Exploring the Relation between Information Security Policy Compliance and Cyber Resilience

Abigaïl de Rijp, Tim Huygh, Clara Maathuis,
Rogier van de Wetering, Harald Vranken

Open Universiteit, Faculty of Science, Heerlen, the Netherlands
abigail.derijp@ou.nl, tim.huygh@ou.nl, clara.maathuis@ou.nl,
rogier.vandewetering@ou.nl, harald.vranken@ou.nl

Contemporary digital environments necessitate an increased organizational commitment to safeguarding the confidentiality, integrity and availability of information assets. An indispensable element of this endeavor lies in issuing and enforcing Information Security Policies (ISP) that delineate appropriate handling and use of the organization's information assets. While prior research predominantly examined the impact of ISPs on employee cyber behavior, limited attention was given to the organizational-level effects of ISP compliance (ISPC). In particular, the extent to which ISPC and cyber resilience (CR) are interrelated is still insufficiently understood. In light thereof, this article explores mechanisms that can be implemented to increase ISPC, the general organizational-level effects of ISPC, and how ISPC relates to CR specifically. Drawing on an integrative literature review and a holistic case study, this article explores the role of ISPC in driving organizational CR.

DOI
https://doi.org/10.18690/um.fov.4.2026.11

ISBN
978-961-299-152-4

Keywords:
information security management, information security policy, compliance, AMC-framework, cyber resilience

University of Maribor Press

1 Introduction

A characteristic of the 21st century is the interwovenness of the digital and physical world, making online shopping, social media and digitalized business processes increasingly ordinary. This coalescence also provokes the transition of traditionally unwanted physical behavior to its digital counterpart. On this matter, the following applies: "But people themselves alter so much, that there is something new to be observed in them forever." – Jane Austen, Pride & Prejudice. Even though romance novels and an Information Security Management System (ISMS) are not necessarily relatable, both address the unpredictability of human behavior. In fact, within an ISMS, many security weaknesses arise from human behavior and actions (Ncubukezi, 2022). Thus, enforcing an Information Security Policy (ISP) can aid organizations in protecting their information assets (Delso-Vicente et al., 2025). An ISP is "a set of formalized procedures, guidelines, roles and responsibilities to which employees are required to adhere to safeguard and use properly the information and technology resources of their organizations" (Cram et al. 2019, pp. 525-526).

Even though there is a plethora of research and theories on the impact of ISPs on employee behavior (e.g., Xue et al., 2021; Mubarkoot et al., 2023), there seems to be a lack of a comprehensive account of the impact of ISP compliance (ISPC) on organization security (Cram et al., 2019). For instance, previous research focuses on the individual drivers of ISPC (Aggarwal et al, 2024; Balagopal et al., 2024; Sharma, et al. 2025). However, evaluation of ISPC necessitates consideration of both human behavioral as well as organizational factors (Alias et al., 2019; Zhang et al., 2025). This is particularly important as information security threats do not single out the employees whose non-compliant behavior might lead to an incident, but they affect the organization in its entirety (Delso-Vicente et al., 2025).

As seemingly critical elements of an organization's ISMS, pre-emptive planning and preparation for potential cyber-attacks requires a certain amount of cyber resilience (Calder, 2020; Alhidaifi et al., 2025). To this end, Ross et al. (2021, p. 1) describe cyber resilience (CR) as "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources". Subsequently, this article addresses the relation and potential overlap between ISPC and CR. The objective of this paper is bifold. Firstly, it provides an understanding of which organizational mechanisms enable ISPC and

CR. Secondly, it addresses the extent to which ISPC (effects) relate to CR. To successfully achieve these objectives, the main research question is: *Which organizational drivers can enhance Information Security Policy Compliance and Cyber Resilience, and how are these phenomena related?* To answer this question, ISPC and CR are first assessed separately to avoid the assumption that ISPC always leads to CR. The research starts off with an integrative literature review that provides conceptual insight into ISPC and CR found in the literature. The resulting Theoretical Background is provided in section 2. Then, the empirical research – which is discussed in sections 3 and 4 – investigates the existence of the organizational impact of ISPC and its potential overlap with CR. Section 5 discusses the research results and addresses its limitations and aspects for further investigation, and section 6 concludes the article in its entirety.

