Corporate Management Review
Vol. 44 No. 2, 2024
pp. 39-79

Aligning stakeholder goals for effective information security in e-government systems: A grounded theory approach

探討利害關係人目標融合對電子化政府資訊安全效率的提升:使用紮根理論

Chia-ping Yu[1]
Department of Information Management, Tamkang University
Christina Ling-hsing Chang
Department of Information Management, National Sun Yat-sen University
Hsun-Yuan Hsu
Department of Information Management, Tamkang University

Abstract: The e-government system operates autonomously, providing a comprehensive array of services to government personnel. It is essential to consider the costs associated with information security incidents, which include expenses, capital investments, and personnel within the e-government system. The primary objective of this research has been to identify security goals among primary stakeholders in the e-government system, with a particular emphasis on E-Net. Interviews were conducted with 13 participants from five disparate stakeholder groups through selective sampling. The interview data was analyzed using grounded theory methodology. There are several findings: first, security management is crucial in ensuring the integrity of data and promoting system effectiveness. Cooperation among stakeholders in the E-Net system leads to skillful interweaving of common goals, management mechanisms, and resources. Second, satisfaction is a significant factor in optimizing system performance, as technical units, business units, and vendors analyze security requirements, design

[1] Corresponding author: Chia-ping Yu, Department of Information Management, Tamkang University. Email: cpyu@mail.tku.edu.tw.

DOI: 10.53106/102873102024124402002

systems, and provide clear operational processes. Third, system security goals foster awareness and promote its value among technical and business units, directing them to participate in security control activities. Operational processes and control activities help maintain data integrity and system security. This paper explores the importance of common goals in IS security projects, highlighting their role in aligning stakeholders' goals, adjusting management processes, and defining security rules.

Keywords: Information system security, common goal, stakeholder, grounded theory.

摘要：電子化政府系統的運作為民眾提供了全面的自動化服務，在考慮資訊安全議題時，需包括資訊安全維運費用、投資成本以及電子化政府系統內的人員訓練等。本研究的主要目的是觀察電子化政府系統中主要利害關係人的資訊安全目標。本研究採用選擇性抽樣方法，以 **E-Net** 電子化政府系統為例，對來自五個不同利害關係人單位共 **13** 名參與者進行訪談，並使用扎根理論方法進行資料分析。研究發現，首先，資訊安全管理的關鍵在於確保資料完整性以及促進系統效能，而這些都建立在利害關係人之間的共同目標。**E-Net** 系統中，各利害關係人之間的合作、管理機制的建立和資源的管理，都是基於這些共同目標。其次，滿意度是優化系統效能的重要因素。為了達成這一目標，政府技術單位、政府業務單位和資訊系統供應商分析安全需求、設計系統並提供清晰的操作流程，從而合作完成共同目標。第三，系統安全這一共同目標提高了政府技術和業務單位的資安意識，並提升了他們的資安價值觀，引導政府技術和業務單位一同參與資安控制活動。而這些控制活動也有助於維持資料完整性和系統安全。本研究深入探討了共同目標在資訊系統安全專案中的重要性，強調共同目標對於融合利害關係人個別目標、調整管理流程和定義安全規則的重要性。

關鍵詞：資訊安全、共同目標、利害關係人、紮根理論

1. Introduction

Connecting systems to a network intensifies the potential risks they encounter (Whitman and Mattord, 2017). An e-government system, a digital platform that automates and offers a range of services to public servants, residents, public agencies, and corporate groups (Marcuzzo do Canto Cavalheiro and Joia, 2016), is a prime example of such a system. Information system security significantly influences the efficiency, operating expenses, and decision-making quality of public sector systems (Almeida Prado Cestari *et al.*, 2020; Gazley *et al.*, 2010; Rowley, 2011). Consequently, information security events typically result in financial expenses such as labor costs, capital investments, and operating expenditures. Additionally, studies by Almeida Prado Cestari *et al.* (2020), Yeh and Chang (2007), and show that they seriously undermine trust between the general public and their government. As a result, it is imperative that all stakeholders, including public departments, corporate units, vendors, and agencies, collectively prioritize and effectively oversee information system security without any exceptions. Exercising caution and remaining aware is crucial due to the substantial potential risks associated with information system security.

The main area of interest for most researchers has been the procedures used to ensure the security of information systems. The software development lifecycle has provided extensive recommendations for the implementation of information security measures (Kim and Seong Leem, 2005; Ma *et al.*, 2008; Yu *et al.*, 2018). Multiple studies discovered information security concerns by either creating an information system or assessing the adequacy of existing security measures (Dong *et al.*, 2021; Loft *et al.*, 2021; Ma *et al.*, 2008; White, 2009). Researchers have examined the security policies, problems, resources, costs, and benefits associated with the adoption of standards by businesses (Backhouse *et al.*, 2006; Siponen and Willison, 2009). Several studies suggest that information security managers can make their systems safer by looking at different tests that evaluate control management and then putting information security standards into place (Backhouse *et al.*, 2006; Dong *et al.*, 2021; Kim and Seong Leem, 2005; Ma *et al.*,

2008; Niemimaa and Niemimaa, 2017; Siponen and Willison, 2009; Yu *et al.*, 2018). Despite initiatives to implement effective control and management mechanisms, the public sector often suffers from inadequate technological resources (Madaki *et al.*, 2024). Additionally, resistance to change within collaborative units can diminish the resources allocated for e-government security implementation, which is crucial for promoting the goals and values of information system security (Atkins and Lawson, 2021). Insufficient awareness and resistance lead to poor prioritization of security initiatives, further straining the limited resources available (Atkins and Lawson, 2021; Madaki *et al.*, 2024). Moreover, the lack of skilled personnel and inadequate training programs exacerbate these challenges, highlighting the need for qualified personnel and organized training systems in the public sector (Atkins and Lawson, 2021).

Still, the protection of information systems (IS) necessitates collaboration with the appropriate individuals and the incorporation of diverse perspectives into information security goals, methodologies, or assets (D'Aubeterre *et al.*, 2008; Yeh and Chang, 2007; Yu *et al.*, 2018). The e-government system facilitated collaboration among individuals from a variety of units, such as government departments, agencies, enterprises, and technology units. Indeed, public sector information systems often operate with various or conflicting goals that involve the exchange of substantial amounts of sensitive or private information between public and private units. This necessitates a careful balance between facilitating convenient information access and implementing rigorous permission monitoring to prevent unauthorized access (Joshi *et al.*, 2001; St-Hilaire, 2020). For example, the inherent conflict goals make information security management particularly challenging, exacerbating the difficulty of balancing security with operational efficiency (St-Hilaire, 2020). Consequently, the key to information systems security in the public sector is to align goals that are inclusive of the interests, values, goals, and resources of all stakeholders (Gazley *et al.*, 2010; Hsu, 2009; Yu *et al.*, 2018).

However, information systems security projects engage multiple units responsible for addressing their respective concerns and delivering public value,

which may occasionally be at odds with one another. These stakeholders provide varied knowledge that enhances e-governance and information security, leading to better utilization of e-services (Bokhari and Myeong, 2023). However, the diversity of stakeholders can also introduce uncertainty, potentially obstructing the formulation of security goals and effective collaboration (Brockmyer, 2016). Integrating diverse interests and values into security goal setting is essential but challenging, as these stakeholders can affect uncertain outcomes (Gnan *et al.*, 2013). Wong (2005) observed that participants in an information system project possess varying desired values, which may affect their collaboration. Distel *et al.* (2022) proposed that a security project must achieve a balance between system effectiveness and security. Alexopoulos *et al.* (2023) noted that security frequently affects the usability of information system designs. These conflicts may be mitigated through a comprehensive understanding of the interplay between common goals and specific goals, which facilitates cooperation or collaboration among parties (Wong, 2005). This comprehension is essential for effective collaboration among various units to recognize and align goals, ascertain participants' values, and articulate the tensions present among them (Carney *et al.*, 2011).

In conclusion, the uniqueness of information security concerns in the public sector is defined by multiple or conflicting aims, resource restrictions, and the involvement of numerous stakeholders. These variables present particular problems and demands for tackling information security issues in the public sector. While information security concerns are not exclusive to public sector systems, the study highlights the specific characteristics of these challenges in the public sector. Despite considerable public sector research on objectives, resources, and multiple stakeholders in information security, prior studies have disregarded these stakeholders' distinct demands and obstacles when developing information security goals across different groups. This study looks at the alignment of goals for essential players across diverse units to maintain the security of information systems. How do collaborative units define and align their shared and unique goals? How do public sector players interact to achieve various security objectives?

