent but harmonious correspondence with the objectives outlined in its Information Security Plan. Academic contributions by Lebek et al. (2014), Koohang et al. (2020), and Lee et al. (2023) support this statement. As an example, we consider the operational context of Enterprise Resource Planner (ERP) frameworks. In such settings, procedural guidance often converges with the behavioral expectations stipulated in pre-existing security plans, an empirical

reality acknowledged by scholars like Fazlollahi et al. (2013) and Popa (2016) in their clear scholarly works.

These examples powerfully show how a mutually beneficial relationship exists: the focus of IT leadership in optimizing processes is intrinsically linked with the institutionally mandated prerogatives of information security Lee et al. (2023). This relationship is mediated and modulated by individual belief systems that find themselves hemmed in or liberated by technological capabilities and limitations, ask suggested by Hess and Sciuk (2023). Such interactions significantly shape resultant behaviors, an argument convincingly articulated in academic discourse, most notably by Balozian and Leidner (2017).

The grand significance of IT leadership becomes clear when processes display inherent flexibility and adaptability. Under such circumstances, where compliance is no longer a discretionary activity but a non-negotiable imperative, the directing influence of IT leadership is accentuated, as in Rodríguez-González et al. (2023). It serves as the navigational compass that steers organizational behaviors towards a trajectory aligned with security norms and regulatory benchmarks. This particular aspect has been incisively analyzed in contemporary academic discussions, notably in the works of Bendig et al. (2022) and Hess and Sciuk (2023).

The multi-dimensional framework presented here captures the complex, multi-layered interactions between personal attitudes, organizational leadership in IT, and the emergence of compliance-oriented behaviors, Cuzuara (2023), Kang et al. (2023).

The proposed construct ATT places a renewed emphasis on the influence of IT leadership in engendering behavioral conformity with security best practices, particularly when organizational processes are receptive to adaptation and change.

### 5.3 *Construct ACT.*

The (organisational) Actors construct effort—hereafter referred to as ACT — engages in an investigation into the perceptual frameworks of key personnel who are instrumental in enforcing Compliance with Information Security Policies (ISP). The construct contributes to shed light int the dynamics that inform, influence, and perpetuate the commitment to adherence to ISP policies, Nielsen et al. (2023). Unlike generic approaches that may overlook the role of individual actors within the organizational structure, the ACT construct underscores the important role played by distinct members of the organization, especially managerial staff, Hong et al. (2023).

Delving deeper into the specificities, the ACT construct acknowledges that a thorough understanding of ISP compliance cannot be disentangled from the functional roles individuals assume within an organization. These roles, which include but are not limited to managers and employees, serve as connections where ideological commitments to ISP compliance are actualized or compromised Barbera and Ajzen (2020). The conceptual architecture of ACT is rooted in extant academic contributions, including works by Alshaikh et al. (2018, 2020), and Nielsen et al. (2023), that exemplify the interconnectedness between individual actors and policy adherence.

The ACT construct enriches the discourse by affirming the constituent elements of human perception and their role in fortifying or undermining ISP compliance, as outlined in Herath and Rao (2009a). It seeks to advance a more holistic understanding of the organizational mechanisms and individual behaviors that coalesce to either sustain or disrupt the architecture of information security within a professional setting.

Within the architecture of this research's framework of constructs, the Actors Construct (ACT) is specifically engineered to untangle the complex attitudes and beliefs held by key individuals within organizations. These individuals are those who manage substantial influence in driving and shaping compliance initiatives, particularly with respect to Information Security Policies (ISP).

The ACT construct is attentive to the organizational hierarchy, appreciating that one's positional status within the organizational landscape inevitably molds a unique vantage point on matters related to ISP. Such individualized perspectives are not simply role-dependent, but are

further enhanced by a variety of factors such as organizational culture, job functions, and even individual psychological traits, thus ACT is an essential construct to evaluate the organisational effect of Actors involved in enforcing ISP, Alec Cram et al. (2019).

To establish this understanding, the ACT construct draws deeply upon a rich literature of academic scholarship, including, but not limited to, the works of Bulgurcu et al. (2010), Chatterjee et al. (2015), and da Veiga et al. (2020). Each of these scholarly contributions enriches the construct's multidimensional approach, providing both theoretical and empirical layers to this inquiry.

Thus, ACT serves as a powerful analytical instrument. Through ACT, the differing viewpoints of managers and employees on ISP are revealed. It underscores the significance of potential comprehension gaps in ISP enforcement, highlighting the need for a detailed approach to consistent compliance measures, Herath and Rao (2009b), Cerasoli and Ford (2014), Chiu (2018).

### *5.4 Construct INT.*

The Intention (INT) construct describes the dynamics of how the actions and behaviours of organisational actors influence an individual's compliant intention.

Within the scholarly discourse of this research, the Intention (INT) construct serves as an "investigative tool" for examining the varied aspects of governing the actions and behaviors of organizational actors, specifically as they impact an individual's inclination to comply with established guidelines and norms. This analysis operates within the specific domain of compliance-related Behavioral Intention, that represents an area denoted within this study as Personal Intention (INT).

The concept of Personal Intention, as it stands in this study, resonates deeply with established theoretical frameworks, notably the models put forth by Ajzen (1991), Ajzen and Albarracin (2007). These seminal works provide a foundational understanding of the factors that contribute to forming an individual's intent to act in a certain way, particularly in an organizational setting. Moreover, the construct is contemporized by the recent insights offered by Wright and Wilson (2022), who delve into the mutable nature of intention in the complex reality of organizational interactions.

The INT construct aims at illuminate the interconnections among organizational behaviors, individual predispositions, and the overarching organizational culture (i.e. ORG, *supra*) that collectively shape an individual's propensity to comply. The proposed construct comes from the observation that compliance is not an isolated act but rather a behavioral outcome, shaped by a constellation of influencing variables including role expectations, peer actions, and organizational ethos, Laslo-Roth and Schmidt-Barad (2021), Alsmadi et al. (2022).

The INT construct adds a detailed layer of understanding to the academic discourse on behavioral intention, particularly within the compliance context, as described in Razak et al. (2020). It aims to contribute to both the theoretical and empirical richness of the subject, highlighting the powerful factors that inform and shape individual intentions in an organizational environment, Barton et al. (2016). In doing so, the construct INT enhances our understanding of the dialectics of intention and action, particularly how they manifest in complex organizational ecosystems, Contreras et al. (2017), Mees (2017), Zhang and Hu (2017). In the same sense we find the theoretical roots of our INT construct in the cornerstone research findings of Christman (1977) and of Reeder and Brewer (1979).

This construct intends to explain employees' perceptions concerning organisational measures set in place to harmonise productivity levels with essential Information Security Compliance efforts. At the base of the INT construct lies the pursuit of exploring the knowledge about how the collective endeavors and interactions within an organization mold and shape individual behavioral intentions geared towards compliance, as clearly stated in Warkentin and Mutchler (2022), as well in Duzenci et al. (2023), and defined in the outline of perspective directions for research in Crossler et al. (2013).

The construct INT is designed in order to understand the commitments and the adaptations that employees make to comply to ISP. According to Zemba et al. (2006), these commitments and

adaptations aren't just guided by extrinsic drives, rather they are intrinsic cognitive and behavioral efforts that employees consciously make to align themselves with compliance standards set by the organization, in the same sense we find recent research conclusions by Lee et al. (2023) and also by Ogbanufe and Ge (2023).

The INT construct is not just an academic construct; rather it could be regarded as a tool, a conceptual framework that we can use to dig deeper into this complex web of intentions, actions, and organizational realities. As Diefenbach and Sillince (2011) pointed out, INT allows us to explore the dynamics between individual intentions and the broader context within which these intentions come to life.

The INT construct is representing the baseline of employees attitudes entangled into Information Security (IS) Compliance programs. According to Cerasoli et al. (2014), these programs don't just set rules; they shape attitudes. They can effectively mold employees' mindsets and make them more inclined to consistently adhere to regulatory compliance measures.

As intentions translate into actual behavior, as grounded in established research, like in Fishbein and Ajzen (1975), and also argued by Lian et al. (2012), past research demonstrated that there is a strong correlation between what people say they'll do—self-reported behavioral intentions—and their steadfast adherence to specific security protocols, Yoon and Kim (2013), Li et al. (2022). So, when an employee says they're committed to following the rules, there's a good chance they mean it, Hong et al. (2023).

This proves the strong empirical investigation potential and proof of concept of the construct INT of the present paper.

### 5.5 *Construct MOT.*

The Motivation Construct, termed as MOT, is build in order to examine the relationship between an organization's security measures and its governance mechanisms for compliance. While security objectives frequently occupy a primacy in organizational priorities, their materialization becomes markedly salient when framed within a compliance schema, as articulated by Chiu (2018).

Such alignment has ramifications that reverberate across the organizational hierarchy and functions. This phenomenon is aptly captured by scholar works such as those by Cerasoli et al. (2014) and Herath and Rao (2009b), which suggest that a shared vision captures collective commitment to achieving overarching goals. The MOT construct thus serves as a heuristic device to scrutinize the underlying motivations that predict compliance behaviors and elucidate how they are complexly linked to greater organizational objectives.

The construct MOT supply a framework for decoding not merely the motivations but also the contextual enablers and inhibitors that manifest in individual and collective actions aimed at security compliance. By doing so, it contributes to a more in depth understanding of the organizational compliance and security paradigms.

The conceptual underpinning of the Motivation Construct posits that when there exists a cogent alignment between compliance endeavors and security objectives, a potent catalyst for motivation emerges within the organizational structure, as noted by Meso et al. (2013). This motivational catalyst is deeply interdependent from the organizational culture, engendering a collective cognizance and valuation of compliance, as delineated by Bauer and Bernroider (2015). Consequently, organizational members exhibit an augmented propensity for steadfast adherence to compliance protocols, a point emphasized by Sharma and Aparicio (2022).

Incorporated into the elements of the Motivation construct (MOT) is the salient feature of monitoring as an enhancer of motivational impetus. This dimension postulates that awareness of ongoing surveillance serves as a catalyst for behavior congruent with organizational norms and directives, as validated by Hina et al. (2019). Existing scholarly work and empirical analyses corroborate the hypothesis that the extent and rigor of monitoring procedures exert a considerable impact on individual predispositions, which, in turn, modulate compliance behaviors, as

substantiated by Qatawneh (2023).

Expanding the focus of the MOT construct, it permits the conduction of the exploration at the connection between security objectives and compliance methodologies, bringing scholarly attention to these intersections as documented by Sulaiman et al. (2022). By foregrounding the multifaceted roles that motivation plays in shaping behavioral outcomes, the construct offers a more sophisticated understanding of the mechanisms through which organizational interventions and managerial orchestrations geared towards enhancing employee motivation can galvanize collective adherence to prescribed security frameworks, as suggested in Ballet et al. (2011) and, more recently confirmed by Mathiassen et al. (2023), and by Klemsdal and Wittusen (2023).

The MOT construct serves as a conceptual tool for dissecting the relationships among monitoring, motivational vectors, and compliance actions, thereby providing academically grounded insights into the optimization of organizational security strategies. It will also be able to contribute as an eventual empirical research instrument, in the possible future.

## 6. The Proposed Model

The proposed research model achieves great depth by integrating various facets like managers' behaviour, isomorphism, variances in managers and employees' reactions, compliance incentives, and perceptions of information security risks (Razak et al. (2020).

Managerial actions, as key influencers, introduce unique elements into the compliance arena, impacting both the organisational culture and individual behaviour. Their directive and norm-establishing behaviours create a dynamic interaction, leaving a strong managerial mark on the overall structure, Li et al. (2022), Liu et al. (2022), Chiniah and Ghannoo (2023).

Isomorphism, as a key concept, adds depth to the model. It illustrates the synchronisation between external industry standards and internal compliance mechanisms, shaping the constructs of organisational culture, individual roles, and personal attitudes. This reveals a complex matrix of forces impacting compliance behaviour, Zhang and Hu (2017), Ganga Contreras et al. (2017).

The model's depth is further enhanced by highlighting the contrasting perspectives between managers and employees. Such differences shed light on the roles of power dynamics, hierarchy, and varying perceptions of compliance, Lean et al. (2012), Cavallari and Tornieri (2018) Laslo-Roth and Schmidt-Barad (2021), Fruhen et al. (2022), Qatawneh (2023).

Incorporating the role of compliance rewards and perceptions of information security risks further elevates the model's depth. They intertwine with constructs of motivation, individual attitudes, and organizational culture, bridging the gap between compliance incentives and potential security threats, Li et al. (2022), Chiniah and Ghannoo (2023).

We argue that the enhanced research model benefits from including aspects like managerial behaviours, isomorphism, response variations, and compliance incentives. By assimilating these, the model offers a comprehensive view of the dynamics governing compliance behaviour, showcasing the intricate relationship between organisational processes, external standards, managerial influence, individual perceptions, and motivational elements, Hina et al. (2019), Mathiassen et al. (2023).

Embedded within the overarching research framework, the salient role of managers' behavior emerges as a substantial stratum of influence, intricately interweaving with the constructs of organizational culture and individuals as actors. Managers, occupying a dominant position in the organizational hierarchy, manifest as primary agents wielding substantial agency in the orchestration of compliance behavior's trajectory within the organizational context. Their actions, stances, and enforcement strategies collectively constitute a potent fulcrum that has the capacity to decisively shape the prevailing compliance comportment within the organizational tapestry, Myyry et al. (2013), Da Veiga and Martins (2015), Alskar et al. (2015), Bora Kim (2020), Razak et al. (2020).

The presence of managers as instrumental leaders instills a discernible resonance that extends beyond their immediate roles. Managers, emblematic of organizational authority and directive prowess, wield the capacity to wield substantial influence, rendering them agents of considerable

pertinence in the calibration of compliance behavior, as clearly pointed out by Ryutov (2023). Their actions reverberate through the organizational managers, conveying the tone and tenor that underscores the primacy of compliance. The attitudes expressed by managers, whether by design or by default, condition the broader cultural environment with a distinctive compliance *ethos* that goes beyond formalized policies and extends into the space of normative expectations, as in Kacmar et al. (2009), Ifinedo (2014), Razak et al. (2020).

