Applied Computing and Intelligence

https://www.aimspress.com/journal/aci

Applied Computing and Intelligence
6(2): 223–244.
DOI: 10.3934/aci.2026013
Received: 15 October 2026
Revised: 21 October 2026
Accepted: 21 October 2026
Published: 03 November 2026

Research article

Information security compliance for e-government development: A revised framework

Ahmed AlKalbani[1] and Hepu Deng[2,*]

[1] Advanced Cybersecurity Academy, Muscat, Oman
[2] School of Accounting, Information Systems and Supply Chain, RMIT University, Melbourne, VIC 3000, Australia

*** Correspondence:** Email: Hepu.deng@rmit.edu.au; Tel: +61399255823.

Academic Editor: Chih-Cheng Hung

Abstract: The rapid development of e-government has created new ways for governments to interact with their stakeholders, leading to much critical information in e-government systems being exposed to cybercrime. As a result, information security has become a critical issue that needs to be adequately addressed. Using a technology-organization-environment framework and institutional theory, we developed a conceptual framework of information security compliance in e-government. This framework was then revised based on a thematic analysis of the qualitative data collected using interviews from senior managers in public organizations. The study showed that organizational security culture, information security enforcement, technologies, and environments are the critical factors for effective information security compliance in e-government development. This study contributes to information security research by proposing an information security compliance framework to influence the adoption of information security compliance in e-government development.

Keywords: e-government; information security; information security compliance; critical factors

1. Introduction

The rapid development of electronic government (e-government) has provided governments with new means to deliver public services, engage citizens, and improve workflows in public organizations [1–3], resulting in the critical information being exposed to cybercrimes [4,5]. This calls for the adoption of information security compliance in e-government development [3,6,7]. Generally referred to as the implementation of information security standards and policies for protecting organizational information [8,9], information security compliance is critical in gaining the confidence and trust of the

public in embracing e-government [3,10]. This is because user confidence and trust are vital in facilitating the development of e-government [3,8,11].

There are many studies on information security compliance in information systems literature [3,12,13]. These studies focus primarily on the factors related to the attitude, behavior, and intention of employees in engendering information security compliance. Sasse et al. [14], for instance, analyzed the interaction between employees with information security mechanisms for information security compliance. Lee et al. [15] investigated the use of sanctions to improve information security compliance. Bulgurcu et al. [16] investigated the role of information security awareness in changing the attitude of employees toward complying with information security requirements. Safa et al. [17] showed that knowledge sharing, collaboration, intervention, and experience with information security mechanisms strengthen information security compliance. These studies have provided specific insights from different perspectives on how to improve information security compliance.

Information security compliance in e-government development is complex and challenging [6,9]. This is because organizational, technological, and environmental factors are involved [3]. Many stakeholders are present [8], and specific technologies must be implemented [2]. This leads to a critical question that must be properly answered as follows: *What are the critical factors for the adoption of information security compliance in the development of e-government?*

In this study, we investigate the critical factors for the adoption of information security compliance in e-government development. A comprehensive review of the related literature is conducted, leading to the proposition of a conceptual framework for adopting information security compliance within the theoretical background of technology-organization-environment (TOE) framework and institutional theory. This framework is then revised based on a thematic analysis of the qualitative data collected using interviews with senior managers in public organizations. The study shows that organizational security culture, information security enforcement, technologies, and environments are the critical factors for effective information security compliance in e-government development. This study contributes to information security research by proposing an information security compliance framework for influencing the adoption of information security compliance.

In what follows, a review of the related literature is presented first, leading to the development of a conceptual framework for understanding the adoption of information security compliance. The research methodology is then presented, followed by the research findings. Finally, concluding remarks on the contributions and their implications are presented.

2. Related literature

With the rapid development of information and communication technologies, e-government [1,18] has been actively pursued to leverage the potential of latest technologies to transform the delivery of public services for making them more accessible, effective, and accountable [1,2]. As a result, how to protect public information has become critical in e-government development [3,4,11]. Information security is, therefore, about confidentiality, integrity, availability, authenticity, and accountability of information embedded in e-government systems [4,11,19].

The importance of information security in e-government development is well recognized [3,4]. This is because ensuring information security can improve the confidence and trust of stakeholders in their adoption of e-government [8,20]. Citizens, for example, are more likely to provide e-government systems with their private information if such information is believed to be secure. Businesses are more likely to adopt e-government in their dealings with public organizations if the information in e-government systems is deemed to be safe [3].

Ensuring information security in e-government is complex and challenging [11]. This is because e-government development engages many technologies and involves numerous stakeholders [21]. A holistic approach is often pursued for the delivery of public services through information sharing between public organizations. This significantly increases the possibility for security breaches in the adoption of e-government [22]. Furthermore, there are numerous probabilities of having malicious attacks on e-government services [23]. As a result, there is an explicit need to adopt effective approaches to ensure information security in e-government development [3,24].

Information security compliance is increasingly becoming an effective approach for ensuring confidentiality, integrity, availability, authenticity, and accountability of information in e-government development [11,25]. The adoption of information security compliance involves putting in place information security measures and mechanisms that can work together effectively [26]. It can satisfy the legal and security requirements for the delivery of public services and improve the confidence and trust of the public in their use of e-government services [3].

Organizations often introduce different methods to facilitate the adoption of information security compliance [4]. Some organizations, for example, introduce security trainings and awareness programs to provide their employees with the necessary skills and knowledge for evaluating and responding to security threats [16]. Other organizations use technical and administrative controls to guide employees to protect organizational information resources [11]. Such methods have helped organizations to better protect e-government information from different perspectives.

Many researchers have investigated the use of information security compliance for information security. These studies show a predominant focus on (a) changing employees' attitude [16,27–29], (b) understanding employees' behavior [12,15,25,27,30], and (c) improving employees' intention for information security compliance [10,17,31]. They provide specific insights on how information security compliance can be improved based on better understanding of various issues and concerns inherent in the compliance process. Table 1 presents an overview of these studies.

Table 1. Summary of information security compliance studies.

Themes	References	Critical factors	Theories
Attitude	Bulgurcu et al. [12], Ifinedo [25], Shaw [30]	Information security awareness, organizational culture, socialization	Behavioural theories, theory of reasoned action, theory of planned behaviour
Behaviour	Siponen et al. [10], Safa et al. [17], Herath and Rao [27], Lee et al. [31]	Self-efficacy, perceived legitimacy, openness to change, perceived sanctions, conservation, perceived risks, habits, subjective norms	Technology acceptance model, protection motivation theory, social cognitive theory
Intention	Siponen et al. [10], Myyry et al. [32], Puhakainen and Siponen [33]	Organizational commitment, threat appraisal, perceived usefulness, information security policy quality, conventional reasoning	Power framework, social control theory, general deterrence theory

Attitude-based studies examine the attitude of individuals toward information security compliance based on specific theories, including social cognitive theory [32], social bond theory [33], and theory of social control [34]. Bulgurcu et al. [16], for example, investigated the role of information security awareness on employees' attitudes toward complying with information security requirements. Ifinedo [25] found that socialization can change the attitude of employees toward information security compliance. Shaw [30] discovered that organizational culture directly influences the attitude of

employees toward complying with information security policies. These studies have shown the significant role that the attitude of employees plays in information security compliance.