Which key management mechanisms for information security should be considered? These questions are critical for investigating IS security management in e-government systems, which involve several entities working together. This study intends to assist key stakeholders in understanding the process of identifying common goals, aligning diverse particular goals, and conducting management activities to create a comprehensive information security system.

2. Literature review

The primary goal of IS security is to establish proactive measures to mitigate potential risks to the system's integrity and functionality. These proactive measures involve setting security goals, implementing control and administrative interventions, and fairly distributing resources (Hsu, 2009). The primary goals of IS security include the efficient implementation of policies, the promotion of safety consciousness among IS users, and the creation of value (Loft *et al.*, 2021). Resources play a crucial role in the success of IS security management techniques, as demonstrated by various studies(Almeida Prado Cestari *et al.*, 2020; Cao *et al.*, 2011; D'Aubeterre *et al.*, 2008; Rowley, 2011). To achieve the common goals associated with IS security, project managers must understand the collaborative dynamics among IS stakeholders. This understanding involves acknowledging varied priorities and developing a comprehensive and adaptable strategy for resource management. The following sections provide a detailed analysis of the goals, control methods, and essential resources necessary for IS security. A strategic approach to managing resources is emphasized to ensure the successful implementation of security measures and the achievement of IS security goals.

2.1 IS security goals

Organizations must implement exhaustive standards, norms, laws, or regulations that their members must adhere to in order to establish IS security goals. One such standard is the International Organization for Standardization-International Electrotechnical Commission (ISO/IEC) 27002, which is essential in the establishment of international information security standards. For example, the

ISO/IEC 27001 international security standard outlines three fundamental goals of information security: confidentiality, integrity, and availability. Confidentiality ensures that only authorized users can access information, preserving participants' privacy. Integrity requires that the data used in data manipulation or information service delivery be accurate and complete. Availability ensures that authorized users can promptly access correct, related, and complete information and data in the information system.

The laws, rules, and standards related to IS security influence the design and implementation of an organization's IS security mechanisms (Backhouse *et al.*, 2006). For instance, the British Standards Association has proposed a suitable control method for information security (BS7799-1:1999). International IS security standards and certifications, such as ISO 27001, Trusted Computer System Evaluation Criteria, and Control Goals for Information and Related Technology, define clear rules, policies, and concepts for security that managers, users, and technical staff can utilize to achieve IS security goals (Hedström *et al.*, 2011; Loft *et al.*, 2021; Siponen and Willison, 2009; Whitman and Mattord, 2017). For IS project managers, compliance with international standards and IS security regulations is crucial. These managers allocate resources to develop a plan and establish guidelines for IS security management (Dhillon and Torkzadeh, 2006; Hedström *et al.*, 2011).

Achieving information security goals is crucial for the integrity and reliability of organizational information systems. However, the management encounters difficulties in reconciling system efficacy with security. Fadlullah *et al.* (2022) and Huang *et al.* (2006) demonstrate a trade-off between augmenting protection against attacks and minimizing downtime while enhancing user pleasure. Organizations aiming to enhance system performance often prioritize speed and swift reaction times, which may jeopardize security protocols (Dombora, 2016). Centralized and streamlined IT systems can enhance efficiency; nevertheless, Ricker (2018) identified increased vulnerability stemming from inadequate redundancy and adaptability, making them more susceptible to assaults or breakdowns. The public sector faces a significant conflict between system

performance and security due to the complex nature of its information systems. Joshi *et al.* (2001) and St-Hilaire (2020) observe that these systems function within a multi-domain environment characterized by the exchange of substantial amounts of sensitive or private information between public and private entities. This necessitates a careful equilibrium between facilitating convenient information access and implementing rigorous permission monitoring to avert unauthorized access (Joshi *et al.*, 2001). The complexity inherent in public sector projects frequently results in insufficient risk management practices, thereby exacerbating the challenge of balancing security with operational efficiency (St-Hilaire, 2020). Effective risk management processes, encompassing risk identification, analysis, classification, mitigation, and control, are crucial for addressing these trade-offs. These processes, frequently neglected, result in projects failing to achieve their objectives (Joshi *et al.*, 2001; St-Hilaire, 2020).

The stakeholders in a project have distinct goals based on their interests, but their ultimate responsibility is to protect information services from potential risks and ensure the long-term viability of their organization's activities. Technical managers prioritize system performance, security procedures, and system functionalities, which motivates them to allocate significant resources to implement security mechanisms to regulate user behavior. On the other hand, system users prioritize user experience, advocating for security strategies, processes, and methods that prioritize the user interface. Therefore, the common goal among the different stakeholders involved in IS projects is to achieve information security through the implementation of IS security strategies and the careful allocation of resources. When IS managers synchronize the specific goals of each organization involved in the IS and determine common goals, they can prioritize different security control measures and allocate resources accordingly.

To sum up, the security goals set the direction and define what needs to be protected and how. Achieving these goals requires specific management mechanisms and adequate resources. Without clear goals, it is challenging to determine the necessary actions and allocate resources effectively.

2.2 IS security management

Businesses implement security management to safeguard information, services, and ISs, mitigate the consequences of security breaches on the company, and reduce harm to ensure the long-term growth of the business (Dong *et al.*, 2021; Loft *et al.*, 2021; Whitman and Mattord, 2017). Software, hardware, data, and services are valuable assets for businesses and their stakeholders. It is crucial to secure these assets from any unauthorized modifications, destruction, theft, or unavailability (Dong *et al.*, 2021; Siponen and Willison, 2009). IS security management entails strict adherence to the standards, norms, regulations, or laws established by organizations, the international community, industry, or government. Distinct management methodologies encompass control measures, operational protocols, and instructional initiatives.

An organization strives to achieve suitable security measures for its information systems rather than aiming for perfect security (Dong *et al.*, 2021; Vroom, 2004). Organizations must develop a strategic plan that incorporates IS procedures and promotes a common goal of IS security among all stakeholders in the long run (Kim and Seong Leem, 2005; Loft *et al.*, 2021; White, 2009). Hence, in order to achieve the goals of IS security, it is imperative that all individuals or groups involved in IS actively engage in IS security management (Ma *et al.*, 2008; White, 2009; Whitman and Mattord, 2017). The management hierarchy of an organization plays a crucial role in effectively addressing security concerns and other information security issues (Loft *et al.*, 2021; White, 2009). Indeed, the management processes outlined here align with the IS security goals specified by different stakeholders (Hsu, 2009; White, 2009).

It is important to use the right IS security processes or control methods during normal operations to keep data safe, keep information private, and maintain the IS's integrity and availability for safety and effectiveness. During critical incidents such as natural disasters, cyber-attacks, virus infections, hardware failures, or human errors, managers should prioritize the oversight of technical operations, maintenance, and monitoring of individuals and events associated with information security (Loft *et al.*, 2021; Niemimaa and Niemimaa, 2017; Vroom, 2004). Training programs provide immediate benefits by instructing users on the

proper utilization of technology, accessing data, interacting with other individuals, exchanging knowledge, and effectively implementing information system security (White, 2009; Whitman and Mattord, 2017). Consequently, resources play a key role in establishing the appropriate management procedures for high-priority targets in IS security. Adherence to security management is not only a requirement but also a responsibility that ensures the safety and integrity of information systems with limited resources.

Overall, security management is the tools and processes utilized to achieve security goals and translate these goals into actionable steps. In other words, security management serves as the means through which security goals are realized. However, to realize these security goals, security management is heavily dependent on the availability and proper allocation of resources.

2.3 IS security resources

The successful execution of information systems security depends on critical technologies, skilled staff, and organizational assets. Nevertheless, these resources are limited and are possessed by various stakeholders engaged in an IS project, including IT experts, managers, and end-users (Dong *et al.*, 2021; Drnevich and Croson, 2013). The resources can be classified as either tangible or intangible. Tangible resources include information technology, capital, human resources, assets, and expertise. Conversely, intangible resources include company culture, value, characteristics of information technology, innovative skills, and customer service.

To achieve information security objectives and implement effective management systems, organizations must empower themselves by dedicating sufficient resources to information technology, human capital, and organizational assets (Dhillon and Torkzadeh, 2006). Efficient resource acquisition, allocation, sharing, and integration are essential in an information systems project for forming alliances and partnerships. Acquiring and disseminating resources can foster collaboration among key stakeholders, thereby enhancing their engagement and assisting them in attaining information security objectives. Consequently, IS

possesses immense importance. Organizations currently emphasize not only the enhancement of information security to protect their assets but also the formulation of collaborative objectives with other entities to safeguard their informational assets (Dong *et al.*, 2021; Loft *et al.*, 2021; Niemimaa and Niemimaa, 2017; White, 2009).