2 Theoretical Background

2.1 Literature Review

2.1.1 ISPC-enhancing drivers

Literature on ISPs highlights a broad range of organizational drivers that shape how policies are enacted in practice. Albeit obvious, these policies are only effective if they are complied with. Additionally, poorly aligned or rigid policies may fail to deliver intended outcomes (Almuqrin, 2024; Zanke et al., 2024). In light hereof, many authors distinguish various behavioral theories that focus on individual attitudes and behavior relating to ISPC. However, as mentioned above, non-compliant behavior may affect the entire organization, not just the individual transgressor. To address this theoretical gap, this article identifies organizational-level drivers for ISPC by utilizing the awareness-motivation-capability (AMC) framework by Chen et al. (2016). This framework emphasizes an organization's proactive decision-making through a distinction between awareness-, motivation- and capability-enhancing measures, each addressing a different (cognitive) level for the end-user (Dong et al. 2023; Li et al., 2025). Thus, the framework distinguishes directional and behavioral variance, and allows for integration of behavioral, institutional, and resource perspectives. In doing so, it is particularly well suited for ISPC research because it accounts for both intentional and unintentional non-

compliance. Table 1 provides a non-exhaustive synthesis of most relevant measures, based on the following criteria:

- Awareness-enhancing: relates to employees' knowledge of the ISP; these drivers were selected based on reach, frequency, and ability to convey ISP's rationale.
- Motivation-enhancing: relates to reasons why employees would or would not comply with the ISP; these drivers were selected through assessing organizational/ environmental engagement, and perceived value of compliance.
- Capability-enhancing: relates to ease or difficulty of ISPC; these drivers were selected based on usability and ability of enabling performance of duties.

Table 1: AMC-measures for ISPC

Awareness measures	Motivation measures	Capability measure
Onboarding can introduce new employees to the ISP(C) (Vollenweider, 2023).	A **cyber security culture** aids the increase of ISPC (Amankwa et al., 2018; Alassaf et al., 2021; Zhang et al., 2025).	**Infrastructural constraints** can prevent execution of non-compliant behavior (Khando et al., 2021); (Mubarkoot et al., 2023).
Involving end-users in the development of the ISP leads to their active participation in and awareness of the organization's ISMS/ ISP (Amankwa et al., 2018).	**Involvement of managers** (Moody et al., 2018), and their **exemplary ISPC behavior** incentivize compliance by other staff (Whitman et al., 2018; Zhang et al., 2025).	**Monitoring and auditing** enable identification of deviant behavior (D'Arcy et al., 2019), highlighting areas for ISP(C) improvement (Alassaf et al., 2021, Mubarkoot et al., 2023).
Awareness campaigns aim to inform end-users about the existence, scope, and value of the ISP (Bagheri, 2020; Khando et al., 2021).	**Managerial control through sanctions and promotions** can incentivize motivation for complying with the ISP (Cram et al., 2019; Khando et al., 2021).	**Allocation of IS-related tasks and responsibilities** enables employee participation in IS-practices, enriching their self-efficacy (Moody et al., 2018; Ali et al., 2021).
Clear and accessible ISP provisions increase employee compliance with, and engagement in, security practices (Ali et al., 2021).	**Strategies for organizational ISP justice** prevent IS-related injustices that could demotivate end-users to comply with the ISP (Hovav et al., 2016; Ali et al., 2021).	**Cybersecurity exercises** like penetration testing (Balakrishnan et al., 2018) enable vulnerability- and incident preparedness and response (Bartes et al., 2017).
Gamification simplifies communication of ISPC content and importance (Khando et al., 2021).	Promotion, support, and liaising of ISMS activities by an **ISMS coordination team** (Zammani et al., 2019) can enhance motivation.	**Education** cultivates skills and confidence (Cram et al. 2019), and **training** enhances application of taught skills (Tsohou et al., 2018).
Security Education, Training and Awareness **(SETA)-Programs** facilitate knowledge of procedures, guidelines and actionable tasks (Moody et al., 2018; D'Arcy et al., 2019).	Giving employees **freedom** and control to make IS-related decisions can reduce non-compliant behavior, as restriction herein incentivizes noncompliance (Hovav et al., 2016; Stewart, 2021).	Strategically **designed** systems that promote compliant, **user-friendly**, easily comprehensible **interfaces**, facilitate users' understanding and adoption of compliant behavior (Falahati, et al. 2022).

