Journal of Computer Science

Original Research Paper

Integrated Information Security Policy Model for Saudi Arabia Organizations

Wad Ghaban

Department of Computer Science, Applied College, University of Tabuk, Saudi Arabia

Article history
Received: 31-10-2022
Revised: 31-01-2023
Accepted: 10-02-2023

Email: wghaban@ut.edu.sa

Abstract: Information Security Policy (ISP) is an important domain used to preserve the confidentiality, integrity, and availability of sensitive data. However, it is an ambiguous and diverse domain due to the diversity of security policies and the multiplicity nature of organization systems. Numerous specific and generic ISP models have been offered for several purposes. The offered models have numerous redundant procedures, concepts, activities, processes, and tasks that make the ASP domain unorganized, unstructured, and ambiguous among domain experts and users. Thus, the structured and integrated model to simplify sharing, managing, and reusing ISP activities and tasks is still missing. This study applied the design science method to develop a unified model for the ISP domain called the Integrated Information Security Policy Model (IISPM). This aims to identify, recognize, extract, and match different ISP processes, concepts, activities, and tasks from different ISP models in a developed IISPM, thus, allowing domain experts and users to derive/instantiate solution models easily. The developed IISPM consists of six main abstract processes: Information security policy process, information security awareness process, access control process, observing the process, agreement process, and plan process. Each introduced process has specific security practices. The output showed that IISPM assists domain experts and users to create their solution models based on their requirements.

Keywords: Information Security Policy, Metamodeling, Design Science Research

Introduction

Information security is a vital domain used to protect the confidentiality integrity and availability of sensitive data from any misuse conducted by other people who do not have authority. Therefore, organizations have implemented many information securities policies models and frameworks to protect their valuable information from unauthorized entities. Information Security Policy (ISP) is specified as a "written statement that defines the requirements for the organizational security management, the employees' responsibility and obligations, authorizations and countermeasures for non-compliance" (Connolly *et al*., 2018). However, the ISP models are varying and heterogamous amongst organizations which produces several issues and challenges among users and experts. Thus, the ISP domain has suffered from numerous matters and become a confusing, diverse, and unstructured domain (Barkhiya, 2014).

The most significant security issues involved in deployment are protecting data from unauthorized access, preventing malicious software from damaging systems, and ensuring that services are only available to authorized users. Data security involves protecting sensitive information from unauthorized access, modification, or destruction. Malware protection involves preventing malicious software, such as viruses and worms, from damaging systems or stealing data. Authorization involves ensuring that only users with the proper credentials can access specific services or data. Additionally, security measures must be taken to mitigate the risks of Distributed Denial-of-Service (DDoS) attacks, SQL injection attacks, cross-site scripting attacks, and other types of malicious activities.

The primary purpose of this study is to propose an integrated information security policy model for managing and organizing diverse information security policy domains using a design science approach. The developed model consists of six main abstract processes: (1) Information security policy process, (2) Information security awareness process, (3) Access control process, (4) Observing process, (5) Agreement process, and (6) Plan process. The whole procedures, policies, concepts, processes, tasks, and activities of the existing ISP models

will be combined, structured, and organized in the developed model based on such modeling rules. Thus, the scattered ASP knowledge will be organized, structured, managed, reused, and shared among ASP users and experts.

This study will add many values to the kingdom vision 2030 from many angles. One of the important elements of 4IR is cybersecurity. ISP domain is part of the support component in facing cybersecurity attacks and is a key source of electronic security policies for the organization. Regardless of the size of the organizations or the complexity of the infrastructure used from a local building contractor to a massive, multinational company that manages everything, there is a procedure contained within the security policies. ISP comes into play during Intellectual Property (IP) or patent infringement cases, corporate espionage, and even intrusion events like a data breach or an instigated virus infection (Ksibi *et al*., 2022). For this purpose, the developed IISPM is a novel platform and can solve the heterogeneity, interoperability, and ambiguity of the ISP domain. It allows domain experts and users to create their solutions models easily based on their requirements.

The novelty of the developed IISPM for Saudi Arabia organizations lies in its comprehensive approach. It seeks to address the various aspects of information security, from risk management and security governance to technical and organizational measures. It also provides a framework for developing and implementing data security policies that are tailored to the specific needs of Saudi Arabian organizations. The policy model is based on international standards and best practices and it provides guidance to organizations on how to develop and implement effective information security policies. Additionally, the developed policy model considers the cultural and legal environment in Saudi Arabia, which is an important factor in ensuring the effective implementation of the policy.