In addition, the array of enforcement mechanisms harnessed by managers engenders a palpable imprint within the organizational culture, extending tendrils of influence that intermingle with the constructs of individuals as actors and the prevailing cultural landscape, Demjaha et al. (2020), Blythe et al. (2019), Briggs et al. (2017). Managers' strategies, delineating both incentives and punishments, wield the potential to subtly sculpt employees' personal attitudes, underscoring the interplay between external stimuli and internal convictions, Caulfield and Pym (2015). This complex configuration of incentives and deterrents constructs an organizational environment where compliance resonates as a central motif, Alsmadi et al. (2022).

Within this labyrinthine management, the dynamic linkage that emerges cogently underscores the nuanced modes through which managerial conduct resonates through the compliance framework. The varied interplay between managers' behavior, organizational culture, and individuals as actors underscores the profound interdependence of these constructs, as stated in Fruhen et al. (2022), Ryutov (2023) and in Chiniah and Ghannoo (2023). The influence radiating from managers, infused with the imprints of authority and directive orientation, interlaces with the broader cultural dynamics, cascading into the realm of personal attitudes Mees (2017).

The introduction of managers' behavior as a vital determinant within the research framework bequeaths an enriched understanding of compliance behavior's intricacies. This contextualizes managers as architectonic contributors, and their orchestration of compliance resonates with the broader organizational landscape. The nexus of managerial conduct, cultural dynamics, and individual dispositions operates in a symbiotic symphony, underscoring the indispensability of leadership's influence in the cultivation of compliance behaviour, Crossler et al. (2013), Hong et al. (2023).

The introduction of the principle of isomorphism into the conceptual framework engenders a thought-provoking dimension that expounds on the propensity of organizations to emulate the compliance practices observed amongst their peer entities and competitors, Rasnak et al. (2020), Zhang and Hu (2017), Contreras et al. (2017). This conceptual facet, seamlessly assimilated within the framework, serves as a lens through which the dynamics of conformity to external norms and industry benchmarks come to the forefront, Barton et al. (2016).

This theoretical construction unfurls the relationship between extraneous influences, established industry conventions, and the interwoven substance of organizational culture, precipitating an orchestration of managerial conduct and compliance behavior, Chiu (2018), Cerasoli and Ford (2014), Alsmadi et al. (2022), Zhang and Hu (2017).

The concept of isomorphism materializes as a complex interrelation of influence, illuminating the pathways through which external pressures and industry benchmarks interface with the prevailing organizational culture, thereby inevitably impinging upon the comportment of managers, Alhogail and Mirza (2014), Bareton et al. (2016), Mees (2017), hang and Hu (2017). By delving into the dynamics of isomorphism, the framework underscores the capacity of industry norms and peer practices to exude a gravitational force, effectively aligning organizations' compliance trajectories with that of their counterparts. This alignment, a manifestation of the mimetic forces underpinning isomorphism, echoes across the organizational environment, infusing compliance practices with shared industry characteristics, Alskar (2015), Rocha-Flores and Eksted (2016), Ifinedo (2014), Boznjak et al. (2020), Barbera and Ajzen (2020), Zhang and Hu (2017).

Within the framework's complexity of the present proposed model, the concept of isomorphism weaves its thread through the constituent constructs, namely organizational culture, individuals (as actors), and employees' personal attitudes, Ganga Contreras et al. (2017). This threading illuminates

the profound ways in which external pressures synergize with intrinsic organizational dynamics, amplifying the significance of industry benchmarks and compelling organizations to recalibrate their compliance compasses. By traversing this intricate network of constructs, isomorphism emerges as a dynamic force that harmonizes external and internal determinants, catalyzing a nuanced symphony of influences that converge to shape compliance behavior.

The introduction of the principle of isomorphism into the proposed model serves as a powerful conduit that drives the confluence of external as well as internal pressures, lending itself as an explanatory framework within the present research model. This construct, meticulously integrated during research preparation, accentuates the interplay between industry norms and the organizational culture, offering a comprehensive understanding of how compliance behavior is molded by both external expectations and internal dynamics. The threads of isomorphism traverse the fabric of the research model, depicting the amalgamation of external influences and internal intricacies, culminating in an enriched perspective on the contours of compliance behavior's evolution within the organizational context, Alsmadi et al. (2022), Ganga Contreras et al. (2017).

The evidence of disparities in responses between managerial and employee cohorts constitutes a predominant factor that accentuates the difficult aspects intrinsic to compliance dynamics Reeder and Brewer (1979), Christman (1977), Zemba et al. (2006). The mentioned divergences in responses, resonating with distinctness, engender a notable layer of complexity within the compliance system. This dimension inherently amplifies the varied and sometimes unpredictable nature of compliance behaviors, expounding upon the rapport among key constructs—namely the "Individuals as Actors" framework—coupled with the constructs of "Employees' Personal Attitudes" and "Behavioral Intention".

The differential perspectives and responses observed within the managerial and employee strata epitomize a unique juncture where the hierarchical positioning intersects with compliance-related beliefs, Zemba et al. (2006), Lian et al. (2012). This interjection manifests within the relation between the "Individuals as Actors" construct—where individuals assume roles of consequence within the compliance framework—and the constructs encapsulating "Employees' Personal Attitudes" and "Behavioral Intention". The vantage points occupied by managers and employees furnish divergent viewpoints that reverberate the hierarchical differences that underscore organizational dynamics, Christman (1977), Lian et al. (2012).

These disparities, as mirrored within the constructs, unfold as an embodiment of power dynamics that are diversely interwoven with compliance considerations. The confluence of hierarchical positioning and compliance-related beliefs crystallizes into variances in responses, denoting a spectrum of viewpoints that traverse the organizational hierarchy. This spectrum is indicative of the divergent ways in which compliance mandates are construed, enacted, and navigated within the organizational continuum (*supra)*.

The distinctiveness in responses between managerial and employee responses serves as a significant dimension that renders compliance dynamics multifaceted Lian et al. (2012). This dimension augments the scholarly discourse by spotlighting the multifarious manifestations of power dynamics and their interface with compliance-related cognitions. By illuminating the spectrum of responses that stem from diverse vantage points, the proposed framework underscores the interconnection of perspectives and serves the role of power dynamics in shaping the varied compliance landscape within the organizational environment (*supra*).

The confluence of rewards for compliance and the personal perception of information security subtle risks introduces a dual-faceted lens through which motivation and intention are collectively examined, Cerasoli et al. (2014). This fusion of dimensions engages in a scholarly discourse that not only enriches the existing research framework but also extends our understanding of the particular dynamics governing compliance behaviors. The integration of these dimensions embarks upon a journey that transcends traditional delineations, unveiling novel insights into the complexities of individuals' motivational dispositions and their subsequent behavioral intentions (*supra*).

Rewards, in this academic exploration, evolve into a essential drive that possesses the capacity

to amplify the influence of the motivational construct (*supra*). By resonating with the core tenets of behavioral psychology, rewards emerge as catalysts that consolidate the nexus between personal attitudes and the expression of behavioral intentions, Li and Hoffman (2023), Balliet et al (2011).

This interplay illustrates how external stimuli, in the form of rewards, can bridge the gap between intrinsic dispositions and the desired trajectory of behaviors, thereby augmenting the likelihood of compliance-driven actions, Chiniah and Ghannoo (2023).

At the same time, the perception of information security risks, a domain often characterised by its intangible and complex nature, converges with the constructs of "Employees' Personal Attitudes" and "Individuals as Actors". This link underscores the relationship between cognitive apprehensions and managerial prerogatives, elucidating the manner in which risk perception interacts with personal convictions and the regulatory machinery. This interaction accentuates the anticipatory inclinations of individuals, catalysed by the interaction between risk perceptions and the influential forces within the organisation, Li et al. (2022).

This above mentioned integration underscores the strength of the reward mechanism in leveraging motivational triggers and solidifying behavioral intentions. Concurrently, it sheds light on the intricate dynamics of risk perception, where the interwoven threads of personal attitudes and managerial enactments create a base of anticipatory inclinations. This dual perspective, harmoniously embedded within the proposed model, reframes the discourse on motivation and intention, presenting a sophisticated vantage point that emboldens the comprehension of the multidimensional of the underpinnings of compliance behaviour with respect to Information Security, Balliet et al (2011), Chiniah and Ghannoo (2023), Li et al. (2022), Liu et al. (2022).

The proposed extended research model encapsulates the complex interrelations between organisational culture, personal attitudes, managerial behaviour, isomorphism, differences in responses, rewards for compliance, and the perception of information security risks. This ample web of interactions, spanning multiple constructs, elucidates the multidimensional nature of compliance behavior within the organisational context, Ukobitz and Faullant (2022).

The present model enriches our understanding by navigating the complex relation through which internal and external factors, leadership actions, and employee perspectives converge to mold compliance dynamics, (*supra*).

## 7. Establishing the Scholarly Groundwork

In light of the preceding discourse and the meticulous scrutiny of existing scholarly literature, the scholarly groundwork has been established for the formalization of the envisaged model, as follows, Donalds and Barclay (2022), Kennedy (2016), Lowry et al. (2017), Sandhu et al. (2017), Myyry et al. (2013), Niemimaa and Niemimaa (2017), Argawal and Karahanna (2000), Motaung and Sifolo (2023), Kacmar et al. (2009), Barron et al. (2015), Lyman and Hammond (2019), Bondarouk and Sikkel (2005), Argots and Morin-Spektor (2011), Alshwayat et al. (2021), Costa et al. (2013), Donner (2023), Teejay and Mohammad (2023), Alhogail (2015), Chang and Lin (2007), Chen et al. (2015), Knapp et al. (2006), Alec Cram et al. (2019), Chatterjee et al. (2015), Chiu (2018), Hong et al. (2023), Razak et al. (2020), Barton et al. (2006), Zhang and Hu (2017), Christmann (1977), Zemba et al. (2006), Lian et al. (2012), Diefenbach and Sillince (2011), Cerasoli et al. (2014), Li and Hoffman (2023), Balliet et al (2011), Chiniah and Ghannoo (2023), Li et al. (2022), Liu et al. (2022).

This important step of establishing the scholarly groundwork, encompasses the delineation of the proposed research model, underscoring the interconnections that weave through the organizational variables under scrutiny. Through an integration of theoretical insights and empirical understanding, this formalization accentuates the relationships and complex dependencies that underlie the dynamics of compliance behavior within the organizational environment, Chiniah and Ghannoo (2023), Motaung and Sifolo (2023), Teejay and Mohammad (2023), Li and Hoffman (2023).

The contribution of prior reasoning and comprehensive literature review (*supra*) has permitted a scholarly approach to the landscape of interdependencies among organisational variables and the

proposed constructs. Within this formalized model, the interaction of organizational culture, individual attitudes, managerial behaviors, external influences, and varied perspectives form a complex matrix of relationships. This matrix captures the interdependencies between organisational variables, but also provides a systematic framework to understand the organizational determinants that shape compliance behavior.

This formalized model represents the very deep nature of organizational dynamics, portraying them as a vast scope with the threads of theoretical constructs.

The model's articulation serves as a guide for researchers through the complicate matrix of organizational variables, in the envisaged future empirical research.

## 8. Discussion and Hypotheses

### *8.1 Discussion and scope*

In our discussion, we introduce a refined and elaborated conceptual model, crafted with scrupulous attention to detail, primed for an empirical investigation. This model, a synthesis of profound academic thought, finds its foundation in a harmonized framework.

This framework has been built to facilitate the eventual empirical endorsement of hypotheses which span a spectrum of research paradigms. These hypotheses draw their essence from a rich ground of academic contributions, commencing with foundational works such as Yoon and Kim (2013) and culminating in contemporary insights, notably those by Ryutov (2023). Through this integration of past and present scholarship, our model endeavors to bridge the temporal continuum of research, offering a new perspective while honoring the intellectual legacies that have paved the way.

The research hypotheses stand out as meticulously fashioned pieces. These aren't merely the outcomes of deep academic reflection; they are also the very tools that prepare the ground for an imminent, expansive wave of empirical exploration. Discussing our research findings is serving as guiding lights, while these hypotheses elucidate the trajectory of our academic discussion, poised to function as foundational supports for upcoming empirical undertakings, both by academics as well as from companies and managers. Integrating these hypotheses within our envisioned framework not only fosters their in-depth assessment and validation but also provides a comprehensive lens to discern the complex filed of relationships that characterize the essence of organizational dynamics. Through this synthesis, we endeavor to cultivate a richer comprehension of the vast number of interactions and dynamics at play in organizational studies, with each hypothesis acting as a link of past wisdom and future inquiry.

Supported by the insights of Aurigemma (2013), our conceptual model stands out as a resilient structure designed for future empirical validation, promoting a more profound journey into academic and organizations' reflection. This model provides a lucid view, enhancing the scrutiny of hypotheses by facilitating their rigorous appraisal. Such an evaluative approach sharpens our understanding of the dynamics that influence compliance behaviors in organizational settings. Beyond merely serving as a tool for validation, the model acts as a bridge, connecting theoretical postulations with empirical realities, and offering a deeper dive into the nuances that shape organizational behavior and compliance mechanisms. Through this enriched perspective, we are better equipped to go through and to comprehend the multifaceted aspects governing organizational environment, with respect to compliance and ISP.

The discussion we present is meticulously crafted, reflecting precision and clarity, aiming to pave the way for future empirical investigations. Intertwined with both theoretical insights and the vast landscape of existing scholarly works, hypotheses serve as a strong baseline. Esteemed studies, including those by Myrry et al. (2013), Costa et al. (2013), lend weight and credibility to our discussion's foundational significance. As we delve further into this scholarly literature, our hypotheses draw attention to distinct interrelationships and patterns that are demonstrated from

extant literature and could benefit academic discourse as well as the organisational business field. By positioning these hypotheses as the core of our discussion, we design a structured roadmap for future empirical endeavors, allowing for a deeper exploration of the complex interrelations that exist among current research themes within organizational frameworks.