Behavior-oriented studies explore the impact of the behavior of employees on information security compliance with the use of various behavioral theories, including theory of planned behavior and reasoned action [35], deterrence theory [36], threat avoidance theory [37], and moral judgment theory [32]. Siponen et al. [10], for example, suggested that information security training can motivate employees toward information security compliance. Lee et al. [15] investigated employees' information security compliance behaviors with a focus on the abuse or misuse of information security practices under different scenarios. Safa et al. [17] found that knowledge sharing, collaboration, intervention, and experience encourage information security compliance in organizations. Herath and Rao [27] found that the fear of sanctioning non-compliance with information security policies has a significant impact on the behavior of employees in information security compliance. These studies have shown the importance of understanding the behavior of employees in the implementation of information security compliance.

Intention-focused studies entail how to improve the intention of employees toward information security compliance. Siponen et al. [10], for example, found that understanding perceived consequence of non-compliance can improve the intention of employees toward information security compliance. Myyry et al. [32] revealed that employees with punishment are more likely to follow information security compliance policies. Puhakainen and Siponen [33] developed a training and education program for improving employees' intention toward information security compliance. These studies have shown that improving the intention of employees to comply with information security policies can lead to better information security compliance.

The discussion above shows that most information security compliance studies have focused on understanding the attitude, behavior, and intention of employees in complying with information security policies [34,35]. There are, however, other issues and concerns that affect information security compliance in e-government development [36,37]. These issues and concerns include the active support of senior management [38], the legislative requirement [39], the availability of information security strategies and policies [38], and the construction of advanced security technologies [3]. To better understand the information security compliance process, there is a need to investigate these issues and concerns for information security compliance.

The government of Oman in 2003 officially launched its e-government initiative for improving the delivery of its public services [40,41]. Many e-government projects have been delivered, including the National Statistics Online project, the e-Tendering, the Educational Portal, and the National Registration System. The implementation of these projects has greatly improved the delivery of public services. These services have become the most important and efficient means by which the government of Oman interacts with businesses and citizens. Such a development, however, has also brought serious information security challenges. Therefore, it has become imperative to ensure confidentiality, integrity, and availability of critical information in e-government systems.

3. An information security compliance framework

There is an increasing recognition of the need to consider technological and socio-organizational factors in exploring the adoption of information security compliance in organizations [16]. This is because information security research can leverage available theories [35–37] to better frame specific inquiries for investigating information security compliance in organizations. In this study, we investigate information security compliance in e-government development. To adequately conduct the

research, two established theories, including TOE framework [42] and institutional theory [43], have been adopted in examining the information security compliance process.

TOE theory argues that the process by which technological innovations are adopted is conspired by the technological, organizational, and environmental contexts surrounding their operations [42]. The technological context is related to the characteristics of available technologies. The organization context is about the organizational characteristics. The environment context is determined by the external environment in which an organization conducts its business. These three sets of factors present "*both constraints and opportunities for technological innovation*" [42], shaping the way that organizations appraise their needs and options for technological innovations.

In information security compliance, the technological context is about the reliability of available technologies capable of satisfying the requirement of information security policies and standards [44]. Technologies play a critical role in information security by providing organizations with secure transactions, protected access to information, and adequate defense against hacker attacks [3]. Having the ability to fulfil the technical security requirements increases the trust and confidence of users, leading to greater information security compliance [44,45].

Adopting adequate security technologies with diverse security capabilities can help enforce information security policies, monitor and alert violations, and strengthen information protection [3]. Kaliontzoglou et al. [46], for example, assessed the effectiveness of different security technologies, such as digital signature, in enforcing security requirements over Web portal technologies. Ebrahim and Irani [24] asserted that security technologies could improve the normal functioning of e-government systems by reducing security risks. The discussion above demonstrates the relevance of the technology context and its role and influence on the adoption of information security compliance.

The organizational context focuses on promoting organizational security that increases the belief of employees on the value of compliance with information security standards and policies [3,4]. Well-developed organizational initiatives on information security such as the active commitment of top management directly affect the behaviors of employees in complying with information security standards and policies [3] and organizational processes in managing information security compliance [47]. It is well recognized that lack of management support in encouraging adherence to information security policies has been singled out as a common reason for the poor implementation of information security policies and standards [48].

Promoting information security is essential for improving information security compliance in organizations [49]. There are various means for promoting information security. Having information security awareness programs in place, for example, can raise the knowledge and understanding of employees on information security policies and mechanisms [12]. Emphasizing on the roles and responsibilities of individual employees toward information security is another way to promote information security [27]. This is because employees with well-defined roles and responsibilities are more proactive in undertaking information security precautions. The discussion above shows that promoting information security through various means can improve information security compliance in public organizations for e-government development.

The environmental context is related to external pressures that an organization faces for adopting information security compliance. In such a situation, institutional theory is often applied to better understand the environmental pressure on information security compliance adoption [49,50]. Institutional theory posits that organizations must secure legitimacy from stakeholders by conforming to external expectations [43]. It classifies external pressures into coercive pressures based on political and legislative influences to adopt a specific organizational practice, mimetic pressures that cause organizations to imitate success actions and practices, and normative pressures originated from

business partners and professional associations for influencing an organization's decision to adopt new technologies and organizational practices.

There are significant external pressures on public organizations for enforcing information security compliance [1,27,51,52]. Such pressures propel organizations to integrate information security mechanisms into their daily practices by motivating employees to comply with information security practices [53]. Hu et al. [54], for example, showed that coercive pressures from legal requirements can force organizations to comply with information security policies and standards. Delmas et al. [55] found that the demand of stakeholders plays an important role in improving information security compliance. These studies demonstrate the important role of environmental factors in the adoption of information security compliance.

Developing appropriate operational processes to enhance information security can result in efficient execution of information security policies and standards [56]. Such operational processes can influence the acceptance of information security mechanisms. It is well recognized that information security operational processes and the way in which they are presented, integrated, and enforced are a fundamental leverage point for effective information security compliance [3,56]. Beautement et al. [39], for example, found out that information security compliance can be improved by integrating information security mechanisms with business processes. Vroom et al. [57] asserted that compliance with information security policies can be improved if information security mechanisms are well integrated with the daily work practices of individual employees. These studies illustrate the importance of adequate operational processes for improving information security compliance.

Process integration is about mapping information security mechanisms into business processes for information security [58]. Beautement et al. [47], for example, demonstrated that improving organizational processes can enhance information security compliance. Knorr et al. [56] found that developing appropriate business processes facilitates the implementation of information security mechanisms. Backes et al. [58] discovered that integrating security requirements into organizational processes can improve information security. These studies have shown that integrating security mechanisms into business processes can improve information security compliance.

Information security auditing and monitoring is about examining the implementation of information security policies and standards [59]. It is widely used for improving the overall effectiveness of information security compliance [3,59]. Steinbart et al. [60], for instance, found that auditing and monitoring improve the acceptance of information security policies and standards. Kolkowska and Dhillon [61] asserted that auditing and monitoring processes can enhance information security compliance. These studies show that the adoption of appropriate auditing and monitoring processes can improve information security compliance.

