
Proceedings Paper:
Tyas Darmaningrat, E.W., Foster, J.J. and Israilidis, J. (2026) Developing information security policy in a multi-stakeholder urban environment: lessons from Surabaya, Indonesia. In: Ramayah, T., (ed.) Procedia Computer Science. The Eighth Information Systems International Conference (ISICO 2025), 04-06 Aug 2025, Sanur, Bali, Indonesia. Elsevier BV, pp. 1519-1527. ISSN: 1877-0509. EISSN: 1877-0509.

https://doi.org/10.1016/j.procs.2026.07.143

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 284 (2026) 1519–1527

Procedia Computer Science

www.elsevier.com/locate/procedia

The Eighth Information Systems International Conference (ISICO 2025)

Developing information security policy in a multi-stakeholder urban environment: lessons from Surabaya, Indonesia

Eko Wahyu Tyas Darmaningrat[a,b*], Jonathan J. Foster[a], John Israilidis[a]

[a]*Information School, Faculty of Social Sciences, The University of Sheffield, Sheffield S10 2TN, United Kingdom*
[b]*Department of Information Systems, Faculty of Intelligent Electrical and Informatics Technology, Institut Teknologi Sepuluh Nopember, Surabaya 60117, Indonesia*

Abstract

While ISPs were originally designed within single organisations, urban environments now require policies that accommodate the interests of multiple stakeholders. Focusing on Surabaya, Indonesia, and guided by the research question "what are the factors that influence development of ISPs in a multi-stakeholder context," this study explores key dimensions in the development and implementation of ISPs in multi-stakeholder urban settings. Based on 40 semi-structured interviews, a thematic analysis was conducted to identify key recurring patterns across stakeholder perspectives. This paper identifies synergies between organisational and city-level contexts and proposes a set of extended features needed when government agencies, market providers, IT consultants, and citizens all interact and contribute to ISPs development. Recommendations for achieving better compliance include the importance of clear communication, inclusive stakeholder involvement beyond bureaucracy, inter-agency coordination, and an expanded feedback loop incorporating insights from both staff and citizens.

Keywords: information security policy (ISP); compliance; multi-stakeholder context; inter-organisational coordination; governance; thematic analysis

1. Introduction

Information security policies (ISPs) are an essential strategy to managing the risks posed by insiders, as threats from employee behaviour continue to challenge modern organisations [1]. ISPs establish guidelines, restrictions, and

* Corresponding author.
E-mail address: tyas.darmaningrat@its.ac.id

responsibilities for users of information and technological resources to help prevent, detect, and address security issues [2,3]. ISPs vary widely among organisations based on the significance, value, and sensitivity of data and technology assets, as well as the potential consequences of data loss, alteration, or exposure [4,5]. Previous studies show how ISPs were developed and implemented primarily within the boundaries of individual, single organisations [1,6–11]. It is essential to recognise that ISPs are designed for authorised users of the information [12], which can also encompass individuals outside the organisation [13]. Although this can be helpful in identifying broader key processes, it does not sufficiently represent situations where complex interdependencies between organisations are formed, particularly when public and private sectors are both involved and need to work in an intertwined and interconnected way. This is typically where modern cities find themselves in.

Government agencies, market providers, and other institutional actors now share data, systems, and infrastructure in their day-to-day business processes. This shift necessitates a transition in ISP design towards an inter-organisational approach, where security is no longer the sole responsibility of a single entity, but a shared concern that must be addressed collaboratively [14]. Karlsson et al. [14] also note that there was a lack of comprehensive literature reviews on inter-organisational information security that systematically examine current research trends across a broad range of publication sources. As a result, there remains a significant gap in understanding the current state and progression of research in inter-organisational information security. Beyond organisational collaboration, cities today are becoming dynamic digital ecosystems involving multiple stakeholders. In this context, ISPs must evolve to reflect a multi-stakeholder perspective. In this multi-stakeholder environment, ISPs must consider diverse and sometimes competing interests, values, and legal obligations [15]. Therefore, this study aims to explore how ISP development in a multi-stakeholder setting differs from well-established ISP frameworks, including differing factors and priorities of different organisations, focusing on Surabaya city, Indonesia. Specifically, we pose the following research question: *what are the factors that influence development of ISPs in a multi-stakeholder context?*