Emphasizing the rigorous construction of these hypotheses accentuates our steadfast dedication to methodological precision and the unyielding quest for empirical wisdom.

This commitment finds resonance in the contributions of scholars like Gundu (2019), Hu et al. (2012), Aurigemma and Mattson (2017), West (2008), and the insights of Alahmari and Duncan (2020).

*8.2 Hypotheses discussion*

**H1: There is positive relation between organizational culture and the perception of the importance of enforcing ISP.**

The first hypothesis postulates a positive relationship between organizational culture and the perception of the importance of Information Security Policy (ISP). This proposition is grounded in the fundamental notion that an organization's culture exercises a great influence on employees' attitudes, behaviors, and perceptions. Moreover, a strong organizational culture serves as a defining element that shapes the prevailing norms, values, and expectations within the organizational environment, Büschgens et al. (2023).

Organizational culture is a combination of shared beliefs, values, and behaviors that collectively contribute to define the organization's identity. It serves as a powerful reference against which employees evaluate their roles, responsibilities, and the significance of compliance-related efforts. The varied aspects of an organization's culture, while leading to a culture of compliance, explicitly and implicitly communicate the priorities and the expectations that resonate across all levels of the organization, Dhillon et al. (2016).

In this context, the hypothesis stands that a positive relationship exists between organizational culture and the perception of the importance of enforcing ISP. When an organizational culture emphasizes the value of information security, it automatically communicates a commitment and affirming a culture of compliance. Employees who are part of this culture tend to see the ISP implementation as important, shaping their views on cultural elements.

This argument draws support from extant research that has consistently underscored the central role of organizational culture in influencing employees' compliance-related attitudes and behaviors.

When a company's culture really focuses on security, it creates a workplace where security is a natural part of work, not just an afterthought. This kind of organizational culture makes everyone feel responsible for keeping things safe and highlights how crucial it is to follow ISP to protect the company, as mentioned by Davis et al. (2023).

The first hypothesis postulates a coherent and plausible assertion. It stems from the premise that organizational culture serves as a contextual backdrop that influences individuals' perceptions and attitudes, thereby influencing their views on the importance of enforcing ISP. Empirical examination of this hypothesis stands to contribute valuable insights into the intricate nexus between organizational culture and the prominence attributed to enforcing ISP within the organizational setting, Costa et al. (2013), Ifinedo (2014), Bulgurcu et al. (2010), Ryutov (2023).

**H2: There is positive relation between organizational culture and personal attitudes.**

The second hypothesis posits a positive relationship between organizational culture and individuals' personal attitudes towards compliance. This assertion is founded upon the premise that an organization's culture plays a core role in shaping employees' beliefs, values, and perspectives, thereby extending its influence to their attitudes towards compliance-related matters Dhillon et al. (2016).

Organizational culture, as a pervasive force, imbues the workplace with shared norms, values,

and expectations that collectively form the cultural environment. This cultural backdrop often contributes in molding individuals' cognitive frameworks and guides their evaluative thinking when it comes to various aspects of organizational behavior, including compliance. Organizations with strong compliance-oriented cultures tend to instill a sense of duty, responsibility, and adherence to established guidelines within their employees, Moody et al. (2018), Cury (2005), Obganufe and Ge (2023).

Drawing from this foundation, the hypothesis postulates that a positive association exists between organizational culture and personal attitudes towards compliance. When organizational culture places a premium on compliance, it sends a clear signal that adhering to regulations and policies is a priority. Employees enveloped in such a culture internalize these cues, leading to the cultivation of positive attitudes towards compliance, Pattnaik et al. ((2023), Chen et al. (2018). They perceive compliance not merely as an external mandate, but as an integral element of their professional identity within the organizational context.

This proposition aligns with the broader theoretical understanding of organizational socialization and cultural alignment. As employees integrate into an organization, they internalize the prevailing cultural norms and adapt their behaviors to align with these norms. This process extends to compliance-related attitudes, where employees internalize the cultural emphasis on adhering to rules and regulations, thus fostering positive attitudes towards compliance.

Empirical research and scholarly literature furnish support for this hypothesis, revealing that organizational culture significantly impacts employees' attitudes and behaviors, Dewies et al. (2021), Ajzen and Fishbein (1980), Fishbein and Ajzen (1975), Kacmar et al. (2009), Aurigemma and Mattson (2017), Papadaki and Furnell (2010), Cuganesan et al. (2018).

Organizations with compliance-centric cultures tend to experience higher levels of commitment to rules, a sense of ethical obligation, and a proactive approach to meeting regulatory demands, Hu et al. (2012). These facets echo the influence of organisational culture in shaping individual perceptions and attitudes, Azhar et al. (2023).

The second hypothesis stands as a cogent proposition within the proposed model. By anchoring the argument in the theoretical intersections of organisational culture and individual attitudes, this hypothesis offers an avenue for empirical investigation into the interplay between cultural orientations and personal attitudes towards compliance.

**H3: There is an inverse relationship between the organisational culture about Compliance and ISP and the perception of Compliance as simply an administrative tasks.**

The third hypothesis states an inverse relationship between the organizational culture about compliance (ISP) and the perception of compliance as simply administrative tasks. This assertion digs into the relationship between the prevailing organisational culture, which encompasses attitudes and values towards compliance, and the way in which compliance is perceived by employees, Li et al. (2021).

Organisational culture, as a combination of shared values, norms, and behaviors, establishes an important baseline that influence employees' perceptions of various organisational aspects, including the efforts put into compliance. A culture that places a strong emphasis on compliance as a fundamental component of its identity reinforces the significance of adhering to regulations, viewing compliance as a strategic matter rather than a typical bureaucratic tasks, Chen et al. (2021).

In line with the hypothesis, an inverse relationship is stated. When organisations push an environment where compliance is perceived primarily as an administrative task, it potentially reflects a culture that does not prioritise the importance of compliance itself.

Employees operating within such a culture may perceive compliance-related activities as obligatory checkboxes voided of significance.

In contrast, organisational cultures that integrate compliance as a core element of their identity tend to communicate the critical role of following the rules as a means to safeguard the organisation's interests and integrity.

The theoretical foundations of this hypothesis draw from the broader literature on

Organisational Culture, Devi et al. (2023), Alshwaiat et al. (2021), Büschgens et al. (2013), Tejay and Mohammed (2023), Alhogail (2015), Chang and Lin (2007), Chen et al. (2015), da Veiga and Martins (2015), Knapp et al. (2006), Alhogail and Mirza (2014), Rocha-Flores and Ekstedt(2016), da Veiga et al. (2020), Zambia et al. (2006), Hu et al. (2012), Dhillon et al. (2016), Alshaikh (2020); on Compliance Ali et al. (2021), Sulaiman (2022), Alraja et al. (2023), Hina et al. (2019), Donalds and Barclay (2022), Herath and Rao (2009a,b), Ifinedo (2014), Balozian and Leidner (2017), Alec Cram et al. (2019), Li and Hoffman (2023), Ryutov (2023), Aurigemma (2013), Moody et al. (2018), Hong and Furnell (2022), Merhi and Ahluwalia (2023); and on Employee Motivation, Hine et al. (2019), Lee et al. (2023), Chiu (2018), Cerasoli and Ford (2014), Cerasoli et al. (2014), Obganufe (2023), Meso et al. (2013), Bauer and Bernroider (2015).

Empirical support for this hypothesis can be found in studies that investigate the impact of organisational culture on employees' attitudes and behaviours, Chang and Lin (2007), Bulgurcu et al. (2010), Myyry et al. (2013), Meso et al. (2013), Bauer and Bernroider (2015), Yoon and Kim (2013), Costa et al. (2013), Ifinedo (2014), Alzahrani (2021), Ryutov (2023).

Organisational cultures that underscore the strategic significance of compliance have been shown to facilitate greater commitment to regulatory adherence and ethical conduct. On the contrary, cultures that marginalise compliance may inadvertently encourage a perception of it as an administrative obligation.

The third hypothesis can be considered well grounded into theory, presenting an interesting notion to be included into present research and into the academic discourse. By outlining an inverse connection between organisational culture and the perception of compliance as mere administrative duties, this hypothesis contributes to a better understanding of how cultural orientations influence employees' perception of tasks related to compliance.

**H4: There is a positive relationship between the perception of managers' behavior regarding Compliance and the behavioral isomorphism (convergence) of other employees.**

The fourth hypothesis advances the proposition of a positive relationship between the perception of managers' behavior concerning compliance and the behavioral isomorphism, or convergence, among other employees within the organization. This hypothesis delves into the numerous dynamics of managerial conduct and its potential to influence the behavioral alignment of the broader employee base, Laslo-Roth and Schmidt-Barad (2021), Razak et al. (2020), Barton et al. (2016), Mees (2017).

The perception of managers' behavior holds a significant sway over how employees interpret and model their own behaviors, Jensen (2023). Managers, often regarded as exemplars of organizational conduct, serve as influential figures whose actions carry substantial weight. When managers consistently demonstrate compliance-oriented behavior, their actions communicate a tacit endorsement of the organization's values and norms, including those related to compliance Zhang and Hu (2017), Ganga Contreras et al. (2017).

In alignment with the hypothesis, it is postulated that a positive relationship exists between the perception of managers' behavior regarding compliance and the degree of behavioral isomorphism or convergence among other employees. In other words, employees are more likely to emulate the behaviors exhibited by their managers, particularly when those behaviors are perceived as endorsing compliance. This influence extends beyond the simple example and aligns with the theoretical notion of behavioral isomorphism, where individuals adopt similar behaviors due to the perceived legitimacy and efficacy of those behaviors, Sullivan et al. (2023), Sommerstadt et al. (2014), [132].

This argument is grounded in organizational theory, Ajzen (1985), DiMaggio and Powell (1991), Liu et al. (2023), Boxenbaum and Jonsson (2017), Iliya Nyahas et al. (2017) and the established concept of behavioral isomorphism, the proper phenomenon also regarded as institutional isomorphism, as in Bihari and Shajahan (2023), Ahyaruddin et al. (2023), Lai et al. (2006) and in Amoako et al. (2021). The hypothesis draws from the understanding that employees tend to observe and mirror the behaviors of authoritative figures, such as managers, CEOs, directors, in an attempt to navigate their roles and align with organizational expectations and norms. Consequently, when managers exhibit

compliance-centric behavior, employees are more likely to internalize these actions and integrate them into their own conduct, fostering a sense of behavioral isomorphism, Setyorini (2012), Khatib and Barki (2022).

Scholar research supports this hypothesis as it can be observed in studies that explore the influence of managerial behavior on employee conduct and the diffusion of organizational norms Siponene et al. (2022), Merhi et al. (2019), Nasirpouri Shadbad and Biros (2021).

Organizational research has consistently highlighted the role of leadership behavior as a catalyst for shaping employee attitudes and behaviors, Krajnovic (2018). Moreover, studies investigating behavioral isomorphism have underscored how employees' perceptions of managers' behaviors are correlated with their own behavioral emulation, Freeman (2007), Manville and Greatbanks (2023).

We can observe that the robust conceptual framework proves the fourth hypothesis introducing a challenging proposition into the academic discourse, accentuating the principal influence of managerial behavior on shaping organizational behaviors Wulaningrum (2020). By postulating this positive relationship between the perception of managers' compliance-oriented conduct and the behavioral isomorphism among employees, this theoretical hypothesis offers a lens through which the intricate interplay between leadership actions and employee behavior is expounded. Eventual empirical validation of this hypothesis holds the promise of unveiling the complex mechanisms that drive the diffusion of compliance-related behaviors within the organizational environment.

**H5: There is a positive relationship between the organizational role about ISP and compliant behavior.**

The present fifth hypothesis postulates a positive correlation between the organizational role regarding Information Security Policy (ISP) and compliant behavior within the organizational context, Sanson and Courpasson (2022), Leering et al. (2022), Pradhan (2019). This assertion digs deep into the complex interconnection between assigned roles of individuals within the organization and their subsequent adherence to ISP, shedding light on the interaction between organizational expectations and individual actions, as argued in several research studies as, Warkentin and Willison (2009), Alaska et al. (2015), Hagger et al. (2022), Alhogail (2015), Vroom and Von Solms (2004), Lebek et al. (2014), Chatterjee et al. (2015), Obganufe (2023), Alshaikh (2020), Aggarwal and Dhurkari (2023).

The organizational role embodies the responsibilities, duties, and functions assigned to individuals within the organizational structure Khatib and Barki (2020). It serves as a framework that delineates the scope of an individual's professional engagement and the tasks they are expected to perform. This hypothesis centers on the notion that individuals' roles within the organization exert a tangible influence on their behaviors, particularly when it comes to compliance with ISP , Alraja et al. (2023), Lee et al. (2023).

The proposition argues that a positive relationship exists between the organizational role related to ISP and compliant behavior. Individuals occupying roles that explicitly encompass information security responsibilities are more inclined to demonstrate compliant behavior.

This alignment can be attributed to the nature of their roles, which inherently necessitate a heightened awareness of and commitment to ISP, Bansal et al. (2021).

The theoretical foundation of this hypothesis can be traced to the concept of role theory and organisational role expectations, Crosby (1999), Leering et al. (2022), Frank and Kohn (2023), Castilla and Ranganathan (2020). Role theory suggests that individuals adhere to behaviours that are congruent with the roles they occupy, driven by the expectations associated with those roles, Bandura (1977), Bandura (1997), Eccles and Wigfield (2020).

Within an organisational context, this theory implies that individuals fulfilling roles involving ISP-related functions are more likely to exhibit behaviours that align with compliance expectations (*supra*).