Public sector organizations frequently encounter resource constraints in the implementation of information security measures. The study (Madaki *et al.*, 2024) highlights inadequate technological resources in the e-government sector, despite public sector initiatives to implement technologies that effectively tackle security challenges. Research (Atkins and Lawson, 2021) indicates that resistance to change within organizations can diminish resources allocated for the implementation of e-government security. This resistance is essential for promoting awareness of information system security. Insufficient awareness of information system security can result in poor prioritization of security initiatives, thereby exacerbating the strain on available resources (Atkins and Lawson, 2021; Madaki *et al.*, 2024). Research indicates that the implementation of information security in the public sector frequently faces challenges related to a lack of skilled personnel, inadequate technological resources, and insufficient training programs (Atkins and Lawson, 2021; Madaki *et al.*, 2024). Additionally, Atkins and Lawson (2021) highlight the importance of having both qualified personnel and an organized system for training and support in the public sector.

To improve the efficacy of their IS security, organizations must first identify their security objectives and subsequently formulate complete management strategies that include IS security maintenance, resource allocation, and safety measures (Ma *et al.*, 2008). By creating appropriate information systems security objectives and executing effective resource allocation, a business can improve its security management strategy, augmenting its value and securing a competitive advantage.

Ultimately, sufficient resources are essential for the effective implementation and maintenance of management processes. Resources are crucial for the implementation and upkeep of management systems. The organization can

efficiently execute security protocols and address and alleviate threats with sufficient resources. Inadequate resources might cause even the most well-structured processes to fail in attaining security objectives.

2.4 IS security in the public sector

The government agency may establish an e-government platform to provide services to citizens at any time and from any location. The data on the e-government platform is characterized by its personal, private, and sensitive nature and is substantial in volume (Joshi *et al.*, 2001; St-Hilaire, 2020). To safeguard this data, the e-government system must implement services with rigorous authentication and data encryption mechanisms (Joshi *et al.*, 2001). Safeguarding mechanisms enhance system security while concurrently diminishing overall system performance and user convenience. In this context, public sector managers not only align security objectives but also balance various goals, such as security and efficiency, to ensure that e-government services are reliable, secure, user-friendly, and effective (St-Hilaire, 2020).

Moreover, stakeholders in the public sector are essential for the effective implementation of robust information security (Bokhari and Myeong, 2023; Gnan *et al.*, 2013). Stakeholders may include government entities, private sector vendors, and civil society organizations. Bokhari and Myeong (2023) demonstrate that stakeholders provide varied knowledge that enhances e-governance and information security, resulting in better utilization of e-services. Gnan *et al.* (2013) highlighted the significance of stakeholder involvement in the integration of diverse interests and values into security goal setting, as these stakeholders can affect uncertain outcomes. This poses a considerable challenge to public sector government security, potentially obstructing the formulation of security goals and the effective collaboration among diverse stakeholders (Brockmyer, 2016).

Overall, previous research has contributed to the security goal identification, security management design, and resource allocation separately (Distel *et al.*, 2022; Drnevich and Croson, 2013; Niemimaa and Niemimaa, 2017). In addition, the recent literature recognizes that security goals, security management, and

resources are the keys to ensuring information security to collaborate with cross-unit stakeholders as they have to comply with different security standards, engage in different tasks, and do not have the same value about the information security (Dong *et al.*, 2021; Loft *et al.*, 2021; Yu and Hsiao, 2022). It is crucial to note that the alignment of goals for IS project coordination is particularly efficient for participants involved in IS security projects within the realm of e-governance. This context encompasses the application of information and communication technologies in public administration aimed at improving service delivery, fostering citizen participation, and increasing transparency. Therefore, the alignment of goals in the IS security project holds considerable importance.

3. Research method

The study is to investigate how different participants identify their security goals, compile the security policy, and collaborate with participants on the information security management process. It is particularly complex in security management within various stakeholders who have their value, security policy, and resources. Grounded theory is particularly suited to studying complex phenomena, where it is essential to comprehend the process, actions, and interactions involved (Paré *et al.*, 2015; Rivard, 2020). Therefore, the grounded theory could help generate concepts about the information security management process through iterative data collection and systematic analysis. This approach allowed us to examine the identification of security goals and reveal how various participants engage in security management activities and collaborate.

3.1 Site selection

The land administration information system in Kaohsiung City, Taiwan, commenced in the early 1990s with the digitization of land records by the Land Administration Bureau of the Kaohsiung City Government. In 1993, the agency initiated the E-Net, which transformed land information services. It provided real-time internet access in 1997 and added cadastral mapping capabilities in 1998. In 1999, it incorporated Geographic Information System (GIS) technology and

spatial maps, offering a more thorough perspective on land information. By 2007, it possessed 3D and 3G functions, intending to enhance land information services and network capacities throughout Taiwan.

E-Net, an innovative system in national land administration information services, has received multiple honors and accolades. It initiated paid retrieval and services beyond designated areas and times, receiving the "Golden Axe Award" from the Executive Yuan's Council for Economic Planning and Development in 2002. In 2003, it was awarded the "Outstanding Agency Award" at the Ministry of the Interior's National Land Information System 10-year Achievement Exhibition. The "Golden Axe Award" and "Outstanding Agency Award" recognize outstanding work teams in public sectors that promote business reform and enhance administrative efficiency. This award encourages public servants to improve service quality through collaboration and to foster innovation and reinvention within government agencies. The E-Net system received these awards, indicating that it has introduced new technologies to enhance multi-party cooperation efficiency while simplifying administrative processes and thereby improving the operational efficiency and quality of government agencies.

The E-Net is an intricate system with several stakeholders. Government entities, technical collaborators, and end users are essential stakeholders. The E-Net originally had 23 agencies across 21 cities and counties, but it has now contracted to 20 agencies across 18 cities and counties. Technical partners furnish essential assistance and innovation. End-users, comprising people and public personnel, gain convenient access to land management information and associated services.

E-Net provides a range of services to enhance land administration and public service efficiency. It facilitates access to land and property information via personal computers, enabling users to query registration data electronically. The system amalgamates cadastral and registration data from multiple government entities, establishing a geographic database for public land. It additionally provides statistical analysis, report generation, and map output. The system incorporates GIS technology to provide cohesive cadastral and topographic map data,

facilitating the viewing and querying of urban planning maps and topographic features. Users can get land administration information via 3G devices and visualize data in three-dimensional graphics. E-Net emphasizes security and integrity, thwarting the forgery of ownership certificates, land registration documents, and cadastral records. In detail, the E-Net system's information security measures include a real-time network intrusion detection system, regular government assessments, and ongoing personnel training. These measures protect the system and user data but may cause inconvenience for the public, such as temporary system shutdowns or network speed delays. The government must balance security and convenience to ensure system effectiveness.

To ensure the sample is capable of providing meaningful insights into IS security, this study employs purposive sampling. There are several reasons why the E-Net project presents a suitable case for studying IS security. First, E-Net has been in operation for over two decades and has consistently implemented ongoing enhancements. This long-term perspective offers valuable insights into the development and implementation of effective IS security strategies over time. Second, E-Net involves multiple stakeholders, including land administrations, urban development administrations, technology support, and service agencies. This multi-stakeholder approach is a classic way to study cooperation in IS security management. Third, E-Net serves as the foundation for essential functions such as property rights, land-use planning, data access, and taxation, all aimed at serving a large number of citizens and promoting economic development. Lastly, the E-Net project needs to strike a balance between ensuring the quality of system services and adhering to security policies, all while managing limited resources across its diverse unit participants. This trade-off is a central theme in IS security. In conclusion, E-Net is an ideal case for studying IS security due to its critical role in governance, the need to balance security with efficiency, the involvement of multiple stakeholders, adherence to established collaboration strategies.

3.2 Data collection

Participants in this study were required to have extensive involvement in the

development and implementation of E-Net. Their roles included technical and business government employees, as well as vendor project managers. The technical units have the responsibility of building the E-Net system, providing assistance to the business units, and facilitating contact with the vendor. The business units, which are in charge of manipulating the data and offering services to citizens, primarily use E-Net. The vendor provides technical assistance and collaborates with the technical departments to maintain E-Net's functionality. Furthermore, E-Net distributes the financial gains to the technical units, business units, and vendors involved in the system's operational management based on their respective contributions to the project. Furthermore, they are critical stakeholders in E-Net's security project.