The contributions of the developed IISPM for Saudi Arabia organizations may include:

a) Provides a comprehensive and cohesive framework for organizations to effectively manage their data and information security risks
b) Provides clear guidance on how to identify, assess and respond to security threats and ensure the security of critical data
c) Offers a comprehensive approach to information security management by providing guidance on how to develop and implement an effective security policy that meets the specific needs of the organization
d) The model helps organizations develop a culture of security awareness and promotes the development of best practices that can be used to protect the organization's information assets
e) Provides a comprehensive view of the security landscape for organizations operating in the region, allowing them to better understand and respond to the ever-evolving risks posed by malicious actors

Materials and Methods and Development Process

This study applied two methods to develop the integrated information security policy model adapted from (Wolfswinkel *et al*., 2013; Al-Dhaqm *et al*., 2017a). The first method is used to review and discover the issues of the information security policy domain and, the second method is used to develop an integrated information security policy model for managing and organizing diverse information security policy domains. Figure 1 illustrates the adapted methodology for this study.

Defining research questions and keywords: This stage aims to restrict the scope of the study through assigned protocols that help authors to concentrate on the aim of the study. The first protocol is defining the research questions and the second protocol is defining the specific keywords. Thus, this study follows these research questions:

a) What are the existing ISP models and frameworks?
b) What are the limitations and issues of the existing ISP models and frameworks?
c) Does the information security policy domain have a unified model to manage and organize the information security policy domain knowledge?

Secondly, the keywords must assign to help researchers find relevant articles. For example, “information security policy”; “security policy” is the specific keywords used in this study.

Searching in the popular search engines: Based on the assigned/defined keywords in the stage above, authors are searching in the common/popular search engines such as IEEE explorer, Scopus, web of science, springer, and google scholar. A detailed study of the existing information security policy models was conducted to understand the common processes, concepts, tasks, procedures, and activities in the ISP domain. This gives a basic understanding and knowledge of the ISP domain. The web of science, Scopus, IEEE explore, springer links, and google scholar is the famous database search engines that were used to discover the ISP domain. For this purpose, this study used the following search keyword: “Information security policy”. Searching was limited to the period 2000-2022. This produced a total of 24565 articles from the whole database search engines. In this study, research articles, conference papers, books, book chapters, and dissertations are considered while other types of documents were excluded from the analysis. The details of the search protocols are summarized in Table 1 displays the results of search engines.

Table 1: Summary of information security policies articles

Search engine	Results
IEEE Xplore	5299
Scopus	877
Web of science	380
Springer	1209
Google scholar	16,800
Total articles	24565

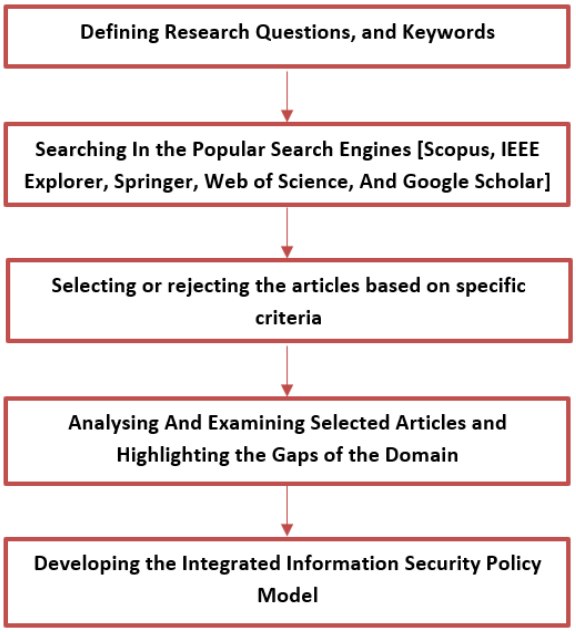

Fig. 1: The research methodology and the development process

Selecting or rejecting the articles based on specific criteria: In this stage, authors put some criteria to select the relevant articles which focused on the ISP domain purely. Thus, the authors follow these criteria adapted from (Al-Dhaqm *et al*., 2020a; Panda and Jana, 2015):

a) Excluding the title, abstract, related works, and conclusion of the information security policy model
b) Including the main text or figure which discussed the proposed work
c) Excluding irrelevant models