Notably, the AMC-framework provides a diagnostic lens for addressing barriers that might cause non-compliance and subsequently identify necessary adjustments. However, the AMC-framework does not explicitly account for organizational ISPC effects, thereby requiring additional research that will highlight its relation to CR.

2.1.2 CR-enhancing drivers

Table 2: Organizational drivers for CR

Planning ***Parameter:*** knowledge and decision-making prior to an incident	Cyber resilience **awareness and training** contribute to long-term enhancement of organizational cyber resilience (Kott et al., 2019; Bagheri, 2020; Annarelli, 2021).
	A **cyber security culture** can facilitate cyber resilience planning through integration of cyber security practices in the business operations (Kott et al., 2019), emphasizing the crucial role of management and leadership (Bagheri, 2020).
	A **Response and recovery plan** is crucial for the efficacy and sustainability of a resilience program. Through established policies (pre-event), these programs prescribe the organization's approach for handling threats and incidents (Bagheri, 2020; Staves et al., 2022), as well as **appropriate roles and responsibilities** (Annarelli et al., 2021).
Detecting ***Parameter:*** recognition and interpretation of anomalies and incidents	**Governance and monitoring programs** facilitate structural documentation of CR procedures and issues (Bagheri, 2020; Petrenko, 2022), enabling identification of gaps and areas for improvement (Rieger, et al., 2021). Expansive analysis by for e.g. Artificial Intelligence can aid quick and effective detection and response (Balakrishnan et al., 2018; Klioskli et al., 2023).
	Cybersecurity exercises – for e.g. staged attacks (Balakrishnan et al., 2018) – create opportunities for identification and assessment of risks and threats, stakeholders' familiarity therewith, and the efficacy of existing response (Petrenko, 2022; Staves et al., 2022).
	Employee reporting plays a critical role in detecting anomalies; they should have access to **reporting mechanisms** for potential security incidents (Abrahams et al., 2024).
Recovery/ post-incident ***Parameter:*** reaction to and lessons learned from incidents	**Proactive response coordination** to threats and incidents is vital for organizations (Ross et al., 2021). This response should be based on established policies that prescribe actionable tasks (Annarelli et al., 2021) that can be executed and/ or coordinated by capable (external) IS-staff (Linkov et al., 2013; Bagheri, 2020), for e.g. a Cyber Incident Response Team (CIRT).
	Organizational **responses** to cyber incidents should be **evaluated** in order to allocate appropriate human resources and maintain up-to-date awareness of evolving cyber risks. In line herewith, addressing system issues and risks is vital and evaluating recovery durations will enable the organization to modify or replace non-recoverable components (Bagheri et al. 2023).

To commence, CR reflects an organization's capability to endure and adapt to disruptions in its information systems while continuing to achieve its operational objectives (Bagheri, 2021; Eling et al., 2021). Not to be confused with cyber security, CR is commonly regarded as a post-incident construct (Rieger et al., 2021). Cyber security, on the other hand, focuses on the pre-incident protection of electronic information (Calder, 2020). Even so, CR is strongly rooted in pre-incident measures, particularly the deliberate design of resilient systems that enable effective response and recovery from attacks or failures, making cyber security a core element of a CR-strategy. In essence, preparedness, detection, and recovery capabilities are key

enabling conditions for organizational CR (Annarelli et al., 2021; Ross et al., 2021). As such, CR can be divided into three phases, namely (1) planning, (2) detecting, and (3) recovery/post-incident (Linkov et al., 2013; Bagheri, 2020). Table 2 provides a non-exhaustive synthesis of relevant organizational drivers divided over each phase.

2.1.3 ISPC effects and correlation with CR

With regards to the ISPC effects, existing literature suggests that poorly aligned or rigidly implemented security frameworks may fail to deliver intended outcomes (Almuqrin, 2024; Zanke et al., 2024). Thus, organizational context – including culture, leadership and strategic goals – influence the effectiveness of these frameworks. Additionally, given the significant role employees have in security incidents (Fatoki et al., 2024), their involvement in risk management and open dialogue are critical to the effectiveness of an ISMS and ISPC (Ali et al., 2020).