The discussion above suggests that the adoption of information security compliance is influenced by the characteristics of technological, organizational, environmental, and operational processes contexts on the theoretical background of TOE and institutional theory. Figure 1 presents a conceptual framework for better understanding the adoption of information security compliance in public organizations for e-government development. Such a framework is then tested and validated in the subsequent empirical study.

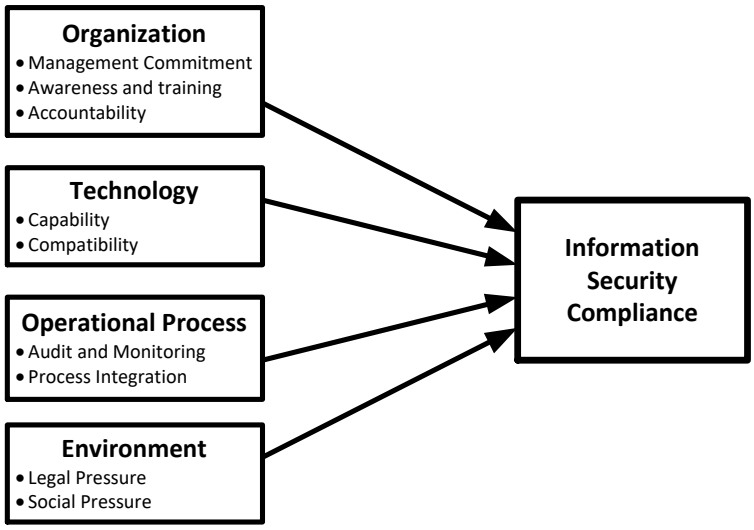


Figure 1. A framework for adopting information security compliance.

4. Research methodology

In this study, we adopt a qualitative approach for investigating information security compliance in e-government development in Oman. The adoption of this approach is due to the exploratory nature of the research [1] to identify the critical factors for the adoption of information security compliance.

Nine purposive interviews are conducted to obtain the inside views of the information security compliance practice in public organizations in Oman. Nine interviews are selected in this study due to the observations that the study has made in which no new information or themes could be observed in more interviews in the study [62]. Seven public organizations involved in e-government development in Oman are sampled. These organizations represent different sectors to triangulate the research findings, leading to better understanding of information security compliance.

Identifying participants and organizations for interview begins by contacting the Information Technology Authority (ITA) in Oman that manages the development of e-government initiatives. This leads to the identification of 64 public organizations that are involved in e-government projects. A simple selection process with two steps is used to choose participants from these organizations. The first step is based on the active involvement of the participant's organization in e-government development. This has been determined with the help of ITA and verified by an online investigation of information security practices. The second step is based on the knowledge, experience, and role of the potential participants in information security. This leads to the identification of 15 participants at the first stage for conducting interviews.

There are 9 information security managers from 7 organizations that are selected for interviews. These 9 managers have agreed to participate in semi-structured interviews. The interviews were conducted from July 2014 to August 2014 and took place at the participant's organization. Each interview takes about one hour and a half. Table 2 presents the profile of the participants and the details of their respective organizations.

Interview questions are developed based on a comprehensive review of the related literature together with the secondary data published on e-government development in Oman [63]. Using the secondary data for developing interview questions is useful to understand the level of maturity in e-government development. The interview questions are organized into three parts. The first part focuses on the demographic information of the interviewee. The second part comprises general questions on

the practices for information security compliance. The third part contains specific questions about the factors that influence the adoption of information security compliance. The interview questions are pretested with the help of academic experts, higher degree research scholars, and information security practitioners. The interviews are recorded and transcribed.

Table 2. An overview of the profile of participants.

Participants	Current position	Experience	Sector	Organization size
A	Information Security & Risk Management Officer	6 years	Finance	700
B	Information Security Manager	11 years	ICT	500
C	Head of Information security and audit Section	7 years	Governance	3900
D	Information Security Supervisor	8 years	Audit	800
E	Information Security Manager	7 years	ICT	400
F	Information Security Director	14 years	ICT	400
G	Information Security Director	10 years	Audit	150
H	Security and Infrastructure Director	7 years	Health	5000
I	Information Security Officer	10 years	ICT	70

Deductive and inductive analyses are used in analyzing the interview data [64,65]. The deductive analysis [66] is used to test and validate the conceptual framework shown in Figure 1. This leads to the identification of the critical factors for the adoption of information security compliance in e-government development. The inductive analysis is applied to explore the underlying themes that appear and re-appear within the data set that describe the inter-relationship between such themes [64]. Together with such holistic analysis, the interview data provides better understanding of the critical factors affecting the adoption of information security compliance.

5. Research findings

5.1. Deductive analysis findings

Deductive analysis investigates the relationship between the dimensions depicted as in Figure 1. The findings confirm that organization, technology, external environment, and operational processes most likely influence the adoption of information security compliance. Each dimension consists of the critical factors identified in the interview for the adoption of information security compliance.

5.1.1. Organizational context

Nine interviewees confirm that a well-developed organizational security context motivates employees to comply with information security policies and standards. They indicate that the more security minded an organization is, the less friction the compliance with information security policies and standards would create. The deductive analysis confirms that organizational security is underscored by management commitment, accountability, and awareness and training.

Management commitment is about the efforts of senior management in supporting information security compliance. Interviewees agree that senior management commitment directly influences employees to comply with information security policies and standards. Having senior management's (a) active support in decision making, investments, and actions taken for enforcing the information security policy, (b) involvement in maintaining organization's information security awareness, (c) push to align the goals of information security policy with organizational goals, (d) raising employees' loyalty using pride, respect, gratitude, and ownership strategies, and (e) ongoing communication of

information security policies and procedures are the prime motivations that could increase the belief and value of employees on compliance with information security policies and procedures. Most interviewees stress that employees' behaviors can be influenced by their superiors because people tend to follow what other people do or what they have been told. An interviewee explained:

> *"… active support of senior management is vital for information security, as employees within that organization generally live by example.."*

Accountability is found to affect information security compliance. It creates an organizational environment that inculcates individuals to take responsibility toward information security compliance [66]. Imposing accountability for information security practices is widely believed to be able to change employees' behaviors to comply with information security policies and standards [4]. Interviewees agree that individuals with well-defined roles and responsibilities are more proactive in undertaking higher information security precautions. The clarity of roles and responsibilities and the appropriateness of sanctions are highlighted as the critical factors that could generate impact on changing the intention of employees to comply with information security policies and standards. Interviewees point out that the belief of employees that noncompliance with information security policies would be detected and sanctions would be applied directly affect the adoption of information security compliance. As the following interview transcript suggests, due to the lack of accountability, some employees have violated information security policies:

> *"...If we want to minimize omissive behaviors and policy violation, we have to CLEARLY clarify the roles and responsibilities towards information security compliance in organizations and then we can enforce sanctions across the organization..."*

Awareness and training are an integral part of the organizational security context [4]. All the interviewees believe that it is important to maintain a functional pool of knowledge for employees to protect organizational information, especially when regular changes in the workforce are common. The interviewees agree that raising awareness on the risks and vulnerabilities increases perceived benefits of information security compliance. The interview reveals that effectiveness, usefulness, and visibility are the desirable outcomes when conducting awareness and training programs. Most interviewees stress that if employees think that the design and implementation of awareness and training programs are useful, they will exhibit compliance behaviors, therefore trying to avoid any deviant behavior that could harm information security.