This study contributes to existing academic knowledge by providing an examination of the processes and factors influencing the development of ISPs in a multi-stakeholder setting, addressing gaps in prior research, which often focus on single organisations [1,16,17]. Practically, on the other hand, this research can benefit stakeholders within Indonesian local government institutions by offering specific guidance on creating ISPs that align with organisational culture and recommendations for enhancing the ISP development processes. Engaging stakeholders in policy development is anticipated to increase their awareness of ISP importance and support successful ISP implementation within their organisations. The remainder of this paper is organised as follows: Section 2 discusses theoretical background related to this study, Section 3 outlines the context of this study, Section 4 presents the results of this study and followed by discussion about the results. Finally, Section 5 presents the conclusions drawn from this study.

2. Theoretical Background

2.1. Information Security Policies (ISPs)

Information security policies establish guidelines for safeguarding the information assets of an organisation. The intention of top management on the protection of information systems and the privacy and security of sensitive data is expressed in information security policies [4]. A well-developed ISP protects the organisation's sustainable development, improves employees' quality of life, and produces insights based on data [18]. Supportive organisational culture and end-user participation in policy development processes substantially influence employees' opinions about compliance [19]. Once employees' opinions about ISP compliance are enhanced, and the compliance culture is well-founded, the threat to the organisations' information assets and data is ultimately diminished [20]. In a city context, the concern is not only about the government employees' compliance with the ISP, but it should also be concerned about various stakeholders in the city environment, such as citizens and commercial providers. While individual businesses do face information security risks, collaborating across organisations brings additional risks, creating new opportunities for breaches, regulatory violations, and data exposure [14,21]. Hence, ensuring that citizens, government employees, and other stakeholders abide by the ISP should be considered during the ISP development stages. In addition, citizens will also be interested in how commercial providers and government employees are participating in the development of ISP and complying with information security standards, since

they will be interested in how their personal data is captured, stored securely, and shared responsibly. Therefore, there are privacy and security implications here which hopefully will prevent data breaches caused by irresponsible data handling.

2.2. International Standards of Information Security

International information security standards offer requirements for developing information security policies. According to Merchan-Lima et al. [22], Higher Education Institutions frequently employ COBIT, ISO 27000, ITIL, NIST, and EDUCAUSE as information security management standards. COBIT 5 for information security is a widely known framework that helps organisations achieve their goals and offers benefits from good governance and management of enterprise IT. Wolden et al. [23] examine the efficacy of COBIT 5 for information security framework implementation in lowering the risk of cyber-attacks on the Supply Chain Management Systems (SCMS). The findings suggest that COBIT 5 enhances the security of enterprise applications by introducing a new level of governance for information systems security. In several case studies, ISO 27001 and COBIT 5 are adopted simultaneously to achieve the full benefits of enterprise governance information technology [24,25]. ISO/IEC 27001 is another international standard that is globally recognised as an Information Security Management System (ISMS) specification issued by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). According to Höne & Eloff [26], information security policy standards are a valuable start for establishing an ISP. However, they should not be relied upon solely for the guidance given that their coverage is not thorough and frequently place more emphasis on the processes required to execute the ISP successfully than they do on the design of the policy [26]. Therefore, organisations should utilise international standards as one of many sources of guidance when developing ISPs rather than an exclusive reference.

2.3. ISPs Development Processes

There are various methodologies offered for ISPs development. Generally, there are three phases in ISPs development processes: input, development processes, and output [16]. The model proposed by Ward & Smith [11] outlines five stages in developing a policy for access control. This approach defines in detail the processing and outcomes of the policy but needs more detail in explaining the input and processing of raw data. In addition, an information security meta-policy has been developed by Baskerville and Siponen [6] to support different characteristics and environments in evolving organisations where the policy might need to be updated regularly. Moreover, Howard [8] offers eleven tasks over the life of a security policy. Some developmental tasks are rough compared to other models with a life cycle; for instance, authorisation, consultation, execution, familiarisation, and exemptions may be regarded as the implementation phase. Moreover, a Policy Framework for Interpreting Risk in eCommerce Security (PFIRES) has been initiated by Rees et al. [10]. This model is more straightforward in defining activities in the input, construction, and application phases as policy shifts over its lifetime. Nevertheless, this model needs to consider continuing preservation concerns and consider how to analyse the input before constructing the policy. Besides, Knapp et al. [27] establish a process model representation at the organisation level that incorporates inner and outer attributes and extends beyond the team of ISP development. This model also recognises the policy retiral, assessments, and automatic monitoring tools. Additionally, Flowerday and Tuyikeze [7] proposed another wide-reaching viewpoint on ISP development which also discusses the stakeholders who should be engaged in the process. However, they did not further examine the framework's implementation processes or additional inputs. Another ISP development framework proposed by Cram et al. [1] summarises a sequence of opportunities to tackle gaps and inconsistencies in the study of ISPs development (as presented in Fig. 1). The model incorporates social qualities of security constraints, for example, culture, emotions, personality traits, and policy fairness. Policy development still needs to improve these aspects [16]. This condition is also supporting the purpose of this study to uncover the impact of stakeholder participation in ISP development to achieve better ISP compliance. Furthermore, in the recent study, Stewart [17] proposed a general framework based on the Nine-Five-circle for developing, implementing and evaluating an organisation’s ISP. Based on this work, the author has proposed six constructs that can influence ISP development and outcomes, i.e. external partners or stakeholders, information security misperceptions, information security investment, organisational commitment, security intelligence, and cyber threat