For the purpose of comprehending the planning and construction procedures of the IS for E-Net, we conducted interviews with 13 employees from five distinct organizations, as illustrated in Table 1. The interview questionnaire facilitated discussions regarding the E-Net security plan and design phase, as illustrated in Table 2. Interviewers asked participants to identify pertinent information security management activities or policies in relation to their organization's IS security goals and principles. Interviewers encouraged them to identify the management practices and implementations that were instrumental in the attainment of their information security objectives. The questions listed in Table 2 serve as a guide for the interview process. Furthermore, respondents offered their perspectives

Table 1
Interviewee information

Unit	Organization (interviewee)	Job title	Number of interviewees (number of words transcribed verbatim)
Technical Units	Unit T1 (TU-A、TU-B)	Leader	2 (52,785)
	Unit T2 (TU-C、TU-D)	IS personnel	2 (28,345)
Business Units	Unit B1 (BU-E、BU-F、BU-G、BU-H、BU-I)	Leader	5 (24,354)
	Unit B2 (BU-J、BU-K)	Employee	2 (28.763)
Vendor	Company V(V-L、V-M)	Project manager	2 (56,496)

Table 2
Interview scheme

Core issues and example questions
1) What information security objectives have been established within the E-Net system?
2) How has your experience in the public sector shaped your understanding of information security, especially the challenges and security requirements of the E-Net system?
3) What information system security challenges have you encountered during the integration process with other parties?
4) What information system security challenges have been encountered during the integration process with other counties?

on the allocation of resources and the activities of IS security administration. The data analysis process employed these insights to clarify the relationships between common goals, management procedures, and resources within E-Net.

3.3 Data analysis and reliability

Our grounded theory data analysis was a comprehensive process that implemented three coding procedures: selective coding, axial coding, and open coding (Corbin and Strauss, 2014). (1) The verbatim transcript was carefully segmented during the open coding process, and each segment was transformed into a unique conception. We subsequently designated appropriate names to these conceptualizations in accordance with Corbin and Strauss (2014). For example, a participant in the interview stated, "Users are prompted to enter a verification code when they log into the information system for online verification." The verification code is an indispensable element of security control operations. As a result, we have designated it as a subcategory of the IS security administration activity. The research topic was established with clarity and structure as a result of the

researchers' systematic iteration through this process. A total of 25 items were identified and categorized into five subcategories (which include resources, activities, policy, objectives, and value) according to their respective attributes in this study. 25 items were generated during this open coding phase, which encompassed 2,055 text segments.

(2) The purpose of axial coding was to ascertain the relationships between the various subcategories that were identified during the open coding procedure. For instance, the principal category, which is referred to as "IS Security Goals and Value," is defined by the Goals and Value subcategories. 'IS security management' is defined by the Activities and Policy subcategories. Table 3 illustrates the relationships between subcategories and items, as well as the definitions of each subcategory.

(3) The goal-setting process was implemented during the selective coding process, which involved numerous cycles between the open and selective phases. This investigation emphasizes the significance of 25 specific items within the domain of IS security management, which function as critical indicators of the efficacy of security measures. A comprehensive and robust framework for strategic decision-making and analysis in IS security management has been established by meticulously classifying these items into five primary subcategories: roles, resources, policy, activities, and objectives. According to their inherent characteristics, these subcategories are further divided into three axes: IS Security Management (Activities and Policy), Resources, and IS Security Goals and Values. Table 3 provides a comprehensive analysis of each category and subcategory. After a careful study of the exact transcripts, items, subcategories, and how they related to each other, the three main groups of IS Security Management, Resources, and IS Security Goals and Values were found. An IS security goal-setting model is subsequently developed. Figure 1 illustrates the data structuring process, as well as the observations and relationships that underline the developing theoretical framework.

We analyzed the data using a grounded theory approach. A group of three researchers conducted the data analyses, ensuring the highest level of reliability

Table 3
Category definition

Category	Sub-Category	Definition	Items
IS security goals and value	Goal	The specific objectives or states that an organization aspires to attain.	G1: confidentiality G2: integrity G3: usability G4: reliability G5: maintenance G6: prevention G7: non-repudiation
	Value	The fundamental principles and beliefs that information security brings to an organization or individual are embodied by values.	V1: Revenue V2: Satisfaction V3: System Security V4: System Effectiveness
IS security management	Activity	A sequence of actions that are implemented to promote the ongoing development of system security, including planning, execution, monitoring, and enhancement.	A1: Control Approach A2: Verification A3: Education and Training A4: Promotion A5: Routing Meeting A6: Security and Defense
	Policy	A policy is a collection of formalized rules, guidelines, and procedures that an organization establishes to safeguard its information assets or to regulate the security of its information systems.	P1: International Standards P2: Law P3: Rule P4: Operational processs
Resource	Resource	The term "resources" encompasses a variety of assets, both tangible and ethereal, that are indispensable for the operation and security of public information systems.	R1: Information Technology R2: Human Resource R3: Organization R4: Cost

by having ongoing discussions about the coding procedure until they agreed (Dubé and Paré, 2003; Eisenhardt, 1989). Three researchers, each bringing their unique expertise in IS security and IS project management, participated in this study. The data analysis process was thorough, with the researchers encountering divergent viewpoints regarding data coding. Through collaborative efforts, they compared their respective codes and engaged in discussions to resolve disagreements, ultimately establishing consensus. The research partners followed a systematic coding approach and obtained rich results, demonstrating the thoroughness and

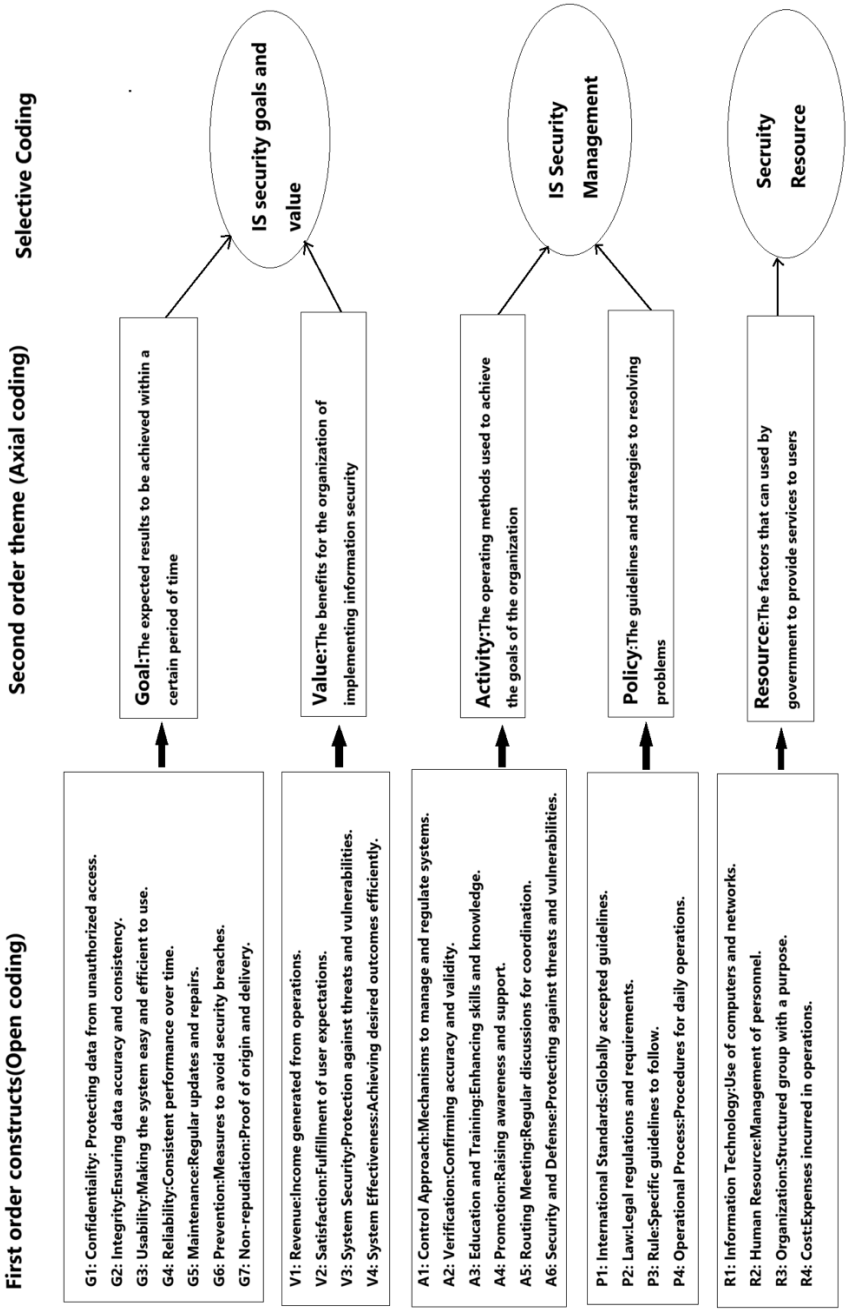

Figure 1

Data structure overview

reliability of the study. This collaborative approach ensured that all perspectives were considered, making the study more comprehensive and robust.