5.1.2. Operational processes context

Explicit alignment between information security controls and business processes is critical in reducing incidents and the severity of security breaches. This confirms that operational processes are an important dimension influencing information security compliance. Operational processes are underlined by efficient integration and audit and monitoring.

Interviewees indicate that misalignment between security controls and business processes introduces friction. This strikes at the heart of the compliance for information security. The most effective way to avoid this friction is to improve the design and integration of security controls. Most interviewees stress that security control integration can provide employees and organizations with improved performance. In the opinion of one interviewee:

"…in integrating the security controls with the business processes, organizations can move from a reactive mode of security management to a proactive mode that can influence information security compliance through the operational processes…"

Effective auditing and monitoring are another important element identified as having significant impact on information security compliance. Interviewees state that constant auditing and monitoring can be employed to compel employees to comply with information security policies and to ensure the effectiveness of information security controls. Most interviewees acknowledge that the appropriateness of auditing and monitoring activities and perceived benefits of audit and monitoring processes increase their acceptance. Furthermore, management must maintain a continuous responsive attitude toward meeting the auditing and monitoring requirements to improve the effectiveness of auditing and monitoring activities.

5.1.3. Technology context

Technologies are confirmed as one of the four dimensions with a significant influence on information security compliance. Two factors are identified in this dimension, including technology compatibility and technology capability.

Technology compatibility facilitates the integration of security technologies available in enforcing security requirements [4]. Interviewees believe that incompatible technologies increase the complexity of information security controls. They point out that different information security compliance issues need to be addressed differently from the perspective of technology compatibility. These include the appropriateness of the security requirements, the interoperability of security technologies with the operational technologies, and the perceived impact. An interviewee, for example, states that:

"….better technology compatibility is more reduction of technical burdens and cost that leads to information security acceptance"

Another technology factor is the capability of security technologies. Interviewees think that technology capability increases the confidence of employees in information security compliance, leading to better acceptance of security controls. Interviewees confirm that having diverse security technology capabilities can increase the flexibility of implementing information security controls. All participants agree that the reliability of technologies in detecting and preventing information security threats, the extent of ease-to-use and ease-to-setup, and the availability of technical support need to be met to increase the acceptance of technical security controls.

5.1.4. External environmental context

The interviewees agree that the external environment is one of the four dimensions influencing information security compliance. The external environment is determined by legal pressures and social pressures [43]. Legal pressures are a prime example of institutional pressures that force public organizations to satisfy information security requirements. Interviewees indicate that regulating agencies play a major role in enforcing information security compliance. The interviewees believe there should be an appropriate methodology for auditing information security compliance to detect legal violations.

Social pressures are another form of institutional pressures that have a strong influence on information security compliance [66]. Privacy, trust, and quality of services, for example, are socially desirable needs that must be adequately addressed in e-government services. Most of the interviewees

recognize that the current citizens' knowledge, understanding, and perception of information security issues and social obligations create high pressures on public organizations to comply with information security standards and policies.

Overall, the deductive analysis findings confirm the importance of organizational, operational processes, technology, and environment characteristics for adopting information security compliance. The proposed relationships in Figure 1 are largely acknowledged.

5.2. Inductive analysis findings

Inductive analysis findings lead to the identification of four core constructs for adopting information security compliance in e-government development: organizational information security culture, information security enforcement, information security systems, and external pressure. Each construct consists of factors that have been identified, a total of 11 factors for influencing public organizations to comply with information security policies and standards. These factors include management commitment, awareness and training, loyalty, accountability, process integration, auditing and monitoring, technology compatibility, technology reliability, technology capability, legal pressure, and social pressure.

Validating the reliability of these factors is based on the triangulation of the evidence [67] from at least three interviews in two sectors. Table 3 summarizes the frequency of triangulation. For example, the validation of management commitment factor is supported by the triangulation of evidence from interviewees C, D, and I from three public organizations representing three sectors ICT, Audit, and Governance; technology reliability, from interviewees A, B, E, and F from two sectors ICT, and Finance; and social pressure, from interviewees D, E, and F from sectors ICT and Audit. This validation process, based on the triangulation of evidence from multiple sources, is used to enhance the reliability of the identified factors [66,67].

Table 3. Frequency of the triangulation of factors.

Factors	Frequency of triangulation	
	Cumulative sources	Cumulative sectors
Organizational information security culture		
Management commitment	4	3
Employee loyalty	3	2
Employee awareness	8	5
Information security systems		
Technology reliability	4	2
Technology capability	4	3
Technology compatibility	6	3
Information security enforcement		
Process integration	4	2
Accountability	7	4
Audit and monitoring	5	5
Environment pressure		
Regulatory pressure	6	4
Social pressure	3	2

The findings provide the basis for a revised framework of information security compliance adoption in e-government development. Figure 2 depicts a revised framework that incorporates the

changes in the early-proposed information security compliance framework in Figure 1. These changes include the disaggregation of the organizational construct into 'culture' and 'enforcement', the identification of new factors, and the modification of the relationship between constructs. These changes are discussed below.

The results of the interviews report a significant role that awareness of security issues plays in shaping the attitudes and behavior of individuals. They show that success in maintaining the effectiveness of information security awareness programs can encourage employees to behave securely. For example, using persuasive technologies such as interactive computing systems designed to change people's attitudes and behaviors to educate users, rather than providing traditional information security instructions on creating memorable yet secure passwords. The interview results further suggest that understanding and appreciating (a) the security risks and threats faced by an organization, (b) the responsibilities associated with the security policies and practices put in place to address these risks, and (c) the costs of losing or consequences are important factors that must be addressed by the information security awareness programs. This suggests that the design of the security awareness and training program in organizations should be tailored to reflect the organization's circumstances and should be commensurate with the nature of the organization's operations.

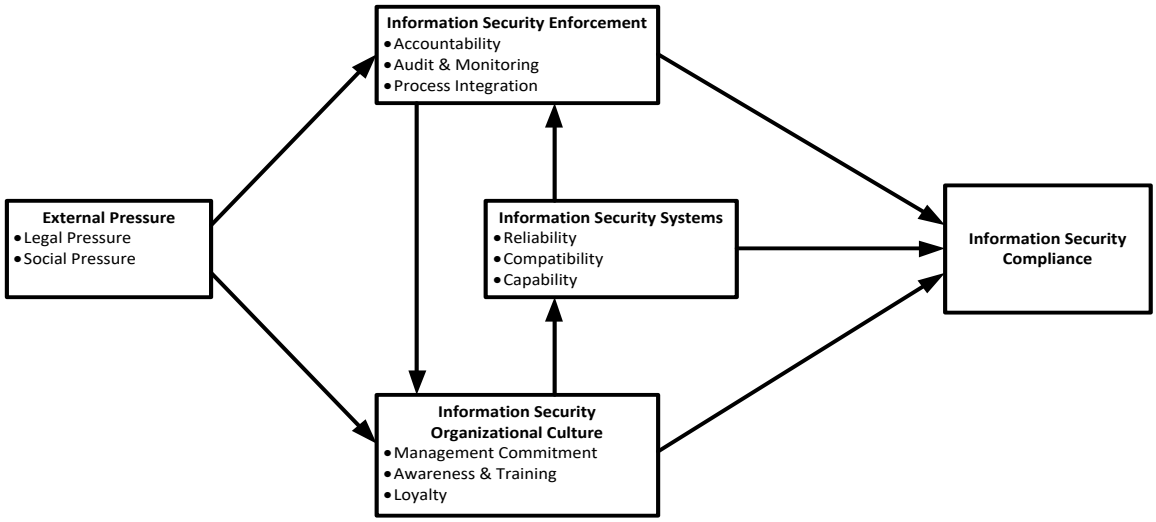


Figure 2. A Revised Information Security Compliance Framework.