Scholarly research support for this hypothesis can be gleaned from studies that investigate the correlation between organisational roles and compliance behaviors, D'Arcy and Lowry (2019), Guhr et al. (2019). Research has shown that individuals who are designated as custodians of information

security, such as IT administrators or compliance officers, tend to exhibit more conscientious and compliant behavior due to the nature of their roles, Celis (2018).

These roles inherently carry a responsibility for safeguarding sensitive data and maintaining information security, which reinforces their adherence to ISP, Obganufe (2023).

The confirmed positive correlation asserted in the fifth hypothesis between the organizational role concerning ISP and compliant behavior, underscores the impact of role expectations on individuals' decisions pertaining one's behavior, Hadasch et al. (2016).

By situating this hypothesis within the theoretical framework of role theory, it elucidates how organizational roles serve as mechanisms that engender compliance behaviors, Sillic (2019), Lockwood and Kunda (1997).

Future empirical exploration of this conceptually confirmed hypothesis stands to contribute valuable insights into the dynamic relationship between organizational roles and compliance conduct, further enriching our understanding of the interaction between individual roles and the broader organizational compliance landscape (*supra*).

**H6: Organizational behavior of managers and executives are perceived as a driving force influencing others to comply with ISP.**

The behavior displayed by managers and executives in the organization is widely perceived as a significant factor that influences others to conform to Information Security Policy (ISP). This assertion highlights the substantial role that leadership behavior plays in shaping the compliance behaviors of the broader workforce and aligning their actions with the stipulated information security guidelines, Chiu (2018), Castilla and Ranganathan (2020), Edge et al. (2023).

Leadership within the organizational context encompasses the conduct, attitudes, and actions exhibited by managers and executives occupying influential positions. Their behavior serves as a visible and influential point of reference for employees across various levels. This proposition emphasizes that the actions of these leaders act as a powerful mechanism that molds the prevailing organizational culture with respect to compliance, effectively communicating the organizational emphasis on information security practices, Topa and Karida (2023).

The fundament of this assertion lies in the recognition that managers and executives are regarded as exemplars whose behaviors extend beyond their immediate functional responsibilities. When these leaders actively embrace and endorse ISP, their actions send a strong message about the organizational value placed on information security. Employees, influenced by their leaders, are more likely to emulate these behaviors, thus leading to the cultivation of a culture where compliance becomes an integral part of the organizational ethos rather than just a requirement, Arellano-Gault and del Castillo (2023).

The theoretical foundations of this assertion can be traced back to theories of leadership and social learning, Hafez et al. (2022), Amir et al. (2022), Keller and Kokkinis (2022), Donalds and Barklay (2022), Alzahrani (2021).

The transformational leadership theory underscores leaders' capacity to inspire and motivate through their behavior, fostering higher commitment and performance levels among employees, Lin (2023). The theory posits that individuals acquire behaviors through observation and imitation of influential figures, such as leaders. Therefore, leaders who consistently display behavior aligned with compliance are more likely to foster a culture where information security practices are ingrained.

Empirical support for this assertion can be found in research that examines the link between leadership behavior and employee compliance. Studies consistently demonstrate that leaders who actively participate in and endorse compliance-related activities tend to create a culture of adherence among their subordinates. Furthermore, the impact of leadership behavior on organizational culture is widely acknowledged, with leadership practices influencing the collective mindset and behaviors of the workforce, Lord et al. (2017), Nani and Safitri (2021).

We can therefore assume that the assertion that the behavior of managers and executives plays in influencing compliance behaviors within an organization. By positioning this assertion within the theoretical frameworks of leadership and social learning, it underscores the crucial connection

between leadership behavior and the establishment of compliance-oriented organizational cultures, Xue et al. (2020). Empirical exploration of this assertion holds the promise of yielding valuable insights into the profound influence of leadership behavior on the compliance landscape and the broader implications for organizational information security practices.

**H7: Responses from managers and executives are different from those of the employees.**

Within the context of Information Security Compliance, a significant phenomenon emerges wherein discernible contrasts in responses manifest between managerial and executive echelons in comparison to those observed among employees. This noteworthy occurrence encapsulates the distinct ways in which individuals occupying different strata within the organizational hierarchy perceive and react to matters entailing compliance in the realm of information security. This dynamic contrast in responses is inherently rooted in the diverse roles, responsibilities, and vantage points that characterise these diverse environment,Detert and Burris (2007).

The dissimilarities in responses between managerial and executive tiers, on one hand, and employees, on the other, are underpinned by the unique functional roles and perspectives that each group occupies within the organizational framework. Managers and executives, occupying positions of leadership, decision-making, and strategic guidance, inherently possess a more panoramic view of compliance considerations in relation to information security. Their responses tend to encompass a broader spectrum of concerns, such as strategic alignment, risk mitigation, and the overarching organizational landscape, Carpenter et al. (2004).

In direct contrast, employees' responses emanate from their operational roles, which tend to be more task-oriented and aligned with the immediate execution of day-to-day functions. This inherent dichotomy in perspectives begets varied attitudes and behavioral tendencies with regards to information security compliance. While managers and executives may prioritize the congruence between compliance efforts and strategic objectives, employees often tend to be more influenced by factors like the practicality of task completion, convenience, and perceived operational efficiency, Mishra and Chakraborty (2021).

This phenomenon is substantiated by empirical investigations that underscore the distinct cognitive frameworks through which managerial and employee groups evaluate compliance-related issues, Chakraborty et al. (2021). Empirical research highlights that managers and executives tend to assess compliance matters from a strategic standpoint, considering their potential impact on factors like the organization's reputation, legal ramifications, and industry benchmarks (*supra*). Conversely, employees' responses are often molded by considerations more closely tied to immediate task execution and the perceived effect of compliance on their day-to-day responsibilities, Mishra and Chakraborty (2021), Chakraborty et al. (2021).

The implications of these discernible responses are far-reaching and possess ramifications for cultivating a robust culture of information security compliance within organizations. Managers and executives, acting as prime catalysts, exert considerable influence in setting compliance expectations and fostering a culture of vigilance, Najrani (2016). Their responses become instrumental in shaping the broader organizational sentiment surrounding compliance. On the other hand, employees, as the operational front-line, contribute significantly to the collective compliance landscape through their day-to-day actions and attitudes.

We can assume, at this point, that the conspicuous divergence in responses witnessed between managerial and executive tiers, and the workforce at large, within the precincts of Information Security Compliance, draws attention to the intricacies that disparate hierarchical levels introduce into compliance dynamics, Cai et al (2023). This interaction between roles, perspectives, and organizational actions accentuates the complex balance that must be maintained when addressing compliance attitudes and behaviors.

The empirical substantiation of this divergence reinforces the need for tailored strategies that take into account the distinctive viewpoints and priorities of different cohorts within the organization, Zhu et al (2023).

**H8: Intention to compliant behavior is positively associated to managers' intention.**

The correlation between the inclination towards compliant behavior and the intentions of managers presents a salient relationship worthy of examination within the domain of organizational dynamics. This assertion underscores the interconnectedness between the willingness to adhere to regulatory norms and the strategic intentions harbored by managerial personnel. This mutual linkage encapsulates a realm of organizational behavior that traverses beyond the individual sphere, warranting scholarly exploration, Egorov et al. (2020).

The assertion posits that an individual's intention to exhibit compliant behavior is favorably aligned with the intentions emanating from managers. This implies that when managers exhibit a proclivity towards adherence to compliance measures, their actions inadvertently contribute to fostering an environment conducive to compliant behavior among their subordinates. In essence, the managers' intentional commitment towards compliance initiatives serves as an influential determinant that influences the subordinates' own intentions to adhere to the stipulated regulations and protocols, Kalshoven and Taylor (2018).

This relationship finds resonance in extant literature on leadership influence and social learning within organizational settings. Research suggests that managerial behavior serves as a prominent source of guidance and emulation for employees, thereby shaping their attitudes and behavioral intentions. When managers prioritize and endorse compliance through their actions, it communicates a strong message regarding the significance accorded to adherence to regulatory frameworks, Pircher Verdorfer and Peus (2020).

Theoretical perspectives such as the Theory of Planned Behavior, underscore the role of intentions in driving behavior, Ajzen and Fishbein (1980), Ajzen (1991), Ajzen and Albarracin (2007), Fishbein and Ajzen (1975). In this context, managers' intentions to comply act as catalysts that can stimulate similar intentions among employees. This alignment of intentions contributes to the establishment of a coherent and synchronized compliance culture within the organizational environment, Azhar et al. (2023).

Empirical support for this assertion can be found in studies that examine the relationship between leadership behaviors and employee compliance, Yoon and Kim (2013). Literature on transformational leadership, ethical leadership, and role modeling affirms that the conduct of managers significantly influences employees' behavioral inclinations. When managers exemplify a commitment to compliance, employees are more likely to mirror these intentions in their own conduct, Sue et al. (2020).

We can then assert that the eighth substantiated proposition, which underscores the positive correlation between the inclination to demonstrate compliant behavior and the intentions of managers, sheds light on a crucial aspect of organizational behavior Den Hartog (2015). This interplay between managerial intentions and employee compliance aspirations underscores the central role that managerial conduct plays in shaping the compliance landscape within organizations. The theoretical underpinnings of this relationship align with established notions of leadership influence and intention-based behavior, further endorsing the significance of managerial intentions in fostering a culture of compliance, Cai et al. (2023), Alzharani (2020).

**H9: Intention to compliant behavior is positively associated to reward for compliant behavior.**

The assertion that a positive linkage exists between the intention to engage in compliant behavior and the availability of rewards for such behavior represents a concept of substantive interest within the realm of organizational behavior and compliance studies, Li and Hoffman (2023), Chiniah and Gannoo (2023), Li et al. (2022), Khatib and Barki (2022), Brooks et al. (2023).

This notion underscores a relationship that revolves around the interplay between an individual's intention to adhere to regulatory norms and the presence of incentives or rewards as potential catalysts for encouraging compliance. This relationship delves into the domain of motivational dynamics and organizational governance, warranting thorough academic examination.

The assertion suggests that individuals who possess an intent to conform to compliance standards can potentially be swayed by the possibility of obtaining rewards for their adherence to

compliant conduct. This implies that the presence of incentives, either in the form of tangible rewards or non-monetary recognition, can significantly impact individuals' intentions to align their actions with established regulatory frameworks. In essence, the anticipation of rewards is postulated to serve as an enhancer that reinforces the intention to exhibit compliant behaviour.

This relationship draws theoretical support from concepts of behavioral motivation and reinforcement theory, Han (2022), Khatib and Barki (2022), Chiniah and Gannoo (2023).

According to reinforcement theory, behaviors that are followed by rewards are more likely to be repeated, Belmondo and Sargis-Roussel (2023). Therefore, the alignment of individuals' compliance intentions with the anticipation of rewards offers an avenue for organizations to harness positive reinforcement mechanisms that can bolster adherence to compliance standards.

Empirical studies substantiate this proposition by revealing that reward systems play a vital role in influencing compliance behavior. Research on organizational behavior has consistently demonstrated that rewards, whether tangible or intangible, can act as potent drivers of employee conduct, Hwang et al. (2021), Wang et al. (2022). Organizations that incorporate effective reward structures into their compliance programs tend to observe higher levels of adherence among employees, as the anticipation of rewards encourages individuals to actively engage in compliant actions.

Moreover, the cognitive aspect of this relationship is rooted in the perception of a reciprocal exchange between individual effort and organizational recognition Angraini et al. (2022). Empirical evidences confirm that employees who perceive that their compliant behavior is acknowledged and rewarded, are more likely to view their adherence to regulatory norms as a valuable contribution to the organization, Thangavelu et al (2021). This sense of reciprocity cultivates a positive organizational climate wherein individuals are motivated to align their intentions with the pursuit of compliance, Wilson and McDonald (2023).

At this point, it is plausible to infer that the assertion posited by the ninth hypothesis, establishing a positive correlation between the intent to participate in compliant behavior and the presence of incentives, is firmly substantiated and merits inclusion within the model.

This assertion underscores a notable interplay between motivational dynamics and the adherence to regulatory requirements. This relationship resonates with cited theories and referenced empirical evidence that showcases the impact of reward systems on employee behavior.

By acknowledging the central role of rewards in shaping compliance intentions, organizations can strategically utilize motivation-enhancing mechanisms to foster a culture of adherence to regulatory standards.

**H10: Motivation to compliance is positively associated to organizational culture.**

The tenth hypothesis postulates a positive linkage between the motivation to comply with regulatory measures and the prevailing organizational culture within a given organizational context. This proposition introduces an avenue of inquiry that holds substantive significance in understanding the interplay of motivational dynamics and the overarching cultural fabric, thereby warranting comprehensive academic exploration, Hafeez et al. (2022), Keller and Kokkinis (2022), Chakraborty et al. (2021).

At the heart of this hypothesis lies the notion that individuals' impetus to conform to compliance norms is harmoniously intertwined with the pervasive organizational culture that envelops the operational milieu. In essence, an organizational culture that inherently values and champions compliance is purported to wield a considerable influence in bolstering individuals' inherent motivation to adhere to stipulated regulatory mandates, Chiu (2018), Cerasoli and Ford (2014), Ogbanufe (2023), Meso et al. (2013), Bauer and Bernroider (2015), Edeh et al. (2023).

The foundation of this assertion draws theoretical support from established psychological theories of motivation and organizational behavior. Within a culture that consistently underscores the key role of compliance, individuals are anticipated to perceive compliance as an intrinsic component of their professional identity.

Empirical substantiation lends credence to this hypothesized relationship, revealing that

organizational cultures underpinned by a resolute commitment to compliance tend to cultivate higher levels of employee dedication to regulatory adherence. Research investigations into ethical organizational cultures corroborate that individuals who identify resonance between their own values and those upheld by the organizational culture are more likely to manifest behaviors that resonate with the overarching ethics AlGhamboosi et al. (2023), Sharma and Aparicio (2022).