Analyzing and examining selected articles and highlighting the domain gaps: There are several studies on the development of ISP that discussed different development processes of the ISPs which are varying in processes, practices, tasks, procedures, and activities. For example, (Thakur *et al*., 2016) introduced a study that identified and discovered the main issues which affect sellers in Saudi Arabia including the agreement of E-commerce. The authors (Alzamil, 2018) investigated the status of the ISP at a subgroup of Saudi companies by realizing the opinions of their information technology workers. The authors of (Talib *et al*., 2018) proposed (11) Security policies as a basis for the Saudi Arabia ISP domain: (1) Security documentation of risks, (2) Security awareness, (3) Security insurance, (4) Privacy, (5) Reliability, (6) Accessibility, (7) Confidentiality, (8) Verification, (9) Permission, (10) Access control and (11) Responsibility. Alsaif *et al*. (2015) introduced awareness and efficiency of the ISP of the company among workers. However, the study discovered that the workers are not concerned about the policies and the effects of breaches. Also, the recognition of breaches is not performed methodically. Almubayedh *et al*. (2018) discussed ISP problems in Saudi Arabia companies and concentrated on an audit that was presented for a small company in Saudi Arabia. The authors (Aljuryyed, 2022) explored the several cyber-attacks installed upon Saudi Arabia, their influences and present cybersecurity creativities pitched about a permanent solution. Alghamdi *et al*. (2022); Evers (2023) proposed a model to discover employees' changes and recognize the issues that can affect their opinions and goals toward agreement. However, the study the absence of an information security policy that proposes strong safeguards for the organization. Olnes (1994) the authors developed a model for the development, implementation, and maintenance of security policies. They stressed the importance of having a methodological approach in developing, implementing, and maintaining security policy. However, the developed model of policy development is not holistic in that it does not specifically address how policy document is developed, communicated, enforced, and evaluated (Alshaikh *et al*., 2016). Bayuk and Price Waterhouse (1997) the authors proposed a process with a narrow view that focuses on the development of policy documents and does not include any practices associated with the execution and preservation of the policy. The proposed process consists of several steps. It starts by identifying assets and then forming a team to develop the policy. Then the draft policy is produced. The draft policy goes through a review process leading to approval and publishing. Tipton and Krause (2007) the authors proposed the development process of security policy in a systematic way, however, details are lacking about how the policy will be published and how it will be communicated and enforced. In addition, (Pierson, 2005) did not discuss the issue of user compliance with the policy and the importance of user awareness and training in communicating and enforcing security policy in organizations. The authors presented a more holistic view of the policy development process, however, there are a few overlapping concepts such as compliance, monitoring, and enforcement. These three concepts are presented in the approach as three distinct activities, while they represent the management efforts to ensure that the policy is being adhered to by employees. Stating one concept in three different terms or stating two different activities in one term may confuse security practitioners embarking on the process of policy development. Rees *et al*. (2003) the authors proposed a framework called Policy Framework for Information Security (PFIRES). It contains four main stages: Review, development, supply, and control. Each is sharply defined with specific exit criteria that should be met before transitioning to the next phase. Karyda *et al*. (2005) the