Prior research suggests that ISPC may contribute to reducing cybersecurity incidents, safeguarding the Confidentiality, Integrity and Availability of information systems, and enhancing business continuity, organizational reputation, and risk management capabilities (Cram et al., 2019; Ali et al., 2020; Donalds et al., 2022; Mohamud, 2024). On the other hand, the notoriety of attributing security incidents to human behavior is contradicted by a lack of empirical evidence clearly linking ISPC to reduced security incidents. Thus, the validation of the presumed ISPC effects requires more controlled empirical work (e.g., longitudinal or experimental designs) that quantifies their magnitude.

Collectively, the literature indicates that well-established security policies support organizational security by protecting sensitive information and mitigating vulnerabilities, suggesting a meaningful convergence between ISPC and CR. Moreover, the implementation of policies can be considered the highest level of reactive defense since, for example, access management policies add more layers to information protection than physical and network security alone (Balakrishnan et al., 2018). Ultimately, well-formulated policies that are easily integrated into daily activities enable a better alignment between restrictive and protective security objectives within organizations (Qiu et al., 2020).

Both ISPC and CR encompass an organization's motivation to safeguard valuable information assets. While ISPC includes prescription of responsibilities for mitigating cyber-related risks, CR enables consistent delivery of the intended business outcome despite incidents (Eling et al., 2021). Notably, except for incident response, we also identified all CR-drivers in light of ISPC-drivers. Figure 1 presents the overlap between ISPC and CR.

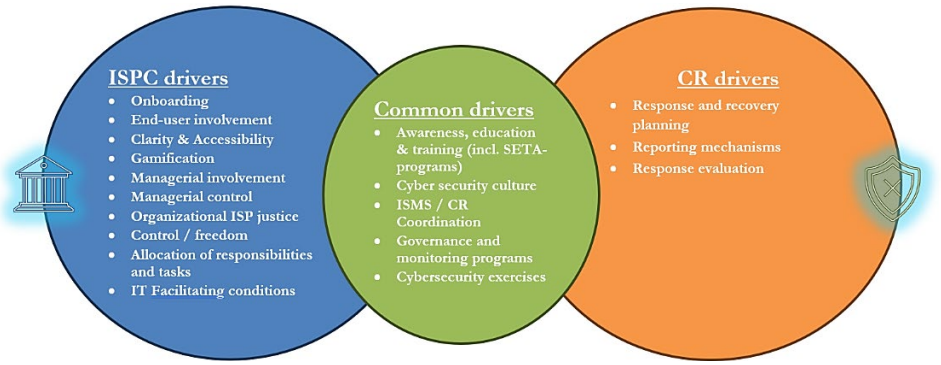

Figure 1: ISPC and CR overlap

In conclusion, effective use of IT systems – perhaps by enhanced ISPC capabilities – contributes to CR (Annarelli et. al, 2021), because consistently secure behavior aids in mitigating risks and enhancing organizational resilience (Oroni et al., 2025).

2.2 State of the art and perspectives for empirical research

A non-exhaustive set of mechanisms that may enhance ISPC and CR emerges from literature. For instance, regarding awareness, an employee may be first introduced to the ISP through onboarding. Subsequently, considering motivation, organizational security culture creates an environment for motivating their compliance with the ISP. Then, relating to capability, appropriate security training enables end-user's capability of utilizing obtained knowledge and necessary related skills. Despite this division, some mechanisms are complementary, and even fluid throughout the AMC-levels. For example, a security culture can also be an introduction to the ISP or enhance capabilities for ISPC for e.g. through security related conversations.

Furthermore, there are many notable similarities between ISPC and CR drivers, such as increased organizational awareness of security activities, security culture, and enhanced IT-capabilities (detection and monitoring). Basically, thus far, ISPC-enhancing drivers seem to be re-usable for CR as both elements are essentially aimed at safeguarding valuable organizational information assets. Nevertheless, our following empirical research further explores the effects of ISPC on the case organization, and how this potentially contributes to their CR.

3 Methodology

Our study adopts a qualitative case study design based on a single holistic case study that facilitated an exploration of the effects of ISPC and its relation to CR in practice. The methodological rigor and quality of this case study is ensured through several strategies (Yin, 2014). Construct validity was guaranteed using multiple sources of evidence – such as document analysis, semi-structured interviews and an exploratory survey – which enabled data triangulation. Internal validity was facilitated by comparing expected theoretical patterns with observed data (pattern matching) and by iteratively refining explanations based on evidence from multiple data sources (explanation building. Regarding external validity, the case organization, further anonymized as ALX, was selected based on its analytical relevance rather than statistical representativeness, thereby supporting analytical generalization. ALX provided a formally implemented and documented ISMS that is governed by a dedicated Information Security department. Finally, reliability was ensured by maintaining a chain of evidence and inviting key informants to review draft findings.