Furthermore, this nexus between motivation and organizational culture assumes a bidirectional dynamic. While an organizational culture that champions compliance can indeed augment individuals' motivation, motivated individuals can reciprocally contribute to nurturing and perpetuating an organizational culture that firmly esteems compliance. Individuals who are intrinsically motivated to conform to regulatory norms are poised to function as advocates and exemplars, thereby fostering an environment where regulatory adherence becomes synonymous with the organizational identity.

The tenth hypothesis, elucidating a positive linkage between motivation to comply and organizational culture, serves as a substantive way of inquiry within the realm of organizational behavior. This dynamic is congruent with well-established psychological theories of motivation and is reinforced by empirical evidence, Hafeez et al. (2022), Keller and Kokkinis (2022), Chakraborty et al. (2021).

By acknowledging the strong relationship between motivation, Chiu (2018), Cerasoli and Ford (2014), Ogbanufe (2023), Meso et al. (2013), Bauer and Bernroider (2015), and organizational culture, Alshwayat et al. (2021), Büschgens et al (2013), Tejay and Mohammed (2023), organizations stand to harness this dynamic for cultivating a culture of compliance that derives its vigor from individuals' intrinsic dedication to regulatory adherence, as also confirmed in Sharma and Aparicio (2022).

**H11: Motivation to compliance is positively associated to managers' behavior.**

The eleventh hypothesis delineates a constructive and meaningful connection that links the motivation of individuals to uphold compliance standards with the observable behaviors exhibited by managers operating within the organizational environment, Chiu (2018).

This assertion introduces a new avenue of inquiry that holds profound implications for delving into the complex and nuanced interactions between motivational forces and the actions demonstrated by managerial entities. This hypothesis beckons for a comprehensive academic exploration that ventures into the depths of this delicate relationship, Bakhshandeh et al. (2023).

At the heart of this hypothesized relationship lies a fundamental proposition – the motivation of individuals to align with established regulatory norms is intricately intertwined with the behaviors exemplified by managerial personnel, Castilla and Ranganathan (2020), Keller and Kokkinis (2022), Sue et al. (2020).

In essence, the eleventh hypothesis postulates that when managers display behaviors that not only prioritize but also actively endorse compliance with regulations, the ripple effect is expected to resonate with the intrinsic motivation of individuals to adhere to the prescribed regulatory framework.

This hypothesis serves as an intriguing focal point for scholarly investigation, as it delves into the potential synergies between managerial conduct and individual motivation within the compliance landscape. As the research journey unfolds, this proposition guides the exploration into how managerial actions can shape the organizational climate, impacting individuals' perceptions and intentions towards regulatory adherence. By shedding light on this relationship, the hypothesis contributes to an enhanced understanding of the complex interplay between organizational actors, motivational dynamics, and compliance behaviors.

The foundation of this assertion derives theoretical backing from established theories of organizational behavior and leadership, Amir et al. (2022), Kalshoven and Taylor (2018), Azhar et al. (2023), Den Hartog (2015), Bakhshandeh et al. (2023).

Transformational leadership, for instance, posits that leaders who inspire and motivate their subordinates through their actions are likely to influence followers' attitudes and behaviors Lawrason et al. (2023).

In this context, managers' behaviors that underscore the importance of compliance serve as a means of communicating organizational values, thereby potentially enhancing individuals' motivation to align their actions with regulatory requirements, Wu et al. (2023).

Empirical validation lends credence to this postulated relationship, revealing that managers who actively endorse and prioritize compliance through their conduct tend to stimulate higher levels of commitment among employees towards regulatory adherence, Sharma and Aparicio (2022), (*supra*).

Research investigations into ethical leadership corroborate that employees who perceive their managers as role models for ethical behavior are more inclined to emulate such behavior themselves, Al Halbusi et al. (2023).

Furthermore, the dynamic between motivation and managers' behavior exhibits a bidirectional interaction. While managers' behaviors that accentuate compliance can indeed enhance individuals' motivation, motivated individuals can reciprocally contribute to shaping managerial behaviors that champion compliance. Employees who are intrinsically motivated to adhere to regulatory norms are poised to set an example for their colleagues and managers, thereby fostering an environment where compliance is deemed a shared organizational value.

The proposed elenth hypothesis, highlighting a positive nexus between motivation to comply and managers' behavior, serves as a noteworthy area of inquiry within the domain of organizational behavior. This dynamic aligns with established theories of leadership influence and is substantiated by empirical evidence, Burns et al. (2017), Kweon et al. (2021).

By recognizing and harnessing the interplay between motivation and managers' behavior, organizations can strategically leverage this relationship to cultivate a culture of compliance that is grounded in individuals' intrinsic commitment to regulatory adherence.

The graphical representation of proposed model is drawn in Figure 1.

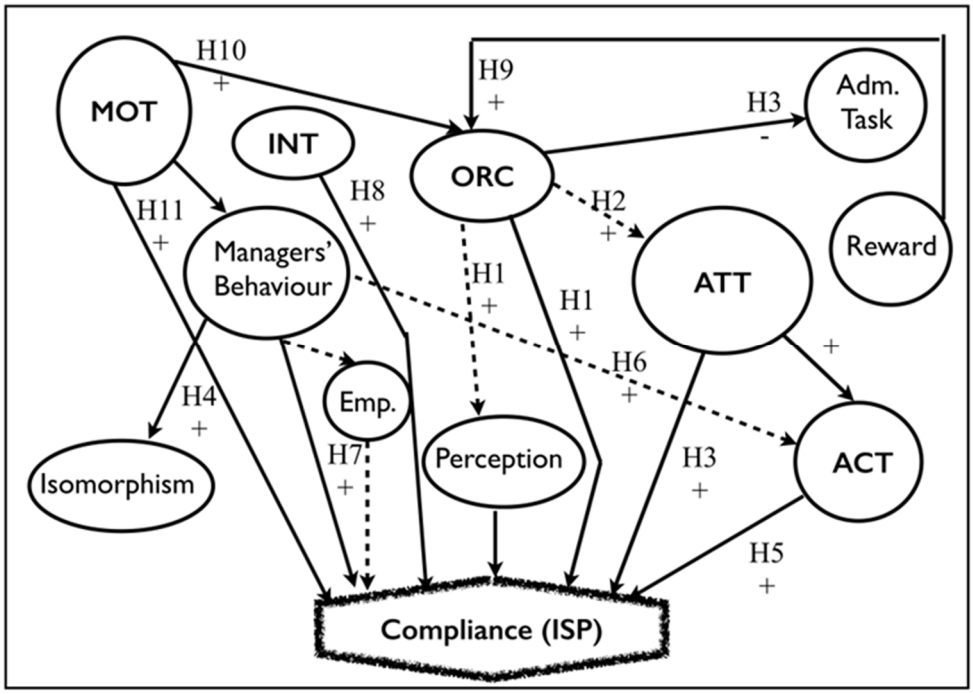


**Figure 1.** Proposed model of investigation, with connection to previously published model

**Table 1.** Relation between Hypothesis and Constructs

| Hypotheses | Type of Relationship | Constructs |
|---|---|---|
| Hypotheses 1 and 2 | Belong to | Organizational Culture |
| Hypotheses 3 and 4 | Belong to | Attitude |
| Hypotheses 5, 6 and 7 | Belong to | Actors |
| Hypotheses 8 and 9 | Belong to | Intention |
| Hypotheses 10 and 11 | Belong to | Motivation |

## 9. Conclusions and Future Research Work

The arguments posited within this paper are anchored in a robust foundation of pre-existing research findings, encompassing both theoretical underpinnings and empirical investigations.

The current paper serves as a further development and enhancement of the existing body of research, building upon the insights gleaned from prior scholarly results.

**Novelty.** Although the paper relies on pre-existing research findings, it introduces the novelty of conglomerate a new scheme for investigation into compliance, organisational behaviour and information security, that had never been tested before. This could mean that novel viewpoints might not have been adequately considered in past research, especially those investigating the organiziational variable such as Organizational Culture, Personal Attitudes, (organisational) Actors, Intention and Motivation as a single model.

This enriched framework delves deeper into the relationships among the mentioned constructs and research hypotheses, offering a broader insight, available for further investigation, into the dynamics governing compliance behaviour within organisations.

In this context, the scholarly discourse embraced by this paper finds support within the broader academic landscape. The paper's assertions and contentions rest upon a well-established scaffolding of prior research findings and arguments, which have contributed to the formation of the present substantive framework for understanding the subject matter at hand. These antecedent studies, spanning theoretical explorations and empirical examinations, have collectively furnished the groundwork upon which the present paper builds.

The theoretical framework (the model) into this paper draws upon the reservoir of insights accumulated from prior theoretical frameworks. It signifies a refinement and expansion of the existing theoretical paradigms, as delineated by the cited references, signifying an intellectual evolution that enriches the discourse.

By situating itself within the continuum of scholarly exploration, this paper aligns with and contributes to the ongoing academic conversation, resonating with established themes and progressing the discourse forward.

Furthermore, the eventual empirical dimension of this paper finds resonance in the empirical investigations undertaken by scholars in past research efforts. The references point to empirical findings that have probed into the subject matter, paving the way for the present paper's endeavor to deepen and broaden the empirical understanding of the phenomenon under scrutiny.

## 10. Broader Scope

Through the integration of these prior empirical insights, this paper seeks to amplify the depth and comprehensiveness of the scholarly understanding, thereby advancing the collective body of empirical knowledge.

In conclusion, the arguments and the model presented within this paper draw sustenance from a strong scholarly foundation, encompassing both theoretical and empirical dimensions. The paper's contribution lies in its role as an extension and refinement of the existing research landscape, proposing a new model, accentuating the evolution of ideas within the field and contributing to the

ongoing academic exploration.

The theoretical framework built within this study forms the basis for hypotheses that warrant empirical confirmation to establish their empirical validity.

The transition from theoretical constructs to empirical validation follows a logical sequence, serving as an essential step in substantiating the stated propositions.

As we embarked on the effort of investigation, these hypotheses will serve as the lenses through which we will be able to examine real-world data, eventually seeking to establish meaningful associations and draw conclusions that contribute to the broader academic arguments.

This envisaged progression from theory to empirical confirmation will mark a significant phase in the research process, enabling the bridge between conceptual constructs and empirical observations.

## 11. Limitations

The purpose of this study is to lay the groundwork for a future empirical investigation by establishing the theoretical foundations. To substantiate the proposed hypotheses, it is essential to gather empirical evidence. Hence, there is a requirement for conducting an empirical examination to assess the assumptions introduced in this study.

Given that this study is primarily concerned with theoretical elaboration, it naturally paves the way for subsequent empirical inquiry that strengthens the conceptual propositions put forth.

There are of course some limitations which can be summarised as:

Theoretical Orientation: The study is primarily theoretical in nature. Without empirical evidence to back up theoretical assertions, the conclusions remain speculative, although based on robust past research.

Potential for Confirmation Bias: Given that the paper aligns with broader academic conversations, there's a possibility that only conforming views were taken into account, potentially overlooking, possible, contradicting evidences.

Future Empirical Scrutiny: The study underscores the importance of future empirical investigation, suggesting that its conclusions are not definitive until such examination is undertaken.

## 12. Acknowledgments

A preliminary, abridged, version of the study was presented at the Italian Chapter of AIS (Association for Information Systems) itAIS2016, Verona, I, October 7-8, 2016.

## References

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. MIS Quarterly: Management Information Systems, 24(4), 665-694. https://doi.org/10.2307/3250951.

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

Ahyaruddin M., Yusoff M.N.H., Zainuddin S.A. (2023) Institutional Isomorphism, Accountability, and Local Government Performance in Era of Public Governance: A Conceptual Framework (2023) Contributions to Management Science, Part F1060, pp. 623 - 633, DOI: 10.1007/978-3-031-27296-7_57.

Ajzen, I. (1985) Action control, pp. 11-39, From intentions to actions: A theory of planned behavior. Berlin: Springer.

Ajzen, I. (1991). Theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

Ajzen, I., & Albarracin, D. (2007). Predicting and changing behavior: A reasoned action approach. In Prediction and change of health behavior: Applying the reasoned action approach.

Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Al Halbusi, H., Alhaidan, H., Ramayah, T., & AlAbri, S. (2023). Ethical Leadership and Employees' Ethical Behavior: Modeling the Contingent Role of Moral Identity. Business and Professional Ethics Journal, 42(1), 1-31. https://doi.org/10.5840/bpej202344135.

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, art. no. 9139638. https://doi.org/10.1109/CyberSA49311.2020.9139638.

Alec Cram, W., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly: Management Information Systems, 43(2), 525-554. https://doi.org/10.25300/MISQ/2019/15117.

AlGhanboosi, B., Ali, S., & Tarhini, A. (2023). Examining the effect of regulatory factors on avoiding online blackmail threats on social media: A structural equation modeling approach. Computers in Human Behavior, 144. https://doi.org/10.1016/j.chb.2023.107702.

Alhogail A. (2015) Design and validation of information security culture framework (2015) Computers in Human Behavior, 49, pp. 567 - 575 DOI: 10.1016/j.chb.2015.03.054.

Alhogail A., Mirza (2014) A. A proposal of an organizational information security *culture* framework (2014) Proceedings of 2014 International Conference on Information, Communication Technology and System, ICTS 2014, art. no. 7010591, pp. 243 - 249 DOI: 10.1109/ICTS.2014.7010591.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., 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, 3383. https://doi.org/10.3390/app11083383.

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

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers and Security, 98, art. no. 102003. https://doi.org/10.1016/j.cose.2020.102003.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. Proceedings of the Annual Hawaii International Conference on System Sciences, 5085-5094.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2020). Toward sustainable behaviour change: An approach for cyber security education training and awareness. 27th European Conference on Information Systems - Information Systems for a Sharing Society, ECIS 2019.

Alshwayat D., MacVaugh J.A., Akbar H. (2021) A multi-level perspective on trust, collaboration and knowledge sharing cultures in a highly formalized organization (2021) Journal of Knowledge Management, 25 (9), pp. 2220 - 2244 DOI: 10.1108/JKM-05-2020-0354.