authors proposed a development model on risk evaluation, organizational culture, knowledge, security management, building, execution, and protection. The authors proposed a development process model that consists of 5 phases: Team development, risk assessment, policy construction, implementation, and maintenance. Tuyikeze and Pottas (2001) the authors proposed the ISP development model that consists of four major phases: Risk assessment, policy construction, policy implementation, policy monitoring, and maintenance. Each phase can be expanded into steps detailing the activities that occur within each phase. Tuyikeze and Flowerday (2014) the authors proposed 4 information security policy development and implementation processes: Security policy development, security policy drivers, security policy guidance, and existing theories. Alshaikh *et al*. (2016) the authors proposed a development process model which consists of three phases: Develop, implement and maintain and evaluate. It has several practices and activities. A generic framework was proposed by Ismail *et al*. (2017) to improve and establish the development process of security policies in institutions of higher education. It consists of three main phases of security policy development, namely the pre-development, development, and implementation phases. Almeida *et al*. (2018) the authors discovered that the top three most important elements in the structure of a security policy are asset management, security risk management, and defining the scope of the policy. However, the security strategies controls did not cover by the study. Moody *et al*. (2018) the authors proposed an ISP compliance model that included variables such as Self Efficacy (SE), understanding the vulnerability of resources, and awareness. Park and Chai (2018) the authors developed an instrument to examine the difference between employees' internalization of and compliance with information security policies and verify the instrument's validity and reliability. Results provided a foundation for devising solutions to the weaknesses in employees' compliance with information security practices and for inspiring information security practices consistently based on employee autonomy. Kaušpadienė *et al*. (2019) the authors designed a practical and reliable model for assessing information security management framework quality and suitability for application in small and medium sized enterprises. However, it will not provide the type of flexibility that may be required for small and medium sized enterprises. Ofori *et al*. (2022) provided a systematic insight into the factors affecting information security policy compliance. Hengstler *et al*. (2022) the authors developed a taxonomy to classify different types of information security policy non-compliance behaviours. Kabanda and Mogoane (2022) the authors identified the factors influencing ISP compliance within emerging economies of small organizations. On the other hand, several studies have been proposed to capture and analyze different kinds of cybercrimes. Al-Dhaqm *et al*. (2017b-c; 2013; 2020b; 2021a-b; 2018); Ghabban *et al*. (2021); Alhussan *et al*. (2022) authors offered different kinds of models, frameworks, methods, and security policies to identify, capture and analyze the cybercrimes.

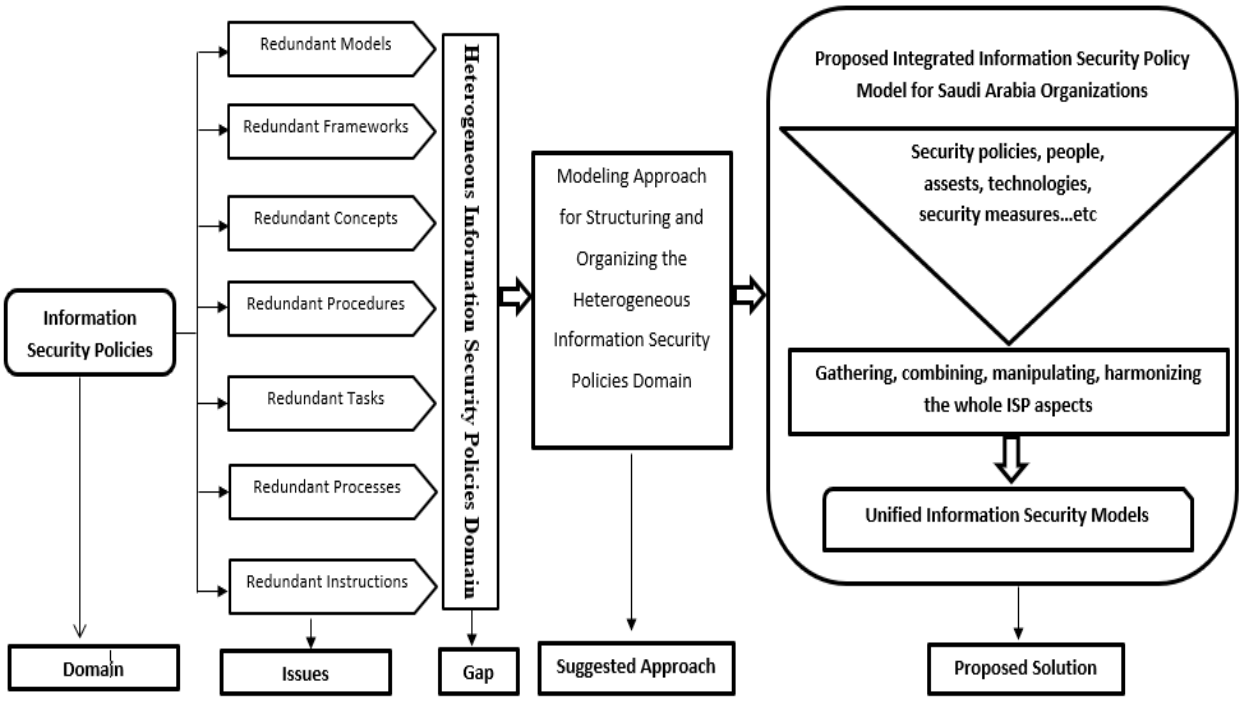

Fig. 2: The main issues and suggested solutions for the ISP domain

Therefore, through this analysis, the ISP is a diverse, ambiguous, and unstructured domain. It lacks a unified model to organize and manage the information security policies knowledge. Figure 2 shows the main issues discovered in the ISP domain and the proposed solution.