The analyzed documents applicable to ALX were: the ISP, an Annual Awareness Plan (2023-2024), a Risk Control Standard (2017), an Awareness Survey Report (2023), and an Information Security Baseline (2024). Furthermore, the interviewees consisted of the Chief Information Security Officer (CISO), two Information Security Officers (ISOs), an IT Security Officer (ITSO), and an Awareness Officer (AO). These interviewees have an average of 6+ years of experience in Information Security. Lastly, the survey only required employment by ALX. As just 27 of ± 5000 employees completed the survey, its results served an exploratory triangulation purpose, providing indicative insights rather than empirically generalizable findings.

4 Results: applying theory to practice

4.1 ISPC and CR drivers

The research findings suggest that ISPC at ALX is supported by mechanisms spanning all AMC levels, including formal training initiatives, awareness campaigns, and technical infrastructure. Figure 2 presents the identified ISPC and CR drivers within ALX, which were categorized using a three-level index: low (not or rarely identified), medium (partially identified), and high (frequently identified). Notably, despite their formal inclusion in ALX's strategic documentation, security culture and managerial involvement were perceived as relatively weak by interviewees and survey respondents. This can suggest a misalignment in design and implementation regarding leadership and community.

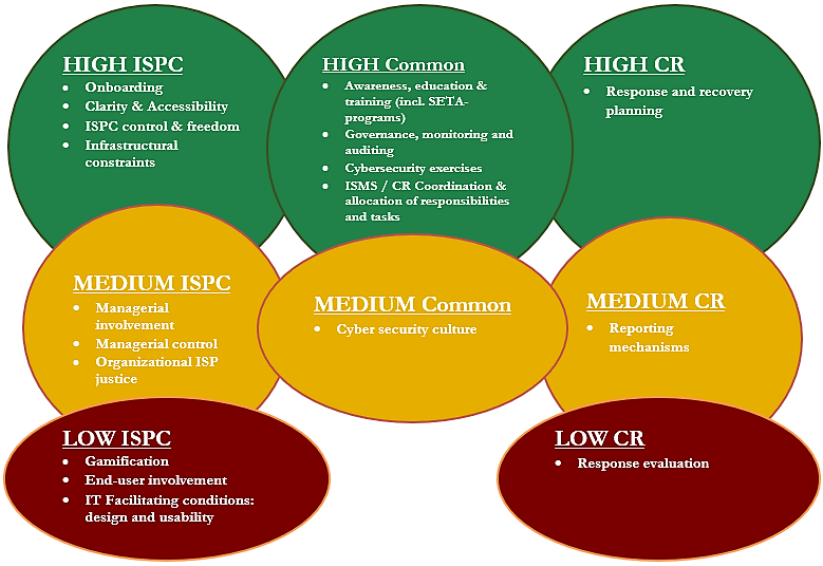

Figure 2: ISPC and CR overlap in ALX

4.2 ISPC effects

ALX's ISP prescribes the contours for how the organization should handle information systems, including processes for identifying, assessing, monitoring, reporting and controlling operational risks and incidents. Hence, through

implementation of its Information Risk Management Policy (and procedures), ALX is better equipped to detect vulnerabilities and threats prior to the maturing of these risks into incidents, providing opportunities for making informed security decisions. In light hereof, the CISO, ISO's and ITSO noted that risk management through ISPC enables ALX to become increasingly better at managing, identifying and mitigating risks. The ITSO mentioned that the ISP describes 'erroneous behavior'; therefore, if employees are aware of what they should comply with, they can report deviations therefrom. Subsequently, the ITSO and AO presume that heightened employee awareness may contribute to incident reduction by enabling earlier reporting and more secure information handling practices. They also infer that ALX's mandatory training "Digital Safety Online" and routine phishing simulations enable a combination of ISPC monitoring, auditing and exercising that facilitate the detection of AMC-related security gaps. Even so, the interviewees explicitly mentioned that ISPC effects can only be clear if ISPC is consistently and properly monitored. Nevertheless, the interviewees agreed that ISPC supports the maintenance of the confidentiality, integrity, and availability of information systems by strengthening risk, incident, and vulnerability management.