Alskar, M., Vodanovich, S., & Shen, K.N. (2015). Evolvement of information security research on employees' behavior: A systematic review and future direction. Proceedings of the Annual Hawaii International Conference on System Sciences, 2015-March, art. no. 7070327, 4241-4250.

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. Kybernetes. https://doi.org/10.1108/K-08-2022-1104.

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2020). Exploring IS security themes: A literature analysis. Journal of Decision Systems, 29(sup1), 425-437.

Alzahrani, L. (2021). Factors Impacting Users 'Compliance with Information Security Policies: An Empirical Study. International Journal of Advanced Computer Science and Applications, 12(10), 437-447. https://doi.org/10.14569/IJACSA.2021.0121049.

Amir, M., Siddique, M., & Ali, K. (2022). Responsible leadership and business sustainability: Exploring the role of corporate social responsibility and managerial discretion. Business and Society Review. https://doi.org/10.1111/basr.12284.

Amoako G.K., Adam A.M., Tackie G., Arthur C.L. (2021) Environmental accountability practices of environmentally sensitive firms in ghana: Does institutional isomorphism matter? (2021) Sustainability (Switzerland), 13 (17), art. no. 9489, DOI: 10.3390/su13179489.

Angraini, Alias, R. A., & Okfalisa. (2022). Information Security Policy Compliance: An Exploration of User Behaviour and Organizational Factors. Lecture Notes on Data Engineering and Communications Technologies, 127, 641-650. https://doi.org/10.1007/978-3-030-98741-1_53.

Arellano-Gault, D., & del Castillo, A. (2023). The Promises and Perils of Compliance: Organizational factors in the success (or failure) of compliance programs. https://doi.org/10.1515/9783110749113.

Argote, L., & Miron-Spektor, E. (2011). Organizational learning: From experience to knowledge. Organization Science, 22(5), 1123-1137. https://doi.org/10.1287/orsc.1100.0621.

Aurigemma, S. (2013). A composite framework for behavioral compliance with information security policies. Journal of Organizational and End User Computing, 25(3), 67-82. https://doi.org/10.4018/joeuc.2013070103.

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. Information and Computer Security, 25(4), 421-436. https://doi.org/10.1108/ICS-11-2016-0089.

Azhar, S., Zhe, Z., & Simha, A. (2023). The congruence effect of ethical values of leaders and followers on ethical climate. Current Psychology. https://doi.org/10.1007/s12144-023-04920-7.

Bakhshandeh, B., Rothwell, W. J., Imroz, S. M., & Sadique, F. (2023). Transformational Coaching for Effective Leadership: Implementing Sustainable Change Through Shifting Paradigms. https://doi.org/10.4324/9781003304074.

Balliet, D., Mulder, L. B., & Van Lange, P. A. M. (2011). Reward, punishment, and cooperation: A meta-analysis. Psychological Bulletin, 137(4), 594-615. https://doi.org/10.1037/a0023489.

Balozian, P., & Leidner, D. (2017). Review of IS security policy compliance: Toward the building blocks of an IS security theory. Data Base for Advances in Information Systems, 48(3), 11-43. https://doi.org/10.1145/3130515.3130518.

Bandura A. (1977) Self-efficacy: Toward a unifying theory of behavioral change (1977) Psychological Review, 84 (2), pp. 191 - 215, DOI: 10.1037/0033-295X.84.2.191.

Bandura, A. (1997) Self-efficacy: The exercise of control. W. H. Freeman.

Bansal, G. (2021). Restoring trust after an insider breach: Both the genders matter—CEOs and users. Journal of Computer Information Systems, 61(1), 11-29.

Bansal, G., Muzatko, S., & Shin, S.I. (2021). Information system security policy noncompliance: the role of situation-specific ethical orientation. Information Technology and People, 34(1), 250-296. https://doi.org/10.1108/ITP-03-2019-0109.

Barbera, F. L., & Ajzen, I. (2020). Control interactions in the theory of planned behavior: Rethinking the role of subjective norm. Europe's Journal of Psychology, 16(3), 401-417. https://doi.org/10.5964/ejop.v16i3.2056.

Barron, A. B., Hebets, E. A., Cleland, T. A., Fitzpatrick, C. L., Hauber, M. E., & Stevens, J. R. (2015). Embracing multiple definitions of learning. Trends in Neurosciences, 38(7), 405-407. https://doi.org/10.1016/j.tins.2015.04.008.

Barton, K.B., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: a study of external influences on senior management. Computers & Security.

Bauer, S., & Bernroider, E.W. (2015). The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring. Lecture Notes in Computer Science, 9190, 154-164.

Belmondo C., Sargis-Roussel C. (2023) The Political Dynamics of Opening Participation in Strategy: The role of strategy specialists 'legitimacy and disposition to openness (2023) Organization Studies, 44 (4), pp. 613 - 635 DOI: 10.1177/01708406221080123.

Bendig D., Wagner R., Jung C., Nüesch S. (2022) When and why technology leadership enters the C-suite: An antecedents perspective on CIO presence (2022) Journal of Strategic Information Systems, 31 (1), art. no. 101705 DOI: 10.1016/j.jsis.2022.101705.

Bihari A., Shajahan P.K. (2023) Changing CSR practices of corporates – a study of institutionalization of mandated corporate social responsibility in India (2023) International Journal of Law and Management, 65 (2), pp. 105 - 124, DOI: 10.1108/IJLMA-09-2022-0198.

Blythe J.M., Coventry L., Little L. (2019) Unpacking security policy compliance: The motivators and barriers of employees' security behaviors (2019) SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security, pp. 103 - 122.

Bondarouk, T., & Sikkel, K. (2005). Explaining IT implementation through group learning. Information Resources Management Journal, 18(1), 42-60. https://doi.org/10.4018/irmj.2005010104.

Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behavior: Selected recent advances and applications. Europe's Journal of Psychology, 16(3), 352-356. https://doi.org/10.5964/ejop.v16i3.3107.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., & Boss, R.W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164.

Boxenbaum, E., Jonsson, S. (2017) Isomorphism, diffusion and decoupling: Concept evolution and theoretical challenges (2017) The Sage Handbook of Organizational Institutionalism, 2, pp. 79-104. SAGE: Los Angeles, CA, USA.

Briggs P., Jeske D., Coventry L. (2017) Behavior Change Interventions for Cybersecurity (2017) Behavior Change Research and Theory: Psychological and Technological Perspectives, pp. 115 - 136 DOI: 10.1016/B978-0-12-802690-8.00004-9.

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.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Quality and fairness of an information security policy as antecedents of employees' security engagement in the workplace: An empirical investigation. Proceedings of the Annual Hawaii International Conference on System Sciences. https://doi.org/10.1109/HICSS.2010.396.

Burns, A. J., Posey, C., Courtney, J. F., Roberts, T. L., & Nanayakkara, P. (2017). Organizational information security as a complex adaptive system: insights from three agent-based models. Information Systems Frontiers, 19(3), 509-524. https://doi.org/10.1007/s10796-015-9608-8.

Büschgens T., Bausch A., Balkin D.B. (2013) Organizational culture and innovation: A meta-analytic review (2013) Journal of Product Innovation Management, 30 (4), pp. 763 - 781 DOI: 10.1111/jpim.12021.

Cai, Y., Liu, P., Tang, R., & Bo, Y. (2023). Distributed leadership and teacher work engagement: The mediating role of teacher efficacy and the moderating role of interpersonal trust. Asia Pacific Education Review, 24(3), 383-397. https://doi.org/10.1007/s12564-022-09760-x.

Caldwell, T. (2012). Training - the weakest link. Computer Fraud & Security, (9), 8.

Carpenter, M.A., Geletkancz, M.A., & Sanders, Wm.G. (2004). Upper echelons research revisited: Antecedents, elements, and consequences of top management team composition. Journal of Management, 30(6), 749-778. https://doi.org/10.1016/j.jm.2004.06.001.

Cascavilla, G., Conti, M., Schwartz, D.G., & Yahav, I. (2018). The insider on the outside: A novel system for the detection of information leakers in social networks. European Journal of Information Systems, 27(4), 470-485.

Castilla, E.J., & Ranganathan, A. (2020). The production of merit: How managers understand and apply merit in the workplace. Organization Science, 31(4), 909-935. https://doi.org/10.1287/orsc.2019.1335.

Caulfield T., Pym D. (2015) Improving Security Policy Decisions with Models (2015) IEEE Security and Privacy, 13 (5), art. no. 7310818, pp. 34 - 41 DOI: 10.1109/MSP.2015.97.

Cavallari M. (2010) Information systems security and end-user consciousness - A strategic matter (2010) Management of the Interconnected World - ItAIS: The Italian Association for Information Systems, pp. 251 - 258, DOI: 10.1007/978-3-7908-2404-9_29.

Cavallari, M. (2011). The organizational relationship between compliance and information security. International Journal of the Academic Business World, 5(2), JW Press, Martin Tennessee, USA.

Cavallari M., Tornieri F. (2018) Information systems architecture and organization in the Era of MicroServices (2018) Lecture Notes in Information Systems and Organisation, 24, pp. 165 - 177 DOI: 10.1007/978-3-319-62636-9_11.

Celis N.J. (2018) Compliance theory: A case study approach in understanding organizational commitment (2018) DLSU Business and Economics Review, 27 (2), pp. 88 - 118.

Cerasoli, C. P., & Ford, M. T. (2014). Intrinsic motivation, performance, and the mediating role of mastery goal orientation: A test of self-determination theory. Journal of Psychology: Interdisciplinary and Applied, 148(3), 267-286. https://doi.org/10.1080/00223980.2013.783778.

Cerasoli, C. P., Nicklin, J. M., & Ford, M. T. (2014). Intrinsic motivation and extrinsic incentives jointly predict performance: A 40-year meta-analysis. Psychological Bulletin, 140(4), 980-1008. https://doi.org/10.1037/a0035661.

Chakraborty, T., Tripathi, M., & Saha, S. (2021). The dynamics of employee relationships in a digitalized workplace: The role of media richness on workplace culture. In Critical Issues on Changing Dynamics in Employee Relations and Workforce Diversity (pp. 175-205). https://doi.org/10.4018/978-1-7998-3515-8.ch010.

Chang, S.E., & Lin, C.-S. (2007). Exploring organizational culture for information security management. Industrial Management and Data Systems, 107(3), 438-458.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. Journal of Management Information Systems, 31(4), 49-87. https://doi.org/10.1080/07421222.2014.1001257.

Che T., Cai J., Yang R., Lai F. (2023) Digital transformation drives product quality improvement: An organizational transparency perspective (2023) Technological Forecasting and Social Change, 197, art. no. 122888 DOI: 10.1016/j.techfore.2023.122888.

Chen Y., Ramamurthy K., Wen K.-W. (2015) Impacts of comprehensive information security programs on information security culture (2015) Journal of Computer Information Systems, 55 (3), pp. 11 - 19 DOI: 10.1080/08874417.2015.11645767.

Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees 'security policy compliance: An awareness-motivation- capability perspective. Journal of Computer Information Systems, 58(4), 312-324.

Chen, X., Wu, D., Chen, L., & Teng, J.K.L. (2018). Sanction severity and employees 'information security policy compliance: Investigating mediating, moderating, and control variables. Information and Management, 55(8), 1049-1060. https://doi.org/10.1016/j.im.2018.05.011.

Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. Information Systems Research, 32(3), 1043-1065. https://doi.org/10.1287/ISRE.2021.1014.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers & Security, 39(B), 447–459.

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), 19-29. https://doi.org/10.1504/IJSN.2023.129949.

Chiu, H. H. (2018). Employees 'intrinsic and extrinsic motivations in innovation implementation: The moderation role of managers 'persuasive and assertive strategies. Journal of Change Management, 18(3), 218-239. https://doi.org/10.1080/14697017.2017.1407353.

Christman, L. (1977). Hierarchy in organizations. Nursing Administration Quarterly, 1(4), 87-89. https://doi.org/10.1097/00006216-197701040-00011.

Contreras, F. G., Pedraja-Rejas, L., Castillo, J. Q. Q., & Rodríguezponce, E. (2017). Organizational Isomorphism (OI): Brief theoretical approaches and some applications to higher education. Espacios, 38(20), art. no. 31.

Costa P.L., Graça A.M., Marques-Quinteiro P., Santos C.M., Caetano A., Passos A.M. (2013) Multilevel research in the field of organizational behavior: An empirical look at 10 years of theory and research (2013) SAGE Open, 3 (3), pp. 1 - 17 DOI: 10.1177/2158244013498244.

Crosby, F. J. (1999) The developing literature on developmental relationships, Mentoring Dilemmas: Developmental Relationships within Multicultural Organizations, pp. 3-20. In A. J. Murrell, F. J. Crosby, & R. J. Ely (Eds.).

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers and Security, 32, 90-101. https://doi.org/10.1016/j.cose.2012.09.010.

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour and Information Technology, 37(1), 50-65. https://doi.org/10.1080/0144929X.2017.1397193.

Curry, T.R. (2005). Integrating motivating and constraining forces in deviance causation: A test of causal chain hypotheses in control balance theory. Deviant Behavior, 26(6), 571-599. https://doi.org/10.1080/01639620500218286.

Cuzara G., Frega J.R. (2023) Business Models, Dynamic Capabilities and Industry 4.0: A Framework to Explore This Relationship, International Journal of Innovation and Technology Management, Volume 20, Issue 61 October 2023.

D'Arcy, J., & Lowry, P.B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29(1), 43-69. https://doi.org/10.1111/isj.12173.

da Veiga A., Martins N. (2015) Improving the information security culture through monitoring and implementation actions illustrated through a case study (2015) Computers and Security, 49, pp. 162 - 176 DOI: 10.1016/j.cose.2014.12.006.

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers and Security, 92. https://doi.org/10.1016/j.cos e.2020.101713.