Thirteen interviewees from various organizations—technical units, business units, and vendors—provided the data for this study, offering a diverse range of perspectives. Both researchers and interviewees meticulously reviewed the full transcripts to confirm the accuracy of the interview content. We asked the interviewees for further clarification if they provided insufficient or unclear information. By following these strict procedures, our study achieved data that is both reliable and valid, ensuring a comprehensive and inclusive view of the subject.

4. Results

Our study, aimed at validating the primary value and goal of the E-Net project, IS security management, and its resources, involved a thorough analysis of the frequency of items that emerged during the open coding stage. The result, as depicted in Table 4, highlights the interviewees' crucial role in identifying "satisfaction," "system security," and "system effectiveness" as the key values of the E-Net project. The most impactful goal, "integrity," serves as a guide in operational processes. The interviewees' recognition of "maintenance" and "usability" as essential IS security goals underscores their importance in the project and their integral role in ensuring its success.

Our research has identified the crucial activities and policies of IS security management that are instrumental in pursuing the values and goals of the E-Net project. The operational processes, which play a key role in achieving "integrity," "satisfaction," "system security," and "system effectiveness" by implementing control approaches, provide a clear direction for the project. Equally important is the "promotion," which not only declares executive support for the IS security project but also highlights the security governance directions and resource allocation. "Promotion" can also demonstrate changes in both technology and organization.

Finally, "information technology" is a vital resource for managing IS security. It plays a crucial role in various functions, such as monitoring, controlling,

Table 4

IS security value and goal, IS security management and resource categories in the E-Net

Category	**IS security value and goal**				
Sub-Category	items	Frequency	Category	items	Frequency
Value	V1: Revenue	162	Goal	G1: confidentiality	30
	V2: Satisfaction	251		G2: integrity	202
	V3: System Security	221		G3: usability	134
	V4: System Effectiveness	200		G4: reliability	46
				G5: maintenance	187
				G6: prevention	59
				G7: non-repudiation	11
Total Frequency		834	Total Frequency		669
Category	**IS security Management**				
Sub-Category	items	Frequency	Category	items	Frequency
Activity	A1: Control Approach	146	Policy	P1: International Standards	61
	A2: Verification	51		P2: Law	130
	A3: Education and Training	16		P3: Rule	111
	A4: Promotion	274			
	A5: Routing Meeting	153		P4: Operational process	525
	A6: Security and Defense	22			
Total Frequency		662	Total Frequency		827
Category	**Resource**				
Sub-Category	items	Frequency			
Resource	R1: Information Technology	992			
	R2: Human Resource	97			
	R3: Organization	258			
	R4: Cost	156			
Total Frequency		1,503			

operating, verification, and maintenance. These functions are essential for ensuring the security, effectiveness, and satisfaction of the E-Net project. Therefore, 'information technology' is not just a tool but a key enabler in the successful management of IS security.

To align the three different units to implement IS security management, we adopt selective coding, which presents the collaboration process under the common goals, shared goals, and unit-specific goals. Figure 2 outlines the selective coding and presents the common goals, shared goals, and unit-specific goals. The common goals are unified among technical units, business units, and vendors, emphasizing the importance of "system effectiveness," "integrity," and "satisfaction." These common goals among different entities do not merely serve as an observation but act as a potential source of inspiration and motivation. Also, the shared goals reflect the shared vision among technical and business units and cultivate a mutual understanding, significantly boosting the efficacy of IS security management and illustrating the collaborative efforts among technical and business units. In order to accomplish the common goals and shared goals, the three units put lots of resources into the same security activities and policies. These implemented activities and policies also achieved the unit-specific goal, highlighting the individual contributions and their impact on collective success.

The findings show that access to information technology resources is a universal requirement for all stakeholders to achieve not only collective goals but also their distinct goals within the information system. Technical units and vendors utilize a variety of IT resources, including staff, hardware, and software, to bolster the E-Net system. In contrast, business units contribute their understanding of system procedures and data ownership. It is critical to acknowledge that resource sharing acts as a significant incentive, promoting stakeholder engagement in IS security management and advancing momentum toward common IS security goals. This synergy not only highlights the contributions' value to the system's overall security but also leads to cost savings, efficiency enhancements, and strengthened collaboration, thus underlining the concrete benefits of resource sharing in IS security management.

4.1 Common goal

4.1.1 System effectiveness

Technical and business units, along with the vendor, aim to achieve system

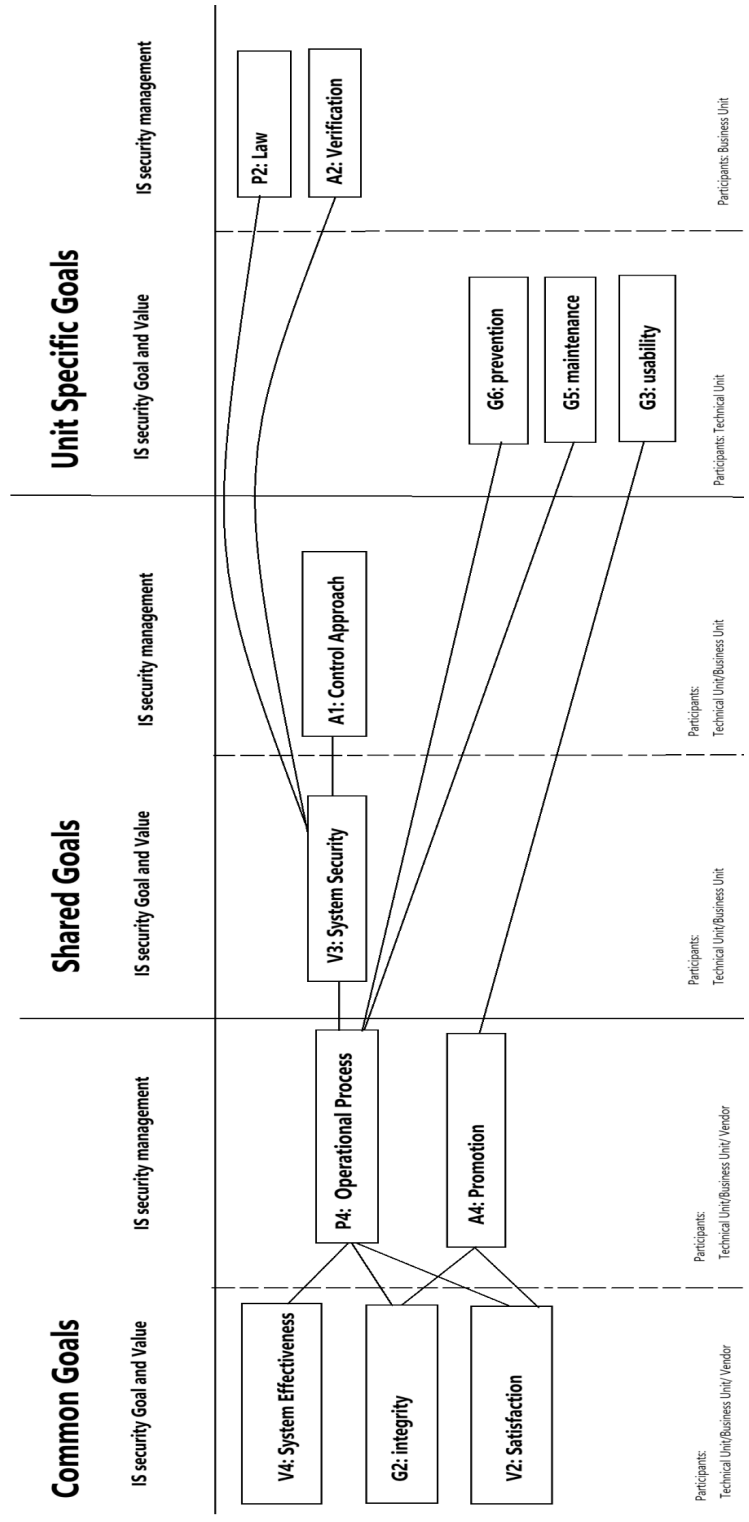

Figure 2

Conceptual model of IS security goals collaboration

effectiveness by designing complex and flexible operational approaches. System effectiveness encompasses various issues, including performance, reliability, and efficiency. Technical and business units, and vendors design and evaluate operational processes to identify risks, implement system reliability, guide security management, and ensure the organization complies with relevant regulations or standards. To manage the vast amount of data, the technical and business units have established a common operational process for system quality. This process aims to prevent security vulnerabilities caused by inconsistent data processing procedures, thereby establishing a secure and efficient information system.