The findings of the interviews highlight the pivotal influence of loyalty of employees in organizational on information security compliance. Organizational loyalty is referred to as the extent to which the individual employees are faithful to the organization, having feelings of bonding, inclusion, care, responsibility, and devotion toward their organizations (Colwill 2009). The interviewees widely believe that raising employees' loyalty reduces the misuse of intention of employees and increases users' avoidance of information security risks and threats. Interviewees suggest that management can use different strategies to raise loyalty, including pride, respect, gratitude, and ownership strategies that require comprehensible and discernible management efforts. An interviewee, for example, states that:

> *"...facilitating the development of personal relationships with employees help to enhance the level of organizational loyalty that may reduce the misuse intentions and increases employees' avoidance of information security risks and threats"*

Job engagement and job satisfaction are critical for raising employees' loyalty in organizations

(Kim 2005). Interviewees imply that by aligning the goals of the business with the goals of the individual improves employees' bonding and engagement that increases employees' organizational loyalty. The interview results show that employees who feel they are part of the organization and their future career is secure tend to avoid neglecting their organization's policies. In the opinion of one interviewee:

> *" ...employees that are attached to their organizations and with strong ties to colleagues tend to be happier with their work, and will make them think twice about harming or neglecting their organization's policy"*

5.2.1. Information security enforcement

The interviews indicate that developing appropriate processes to enforce information security policies and standards in organizations could result in an efficient execution of information security controls. Most of the interviewed security managers recognize the need for strong policies and enforcement processes for building a strong organizational security culture to change employees' attitudes toward information security compliance. This indicates that information security enforcement processes have a significant impact on building information security culture in organizations. In the opinion of one interviewee:

> *"unfortunately, policy development and enforcement is too often delegated to lower-level management, this ultimately diminishing the strength of the security culture"*

The results of the interviews show that employees in organizations with less stringent enforcement may weigh the level of information risks and threats and ignore security policies designed to protect information. Interviewees fully agree with the importance of the existence of information security policies that provides a comprehensive set of written rules and procedures in a sufficiently detailed manner for guiding appropriate information security behaviors in organizations. The interviewees stress that careless employees who do not comply with organization's information security policies and procedures constitute the major threat to information security. One observed suggestion to address this concern is a well-defined roles and responsibilities that obligate individual employees to be more proactive in undertaking higher information security precautions. The following segment of the interview transcript reflects this:

> *"the more the employee information security tasks are defined, the easier it is to determine inappropriate behavior".*

The interview results show that the inequity in sanction enforcement encourages poor compliance. The interviewees indicate that sanctions for security violations must be consistent across the organization so that employees understand the seriousness of the organization about information security enforcement. Furthermore, the interviews show that a delayed response to a violation might imply a lack of management commitment in protecting organization information. This delay enables security risks and violations to go unaddressed.

Effective auditing and monitoring are another important factor identified for enforcing information security policies. Interviewees state that constant auditing and monitoring can be employed to compel employees to comply with information security policy and to ensure the effectiveness of information security controls in public organizations. The interview results also show that these audit activities should not be seen as a chore or unwelcome interruption to day-to-day operational activities. It should be an opportunity to provide feedback on how security is benefiting

the organization or where security controls may be damaging productivity. This encourages employees to view the auditing activities in a more positive light.

The interview results show the real benefits of audit activities come from implementing the recommendations and dealing with the reported concerns. This requires management to maintain a continuous responsiveness toward the execution of auditing and monitoring requirements. Interviewees acknowledge that the responsiveness of management improves the overall effectiveness of auditing and monitoring activities and demonstrates the priority of information security in public organization. The following segment of the interview transcript reflects this:

> *"…if information security continued to be ignored by employees, and not enforced by top managers in public organization, the result of this is that organizational systems will be far less secure than they might and that security breaches will be far more frequent and damaging"*

Another factor for enforcing information security policies is to integrate information security mechanisms into operational processes for supporting business objectives. This integration focuses on facilitating the implementation of information security mechanisms and improving the acceptance of employees on security controls. The interview results indicate that the development of efficient integration between information security processes and operational processes is crucial to the execution of information security controls in organizations. One observed suggestion from the interviews is to consider information security issues earlier during the design and implementation phase of the operational processes. This enables specifying the relationship between the security needs and the functional requirements. Existing studies have shown that security mechanisms must be designed as an integral part of the business processes to be effective and efficient (Backes et al. 2003; Beautement et al. 2009; Knorr et al. 2001). Other observed suggestions to enhance the efficient integration between the security controls and the functional operational requirements are to automate information security activities within the operational processes. The interviewees widely believe that security automation decreases human intervention and therefore the costs and complexity of security activities. Furthermore, interviewees stress that the integration should be able to provide employees and organizations with benefits in terms of performance and productivity, and conformity with employees' expectations and requirements to increase the acceptance of information security practices in organizations. The following segment of the interview transcript indicates the importance of having efficient integration between security controls and the operational processes:

> *"the security controls must demonstrate its efficiency in integrating with users daily operational tasks"*

5.2.2. Information security systems

The interviews results demonstrate the importance of adopting adequate security technologies to enforce policies, monitor and alert violations, and strengthen information protection in organizations. These security technologies can be used to block prohibited activities such as viewing sites or downloading. The following segment of the interview transcript indicates the importance of using security technologies for enforcing security controls in organizations:

> *"Ultimately, security policies must be enforced without disturbing business operation. I believe (security manager) appropriate security technology is one of the key factors to succeed in addressing this challenge"*

Interviewees held the view that the reliability of the security technology in detecting and preventing information security threats increases employees' confidence and performance, which could lead to greater acceptance of security controls. The following segment of the interview transcript reflects this:

> *"… when we discuss about secure communication infrastructure readiness in e-government, the focus on technologies that are robust with minimum failures, ….and available any time with unstoppable secure services….must comply with security best practices"*

The results show that a misfit between technologies on interoperability directly impacts the acceptance of information security controls. Interviewees widely believe that the technical specification of security technologies is essential for enhancing the interoperability with the operational technologies. Such specifications include a protection profile that defines a standard set of security requirements for a specific type of product and evaluation assurance that defines how thoroughly the product is tested. The following interview transcript emphasizes the importance of security technology compatibility:

> *"Three important issues when it comes to security technology compatibility, compatibility with preferred work, compatibility with existing work practices, and compatibilities with values"*

Interviewees confirm that having diverse security system capability increases the flexibility of implementing information security controls. Most interviewees stress that the perceived impact of technology capability influences the acceptance of information security controls. The results show that having the ability to fulfil the technical security specification requirements and the organizational information security policies requirements increases the acceptance of technical security controls in organizations. The following segment of the interview transcript reflects this:

> *"… the competency of information security technologies gives options to customize information security controls to suite the information security requirements, also it can be used to enforce information security controls by hardening its technical characteristics"*

5.2.3. External environment

External pressures force public organizations to pursue information security compliance. Each of the security managers interviewed highlights the pivotal influence of these external pressures as a catalyst for instituting information security reforms. Each of the security managers interviewed stresses that environmental pressures could propel organizations to integrate information security mechanisms into their daily practices by motivating managers and employees to comply with information security standards and polices.