Davis, J., Agrawal, D., Guo, X. (2023). Enhancing users 'security engagement through cultivating commitment: The role of psychological needs fulfilment. European Journal of Information Systems, 32(2), 195-206. https://doi.org/10.1080/0960085X.2021.1927866.

Demjaha A., Parkin S., Pym D. (2022) The boundedly rational employee: Security economics for behaviour intervention support in organizations (2022) Journal of Computer Security, 30 (3), pp. 435 - 464 DOI: 10.3233/JCS-210046.

Den Hartog, D.N. (2015). Ethical Leadership. Annual Review of Organizational Psychology and Organizational Behavior, 2, 409-434. https://doi.org/10.1146/annurev-orgpsych-032414-111237.

Detert, J.R., & Burris, E.R. (2007). Leadership behavior and employee voice: Is the door really open? Academy of Management Journal, 50(4), 869-884. https://doi.org/10.5465/AMJ.2007.26279183.

Devi E.T., Wibisono D., Mulyono N.B., Fitriati R. (2023) Designing an information-sharing system to improve collaboration culture: a soft systems methodology approach in the digital service creation process (2023) Journal of Enterprise Information Management, 36 (5), pp. 1240 - 1269 DOI: 10.1108/JEIM-08-2022-0294.

Dewies, M., Schop-Etman, A., Rohde, K. I. M., & Denktaş, S. (2021). Nudging is ineffective when attitudes are unsupportive: An example from a natural field experiment. Basic and Applied Social Psychology, 43(4), 213-225.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. Computers and Security, 56, 63-69. https://doi.org/10.1016/j.cose.2015.10.001.

Diefenbach, T., & Sillince, J. A. A. (2011). Formal and informal hierarchy in different types of organization. Organization Studies, 32(11), 1515-1537. https://doi.org/10.1177/0170840611421254.

DiMaggio, P.J., Powell, W.W. (1991) Introduction, The New Institutionalism in Organizational Analysis, pp.1-38. Powell W.W., DiMaggio P.J., (eds), Chicago: University of Chicago Press.

Donalds, C., & Barclay, C. (2022). Beyond technical measures: a value-focused thinking appraisal of strategic drivers in improving information security policy compliance. European Journal of Information Systems, 31(1), 58-73. https://doi.org/10.1080/0960085X.2021.1978344.

Donner E.K. (2023) Research data management systems and the organization of universities and research institutes: A systematic literature review (2023) Journal of Librarianship and Information Science, 55 (2), pp. 261 - 281 DOI: 10.1177/09610006211070282.

Dornheim P., Zarnekow R. (2023) Determining cybersecurity culture maturity and deriving verifiable improvement measures (2023) Information and Computer Security.

Duzenci, A., Kitapci, H., & Gok, M.S. (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. Applied Sciences (Switzerland), 13(15). https://doi.org/10.3390/app13158731.

Dwivedi, R., Nerur, S., & Mangalaraj, G. (2023). Predicting insider breaches using employee reviews. Journal of Computer Information Systems, 0(0), 1-15.

Eccles J.S., Wigfield A. (2020) From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation (2020) Contemporary Educational Psychology, 61, art. no. 101859, DOI: 10.1016/j.cedpsych.2020.101859.

Edeh, F.O., Zayed, N.M., Darwish, S., Nitsenko, V., Hanechko, I., & Anwarul Islam, K.M. (2023). Impression Management and Employee Contextual Performance in Service Organizations (Enterprises). Emerging Science Journal, 7(2), 366-384. https://doi.org/10.28991/ESJ-2023-07-02-05.

Egorov, M., Kalshoven, K., Pircher Verdorfer, A., & Peus, C. (2020). It's a Match: Moralization and the Effects of Moral Foundations Congruence on Ethical and Unethical Leadership Perception. Journal of Business Ethics, 167(4), 707-723. https://doi.org/10.1007/s10551-019-04178-9.

Fazlollahi H., Qayyum O., Howlader J., Khademi A., Gu J. (2013) Challenges of integration between MES and ERP systems in the steel industry (2013) AISTech - Iron and Steel Technology Conference Proceedings, 2, pp. 2487 - 2493.

Fishbein, M. (2007). A reasoned action approach: Some issues, questions, and clarifications. In Prediction and change of health behavior: Applying the reasoned action approach (pp. 281-296). Hillsdale, NJ: Lawrence Erlbaum & Associates.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley.

Frank, M., & Kohn, V. (2023). Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. Computers and Security, 132. https://doi.org/10.1016/j.cose.2023.103386.

Freeman, E. H. (2007). Regulatory Compliance and the Chief Compliance Officer. Information Systems Security, 16, 357–361.

Fruhen L.S., Andrei D.M., Griffin M.A. (2022) Leaders as motivators and meaning makers: How perceived leader behaviors and leader safety commitment attributions shape employees 'safety behaviors (2022) Safety Science, 152, art. no. 105775 DOI: 10.1016/j.ssci.2022.105775.

Goel, L., Zhang, J. Z., & Williamson, S. (2023). IT assimilation: Construct, measurement, and implications in cybersecurity. Enterprise Information Systems, 17(7).

Guhr, N., Lebek, B., & Breitner, M.H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. Information Systems Journal, 29(2), 340-362. https://doi.org/10.1111/isj.12202.

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. 14th International Conference on Cyber Warfare and Security, ICCWS 2019, 94-102.

Hadasch F., Maedche A., Gregor S. (2016) The influence of directive explanations on users 'business process compliance performance (2016) Business Process Management Journal, 22 (3), pp. 458 - 483, DOI: 10.1108/BPMJ-05-2015-0067.

Hafeez, H., Abdullah, M.I., Zaheer, M.A., & Ahsan, Q. (2022). Organizational resilience process: integrated model of safety culture. Organization Management Journal, 19(1), 2-21. https://doi.org/10.1108/OMJ-03-2020-0893.

Hagger, M. S., Cheung, M. W.-L., Ajzen, I., & Hamilton, K. (2022). Perceived behavioral control moderating effects in the theory of planned behavior: A meta-analysis. Health Psychology. https://doi.org/10.1037/hea0001153.

Han, T.A. (2022). Institutional incentives for the evolution of committed cooperation: Ensuring participation is as important as enhancing compliance. Journal of the Royal Society Interface, 19(188), 20220036. https://doi.org/10.1098/rsif.2022.0036.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165. https://doi.org/10.1016/j.dss.2009.02.005.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Hess T., Sciuk C. (2023) The evolution of IT leadership (2023) Digitalization and Sustainability: Advancing Digital Value, pp. 257 - 276.

Hina, S., Dominic, D. D. P. S., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees 'security compliance behavior in higher education institutions in the developing world. Computers & Security, 87, 101594. https://doi.org/10.1016/j.cose.2019.101594.

Hong, Y., & Furnell, S. (2022). Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. Journal of Computer Information Systems, 62(1), 19-28. https://doi.org/10.1080/08874417.2019.1683781.

Hong, Y., Xu, M., & Furnell, S. (2023). Situational support and information security behavioural intention: A comparative study using conservation of resources theory. Behaviour and Information Technology. https://doi.org/10.1080/0144929X.2023.2177825.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Decision Sciences, 43(4), 615-660.

Huang, H.-H., & Lin, J.-W. (2023). Inconsistencies between information security policy compliance and shadow IT usage. Journal of Computer Information Systems, 0(0), 1-11.

Hwang I., Wakefield R., Kim S., Kim T. (2021) Security Awareness: The First Step in Information Security Compliance Behavior Journal of Computer Information Systems, 61 (4), pp. 345 - 356 DOI: 10.1080/08874417.2019.1650676.

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition. Information & Management.

Iliya Nyahas S., Munene J.C., Orobia L., Kigongo Kaawaase T. (2017) Isomorphic influences and voluntary disclosure: The mediating role of organizational culture (2017) Cogent Business and Management, 4 (1), art. no. 1351144, DOI: 10.1080/23311975.2017.1351144.

Iniesta J., Verdugo M.A., Schalock R.L. (2023) Organizational change and evidence-based practices in support services for people with intellectual and developmental disabilities (2023) Evaluation and Program Planning, 100, art. no. 102337 DOI: 10.1016/j.evalprogplan.2023.102337.

Jensen A.F. (2023) The philosophical history of projectification: The project society (2023) Projectification of Organizations, Governance and Societies: Theoretical Perspectives and Empirical Implications, pp. 17 - 37, DOI: 10.1007/978-3-031-30411-8_2.

Kacmar, C. J., Fiorito, S. S., & Carey, J. M. (2009). The influence of attitude on the acceptance and use of information systems. Information Resources Management Journal, 22(2), 22-49. https://doi.org/10.4018/irmj.2009040102.

Kalshoven, K., & Taylor, S. (2018). Leadership: Philosophical Perspectives and Qualitative Analysis of Ethics—Looking Back, Looking Forward, Looking Around. Journal of Business Ethics, 148(1). https://doi.org/10.1007/s10551-018-3797-2.

Kang J.Y., Lee M.K., Fairchild E.M., Caubet S.L., Peters D.E., Matti L., Howell T.G., Jr (023) Do Organizational Values and Leadership Impact Staff Engagement, Wellbeing, and Patient Satisfaction? (2023) Journal of Healthcare Leadership, 15, pp. 209 - 219 DOI: 10.2147/JHL.S421692.

Keller, A., & Kokkinis, A. (2022). The senior managers and certification regime in financial firms: an organisational culture analysis. Journal of Corporate Law Studies, 22(1), 299-334. https://doi.org/10.1080/14735970.2022. 2054165.

Kennedy, S.E. (2016). The pathway to security-mitigating user negligence. Information and Computer Security, 24(3), 255-264.

Khan, H.U., & AlShare, K.A. (2019). Violators versus non-violators of information security measures in organizations—A study of distinguishing factors. Journal of Organizational Computing and Electronic Commerce, 29(1), 4-23.

Khatib R., Barki H. (2020) An activity theory approach to information security non-compliance (2020) Information and Computer Security, 28 (4), pp. 485 - 501 DOI: 10.1108/ICS-11-2018-0128.

Khatib, R., & Barki, H. (2022). How different rewards tend to influence employee non-compliance with information security policies. Information and Computer Security, 30(1), 97-116. https://doi.org/10.1108/ICS-01-2021-0008.

Kim, B., Lee, D.-Y., & Kim, B. (2020). Deterrent effects of punishment and training on insider security threats: A field experiment on phishing attacks. Behaviour & Information Technology, 39(11), 1156-1175.

King E., Cordrey T., Gustafson O. (2023) Exploring individual character traits and behaviours of clinical academic allied health professionals: a qualitative study (2023) BMC Health Services Research, 23 (1), art. no. 1025 DOI: 10.1186/s12913-023-10044-2.

Klemsdal L., Wittusen C. (2023) Agency in compliance with institutions: The case of professional expert-organizations and politico-ethical agency (2023) Organization, 30 (4), pp. 712 - 729 DOI: 10.1177/1350508421 1020461.

Knapp K.J., Marshall T.E., Rainer Jr. R.K., Ford F.N. (2006) Information security: Management's effect on culture and policy (2006) Information Management and Computer Security, 14 (1), pp. 24 - 36 DOI: 10.1108/096 852206106483 55.

Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. H. (2020). Information security policy compliance: Leadership, trust, role values, and awareness. Journal of Computer Information Systems, 60(1), 1-8. https://doi.org/10.1080/08874417.2019.1668738.

Krajnovic, A. (2018) Institutional theory and isomorphism: Limitations in mulinational companies (2018) J Corp Gov Insur Risk Manag (JCGIRM), 5 (1), pp. 1-7.

Kweon E., Lee H., Chai S., Yoo K. (2021) The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence (2021) Information Systems Frontiers, 23 (2), pp. 361 - 373, DOI: 10.1007/s10796-019-09977-z.

Lai K.-H., Wong C.W.Y., Cheng T.C.E. (2006) Institutional isomorphism and the adoption of information technology for supply chain management (2006) Computers in Industry, 57 (1), pp. 93-98, DOI: 10.1016/j.compind.2005.05.002.

Laslo-Roth, R., & Schmidt-Barad, T. (2021). Personal sense of power, emotion and compliance in the workplace: a moderated mediation approach. International Journal of Conflict Management, 32(1), 39-61. https://doi.org/10.1108/IJCMA-07-2019-0113.

Lawrason, S. V. C., Shaw, R. B., Turnnidge, J., & Côté, J. (2023). Characteristics of transformational leadership development programs: A scoping review. Evaluation and Program Planning, 101. https://doi.org/10.1016/j .evalprogplan.2023.102354.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. Management Research Review, 37(12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085.

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 and Work, 25(2-3), 273-289. https://doi.org/10.1007/s10111-023-00727-5.

Leering A., van de Wijngaert L., Nikou S. (2022) More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors (2022) Behaviour and Information Technology, 41 (3), pp. 519 - 534, DOI: 10.1080/0144929X.2020.1822444.

Li, W., Liu, R., Sun, L., Guo, Z., & Gao, J. (2022). An Investigation of Employees 'Intention to Comply with Information Security System—A Mixed Approach Based on Regression Analysis and fsQCA. International Journal of Environmental Research and Public Health, 19(23), art. no. 16038. https://doi.org/10.3390 /ijerph192316038.

Li, X., Wang, C., & Hamari, J. (2021). Frontline employees 'compliance with fuzzy requests: A request–appraisal–behavior perspective. Journal of Business Research, 131, 55-68. https://doi.org/10.1016/j.jbusres.2021.03.052.

Li, Y. J., & Hoffman, E. (2023). Designing an incentive mechanism for information security policy compliance: An experiment. Journal of Economic Behavior and Organization, 212, 138-159. https://doi.org/10.1016/j.jebo.202 3.05.033.

Lian, H., Ferris, D. L., & Brown, D. J. (2012). Does power distance exacerbate or mitigate the effects of abusive supervision? It depends on the outcome. Journal of Applied Psychology, 97(1), 107-123. https://doi.org /10.1037/a0024610.