TU-C in unit T2 stated, *"We exchanged ideas and collaborated to discuss the system's weaknesses, review service functions, and analyze operational processes. This helps us maintain the system's functionality, improve it further, and enhance its overall performance."* The business units and the vendor strive to maintain a balance between system performance and security while also ensuring that operational processes adhere to security policies. BU-J in unit B2 stated: *"The business units need to enhance system functions to align with government regulations steadily…However, we have established and evaluated relevant operational processes to ensure data quality and enhance system performance.* " The vendor uses information technology techniques to design functions that comply with operational processes and provide high-level performance. Vendor V-L stated, "*Everyone is welcome to take a look at how the system operates based on their expertise... We refine the performance of the information system under the system processes to comply with the operational processes set by the technical and business units*."

4.1.2 Integrity

Integrity is a critical concern that unites technical units, business units, and vendors within E-Net. The role of technical units is particularly crucial; they address technical challenges to secure IS. Integrity issues can arise quickly because of the complex distribution of data across various business segments and administrative levels. Technical units might revamp operational methods, enhance

data backup processes, and keep a strict check on data quality. A proactive stance is emblematic of their approach, with the leader of the technical unit TU-A explaining, "*We talk to each other every day and not only look for new ways to stop data transaction errors, but we also stress how important it is to follow operational rules so that everyone on the team and our users works together to keep the data safe. It is crucial to keep in mind that many of our issues stem from user behavior. You can help different groups work together better by following standard operating procedures, which I believe are helpful....*" It is crucial for technical units, business units, and vendors to collaborate and protect the data, as it is a shared responsibility.

Business units, on the other hand, play a crucial role in providing accurate and complete data for citizen services, making integrity their primary security concern. Given their limited technical expertise, they often collaborate with technical units and actively participate in operational processes. An interviewee BU-H from business unit B1 provided insight into this collaborative effort: *"Citizens are increasingly calling for information services…The training program allows us to learn about IS security. The training program discusses the operating procedures, such as control activities, periodic update approaches, and the data tracking process..."* Moreover, vendors prompt IS security management to enhance IS security awareness and capabilities, offering training programs as part of their contribution to the systemic improvement of IS security functions.

4.1.3 Satisfaction

In order to ensure user satisfaction, the technical units and business units have developed operational processes that are adaptable to the dynamic nature of the system. The design of these processes focuses on addressing potential issues and achieving specific security goals. Even when the organization faces new security policies or adopts new security technologies, the operational processes can define security goals, guide the accurate implementation of security mechanisms, and improve system satisfaction, which is based on different organizations' interests. Central to all participants' efforts is the critical importance of maintaining and

enhancing system satisfaction across various organizational interests. BU-K in business unit B2 said, "*Even though the business units have different ways of controlling and processing data, it would be less easy for the people, and they would be much less satisfied. Let us say your land is in city A, and you live in city B. Can you access or modify data in City B? Technical solutions may work, but you should also consider operational processes and access rights*." The insights from the technical units underscore the critical need for security management to ensure superior information systems services and to balance IS security with user satisfaction.

To enhance satisfaction, it's pivotal to focus on activities that help users grasp new functionalities and gain valuable knowledge. This can be achieved through interactive training, panels, or workshops. Such detailed efforts not only support less experienced individuals by pairing them with knowledgeable mentors but also deepen the understanding of IS security features, thereby significantly improving user satisfaction. For example, the vendor V-L stated, *"We work closely with business units to plan and carry out at least two big events each year that promote the system. These events are not just meant to promote the system; they are also meant to help us understand how outside stakeholders, like the citizens, feel and what they have been through. We will share their opinion with the business units if it helps make the system safer to use. This will make them an important part of the process…"* Vendors, crucial to this collaborative effort, aim to enhance the promotion activities with technical support, striving for customer satisfaction. This collaboration between technical and business units, along with vendor contributions, exemplifies the unity of purpose within IS security management, fostering a shared sense of commitment and synergy among technical units, business units, and vendors.

4.2 Shared goal

4.2.1 System security

System security is a shared goal of both technical and business units. This

study found consensus among the interviewees regarding the importance of control activities and operational processes in safeguarding data and mitigating potential threats. To enhance the security of E-Net, these control activities, including user account authentication, information system firewalls, website traffic regulation, and, most importantly, continuous security monitoring, are in place to ensure the ongoing protection of data. Indeed, the technical units have developed control approaches to improve IS security through the integration of new technologies. It is risky for technical and business units to integrate new technology with legacy systems while also ensuring a system that is both maintainable and extendable. The business units would continue to evaluate and modify the control approaches to adopt new technology that could fulfill their customers' needs. The technical and business groups also collaborate on operational processes to ensure all stakeholders adhere to stringent regulations. As TU-A in business unit B1 respondent stated, "*Making sure everyone is on the same page and sharing resources is critical to keeping our systems secure...During our regular meetings, we discuss security with the technical teams. We really need to figure out some concrete procedures to keep our data safe...*" The data from interviews revealed that system security serves as a shared goal among the business and technical units so they can work together to implement control approaches and operational processes.

In addition, the business units achieve system security by employing verification mechanisms and adhering to relevant laws. They maintain the quality of IS security through consistent verification and compliance with pertinent security policies, laws, regulations, and standards. For example, the member of business unit B2 stated, *"Unfortunately, I can't always give you the right to access data because we have to follow the rules to verify each step. If technical, business units or vendors want to change their access rights, we have to follow the rules or regulations to prove that we have permission to use the data… "*This shared commitment to system security not only aids in realizing the shared goals between technical and business units but also proactively strengthens their collaborative relationship, uniting them in their efforts.

4.3 Unit-specific goal

Technical units identify prevention, maintenance, and usability as the unit-specific goals. The technical units emphasize the need for security management, which includes operational processes implemented to achieve these unit goals. These operational processes play a crucial role in achieving the unit goals, providing a sense of reassurance and confidence to the stakeholders. While the technical units may find these unit-specific goals beneficial for themselves, both the business units and the vendor have the potential to collaborate under these specific goals. For example, BU-J in business unit B2 responded, "*The business unit in City A is where people can acquire their information, but it is not always accessible via the internet. We can sense something incorrect with the database. We continuously monitor the data to ensure its quality..* " The vendors stated, *"We hope that people will use this system to its full potential. If technical and business units are willing to share their rich data so that we can create new information services, more people may use them. We can integrate data from multiple units to provide various services...*" Fortunately, operational processes and promotion are the key management activities for the common goals. Therefore, the technical and business units and vendors could collaborate to achieve common goals and specific unit goals currently.

To summarize, the common goals of system effectiveness, integrity, and user satisfaction serve as guiding principles for the collaboration among technical units, business units, and vendors. To achieve these goals, all participants—technical units, business units, and vendors—invest significant effort in IS security management, encompassing both operational processes and promotional activities. For the technical and business units, the shared goal of system security drives their cooperation within the E-Net framework. These units collaborate by leveraging their technological resources and expertise to establish appropriate control activities, which are critical to achieving their shared objective. Thus, the operational processes and promotional activities are not only essential for achieving the common goals shared by the three units but also for the shared goals

of the technical and business units and the unit-specific goals of the technical units.

5. Conclusion

This study aims to facilitate key stakeholders' comprehension of the process of identifying common goals and implementing management activities to develop a complete information security system. There are several findings: First, our data revealed that system effectiveness and data integrity significantly influence the implementation of suitable operational processes and training programs. Integrity, a common goal, urges numerous stakeholders to allocate resources to improve the accuracy, integration, and completeness of data. In the same vein, the common goal of system effectiveness motivates all stakeholders to develop operational processes and functions that are feasible. The cooperation between E-Net stakeholders leads to the skillful interweaving of common goals, management mechanisms, and resources.

Second, stakeholders in the E-Net system contribute to a variety of IS security management activities and maximize their resources to achieve common goals. Our investigation determined that satisfaction is a substantial factor in optimizing system performance. The technical units, business units, and vendors carefully analyze the IS security requirements, design the system to be simple to use and valuable, and provide clear operational processes and a training program. This satisfaction facilitates management mechanisms that enhance system performance and link satisfaction with the common goal—system effectiveness. The satisfaction goal encourages technical units, business units, and vendors to provide high-quality information services and attracts business units to work to improve the system's effectiveness.