Developing the integrated information security policy model: In this stage, the IISPM is developed using a metamodeling approach. The metamodeling approach is an iteration process used to construct a high-level model to organize and structure the diverse domains (Al-Dhaqm *et al*., 2017a; 2020c). In the first step, authors identify and select the relevant ISP models based on the coverage criteria adapted from (Al-Dhaqm *et al*., 2017b) and then extract and merge the common concepts and processes from the selected models based on the semantic similarities (Selamat *et al*., 2008). Table 2 displays the identified and selected ISP models as well as the extracted concepts.

The extracted processes and concepts are combined and harmonized in the common abstract terms based on the naming, similar meanings, and activities (Ali *et al*., 2017). Thus, six ISP processes and 42 ISP practices have been proposed in this study. Table 3 displays the proposed common abstract terms for the ISP domain.

Table 2: Identified and selected ISP models

ID	Year	Selected ISP models	Ref.	Extracted concepts
1	1994	Development of security policies	Olnes (1994)	List of resources, list of threats, risk analysis, documentation
2	1997	Security through process management	Bayuk and Price Waterhouse (1997)	Policy, awareness, access, monitoring, compliance, strategy compliance, monitoring, enforcement
3	2002	Developing effective security policies		
4	2003	PFIRES: A policy framework for information security	Rees *et al.* (2003)	Review, develop, supply, control
5	2005	The study of policy development	Pierson (2005)	Risk assessment, policy implementation, security policy guidance
6	2005	Information systems security policies: A contextual perspective	Karyda *et al*. (2005)	Risk evaluation, organizational culture, knowledge, security management, building, execution, protection
7	2007	Information security management	Tipton and Krause (2007)	Security manager, security policy, access control, network security policy, information security governance, risk management
8	2007	Information security policy-a development guide for large and small companies		Team development, risk assessment, policy construction, implementation, maintenance
9	2011	An information security policy development life cycle	Tuyikeze and Pottas (2011)	Risk assessment, policy construction, policy implementation, policy monitoring and maintenance
10	2014	Information security policy development and Implementation: A content analysis approach	Tuyikeze and Flowerday (2014)	Security policy development, security policy drivers, security policy guidance, existing theories
11	2015	Information security management in Saudi Arabian organizations	Alsaif *et al.* (2015)	Security violation, deterrence information security administration, information security policy
12	2016	Information security policy for E-commerce in Saudi Arabia Saudi diplomatic mission	Thakur *et al.* (2016)	Security policy, E-commerce, E-government, Saudi ministry, Saudi government, economic trends, foreign investment
13	2016	Information security policy: A management practice perspective	Alshaikh *et al*. (2016)	Develop policy phase, implement and maintain policy phase, evaluate policy phase
14	2017	A generic framework for information security policy development	Ismail *et al*. (2017)	pre-development, development, and implementation phases
15	2018	Information security practice in Saudi Arabia: case study on Saudi organizations	Alzamil (2018)	Information security, case study, information security policy, information security in Saudi Arabia, information security management, information security procedures
16	2018	Ontology-based cyber security policy implementation in Saudi Arabia	Talib *et al*. (2018)	Security documentation of risks, (2) Security awareness, (3) Security insurance, (4) Privacy, (5) Reliability, (6) Accessibility, (7) Confidentiality, (8) Verification, (9) Permission, (10) Access control, and (11) Responsibility
17	2018	Security related issues in Saudi Arabia small organizations: A Saudi case study	Almubayedh *et al.* (2018)	Information security awareness, information security, procedures, outsourcing, audit, start-up company policy, risk scenarios
18	2018	Cybersecurity Issues in the middle east: Case study of the kingdom of Saudi Arabia	Aljuryyed (2022)	Cyber-attacks, security awareness, asset management
19	2018	Structure and challenges of a security policy on small and medium enterprises	Almeida *et al*. (2018)	Asset management, security risk management, define the scope of the policy
20	2018	Toward a unified model of information security policy compliance	Moody *et al.* (2018)	Self-efficacy, understanding the vulnerability of resources, awareness
21	2018	Internalization of information security policy and information security practice: A comparison with compliance	Park and Chai (2018)	Compliance, employees, reliability, information security practices
22	2019	Information security management framework suitability estimation for small and medium enterprise	Kaušpadienė *et al.* (2019)	Information security policies, organization of information security, human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relationships, information security incident management, information security aspects of business continuity management, compliance, guidelines, community, tools
23	2022	Employees' intentions toward complying with information security controls in Saudi Arabia's public organizations	Alghamdi *et al*. (2022)	Awareness, motivation, attitude, monitoring, detection certainty, measurement, punishment severity
24	2022	Factors influencing information security policy compliance behaviours	Ofori *et al*. (2022)	General deterrence theory, compliance information security climate, intention to comply
25	2022	Towards a taxonomy of information security policy non-compliance behaviours	Hengstler *et al*. (2022)	Personal moral, organizational moral, conscious, not conscious, beneficial, malicious, not malicious, informative, monetary
26	2022	A conceptual framework for exploring the Factors influencing information security policy compliance in emerging economies	Kabanda and Mogoane (2022)	Information security compliance, monitoring, reviewing, awareness
27	2023	Information systems strategy and security Policy: A conceptual framework		Offered a model built on the ITU cybersecurity findings, with the aim of creating a plan for the effective growth and execution of the public cybersecurity policy in Greece