intelligence. The author used a thorough and logical model that can serve as the foundation for a "checklist" for establishing and overseeing ISPs.

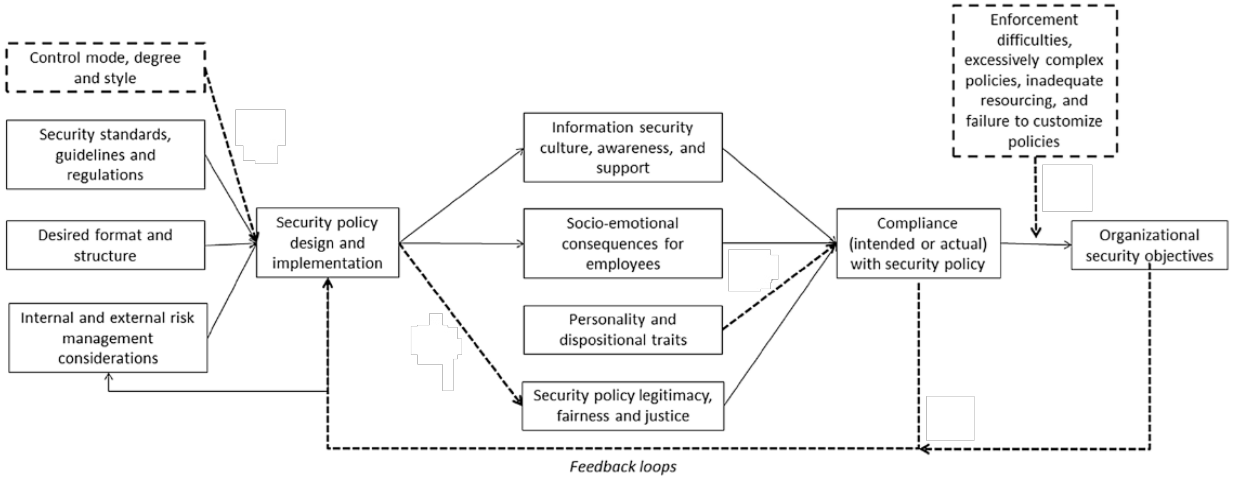

Fig. 1. Information Security Policy Framework Proposed by Cram et al. [1].

2.4. Stakeholders Involvement in ISPs Development

Stakeholders' support is required in the ISPs development and implementation processes. Maynard et al. [15] have reported different stakeholders in ISPs development, including top management, company division representatives, customer group, human resources, ICT professionals, legal teams, third-party representatives, security experts, and public affairs. Moreover, Flowerday and Tuyikeze [7] identified key stakeholders that must be engaged in ISPs development: top management, end-users, legal advocate, ICT specialist, the human resources department, and external agents. However, previous studies have yet to identify stakeholder roles in every phase of ISP development. End users have been recognised as one of the stakeholders in ISP development. In a city, government employees and citizens are also the end users of government-provided public services [18]. According to Wu et al. [18], the publication of ISPs should enable all citizens to read the pertinent rules at their leisure. All citizens must be able to learn and express their comments on the ISP documents. This involvement will impact citizens' moral judgments of the ISP since they will learn how the ISP is addressing data ownership and privacy concerns. Although stakeholder involvement is commonly discussed in other parts of the security policy, mainly concerning compliance, little thought is given to the subject when creating an ISP [1].