Third, our study found that system security goals are instrumental in fostering IS security awareness and promoting its value among the technical and business units. These goals play a pivotal role in directing the technical and business units and vendors to participate in IS security control activities. As a result, the technical and business units accumulate experience in IS security management and alter information security policies, control mechanisms, or regulations to ensure

security. Additionally, operational processes and control activities help maintain the integrity of data and the security of the system. Therefore, by implementing between-unit management mechanisms, we can establish a common goal of system security, thereby facilitating the advancement of various IS security management mechanisms through collaborative efforts.

This paper contributes to the literature by providing new insights regarding goal identification in IS security projects. First, common goals and shared goals are catalysts for aligning stakeholders' particular goals to assess and adjust the management process, resource allocation, and definition of IS security rules. Conversely, IS security management and resources within an IS project are the outcome and the medium through which all stakeholders can identify common goals. Second, common goals are critical in IS security projects because all stakeholders should protect their data, software, procedures, and equipment. The security of the IS will fail; if any party makes a mistake, then the IS's security will fail. Thus, an IS security project is a teamwork project, and each stakeholder must participate in management activities to ensure security. Consequently, for all stakeholders in the IS security project, common goal identification is a reciprocal activity that can maximize individual resources to reach both common and stakeholder-specific goals.

Our findings, compared to previous studies (Hassan *et al.*, 2020; Perkins *et al.*, 2018; Tang and Naumann, 2016; Yu and Hsiao, 2022), confirm the importance of common goals in projects. However, our study highlights that common goals can serve as a strategic tool, catalyzing a cross-organizational management process and creating a developmental link between unit-specific goals and common goals. Our data reveals that shared goals can inspire collaboration among insider and outsider units, even in the face of rapidly changing security guidelines. Furthermore, the information system project, involving a diverse range of stakeholders, can stimulate competition (Amadi *et al.*, 2019; ElWakeel and Andersen, 2019). Our findings indicate that aligning with diverse goals can promote management activity alignment and strengthen collaboration in the short term. Importantly, goal alignment also encourages participants to adopt a cross-

organization-wide view of information system security in the long term, rather than a narrow and single view, thereby reaping lasting benefits. Under common goals, project participants gain a comprehensive understanding of the security management process to enhance teamwork performance. Under specific goals, participants identify their specific role in their cooperative relationship.

This study has several limitations. First, the findings only reflect short-term effects and may not fully capture the long-term dynamics of IS security projects. Second, our study focuses on the E-Net system, an e-government system subject to specific laws, rules, and policies, which limits the generalizability of the findings. However, knowledge of IS security, perceptions of risks, and regional cultures all have a significant impact on an IS security project's success. Future investigations should delve into these exciting aspects of IS security projects, focusing on different organizations and systems that may operate under different regulatory environments and face unique challenges. Third, this study did not explore various IS security standards and regulations to provide a more comprehensive understanding of IS security management. In the future, the researchers could investigate various IS security standards and regulations to understand how different compliance requirements impact IS security management. Consequently, the study's significant finding that common goals guide coordination among stakeholders warrants careful interpretation and further validation in different contexts and over longer periods.

Appendix A. Example quote

Items	**Example Quote(**interviewee**)**
G1: confidentiality	We use high-standard operational environments to make up for any security holes made by people so we can handle the large amount of data and keep highly sensitive information safe. *(by TU-A)*
G2: integrity	It's important to note that our unit and 12 other operating units also have backups and updates that happen at the same time and off-site. *(by TU-A)*

Items	**Example Quote(**interviewee**)**
G3: usability	The system should be available 97% of the time each month (with no more than 8 hours of unplanned downtime), and 99% of the time each year (with no more than 24 hours of unplanned downtime). *(by TU-A)*
G4: reliability	Government agencies need to be careful with public data and online services so that data from this system isn't reprocessed, which could hurt the reliability of the information. *(by TU-A)*
G5: maintenance	The work teams of both sides meet regularly to maintain service functions and go over operations and repairs. *(by TU-A)*
G6: prevention	This information system comes with different forms of application services that each cooperating agency can use. This is so that it can adapt to their different service needs and work environments. *(by TU-B)*
G7: non-repudiation	The platform will use citizen badges to digitally sign the information, which will make each digital signature unique. *(by TU-B)*
V1: Revenue	If government agencies cut back on giving out data, fewer people will use it, which means that the information system will make less money. *(by V-L)*
V2: Satisfaction	The main things we do in the public sector are to make things easier for people and make management easier. The digitization of all the city's data is now complete thanks to this information service project. *(by TU-B)*
V3: System Security	It is our unit's job to work with partners to handle and create government certificates and security measures for electronic signatures. *(by BU-J)*

Items	**Example Quote(**interviewee**)**
V4: System Effectiveness	We asked the data analysis team to create an operational and maintenance management system for the information system so that problems can be fixed faster and the system keeps running well. *(by TU-A)*
A1: Control Approach	It is up to each government body to provide back-end data and oversee and manage the server hosts. *(by TU-A)*
A2: Verification	When it comes to data requests involving personal information, only the people who have a stake in the matter can see all the information; it will not be given to anyone else. *(by TU-A)*
A3: Education and Training	To make sure that all of our partner companies fully understand how the new version of the database works, we've asked engineers from the company that made the original database to lead training classes. *(by TU-B)*
A4: Promotion	As the public sector works to become more digital, city and county governments that don't already offer online services should attend meetings for public sector network service providers. *(by TU-A)*
A5: Routing Meeting	We can talk about operational problems, service function improvements, or operational strategies at regular work meetings or meetings about marketing strategies. *(by TU-B)*
A6: Security and Defense	Our IT department will look at the records kept by the frontend server hosts to find out how partner companies access base data and to keep an eye on how the frontend AP Server and Web Server are used. *(by TU-B)*

Items	**Example Quote(**interviewee**)**
P1: International Standards	Agency A's information security management systems (ISMS) in the public sector have been approved to meet ISO 27001 requirements. *(by TU-A)*
P2: Law	The Personal Data Protection Act always keeps the information that is used for the information services that this project supports safe. *(by BU-F)*
P3: Rule	Some system information is based on the "publicity principle," which aims to protect the rights of honest third parties to know the status of a property before buying it so they don't get ripped off. *(by BU-E)*
P4: Operational process	Under the rules of "BOO (Build, Operate, Own) outsourcing cooperation," "joint supply contracts," and "cross-department, cross-city/county, cross-agency joint development," public sector agencies' databases stay in the background and their operating structure stays the same. *(by TU-B)*
R1: Information Technology	This project combines GIS technology with Agency A's information tools. *(by BU-E)*
R2: Human Resource	People who have worked on building information systems for a long time do the very professional and difficult jobs of data registration, surveying, geographic information, debugging, and clearing up questions. *(by V-L)*
R3: Organization	This project has 18 cities and counties and 20 government departments working on it. The government bought the supplies together. For our partner businesses, the prices are set because the tools have already been bought. *(by TU-A)*
R4: Cost	Proposals from regular work meetings are used to update and improve system functions. As service

Items	Example Quote(interviewee)
	quality needs to be constantly raised, costs gradually rise as well. *(by TU-A)*

References

Alexopoulos, C., Saxena, S., Rizun, N., and Shao, D. (2023). A framework of open government data (OGD) e-service quality dimensions with future research agenda. *Records Management Journal*, *33*(1), 20-32. https://doi.org/10.1108/RMJ-06-2022-0017

Almeida Prado Cestari, J. M., Loures, E. D. F. R., Santos, E. A. P., and Panetto, H. (2020). A capability model for public administration interoperability. *Enterprise Information Systems, 14*(8), 1071-1101. https://doi.org/10.1080/17517575.2018.1564154

Amadi, C., Carrillo, P., and Tuuli, M. (2019). PPP projects: improvements in stakeholder management. *Engineering, Construction and Architectural Management*, *ahead-of-print*. https://doi.org/10.1108/ECAM-07-2018-0289

Atkins, S., and Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab024

Backhouse, J., Hsu, C. W., and Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, *30*, 413-438. https://doi.org/10.2307/25148767

Bokhari, S. A. A., and Myeong, S. (2023). The influence of artificial intelligence on e-governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access*, *11*, 69783-69797. https://doi.org/10.1109/ACCESS.2023.3293480

Brockmyer, B. I. (2016). *Global standards in national contexts: The role of transnational multi-stakeholder initiatives in public sector governance reform* (Publication Number 10242775) [Ph.D., American University]. Political Science Database; ProQuest Dissertations and Theses AandI;

Publicly Available Content Database. United States -- District of Columbia.