The interviews reveal that one source of external pressures for influencing information security compliance comes from the regulatory pressure. The interview results indicate that regulation agencies are powerful for organizational change to enforce regulations, especially when law may place legal obligations on public organizations to satisfy information security requirements. Such obligations include securing electronic transactions and information privacy. Different examples observed from the interviews show business managers who are sharply focused on daily operations often considered security an added burden that does little to improve the bottom line of the business and therefore they resist any changes that are aimed at improving security. Only the power of regulating agencies and the

severe consequences of noncompliance persuade these business managers to act. The following segment of the interview transcript reflects this:

> "*Currently, we hear of many cases in courts that are related to information security. This has created huge pressure on organizations' top managers to take precautions' with their information".*

It is notable that this source of external pressure is not sufficient to successfully influence information security compliance throughout public organizations without an appropriate methodology for auditing to detect any legal violation. An interviewee, for example, states that:

> *"the increased intervention of regulatory agencies can force organizations to comply with information security"*

The interview results show that the legal pressure could motivate top managers to mandate top–down approach for information security related changes across the organization. This mandate could formalize individual initiatives and efforts to promulgate effective security practices for information security compliance.

Other sources of external environment influences information security compliance come from social pressures. The need to protect desirable information coerces public organizations to strive to maintain the trust of citizens and preserve public organization's reputation as a responsible entity in guarding citizen information (Gunningham et al. 2005; Zhang et al. 2005). Privacy, trust, and quality of services, for example, are socially desirable needs that have been observed from the interviews and must be adequately addressed in organizations' services. These observations entail internal organizational efforts and practices for securing legitimacy from stockholders. An interviewee, for example, states that:

> *"The government has considered security as an integrated part of e-service quality. This obligation has created enormous social pressures on public organizations to secure citizen's information"*

Thus, these desirable needs shape what might be the information security efforts and practices at organizations. This, in turn, further suggests how successful the efforts taken by organizations to adopt significant information security related initiatives are.

6. Discussion

Contrary to the common belief that focuses predominantly on the attitude and behaviors of employees for the adoption of information security compliance in organizations [4,5,11], this study suggests that it is necessary to extend our understanding of information security compliance by emphasizing the value of organizational security culture, information security enforcement processes, technologies, and environment to enhance information security compliance in public organizations [3,68]. The revised framework incorporates such extensions to better describe the critical factors and their relationships in facilitating the adoption of information security compliance in public organizations for e-government development [4,69]. It stresses the importance of embedding information security culture and developing information security enforcement processes to encourage the compliance of employees with information security policies and procedures [52,57,70]. The revised framework concedes the pivotal distinctive factor of employees' organizational loyalty [3,12] for information security compliance that requires public organizations to use different strategies for raising employees' loyalty [70].

The revised framework shows the relationships between the core constructs for influencing information security compliance in public organizations. The direct relation, for example, between information security enforcement and information security organizational culture can be reflected by the equity in sanctions enforcement that stabilizes the organizational security culture by changing employees' attitudes toward information security compliance [68,71]. Furthermore, information security systems can be used to enforce information security controls by hardening its technical characteristics [23]. These relationships reflect the solidity of the revised framework.

The role of external environment in adopting information security compliance is well acknowledged in the revised framework [54,72]. The findings provide insight on coercive pressure and normative pressure and their implications for developing information security enforcement, as well as in building information security organizational culture. The findings, however, do not find strong evidence regarding the effects of mimetic pressure for information security compliance. Public organizations seem to believe that imitating success practices is deemed not desirable. Public organizations also have the freedom to respond for copying what others have adopted.

The revised framework for information security compliance has two important implications. First, the framework provides a frame of reference for understanding the factors and their influence on information security compliance. For instance, researchers may find the operational definitions of the core constructs and the associated factors useful for understanding and explaining the factors influencing information security compliance. Second, the generalizability of the framework makes it directly usable to undertake a critical and comparative analysis to validate the critical factors and their influence for information security compliance.

From a practice perspective, there are two immediate implications. First, the revised framework provides a reference for practitioners seeking to develop deep insight and common understanding of the critical factors that influence information security compliance in public organizations for e-government development. Second, owing to the strong exploratory and explanatory capability of the underlying theories, the framework enables the development of a broad view of, and insights into, the critical factors influencing information security compliance in public organizations. The framework is directly usable and therefore has a strong practical relevance that could identify and understand contexts for influencing information security compliance in public organizations.

Finally, the use of TOE theory and institutional theory in this study extend our understanding of information security compliance in terms of the values of organizational security culture, information security enforcement processes, technology, and environment to foster information security compliance in public organizations, rather than focusing predominantly on behavioral theories to change users' attitude and behaviors toward information security compliance

7. Conclusions

Effectively managing information security in public organizations is critical for the success of e-government development because it directly increases the confidence and trust of stakeholders in e-government. In this exploratory research, guided by TOE and institutional theories, we examine the organizational, technical, and environmental characteristics for adopting information security compliance in the pursuit of e-government development in public organizations. This leads to the development of an empirical framework for information security compliance in public organizations for e-government development.

The study shows that management commitment, accountability, awareness and training, loyalty, efficient integration, audit and monitoring, system reliability, technology compatibility, technology

capability, legal pressure, and social pressure are critical for ensuring information security compliance. This contributes to advancing our understanding of the critical factors influencing information security compliance in public organizations for e-government development. Moreover, this suggests that improving the adoption of information security compliance in public organizations need to go beyond the attitude and behavior of employees in public organizations.

The proposed framework is tested and validated by nine in-depth interviews in a single country. This means that this study has limitations. Further research can be done in this area. Replicating the study in other countries, for example, with different organizational and cultural settings would be a fruitful direction to gauge the generalizability of the study. Testing and validating the proposed framework using a confirmatory approach using a large-scale quantitative survey is another possible research direction. Furthermore, there is a need to carry out more comprehensive studies on how to better protect e-government information with the rapid development of artificial intelligence technologies [3] and the increasing use of such technologies in transforming the delivery of public services through e-government.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors very much appreciate the timely support from the Information Technology Authority of Oman in carrying out this study and are grateful for the constructive feedback received form the two reviewers for improving the paper.

Conflict of interest

Hepu Deng is an editorial board member for Applied Computing and Intelligence and was not involved in the editorial review and the decision to publish this article. The authors have no conflict of interest in preparing this manuscript for publication.