2.5. ISPs Compliance

Current research on information security policies (ISPs) has strongly emphasised the drivers of employee security policy compliance. Policy compliance and employee support are essential aspects that should be included in the formulation and execution of ISPs [7]. In order to facilitate employees' compliance with policy requirements, ongoing efforts should be made to ensure that they are aware of the policy [8]. Subsequently, the success of policy implementation efforts should be monitored and reported during the compliance monitoring phase [8]. The organisation culture will significantly influence the general attitude of employees toward security. The security team may encounter difficulties in enforcing a specific policy if the organisation culture cultivates opposition against security regulations that employees deem inappropriate [9]. The information security culture is positively influenced by reading and understanding the ISP [28]. Employees must read and comprehend the ISP to effectively direct behaviour, change attitudes toward policy compliance, and promote a robust information security culture [28]. Therefore, ISPs publication is required in ISPs development processes because it allows stakeholders to read and understand the ISP. Understanding the ISP will also lead to awareness and compliance toward the ISP.

3. Context of The Study

This research selects Surabaya as the study setting because it is one of Indonesia's leading smart cities, utilising technology and data-driven solutions to enhance urban governance, public services, and overall quality of life. The city of Surabaya has received multiple awards for its smart city initiatives. It was awarded the Smart Government and Smart Environment honours by the Ministry of Communication and Informatics at the 2023 National Smart City Forum, recognising its efforts in digital governance and environmental sustainability. Additionally, in 2019, Surabaya won the Indonesia Digital Economy Award in the city category, highlighting its progress in fostering a thriving digital economy [29]. As Surabaya continues to develop as a smart city, its residents are increasingly integrating digital services into their daily lives, including the use of e-government platforms, cashless payment systems, and online public services. The city has also witnessed a significant rise in young professionals and students actively participating in the technology startup ecosystem and contributing to the digital economy sector [30]. To further enhance digital literacy and information technology skills, the Surabaya City Government has established Broadband Learning Centre (BLC) facilities across the city. This initiative is part of the Surabaya Smart City program, designed to bridge the digital divide and ensure equitable access to technology for all segments of society. The BLCs serve as Information and Communication Technology (ICT) learning hubs, offering free training programs focused on essential digital skills, including computer proficiency, internet usage, and digital application literacy [31]. By equipping citizens with these competencies, the initiative supports workforce readiness and digital inclusion in Surabaya.

To accelerate service delivery and streamline administrative procedures, the Surabaya City Government has implemented a range of e-government systems, reducing bureaucratic complexity and increasing accessibility for both citizens and businesses. With the ongoing digital transformation in governance, the Surabaya City Government has also introduced policies aimed at strengthening information security [32]. However, currently there is no unified national standard in Indonesia for formulating information security policies (ISPs). Although the National Cyber and Crypto Agency provides some guidance and international frameworks like ISO 27001 and ISO 27002 are commonly used, there is no overarching national framework that directs ISPs development across various sectors. As a result, organisations often depend on international models or external consultants, which can lead to policies that are either impractical to implement or not well understood by end users. This lack of a comprehensive, cross-sectoral national framework for ISP development represents a significant gap in Indonesia's information security landscape and serves as a key motivation for this study.

Information security policies in a city must evolve from an organisational framework to a broader, multi-stakeholder context by taking into account the interests and responsibilities of various stakeholders. Ensuring comprehensive information protection requires strong synergy between the city government, private sectors, academic institutions, and citizens. By adopting this approach, ISPs in urban settings are not only confined to specific organisations but also serve to safeguard society as a whole through well-defined regulations and effective cross-sector collaboration. However, existing ISP frameworks predominantly focus on individual organisations rather than on a broader, multi-stakeholders' context [1,7,9,10]. This research seeks to analyse the implementation of the organisational ISP framework proposed by Cram et al. [2] and explore its extension to ensure compliance within a multi-stakeholder environment. The framework was chosen for its robustness, adaptability, and broad recognition, offering a valuable structure for understanding how information security policies are developed within organisations. Its clarity, comprehensiveness, and openness to extension make it an ideal foundation for research that seeks to adapt and expand ISP models into more complex, inter-organisational, and urban governance settings, such as in the Surabaya city.