4.3 Potential ISPC and CR overlap

ALX's ISP explicitly identifies CR and business continuity as core information security objectives. The CISO and an ISO emphasized that ISPC and CR require a "human-centered approach" in which employees are proactively engaged in information security practices. One ISO stressed that the absence of policies can complicate the organization's chances of achieving CR. Another ISO adds that ISPC specifically helps with identifying and mitigating security risks, which, in turn increases CR. Additionally, the ITSO highlighted that proactive reporting by end-users – as prescribed by the ISP – is essential for an enhanced response to anomalies, as this will better equip ALX to deal with these on time, hence, aiding CR.

Furthermore, the findings highlight multiple organizational mechanisms associated with both ISPC and CR, including awareness, training, security culture, cyber exercises, governance, monitoring, coordination, and reporting. This follows ALX's adoption of the "Three Lines of Defense" approach wherein specific security-related tasks are divided amongst management, academic and supporting staff. In

conclusion, within ALX, reinforcing ISPC and CR relies on human-centered mechanisms such as security awareness, training, incident reporting, and response capabilities, supplemented by technical mechanisms, such as monitoring.

5 Discussion, limitations and future research

This study advances understanding of ISPC and CR by examining the mechanisms that support both phenomena and by theorizing their interconnection. Most literature treated ISPC and CR as separate domains. For instance, compliance is addressed as a dependent variable for behavioral change, and CR is treated as an outcome of systems, not behavior. Thus, the linkage between the two remains under-theorized. Hence, this study conceptually shifts ISPC from abiding by rules to addressing it as a dynamic capability that strengthens CR, conveying attention from whether compliance occurs to how it is organizationally enabled.

The findings further suggest that ISPC drivers can function as enabling mechanisms as well as observable indicators of compliance-related effects. For example, cyber exercises such as phishing simulations provide insight into employees' level of knowledge, willingness, and capability to respond to cyber threats. When such reporting behavior is institutionalized, organizations may develop a more coordinated approach to threat detection while simultaneously revealing socio-technical vulnerabilities across departments and infrastructures. Subsequently, misalignment within the organization's approach, both in terms of personnel (e.g., departmental differences), and technology (e.g., accessibility of the reporting database) can be identified and addressed, potentially creating evidence-based insights about the organization's overall CR posture.

Additionally, the findings contemplate that alignment of ISPC mechanisms with CR-oriented practices can aid positioning organizations better to withstand and adapt to the cyber threat landscape. Thus, the ISP could form a foundational governance instrument within broader CR strategies. However, the findings equally indicate that compliance alone is not sufficient to ensure CR. Rather, resilience is reinforced when compliance is embedded within an integrated socio-technical configuration spanning people, processes, and technology, whilst balancing prevention and response strategies. This underscores the importance of complementing policy enforcement with leadership engagement, security culture, and continuous capability building.

Limitations and future research

This study is subject to several limitations. First, the findings may reflect perceptual bias concerning the quality, enforceability and effectiveness of the ISPC as insights from the broader employee population were not extensively captured. Second, the relatively short research window of five months essentially implies a cross-sectional design and constrains the ability to observe longer-term longitudinal compliance dynamics. Third, the operationalization and measurement of ISPC effects remain difficult to isolate from broader information security governance outcomes. Finally, the study primarily focuses on organizational compliance mechanisms without explicitly accounting for how rapid technological advancements continuously reshape security requirements and user interactions and may underrepresent the dynamic interplay of innovation and security.

Recommendations for future research

Several avenues for future research emerge from this work. First, longitudinal research designs are needed to generate stronger empirical evidence regarding the organizational effects of ISPC. Such studies should account for dynamic contextual factors, including technological developments, evolving threat landscapes, and the dual retrospective and preparatory nature of information security policies. Moreover, measurable evidence of ISPC-effects could be provided through combining quantitative metrics, comparative analysis, and business impact linkage. Second, further exploration of the design and implementation of mechanisms for monitoring end-user ISPC could provide deeper insight into behavioral compliance and its associated organizational impacts. Third, further research is required to empirically assess the situational and organizational conditions and effectiveness of mechanisms aimed at enhancing ISPC and CR. Finally, considering the Network and Information Security Directive 2, it is particularly valuable to examine how Dutch Higher Education Institutions strengthen their CR strategy in compliance herewith.