References

1. K. Karunasena, H. Deng, Critical factors for evaluating the public value of e-government in Sri Lanka, *Gov. Inform. Q.*, **29** (2012), 76–84. https://doi.org/10.1016/j.giq.2011.04.005
2. A. Almukhlifi, H. Deng, B. Kam, E-government adoption in Saudi Arabia: the moderation effect of Wastta, *Proceedings of the International Conference on Information Resources Management*, 2018, 9.
3. P. Gupta, A. Hooda, A. Jeyaraj, J. J. Seddon, Y. K. Dwivedi, Trust, risk, privacy and security in e-government use: insights from a MASEM analysis, *Inf. Syst. Front.*, **27** (2025), 1089–1105. https://doi.org/10.1007/s10796-024-10497-8
4. A. Alkalnani, H. Deng, B. Kam, A conceptual framework for information security in public organizations for e-government development, *Proceedings of the 25th Australasian Conference on Information Systems*, 2014, 1–11.
5. A. Gafurov, F. Botirov, Information security requirements in monitoring e-government systems, *Procedia Computer Science*, **252** (2025), 424–429. https://doi.org/10.1016/j.procs.2025.01.001

6. A. Alkalnani, H. Deng, B. Kam, X. Zhang, Investigating the impact of institutional pressures on information security compliance in organizations, *Proceedings of the 27th Australasian Conference on Information Systems*, 2016, 26.
7. L. Magnusson, S. Iqbal, P. Elm, F. Dalipi, Information security governance in the public sector: investigations, approaches, measures, and trends, *Int. J. Inf. Secur.*, **24** (2025), 177. https://doi.org/10.1007/s10207-025-01097-x
8. S. Solms, Information security governance-compliance management vs operational management, *Comput. Secur.*, **24** (2005), 443–447. https://doi.org/10.1016/j.cose.2005.07.003
9. P. Li, H. Deng, S. Duan, A compliance-based framework for digital identity management in organizations, *Proceedings of the Australian Conference on Information Systems*, 2022, 76.
10. M. Siponen, S. Pahnila, M. A. Mahmood, Compliance with information security policies: an empirical investigation, *Computer*, **43** (2010), 64–71. https://doi.org/10.1109/MC.2010.35
11. E. Kolkowska, G. Dhillon, Organizational power and information security rule compliance, *Comput. Secur.*, **33** (2013), 3–11. https://doi.org/10.1016/j.cose.2012.07.001
12. M. Siponen, M. A. Mahmood, S. Pahnila, Employees' adherence to information security policies: an exploratory field study, *Inform. Manage.*, **51** (2014), 217–224. https://doi.org/10.1016/j.im.2013.08.006
13. H. Cavusoglu, H. Cavusoglu, J. Y. Son, I. Benbasat, Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources, *Inform. Manage.*, **52** (2015), 385–400. https://doi.org/10.1016/j.im.2014.12.004
14. M. A. Sasse, S. Brostoff, D. Weirich, Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security, *BT Technol. J.*, **19** (2001), 122–131. https://doi.org/10.1023/A:1011902718709
15. S. M. Lee, S. G. Lee, S. Yoo, An integrative model of computer abuse based on social control and general deterrence theories, *Inform. Manage.*, **41** (2004), 707–718. https://doi.org/10.1016/j.im.2003.08.008
16. B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quart.*, **34** (2010), 523–548. https://doi.org/10.2307/25750690
17. N. S. Safa, R. Von Solms, S. Furnell, Information security policy compliance model in organizations, *Comput. Secur.*, **56** (2016), 70–82. https://doi.org/10.1016/j.cose.2015.10.006
18. E. A. Abu-Shanab, E-government familiarity influence on Jordanians' perceptions, *Telemat. Inform.*, **34** (2017), 103–113. https://doi.org/10.1016/j.tele.2016.05.001
19. D. Zissis, D. Lekkas, Securing e-government and e-Voting with an open cloud computing architecture, *Gov. Inform. Q.*, **28** (2011), 239–251. https://doi.org/10.1016/j.giq.2010.05.010
20. C. J. Tolbert, K. Mossberger, The effects of e-government on trust and confidence in government, *Public Admin. Rev.*, **66** (2006), 354–369. https://doi.org/10.1111/j.1540-6210.2006.00594.x
21. W. A. Conklin, Barriers to adoption of e-government, *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 2007, 98–98. https://doi.org/10.1109/HICSS.2007.102
22. S. Benabdallah, S. Gueniara El Fatmi, N. Oudriga, Security issues in e-government models: what governments should do? *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, 2002, 398–403. https://doi.org/10.1109/ICSMC.2002.1173445
23. J. S. Burkett, Business security architecture: weaving information security into your organization's enterprise architecture through SABSA®, *Inf. Secur. J.*, **21** (2012), 47–54. https://doi.org/10.1080/19393555.2011.629341
24. Z. Ebrahim, Z. Irani, E-government adoption: architecture and barriers, *Bus. Process Manag. J.*, **11** (2005), 589–611. https://doi.org/10.1108/14637150510619902

25. P. Ifinedo, Information systems security policy compliance: an empirical study of the effects of socialization, influence, and cognition, *Inform. Manage.*, **51** (2014), 69–79. https://doi.org/10.1016/j.im.2013.10.001
26. T. Neubauer, M. Klemen, S. Biffl, Secure business process management: a roadmap, *Proceedings of the First International Conference on Availability, Reliability and Security*, 2006, 8. https://doi.org/10.1109/ARES.2006.121
27. T. Herath, H. R. Rao, Protection motivation and deterrence: a framework for security policy compliance in organizations, *Eur. J. Inform. Syst.*, **18** (2009), 106–125. https://doi.org/10.1057/ejis.2009.6
28. S. Palvia, S. Sharma, E-government and e-governance: definitions/domain framework and status around the world, *Proceedings of the International Conference on E-governance*, 2007, 1–12.
29. A. C. Johnston, M. Warkentin, Fear appeals and information security behaviors: an empirical study, *MIS Quart.*, **34** (2010), 549–566. https://doi.org/10.2307/25750691
30. R. M. Shaw, The influence of organizational culture on employee attitudes towards information security policy, Ph. D Thesis, Capella University, 2012.
31. M. Chan, I. Woon, A. Kankanhalli, Perceptions of information security at the workplace: linking information security climate to compliant behavior, *Journal of Information Privacy and Security*, **1** (2005), 18–41. https://doi.org/10.1080/15536548.2005.10855772
32. S. M. Lee, S. G. Lee, S. Yoo, An integrative model of computer abuse based on social control and general deterrence theories, *Inform. Manage.*, **41** (2004), 707–718. https://doi.org/10.1016/j.im.2003.08.008
33. L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study, *Eur. J. Inf. Syst.*, **18** (2009), 126–139. https://doi.org/10.1057/ejis.2009.10
34. P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: an action research study, *MIS Quart.*, **34** (2010), 757–778. https://doi.org/10.2307/25750704
35. M. T. Siponen, A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, **8** (2000), 31–41. https://doi.org/10.1108/09685220010371394
36. I. Ajzen, The theory of planned behavior, *Organ. Behav. Hum. Dec.*, **50** (1991), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T
37. D. W. Straub, Effective IS security: an empirical study, *Inform. Syst. Res.*, **1** (1990), 255–276. https://doi.org/10.1287/isre.1.3.255
38. H. Liang, Y. Xue, Understanding security behaviors in personal computer usage: a threat avoidance perspective, *J. Assoc. Inf. Syst.*, **11** (2010), 394–413. https://doi.org/10.17705/1jais.00232
39. S. Smith, R. Jamieson, Determining key factors in e-government information system security, *Inform. Syst. Manage.*, **23** (2006), 23–32. https://doi.org/10.1201/1078.10580530/45925.23.2.20060301/92671.4
40. A. Beautement, M. A. Sasse, M. Wonham, The compliance budget: managing security behavior in organizations, *Proceedings of the 2008 New Security Paradigms Workshop*, 2009, 47–58. https://doi.org/10.1145/1595676.1595684
41. M. Al-Busaidy, V. Weerakkody, E-government diffusion in Oman: a public sector employees' perspective, *Transform. Gov.: People*, **3** (2009), 375–393. https://doi.org/10.1108/17506160910997883
42. Q. Al-Mamari, B. Corbitt, V. O. Gekara, E-government adoption in Oman: motivating factors from a government perspective, *Transform. Gov.: People*, **7** (2013), 199–224. https://doi.org/10.1108/17506161311325369