This research employed 40 semi-structured interviews with ten representatives from each of the four stakeholder groups, each playing a distinct role in the city's information security landscape. These groups include the Surabaya city government as the primary regulatory authority responsible for formulating, enforcing, and overseeing information security policies at the municipal level; IT consultants as experts who support the government in developing, assessing, and improving information security frameworks and policies; Market providers or IT-based companies as representatives from private sector entities that offer IT services, develop digital infrastructure, and manage systems that handle citizens' data as part of the smart city initiative; and Citizens of Surabaya as end-users of digital services provided by both the government and private sector, whose data security and privacy are directly

impacted by ISP regulations and practices. By examining the interactions between these stakeholder groups, this study aims to provide a comprehensive understanding of how ISPs can be effectively implemented in a multi-stakeholder urban environment, ensuring both regulatory compliance and enhanced information security.

4. Results and Discussion

According to Braun & Clarke [33], thematic analysis consists of six stages i.e., familiarisation with data, generating initial codes, searching for themes, reviewing themes, defining and naming themes, and producing the report. In this research, the initial codes were developed based on the Cram's framework [1]. Then, the researcher generated new codes to accommodate excerpts from the interviews that did not match with any codes from the initial codes. For instance, Cram et al. [1] identify three key drivers of ISP compliance: (1) organisational characteristics, managerial and informal controls; (2) emotional impacts; and (3) personality and dispositional traits. However, through the interviews, a much broader set of dimensions was revealed, such as the importance of ethical considerations in promoting policy compliance and change management in dealing with transition periods following the introduction of a new policy. These were translated into 'new codes' and formed part of the analysis as shown in Table 1. Afterward, the codes derived from the preceding phase were analysed to discover their interrelationships and subsequently organised into distinct themes. The themes were referred to the relationships in Cram's framework [1], i.e. ISPs design and implementation factors, the influence of ISPs on both the organisation and individual employees, the organisational and individual factors that drive policy compliance, the impact of ISPs on achieving organisational objectives, the feedback loop, and with one additional theme, multi-stakeholder.

Based on the Cram's framework [1], there are some factors that serve as an input for ISPs design and implementation, namely (1) information security standards, guidelines and regulations, (2) the format and content of ISPs, (3) risk considerations, and (4) the control mode, degree, and style. Based on the interview findings, not all factors from the original framework were evident; instead, Indonesia's bureaucratic structures and regulatory-driven approach emerged as dominant influences, especially in Surabaya. Government regulations largely dictate ISP development and the adoption of international security standards. The second factor, the influence of ISPs on the organisation and individual employees, includes (1) information security culture, awareness and support, (2) socio-emotional consequences of ISPs, and (3) the perceived legitimacy of the policies. Narratives from the interviews suggested that the impact of ISPs in Indonesia centres on raising awareness and ensuring organisational support. As ISPs are still relatively new in the country, widespread dissemination and stakeholder education are crucial. The interviews highlighted that both employees and citizens need greater awareness to improve compliance and reduce risks. Organisational support, particularly through training and awareness programs, is essential, yet government agencies often deprioritise ISPs, resulting in weak enforcement and limited outreach. The third factor, the organisational and individual factors that drive policy compliance, includes (1) the influence of organisational characteristics, managerial and informal controls, (2) emotional impacts, (3) personality traits, and (4) ethical considerations in relation to compliance with ISPs. Insights gathered from interviews reveal that managerial control is key to ensuring compliance with ISPs, especially within Indonesia's top-down organisational structures. Strong leadership support helps embed ISPs into daily operations, shapes employee behaviour, and fosters a security-conscious culture. Public transparency and stakeholder involvement also play vital roles; despite centralised policymaking, citizens and staff express a desire to provide feedback, which could lead to more effective and relevant policies. The fourth factor, the impact of security policies on achieving organisational objectives, explores the challenges that mediate the success of these objectives, such as enforcement issues, resource availability, policy complexity, and the need for policy customisation. Narratives from the interviews indicated that implementing ISPs in Indonesia faces major challenges, including inconsistent enforcement, limited resources, and a lack of leadership prioritisation. Continuous monitoring is essential to ensure compliance and identify non-compliance for corrective action. However, without adequate funding, infrastructure, and top management support, ISPs risk becoming symbolic rather than practical tools. Subsequently, the feedback loop reflects the iterative process of ISPs, acknowledging that they are developed and refined both before and after implementation. Effective feedback loops are essential for refining ISPs and ensuring their ongoing relevance. According to participants' accounts, in a multi-stakeholder environment, feedback mechanisms should be extended to include diverse input from government, private sector, and the public. A strong measurement system is also needed to evaluate policy effectiveness. Lastly, the study highlights factors specific to a multi-stakeholder setting that have not been discussed in the Cram's framework, including communication behaviour and coordination mechanisms. The interview findings