6 Conclusion

Our work highlights the importance of human-centered mechanisms, such as awareness of security activities, security culture, and enhanced IT-capabilities (detection, monitoring, reporting and response) as critical links that influence both

ISPC and CR. This study also contributes to the extant literature by proposing ISPC as an organizational enabler of CR, rather than solely an individual-level behavioral outcome. In doing so, this research extends existing compliance-focused research through positioning CR as a potential complementary outcome of an ISMS. Thus, it demonstrates that ISPC and CR are closely related and mutually reinforcing, suggesting that ISPC can potentially be utilized as a foundational layer of CR, with its strongest contributions concentrated on preparedness. Taken together, this research reconceptualizes ISPC as a resilience-enabling capability, arguing that ISPC-enhancing mechanisms can play a critical role in shaping organizational CR.

References

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. *Computer Science & IT Research Journal*, *5*(1), 100-119.

Aggarwal, A., & Srivastava, S. K. (2024). Synthesizing Information Security Policy Compliance And Non-compliance: A Comprehensive Study And Unified Framework. Journal of Organizational Computing and Electronic Commerce, 34(4), 338–369. https://doi.org/10.1080/10919392.2024.2381303

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. IEEE Access, 9, 162687-162705. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9634004

Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. ACM computing surveys, 56(8), 1-48. https://doi.org/10.1145/3649218

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(8), 3383–. https://doi.org/10.3390/app11083383

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

Almuqrin, A. (2024). How About Enhancing Organizational Security. Journal of Global Information Management, 32(1). https://doi.org/10.4018/JGIM.358745

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. Information and Computer Security, 26(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

Annarelli, A., & Palombi, G. (2021). Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework. Sustainability (Basel, Switzerland), 13(23), 13065-. https://doi.org/10.3390/su132313065

Bagheri, S. (2020). Investigating organisational aspects of cyber resilience in large organisations (Doctoral dissertation, University Of Tasmania). https://web.archive.org/web/20210613091531id_/https://eprints.utas.edu.au/35959/1/Bagheri_whole_thesis.pdf

Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational Cyber Resilience: Management Perspectives. Australasian Journal of Information Systems, 27. https://journal.acs.org.au/index.php/ajis/article/view/4183/1315

Balakrishnan, U. R., Mishra, G., & Bhatt, N. (2018). Strategies for Improving Cyber Resilience of Data-Intensive Business Information Systems. In Handbook of e-Business Security (pp. 285-312). Auerbach Publications. https://doi.org/10.1201/9780429468254

Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. Computers & Security, 147, 104062. https://doi.org/10.1016/j.cose.2024.104062

Calder, A. (2020). The cyber security handbook–Prepare for, respond to and recover from cyber attacks. IT Governance Publishing Ltd.

Cram, W. A., 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, 43(2), 525-554. https://doi.org/10.25300/MISQ/2019/15117

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 (Oxford, England), 29(1), 43–69. https://doi.org/10.1111/isj.12173

Delso-Vicente, AT., Diaz-Marcos, L., Aguado-Tevar, O. et al. (2025) Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. Futur Bus J 11, 28 (2025). https://doi.org/10.1186/s43093-025-00452-7

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

Dong, Y., Chen, S., & Wu, Y. (2023). Keeping up with the Joneses: The role of investee peers corporate environmental responsibility. *Corporate Social Responsibility and Environmental Management*, *30*(4), 1841-1855. https://onlinelibrary.wiley.com/doi/epdf/10.1002/csr.2458?saml_referrer

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.

Falahati, A., Lapointe, L., & Beaudry, A. (2022). Employees' Compliance with ISP: A Socio-Technical Conceptual Model. https://doi.org/10.24251/HICSS.2022.840

Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security*, *141*, 103812. https://doi.org/10.1016/j.cose.2024.103812

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. Pervasive and Mobile Computing, 32, 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007

Keys, B., & Shapiro, S. (2018). Frameworks and Best Practices. In Cyber Resilience of Systems and Networks (pp. 69–92). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_4

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 106, 102267. https://www.sciencedirect.com/science/article/pii/S0167404820300675