Cao, G., Wiengarten, F., and Humphreys, P. (2011). Towards a contingency resource-based view of IT business value. *Systemic Practice and Action Research*, *24*(1), 85-106. https://doi.org/10.1007/s11213-010-9178-0

Carney, M., Gedajlovic, E., and Sur, S. (2011). Corporate governance and stakeholder conflict. *Journal of Management* and *Governance*, *15*(3), 483-507. https://doi.org/10.1007/s10997-010-9135-4

Corbin, J., and Strauss, A. (2014). *The basics of qualitative research: techniques and procedures for developing grounded theory*. CA: Sage.

D'Aubeterre, F., Singh, R., and Iyer, L. (2008). Secure activity resource coordination: Empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems*, *17*, 528. https://doi.org/10.1057/ejis.2008.42

Dhillon, G., and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), 293-314. https://doi.org/https://doi.org/10.1111/j.1365-2575.2006.00219.x

Distel, B., Koelmann, H., Plattfaut, R., and Becker, J. (2022). Watch who you trust! A structured literature review to build a typology of e-government risks. *Information Systems and e-Business Management*, *20*(4), 789-818. https://doi.org/10.1007/s10257-022-00573-4

Dombora, S. (2016). Characteristics of Information Security Implementation Methods. *Proceedings of the 11th International Conference on Management*, Enterprise and Benchmarking (MEB 2016), 57-72.

Dong, K., Lin, R., Yin, X., and Xie, Z. (2021). How does overconfidence affect information security investment and information security performance? *Enterprise Information Systems*, *15*(4), 474-491. https://doi.org/10.1080/17517575.2019.1644672

Drnevich, P., and Croson, D. (2013). Information technology and business-level strategy: Toward an integrated theoretical perspective. *MIS Quarterly*, *37*, 483-510. https://doi.org/10.25300/MISQ/2013/37.2.08

Dubé, L., and Paré, G. (2003). Rigor in information systems positivist case

research: Current practices, trends, and recommendations. *MIS Quarterly*, *27*(4), 597-636. https://doi.org/10.2307/30036550

Eisenhardt, K. M. (1989). Building theories from case study research. *The Academy of Management Review*, *14*(4), 532-550. https://doi.org/10.2307/258557

ElWakeel, O., and Andersen, B. (2019). Stakeholder evolution: A study of stakeholder dynamics in 12 Norwegian projects. *International Journal of Managing Projects in Business*, *13*. https://doi.org/10.1108/IJMPB-10-2018-0218

Fadlullah, Z. M., Mao, B., and Kato, N. (2022). Balancing QoS and security in the edge: Existing practices, challenges, and 6G opportunities with machine learning. *IEEE Communications Surveys* and *Tutorials*, *24*(4), 2419-2448. https://doi.org/10.1109/COMST.2022.3191697

Gazley, B., Chang, W. K., and Bingham, L. B. (2010). Board diversity, stakeholder representation, and collaborative performance in community mediation centers. *Public Administration Review*, *70*(4), 610-620. http://www.jstor.org/stable/40802238

Gnan, L., Hinna, A., Monteduro, F., and Scarozza, D. (2013). Corporate governance and management practices: Stakeholder involvement, quality and sustainability tools adoption: Evidences in local public utilities. *Journal of Management* and *Governance*, *17*(4), 907-937. https://doi.org/https://doi.org/10.1007/s10997-011-9201-6

Hassan, A., Younas, S., and Bhaumik, A. (2020). Exploring an agile plus approach for project scope, time, and cost management. *International Journal of Information Technology Project Management*, *11*, 72-89. https://doi.org/10.4018/IJITPM.2020040105

Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373-384. https://doi.org/https://doi.org/10.1016/j.jsis.2011.06.001

Hsu, C. W. (2009). Frame misalignment: Interpreting the implementation of

information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140-150. https://doi.org/10.1057/ejis.2009.7

Huang, S. M., Lee, C. L., and Kao, A. C. (2006). Balancing performance measures for information security management: A balanced scorecard framework. *Industrial Management* and *Data Systems*, *106*(1/2), 242-255. https://doi.org/https://doi.org/10.1108/02635570610649880

Joshi, J., Ghafoor, A., Aref, W. G., and Spafford, E. H. (2001). Digital government security infrastructure design challenges. *Computer*, *34*(2), 66-72. https://doi.org/10.1109/2.901169

Kim, S., and Seong Leem, C. (2005). Enterprise security architecture in business convergence environments. *Industrial Management* and *Data Systems*, *105*(7), 919-936. https://doi.org/10.1108/02635570510616111

Loft, P., He, Y., Janicke, H., and Wagner, I. (2021). Dying of a hundred good symptoms: why good security can still fail - a literature review and analysis. *Enterprise Information Systems*, *15*(4), 448-473. https://doi.org/10.1080/17517575.2019.1605000

Ma, Q., Johnston, A., and Pearson, J. (2008). Information security management objectives and practices: A parsimonious framework. *Inf. Manag. Comput. Security*, *16*, 251-270. https://doi.org/10.1108/09685220810893207

Madaki, A. S. A., Ahmad, K., and Singh, D. (2024). IT integration implementation in e-government public sector in developing countries: A systematic literature review and model development. *Transforming Government, 18*(3), 451-472. https://doi.org/10.1108/TG-02-2024-0043

Marcuzzo do Canto Cavalheiro, G., and Joia, L. A. (2016). E-government technology transfer: A case study of the implementation of a european patent management system in Brazil. *Public Administration and Development, 36*(3), 215-231. https://ideas.repec.org/a/wly/padxxx/v36y2016i3p215-231.html

Niemimaa, E., and Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices.

European Journal of Information Systems, *26*(1), 1-20. https://doi.org/10.1057/s41303-016-0025-y

Paré, G., Trudel, M. C., Jaana, M., and Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information* and *Management*, *52*(2), 183-199. https://doi.org/https://doi.org/10.1016/j.im.2014.08.008

Perkins, D., Jugdev, K., and Mathur, G. (2018). Characteristics of project management assets and project management process outcomes: An exploratory factor analysis. *International Journal of Information Technology Project Management*, *9*, 59-77. https://doi.org/10.4018/IJITPM.2018010104

Ricker, J. (2018). Efficiency vs. security: Information technology consolidations – resilience, complexity, and monoculture. *Homeland security affairs*.

Rivard, S. (2020). Theory building is neither an art nor a science. It is a craft. *Journal of Information Technology*, *36*(3), 316-328. https://doi.org/10.1177/0268396220911938

Rowley, J. (2011). e-Government stakeholders—Who are they and what do they want? *International Journal of Information Management*, *31*(1), 53-62. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2010.05.005

Siponen, M., and Willison, R. (2009). Information security management standards: Problems and solutions. *Information* and *Management*, *46*(5), 267-270. https://doi.org/https://doi.org/10.1016/j.im.2008.12.007

St-Hilaire, W. A. (2020). *Digital risk governance: Security strategies for the public and private sectors*. Springer.

Tang, C., and Naumann, S. E. (2016). Team diversity, mood, and team creativity: The role of team knowledge sharing in Chinese R & D teams. *Journal of Management* and *Organization*, *22*(3), 420-434. https://doi.org/10.1017/jmo.2015.43

Vroom, C. (2004). Towards information security behavioral compliance. *Computers* and *Security*, *23*, 191-198. https://doi.org/10.1016/j.cose.2004.01.012

White, G. (2009). Strategic, tactical, and operational management security model. *Journal of Computer Information Systems*, *49*, 71-75.

Whitman, M. E., and Mattord, H. J. (2017). *Principles of information security.* Cengage Learning.

Wong, B. (2005). Understanding stakeholder values as a means of dealing with stakeholder conflicts. *Software Quality Journal*, *13*(4), 429-445. https://doi.org/10.1007/s11219-005-4254-x

Yeh, Q. J., and Chang, A. J. T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information* and *Management*, *44*(5), 480-491. https://doi.org/https://doi.org/10.1016/j.im.2007.05.003

Yu, C. P., Chu, C. P., and Lu, P. H. (2018). Applying a security management mechanism to a system development lifecycle. *International Journal of E-Adoption*, *10*, 1-17. https://doi.org/10.4018/IJEA.2018010101

Yu, C. P., and Hsiao, Y. C. (2022). IT project management resource: Identifying your project's common goals. *International Journal of Information Technology Project Management*, *13*, 1-15. https://doi.org/10.4018/IJITPM.304057