demonstrated that clear and consistent communication is essential to ensure all stakeholders, including citizens, understand the ISPs. In a multi-stakeholder environment, the ISPs monitoring process should involve not only internal organisational reviews but also coordination between the government, market providers, and citizens. Effective collaboration among these stakeholders can enhance policy oversight and responsiveness. This coordination may also necessitate the establishment of a dedicated government function responsible for overseeing and facilitating these interactions to ensure alignment and accountability.

Table 1. Themes and sub-themes developed in the thematic analysis process.

Themes	Sub-themes	Sub-ordinate themes
Inputs of ISP design	Security standards, guidelines, and regulations	*Guidelines availability*
	ISP format and content	*Literatures*
	Risk considerations	
	Control mode, degree, and style	*Bureaucracy aspects*
Impacts of ISP on organisation and individual employees	Information security culture, awareness, and support	
	Socio-emotional consequences	
	Perceived legitimacy	
Factors driving compliance	Organisational characteristics, managerial and informal controls	
	Emotional impacts	
	Personality and dispositional traits	
	Ethical issues	*Stakeholder involvement*
		Public transparency
	Change management	
Challenges mediate organisational objectives achievements	Enforcement issues	*Inconsistencies*
	Resources availability	
	Complex policy	
	Policy customisation	
	Top management priorities	*New policy*
		Policy availability
		Incident reporting
Policy adjustment (Feedback loop)	Policy review	*Frequency of reviews*
		Reasons for updates
		Measurement tools
		Knowledge management
	Feedback mechanisms	
Multi-stakeholder context	*Communication behaviour*	
	Coordination mechanisms	

Note:
- The sub-themes printed in italic were new codes.

According to the interview results, the study points out some possible additions to the Cram's framework, which might be beneficial in achieving compliance in a multi-stakeholder context and improving the information security practice in Indonesia. First, in a multi-agency setting, the importance of communicating policies clearly and the intention of policy makers to inform all stakeholders about the policies, including citizens, should be emphasised. ISP development in Surabaya is primarily state driven, following the bureaucratic control mode. All communication activities between the layers needed to implement ISP better seem to be discrete levels of hierarchy, with limited

transparency between communication channels. The involvement of non-government stakeholders (e.g. citizens, market providers, and non-state elements) should be considered to achieve ISP compliance. Hence, there should be a clear mechanism on how to cascade down the policy so that the policy makers and implementers have common understanding. Therefore, how a new policy will be introduced to various stakeholders, what media will be used, who will be responsible for the activities, and when the activities will be conducted need to be carefully considered during the design phase of security policy. Second, coordination mechanisms between the government and market providers as well as citizens in a multi-stakeholder context are crucial. In a multi-agency setting the communication and coordination are not only top-down in a single organisation hierarchy but also horizontal across different agencies. New technologies have enabled new types of organisations in which bureaucracy can take new forms or be combined with or displaced by other coordination mechanisms [34]. In this coordination effort, an intermediate agency may be required to oversee overall coordination. The intermediate agency is a new system of work that could bring incentives for the government, such as better management of resources and cost savings, whilst providing a better service. For market providers, such a setup would require incentivising the private sector to have more direct involvement, thus increasing investment in this area. Lastly, in a multi-agency environment, the 'feedback loops' should be expanded to incorporate input from various entities within the city, reflecting its dynamic nature, and navigating between different levels of the hierarchy. It is also important to consider how the feedback mechanisms in a multi-stakeholder setting will be designed to accommodate input from diverse stakeholders. Citizens and operational staff are currently not involved in any ISP-related process, but hopefully in future changes will emerge to allow for additional feedback opportunities to take place.