Lin, Q. (2023). Transformational leadership and innovative work behavior: The role of identification, voice and innovation climate. International Journal of Hospitality Management, 113. https://doi.org/10.1016/j.ijh m.2023.103521.

Liu D., Lu W., Niu Y. (2023) Isomorphic Pressures to Catalyze Innovation Diffusion in Construction Project-Based Organizations: Identification of Source Factors (2023) Journal of Construction Engineering and Management, 149 (2), art. no. 4022170, DOI: 10.1061/JCEMD4.COENG-12475.

Liu, C., Liang, H., Wang, N., & Xue, Y. (2022). Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender. Information Technology and People, 35(2), 802-834. https://doi.org/10.1108/ITP-09-2019-0452.

Lockwood P., Kunda Z. (1997) Superstars and Me: Predicting the Impact of Role Models on the Self (1997) Journal of Personality and Social Psychology, 73 (1), pp. 91 - 103, DOI: 10.1037/0022-3514.73.1.91.

Lord, R.G., Day, D.V., Zaccaro, S.J., Avolio, B.J., & Eagly, A.H. (2017). Leadership in applied psychology: Three waves of theory and research. Journal of Applied Psychology, 102(3), 434-451. https://doi.org/10.1037/apl00000088.

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. European Journal of Information Systems, 26(6), 546-563.

Lyman, B., Hammond, E. L., & Cox, J. R. (2019). Organizational learning in hospitals: A concept analysis. Journal of Nursing Management, 27(3), 633-646. https://doi.org/10.1111/jonm.12722.

Mady A., Gupta S., Warkentin M. (2023) The effects of knowledge mechanisms on employees' information security threat construal (2023) Information Systems Journal, 33 (4), pp. 790 - 841.

Manville G., Greatbanks R. (2023) Institutional isomorphism and performance management: exploring the linkage and relationship in English social housing (2023) Housing Studies, DOI: 10.1080/02673037.2023.2217769.

Martins A., Eloff J. (2002) Information security culture (2002) IFIP Advances in Information and Communication Technology, 86, pp. 203 - 214 DOI: 10.1007/978-0-387-35586-3_16.

Mathiassen L., Jonsson K., Holmstrom J. (2023) Tensions in transfer, translation, and transformation of information: A sociomaterial perspective on heterogeneous work arrangements (2023) Journal of Information Technology, 38 (3), pp. 334 - 350 DOI: 10.1177/02683962231164426.

Mees, B. (2017). Organizational mimesis and the emergence of industry superannuation in Australia. Journal of Management History, 23(3), 241-258. https://doi.org/10.1108/JMH-03-2017-0013.

Merhi, M.I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. Computers in Human Behavior, 92, 37-46. https://doi.org/10.1016/j.chb.2018.10.031.

Merhi, M.I., & Ahluwalia, P. (2023). Predicting Compliance of Security Policies: Norms and Sanctions. Journal of Computer Information Systems. https://doi.org/10.1080/08874417.2023.2241413.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. Journal of Information Privacy and Security, 9, 47-67.

Mishra, N., & Chakraborty, T. (2023). Employee engagement perspectives in agile organizations: Managing people in Industry 4.0. In Agile Leadership for Industry 4.0: An Indispensable Approach for the Digital Era (pp. 139-154).

Moody, G.D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly: Management Information Systems, 42(1), 285-311. https://doi.org/10.25300/MISQ/2018/13853.

Motaung, J. R., & Sifolo, P. P. S. (2023). Benefits and barriers of digital procurement: Lessons from an airport company. Sustainability, 15(5). https://doi.org/10.3390/su15054610.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2013) What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study, European Journal of Information Systems (18), pp. 126-139.

Najrani, M. (2016). The endless opportunity of organizational agility. Strategic Direction, 32(3), 37-38. https://doi.org/10.1108/SD-02-2015-0026.

Nani, D.A., & Safitri, V.A.D. (2021). Exploring the relationship between formal management control systems, organisational performance and innovation: The role of leadership characteristics. Asian Journal of Business and Accounting, 14(1), 207-224. https://doi.org/10.22452/ajba.vol14no1.8.

Nasirpouri Shadbad, F., & Biros, D. (2021). Understanding Employee Information Security Policy Compliance from Role Theory Perspective. Journal of Computer Information Systems, 61(6), 571-580. https://doi.org/10.1080/08874417.2020.1845584.

Ni, W., & Sun, H. (2009). The relationship among organizational learning, continuous improvement and performance improvement: An evolutionary perspective. Total Quality Management and Business Excellence, 20(10), 1041-1054. https://doi.org/10.1080/14783360903247312.

Nielsen J.A., Mathiassen L., Benfeldt O., Madsen S., Haslam C., Penttinen E. (2023) Organizational resilience and digital resources: Evidence from responding to exogenous shock by going virtual (2023) International Journal of Information Management, 73, art. no. 102687 DOI: 10.1016/j.ijinfomgt.2023.102687.

Niemimaa E., Niemimaa M. (2017) Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems* 26:1, pages 1-20.

Nwankpa J.K., Datta P.M. (2023) Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers (2023) Computers and Security, 130, art. no. 103266.

Ogbanufe, O., & Ge, L. (2023). A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations. Computers and Security, 128, art. no. 103136. https://doi.org/10.1016/j.cose.2023.103136.

Palanisamy, R., Norman, A. A., & Mat Kiah, M. L. (2023). Employees 'BYOD security policy compliance in the public sector. Journal of Computer Information Systems, 0(0), 1-16.

Papadaki, M., Furnell, S. (2010). Vulnerability management: an attitude of mind? Network Security, Issue 10, October 2010, 4-8.

Pattnaik, N., Li, S., & Nurse, J.R.C. (2023). A Survey of User Perspectives on Security and Privacy in a Home Networking Environment. ACM Computing Surveys, 55(9), art. no. 3558095. https://doi.org/10.1145/3558095.

Pircher Verdorfer, A., & Peus, C. (2020). Leading by example: Testing a moderated mediation model of ethical leadership, value congruence, and followers' openness to ethical influence. Business Ethics, 29(2), 314-332. https://doi.org/10.1111/beer.12255.

Popa S., Vaida M.-F. (2016) A practical strategy for ERP to cloud integration (2016) Studies in Informatics and Control, 25 (3), pp. 375 - 384 DOI: 10.24846/v25i3y201611.

Posey, C., Bennett, R.J., & Roberts, T.L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. Computers & Security, 30(6–7), 486-497.

Posey, C., Raja, U., Crossler, R. E., & Burns, A. J. (2017). Taking stock of organisations 'protection of privacy: Categorising and assessing threats to personally identifiable information in the USA. European Journal of Information Systems, 26(6), 585-604.

Pradhan B.B. (2019) Corporate digital responsibility: Review (2019) International Journal of Psychosocial Rehabilitation, 23 (6), pp. 142 - 147, DOI: 10.37200/IJPR/V23I6/PR190749.

Qatawneh, A. M. (2023). The role of employee empowerment in supporting accounting information systems outcomes: A mediated model. Sustainability, 15, 7155. https://doi.org/10.3390/su15097155.

Razak, F.N.A., Ramli, A., & Rasit, Z.A. (2020). Organisation isomorphism as determinants of environmental management accounting practices in Malaysian public listed companies. Humanities and Social Sciences Letters, 8(1), 110-122. https://doi.org/10.18488/journal.73.2020.81.110.122.

Reeder, G. D., & Brewer, M. B. (1979). A schematic model of dispositional attribution in interpersonal perception. Psychological Review, 86(1), 61-79. https://doi.org/10.1037/0033-295X.86.1.61.

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 59, 26-44. https://doi.org/10.1016/j.cose.2016.01.004.

Rodríguez-González R.M., Madrid-Guijarro A., Maldonado-Guzmán G. (2023) Digital organizational culture and absorptive capacity as precursors to supply chain resilience and sustainable performance (2023) Journal of Cleaner Production, 420, art. no. 138411 DOI: 10.1016/j.jclepro.2023.138411.

Ryutov, T. (2023). An Empirical Investigation of Psychological Factors Affecting Compliance with Information Security Organizational Policies. Cybersecurity for Decision Makers, 253-277. https://doi.org/10.1201/9781003319887_15.

Sanson D., Courpasson D. (2022) Resistance as a Way of Life: How a group of workers perpetuated insubordination to neoliberal management (2022) Organization Studies, 43 (11), pp. 1693 - 1717, DOI: 10.1177/01708406221077780.

Setyorini, C.T. (2012) Corporate Social and Environmental Reporting: A Case of Mimetic Isomorphism Universitas Jenderal Soedirman (2012) Am. Int. J. Contemp. Res, 2, pp. 11-17.

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

Sillic M. (2019) Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context (2019) Computers and Security, 80, pp. 108 - 119, DOI: 10.1016/j.cose.2018.09.012.

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. European Journal of Information Systems, 23(3), 289-305.

Siponen, M., Soliman, W., & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions. Data Base for Advances in Information Systems, 53(1), 25-60. https://doi.org/10.1145/3514097.3514101.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies. Information Management & Computer Security, 22(1), 42-75.

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. Social Sciences, 11, 386. https://doi.org/10.3390/socsci11090386.

Sullivan K.R., Rennstam J., Bertilsson J. (2023) Sycomorphism in city branding: The case of Amazon HQ2 (2023) Marketing Theory, 23 (2), pp. 207 - 223, DOI: 10.1177/14705931221108426.

Tejay G.P.S., Mohammed Z.A. (2023) Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective (2023) Information and Management, 60 (3), art. no. 103751, DOI: 10.1016/j.im.2022.103751.

Thangavelu M., Krishnaswamy V., Sharma M. (2021) Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study (2021) Computers and Security, 109, art. no. 102401, DOI: 10.1016/j.cose.2021.102401.

Topa, I., & Karyda, M. (2023). Addressing Organisational, Individual and Technological Aspects and Challenges in Information Security Management: Applying a framework for a case study. Proceedings of the Annual Hawaii International Conference on System Sciences, 470-479.

Ukobitz D.V., Faullant R. (2022) The relative impact of isomorphic pressures on the adoption of radical technology: Evidence from 3D printing, (2022) Technovation, 113, art. no. 102418, DOI: 10.1016/j.technovation.2021.102418.

Van Thuan D., Hai N.L. (2024) The Impact of Project Organizational Culture on Cost Performance of Construction Projects (2024) Lecture Notes in Civil Engineering, 344 LNCE, pp. 121 - 129 DOI: 10.1007/978-981-99-2345-8_11.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. Journal of Management Information Systems, 29(4), 263-290.

Vroom C., Von Solms R. (2004) Towards information security behavioural compliance. Computers and Security, 23 (3), pp. 191 - 198 DOI: 10.1016/j.cose.2004.01.012.

Wang, X., Wang, C., Sun, Z., & Wang, C. (2022). An optimal coupling incentive mechanism concerning insider's compliance behavior towards marine information security policy. Journal of Ocean Engineering and Science. https://doi.org/10.1016/j.joes.2022.05.023.

Warkentin, M., & Mutchler, L. (2022). Behavioral information security management. Computing Handbook: Two-Volume Set, 1-20. https://doi.org/10.1201/b16768-61.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. European Journal of Information Systems, 18(2), 101-105.

West, R. (2008). The Psychology of Security. Communications of the ACM, 51(4), 34-40.

Wilson, M., & McDonald, S. (2023). SME Cybersecurity Misconceptions: A Guide for Decision Makers. In Cybersecurity for Decision Makers (pp. 293-316). https://doi.org/10.1201/9781003319887_17.

Wright, R.T., & Wilson, D.W. (2022). Privacy, accuracy, and accessibility of digital business. Computing Handbook: Two-Volume Set, 1-19. https://doi.org/10.1201/b16768-62.

Wu, Y., Xu, Q., Jiang, J., Li, Y., Ji, M., & You, X. (2023). The influence of safety-specific transformational leadership on safety behavior among Chinese airline pilots: The role of harmonious safety passion and organizational identification. Safety Science, 166. https://doi.org/10.1016/j.ssci.2023.106254.

Wulaningrum P.D., Akbar R., Sari M.R. (2020) Isomorphism, Human Resource Capability and Its Role in Performance Measurement and Accountability (2020) Journal of Asian Finance, Economics and Business, 7 (12), pp. 1099 - 1110, DOI: 10.13106/JAFEB.2020.VOL7.NO12.1099.

Xue, B., Warkentin, M., Mutchler, L. A., & Balozian, P. (2023). Self-efficacy in information security: A replication study. Journal of Computer Information Systems, 63(1), 1-10.

Xue, Y., Fan, Y., & Xie, X. (2020). Relation between senior managers 'safety leadership and safety behavior in the Chinese petrochemical industry. Journal of Loss Prevention in the Process Industries, 65, 104142. https://doi.org/10.1016/j.jlp.2020.104142.

Yang, X., Wang, X., Yue, W.T., Sia, C.L., & Luo, X. (2019). Security policy opt-in decisions in bring-your-own-device (BYOD) – A persuasion and cognitive elaboration perspective. Journal of Organizational Computing and Electronic Commerce, 29(4), 274-293.

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology & People, 26(4), 401.

Zemba, Y., Young, M. J., & Morris, M. W. (2006). Blaming leaders for organizational accidents: Proxy logic in collective- versus individual-agency cultures. Organizational Behavior and Human Decision Processes, 101(1), 36-51. https://doi.org/10.1016/j.obhdp.2006.04.007.

Zhang, H., & Hu, B. (2017). The effects of organizational isomorphism on innovation performance through knowledge search in industrial cluster. Chinese Management Studies, 11(2), 209-229. https://doi.org/10.1108/CMS-04-2016-0076.

Zhu N., Liu Y., Zhang J., Wang N. (2023) Contingent reward versus punishment and compliance behavior: the mediating role of affective attitude and the moderating role of operational capabilities of artificial intelligence (2023) Humanities and Social Sciences Communications, 10 (1), art. no. 590 DOI: 10.1057/s41599-023-02090-2.