Kott, A., & Linkov, I. (Eds.). (2019). Cyber resilience of systems and networks. New York, NY: Springer International Publishing. https://link.springer.com/content/pdf/10.1007/978-3-319-77492-3.pdf

Li, W., Kang, X., He, A., & Zhou, M. (2025). CEO organizational identification and firm strategic change: an AMC framework. *Asia Pacific Journal of Management*, 1-34. https://link.springer.com/article/10.1007/s10490-025-10056-y

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. Environmental Science & Technology, 47(18), 10108–10110. https://doi.org/10.1021/es403443n

Mohamud, A. J. (2024). Impact of information security policies compliance (ISPC) on reducing the incidence of security breaches in organizations: Systematic Literature Review. https://www.preprints.org/manuscript/202409.1715

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

Mubarkoot, M., Altmann, J., Rasti-Barzoki, M., Egger, B., & Lee, H. (2023). Software Compliance Requirements, Factors, and Policies: A Systematic Literature Review. Computers & Security, 124, 102985-. https://doi.org/10.1016/j.cose.2022.102985

Oroni, C. Z., & Xianping, F. (2025). Evaluating the influence of cybersecurity policies and cybersecurity behavior on institutional security performance in remote learning: the moderating role of technological readiness. *Sustainable Futures*, *10*, 101554. https://doi.org/10.1016/j.sftr.2025.101554

Petrenko, S. (2022). Cyber resilience. CRC Press.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., & Fang, B. (2020). A survey on access control in the age of internet of things. IEEE Internet of Things Journal, 7(6), 4682-4696. https://doi.org/10.1109/JIOT.2020.2969326

Rieger, C., Schultz, K., Carroll, T., & McJunkin, T. (2021). Resilient control systems—basis, benchmarking and benefit. IEEE Access, 9, 57565-57577. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9399144

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuiad, R. (2021). NIST Special Publication 800-160, Volume 2 Revision 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. https://doi.org/10.6028/NIST.SP.800-160v2r1

Sharma, A., Koohang, A., & Singh, S. P. (2025). Information Security Policy Compliance: a structured review using scientometric analysis and topic modeling. Journal of Global Information Management (JGIM), 33(1), 1-32. https://doi.org/10.4018/JGIM.389715

Staves, A., Anderson, T., Balderstone, H., Green, B., Gouglidis, A., & Hutchison, D. (2022). A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. International Journal of Critical Infrastructure Protection, 37, 100505–. https://doi.org/10.1016/j.ijcip.2021.100505

Stewart, S. E. (2021). Managerial Control Effects on Information Security Policy Compliance Intentions: Considerations of Formal and Informal Modes of Control. https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=6203&context=etd

Tsohou, A., & Holtkamp, P. (2018). Are users competent to comply with information security policies? An analysis of professional competence models. Information Technology & People (West Linn, Or.), 31(5), 1047–1068. https://doi.org/10.1108/ITP-02-2017-0052

Vollenweider, F., & Jahankhani, H. (2023, January). What Drives Generation Z to Behave Security Compliant? An Extended Analysis Using the Theory of Planned Behaviour. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 315-341). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-20160-8_17

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security. Cengage Learning.

Xue, B., Xu, F., Luo, X., & Warkentin, M. (2021). Ethical leadership and employee information security policy (ISP) violation: Exploring dual-mediation paths. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 5-23. https://www.emerald.com/ocj/article-pdf/1/1/5/2066198/ocj-02-2021-0002.pdf

Yin, R. K. (2018). Case study research and applications (Vol. 6). Thousand Oaks, CA: Sage.

Zammani, M., Razali, R., & Singh, D. (2019). Factors contributing to the success of information security management implementation. International Journal of Advanced Computer Science and Applications, 10(11). https://thesai.org/Downloads/Volume10No11/Paper_53-Factors_Contributing_to_the_Success_of_Information_Security.pdf

Zanke, A., Weber, T., Dornheim, P., & Engel, M. (2024). Assessing information security culture: A mixed-methods approach to navigating challenges in international corporate IT

departments. *Computers & Security*, *144*, 103938. https://www.sciencedirect.com/science/article/pii/S0167404824002438

Zhang, Z., & Gao, Q. (2025). Practice what you preach: how and when does leaders' information security policy compliance influence subordinates' information sharing?. *Journal of Knowledge Management*. https://doi.org/10.1108/JKM-02-2025-0242