5. Conclusions

In conclusion, this study highlights the ISP development processes in a multi-stakeholder setting, demonstrating the importance of communication and coordination, the role of non-government stakeholders, and the extended feedback loop for incorporating views of market providers and citizens. Our findings provide new insights into ISP design by capturing diverse perspectives on the processes and factors shaping ISP development in a multi-stakeholder setting. From a practical standpoint, this research offers guidance to local government institutions in Indonesia and beyond on how to improve ISP development to achieve and sustain higher levels of compliance and commitment. This is currently a challenge for many local authorities, who aim to redefine or tailor existing processes and procedures by drawing on expertise from other agencies, while still maintaining their own service offerings and cultural norms.

Acknowledgements

We would like to thank the Centre for Higher Education Funding and Assessment, Ministry of Higher Education, Science, and Technology of Republic Indonesia for supporting this research under "*Beasiswa Pendidikan Indonesia* (BPI)" award 2021-2025.

References

[1] Cram, W. Alec, Jeffrey G. Proudfoot, and John D'Arcy. (2017) "Organizational information security policies: A review and research framework." *European Journal of Information Systems*; **26 (6)**: 605–41. https://doi.org/10.1057/s41303-017-0059-9.

[2] Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. (2010) "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly*; **34 (3)**: 523-548. https://doi.org/10.2307/25750690.

[3] Lowry, Paul Benjamin, and Gregory D. Moody. (2015) "Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies." *Information Systems Journal*; **25 (5)**: 433–463. https://doi.org/10.1111/isj.12043.

[4] Landoll, Douglas. (2017) "Information Security Policies, Procedures, and Standards". 1st edition. Auerbach Publications.

[5] Whitman, Michael E., Anthony M. Townsend, and Robert J. Aalberts. (2001) "Information Systems Security and the Need for Policy", In: Gurpreet Dhillon (ed) *Information Security Management*, IGI Global, p. 9–18. https://doi.org/10.4018/978-1-878289-78-0.ch002.

[6] Baskerville, Richard, and Mikko Siponen. (2002) "An information security meta-policy for emergent organizations." *Logistics Information Management*; **15 (5/6)**: 337–346. https://doi.org/10.1108/09576050210447019.

[7] Flowerday, Stephen V., and Tite Tuyikeze. (2016) "Information security policy development and implementation: The what, how and who." *Computers and Security*; **61**:169–183. https://doi.org/10.1016/j.cose.2016.06.002.

[8] Howard, Patrick D. (2003) "The Security Policy Life Cycle: Functions and Responsibilities." *Data Security Management*, Auerbach Publications.

[9] Knapp, Kenneth J., R. Franklin Morris, Thomas E. Marshall, and Terry A. Byrd. (2009) "Information security policy: An organizational-level process model." *Computers & Security*; **28 (7)**:493–508. https://doi.org/10.1016/j.cose.2009.07.001.

[10] Rees, Jackie, Subhajyoti Bandyopadhyay, and Eugene H. Spafford. (2003) "PFIRES: A Policy Framework for Information Security." *Communications of the ACM*; **46 (7)**:101–6. https://doi.org/10.1145/792704.792706.

[11] Ward, Peter, and Clifton L Smith. (2002) "The Development of Access Control Policies for Information Technology Systems." *Computers & Security*; **21 (4)**: 356–371. https://doi.org/10.1016/S0167-4048(02)00414-5.

[12] Yeniman Yildirim, Ebru, Gizem Akalp, Serpil Aytac, and Nuran Bayram. (2011) "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey." *International Journal of Information Management*; **31 (4)**: 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006.

[13] Sindhuja, PN. (2014) "Impact of information security initiatives on supply chain performance: An empirical investigation." *Information Management & Computer Security*; **22 (5)**: 450–473. https://doi.org/10.1108/IMCS-05-2013-0035.

[14] Karlsson, Fredrik, Ella Kolkowska, and Frans Prenkert. (2016) "Inter-organisational information security: a systematic literature review." *Information and Computer Security*; **24 (5)**: 418–451. https://doi.org/10.1108/ICS-11-2016-091.

[15] Maynard, SB, A. B. Ruighaver, and A. Ahmad. (2011) "Stakeholders in security policy development." *9th Australian Information Security Management Conference*, p. 5–7. https://doi.org/10.4225/75/57b546fecd8c6.

[16] Paananen, Hanna, Michael Lapke, and Mikko Siponen. (2020) "State of the art in information security policy development." *Computers and Security*; **88**: 1-14. https://doi.org/10.1016/j.cose.2019.101608.