43. L. G. Tornatzky, M. Fleischer, A. K. Chakrabarti, *The processes of technological innovation*, Lexington: Lexington Books, 1990.
44. P. J. DiMaggio, W. W. Powell, The iron cage revisited: institutional isomorphism and collective rationality in organizational fields, *Amer. Sociol. Rev.*, **48** (1983), 147–160. https://doi.org/10.2307/2095101
45. M. Wimmer, B. Von Bredow, A holistic approach for providing security solutions in e-government, *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002, 1715–1724. https://doi.org/10.1109/HICSS.2002.994083
46. D. P. Moynihan, Building secure elections: e-voting, security, and systems theory, *Public Admin. Rev.*, **64** (2004), 515–528.
47. A. Kaliontzoglou, P. Sklavos, T. Karantjias, D. Polemi, A secure e-government platform architecture for small to medium sized public organizations, *Electron. Commer. Res. Appl.*, **4** (2005), 174–186. https://doi.org/10.1016/j.elerap.2004.09.002
48. A. Beautement, M. A. Sasse, M. Wonham, The compliance budget: managing security behavior in organizations, *Proceedings of the 2008 New Security Paradigms Workshop*, 2009, 47–58. https://doi.org/10.1145/1595676.1595684
49. G. Karokola, L. Yngstrom, S. Kowalski, Secure e-government services: a comparative analysis of e-government maturity models for the developing regions-the need for security services, *Int. J. Electron. Gov. Res.*, **8** (2012), 1–25. https://doi.org/10.4018/jegr.2012010101
50. A. McIlwraith, *Information security and employee behavior: how to reduce risk through employee education, training and awareness*, London: Routledge Publishing, 2021. https://doi.org/10.4324/9780429281785
51. J. L. Gibbs, K. L. Kraemer, A cross-country investigation of the determinants of scope of e-commerce use: an institutional approach, *Electron. Mark.*, **14** (2004), 124–137. https://doi.org/10.1080/10196780410001675077
52. A. Kankanhalli, H. H. Teo, B. C. Tan, K. K. Wei, An integrative study of information systems security effectiveness, *Int. J. Inform. Manage.*, **23** (2003), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6
53. H. Deng, K. Karunasena, W. Xu, Evaluating the performance of e-government in developing countries: a public value perspective, *Internet Res.*, **28** (2018), 169–190. https://doi.org/10.1108/IntR-10-2016-0296
54. S. E. Chang, C. B. Ho, Organizational factors to the effectiveness of implementing information security management, *Ind. Manage. Data Syst.*, **106** (2006), 345–361. https://doi.org/10.1108/02635570610653498
55. L. Khansa, D. Liginlal, The influence of regulations on innovation in information security, *Proceedings of the Americas Conference on Information Systems*, 2007, 180.
56. Q. Hu, P. Hart, D. Cooke, The role of external and internal influences on information systems security–a neo-institutional perspective, *J. Strategic Inf. Syst.*, **16** (2007), 153–172. https://doi.org/10.1016/j.jsis.2007.05.004
57. M. A. Delmas, M. W. Toffel, Organizational responses to environmental demands: opening the black box, *Strategic Manage. J.*, **29** (2008), 1027–1055. https://doi.org/10.1002/smj.701
58. K. Knorr, S. Röhrig, Security requirements of e-business processes, In: *Towards the e-society: e-commerce, e-business, and e-government*, Boston: Springer, 2001, 72–86. https://doi.org/10.1007/0-306-47009-8_6
59. C. Vroom, R. Von Solms, Towards information security behavioral compliance, *Comput. Secur.*, **23** (2004), 191–198. https://doi.org/10.1016/j.cose.2004.01.012
60. M. Backes, B. Pfitzmann, M. Waidner, Security in business process engineering, In: *Business process management*, Berlin: Springer, 2003, 168–183. https://doi.org/10.1007/3-540-44895-0_12

61. T. Neubauer, M. Klemen, S. Biffl, Secure business process management: a roadmap, *Proceedings of First International Conference on Availability, Reliability and Security*, 2006, 8. https://doi.org/10.1109/ARES.2006.121
62. P. J. Steinbart, R. L. Raschke, G. Gal, W. N. Dilla, The relationship between internal audit and information security: an exploratory investigation, *Int. J. Account. Inf. Syst.*, **13** (2012), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007
63. E. Kolkowska, G. Dhillon, Organizational power and information security rule compliance, *Comput. Secur.*, **33** (2013), 3–11. https://doi.org/10.1016/j.cose.2012.07.001
64. G. Guest, A. Bunce, L. Johnson, How many interviews are enough? An experiment with data saturation and variability, *Field Method.*, **18** (2006), 59–82. https://doi.org/10.1177/1525822X05279903
65. *Information Technology Authority, Information technology authority annual report*, The official government of Oman, 2013. Available from: https://prod.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/FID20146251144117 65/DJ504797_ITA_e.oman_Annual%20English%20Report%202013_FAW_For%20upload,%2002.06.2014.pdf.
66. D. Howitt, *Introduction to qualitative methods in psychology*, New Jersey: Prentice Hall, 2010.
67. M. Healy, C. Perry, Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm, *Qual. Mark. Res.*, **3** (2000), 118–126. https://doi.org/10.1108/13522750010333861
68. K. Karunasena, H. Deng, K. S. Harasgama, An investigation of the critical factors for evaluating the public value of e-government: a thematic analysis, In: *Information systems and technology for organizations in a networked society*, Hershey: IGI Global, 2013, 213–233. https://doi.org/10.4018/978-1-4666-4062-7.ch012
69. M. B. Miles, A. M. Huberman, *Qualitative data analysis: an expanded sourcebook*, Thousand Oaks: Sage Publications, Inc., 1994.
70. M. O. Alassafi, A. Alharthi, R. J. Walters, G. B. Wills, A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies, *Telemat. Inform.*, **34** (2017), 996–1010. https://doi.org/10.1016/j.tele.2017.04.010
71. J. L. Gómez-Barroso, Experiments on personal information disclosure: past and future avenues, *Telemat. Inform.*, **35** (2018), 1473–1490. https://doi.org/10.1016/j.tele.2018.03.017
72. M. S. Janita, F. J. Miranda, Quality in e-government services: a proposal of dimensions from the perspective of public sector employees, *Telemat. Inform.*, **35** (2018), 457–469. https://doi.org/10.1016/j.tele.2018.01.004



AIMS Press

©2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)