[17] Stewart, Harrison. (2022) "A systematic framework to explore the determinants of information security policy development and outcomes." *Information and Computer Security*. **30 (4)**. https://doi.org/10.1108/ICS-06-2021-0076.

[18] Wu, Yung Chang, Rui Sun, and Yenchun Jim Wu. (2020) "Smart city development in Taiwan: From the perspective of the information security policy." *Sustainability*. **12 (7)**: 1-18 https://doi.org/10.3390/su12072916.

[19] Amankwa, Eric, Marianne Loock, and Elmarie Kritzinger. (2018) "Establishing information security policy compliance culture in organizations." *Information and Computer Security*; **26 (4)**: 420–36. https://doi.org/10.1108/ICS-09-2017-0063.

[20] Parsons, Kathryn M., Elise Young, Marcus A. Butavicius, Agata McCormac, Malcolm R. Pattinson, and Cate Jerram. (2015) "The Influence of Organizational Information Security Culture on Information Security Decision Making." *Journal of Cognitive Engineering and Decision Making*; **9 (2)**: 117–129. https://doi.org/10.1177/1555343415575152.

[21] Goodman, S. E., and Rob Ramer. (2007) "Identify and Mitigate the Risks of Global IT Outsourcing." *Journal of Global Information Technology Management*; **10 (4)**: 1–6. https://doi.org/10.1080/1097198X.2007.10856452.

[22] Merchan-Lima, Jorge, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca, and Dorys Quiroz. (2021) "Information security management frameworks and strategies in higher education institutions: a systematic review." *Annales Des Telecommunications/Annals of Telecommunications*; **76 (3-4)**: 255–270. https://doi.org/10.1007/s12243-020-00783-2.

[23] Wolden, Mark, Raul Valverde, and Malleswara Talla. (2015) "The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system." International Federation of Automatic Control, **48 (3):** 1846–1852. https://doi.org/10.1016/j.ifacol.2015.06.355.

[24] Almeida, Rafael, Renato Lourinho, Miguel M. Da Silva, and Rúben Pereira. (2018) "A model for assessing COBIT 5 and ISO 27001 simultaneously." *Proceeding - 20th IEEE International Conference on Business Informatics*, CBI, vol. 1, Institute of Electrical and Electronics Engineers Inc.; p. 60–69. https://doi.org/10.1109/CBI.2018.00016.

[25] Wendy, Wendy, Wang Gunawan. (2019) "Measuring Information Security And Cybersecurity On Private Cloud Computing." *Journal of Theoretical and Applied Information Technology*; **96 (1)**: 156–168.

[26] Höne, Karin, and J.H.P Eloff. (2002) "Information security policy — what do international information security standards say?" *Computers & Security*; **21 (5)**: 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7.

[27] Knapp, Kenneth J., and Claudia J. Ferrante. (2012) "Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations." *Journal of Management Policy and Practice*; **13 (5):** 66–80.

[28] Da Veiga, Adéle. (2016) "Comparing the information security culture of employees who had read the information security policy and those who had not Illustrated through an empirical study." *Information and Computer Security*; **24 (2)**: 139–151. https://doi.org/10.1108/ICS-12-2015-0048.

[29] Pemkot Surabaya. (2024) "Daftar Prestasi Surabaya Tiap Tahun." https://www.surabaya.go.id/page/0/49215/penghargaan.

[30] Pemkot Surabaya. (2023) "Wali Kota Eri Cahyadi Ajak Anak Muda Surabaya Gerakkan Ekonomi melalui Startup." https://www.surabaya.go.id/id/berita/77399/wali-kota-eri-cahyadi-ajak-anak-muda-surabaya-gerakkan-ekonomi-melalui-startup.

[31] BLC. (2018) "Tentang BLC Surabaya." https://blc.surabaya.go.id/informasi/tentangblc.

[32] Dinkominfo, Surabaya. (2023) "Mayor Regulation Number 62 of 2023."

[33] Braun, Virginia, and Victoria Clarke. (2006) "Using thematic analysis in psychology." *Qualitative Research in Psychology*; **3 (2)**:77–101. https://doi.org/10.1191/1478088706qp063oa.

[34] Monteiro, Pedro, and Paul S. Adler. (2022) "Bureaucracy for the 21st Century: Clarifying and Expanding Our View of Bureaucratic Organization." *Academy of Management Annals*; **16 (2)**: 427–475. https://doi.org/10.5465/annals.2019.0059.