Table 3: Proposed ISP processes and practices

Proposed common information security policy process	Proposed common information security policy practices	Total policy practices for each information security policy process
Information security policy process	• Recognized organization assets to be secured • Recognize organizations that implement security tasks assets • Outline a short policy statement • Assessment and endorse high-level policy declaration • Allocate sub-teams for analysis of each section of a policy document • Outline policy document • Assessment and endorse comprehensive policy document • Distribute accepted security policy documents to users • Recommend policy changes	9
Information security awareness process	• Build a security awareness system • Authorize a security awareness system • Build or support security coaching courses • Offer mailing lists of workers and suppliers • Classify department security relationship • Recognize nominees for security coaching • Distribute regular security status statements • Execute security awareness system	7
Access control process	• Authorizing requesting access and encouraging security policy • Build a repository for official access applications and policy awareness reports • Design user groups and access policy, authorize applications according to the plan • Generate and provide user access agreeing to information security policy • Build and enforce alternative access practices for vendor access • Inform the information security team when a worker or contract expires • Teach department relationships to stop user access • Stop access to the application of information security	8
Observing process	• Produce and retain systems supply • Choose and authorize security monitoring systems for new systems • Screen security alerts • Forward crucial and unsolved security alarms to information security • Screen security alerts • Aid in solving security alerts	6
Agreement process	• Distinguish security weakness or security policy breach • Enter issue in security tracking database • Allocate and obtain department management approval of item responsibility • Fix weakness • Present risk review and build a plan to close weakness • Occasionally assess all risk recognition statements • Support attempts to close weaknesses • Target sets of exceptional weaknesses for technology development • Record issue motion in security tracking database	8
Plan process	• Frequently evaluate great risk assessments • Offer current knowledge of security tools, methods, and best practices • Regularly discuss possible new security strategies for new and existing services • Test security processes for prototype services	4

The proposed six ISP processes and 42 ISP practices are the main blocks of the developed IISPM. The developed IISPM consists of six ISP processes and 42 ISP practices Fig. 2. The first proposed information security policy process is used to identify and recognize the organization assets and assign the security team to assess the existing organization security policy and then propose the proper information security policy for the organization. It consists of nine information security practices and is shown in Fig. 3. The second proposed information security awareness process is used to build a security awareness program, authorize a security awareness program, build or support security training courses, offer mailing lists of workers and suppliers, classify department security relationship, recognize candidates for security training, allocate regular security status statements and execute security awareness program. It consists of seven information security practices Fig. 3. The third proposed process is the access control process which is used to govern the access to the authorized entities to the specific organization assets. The main purpose of this process is to build a repository for official access applications and policy awareness reports, design user groups and access policy, authorize applications according to plan, generate and provide user access agreeing to ISP, build and enforce alternative access practices for vendor access, inform information security team when worker or contract expires, teach department relationship to stop user access and stop access at the application of information security. It consists of eight information security practices Fig. 3.

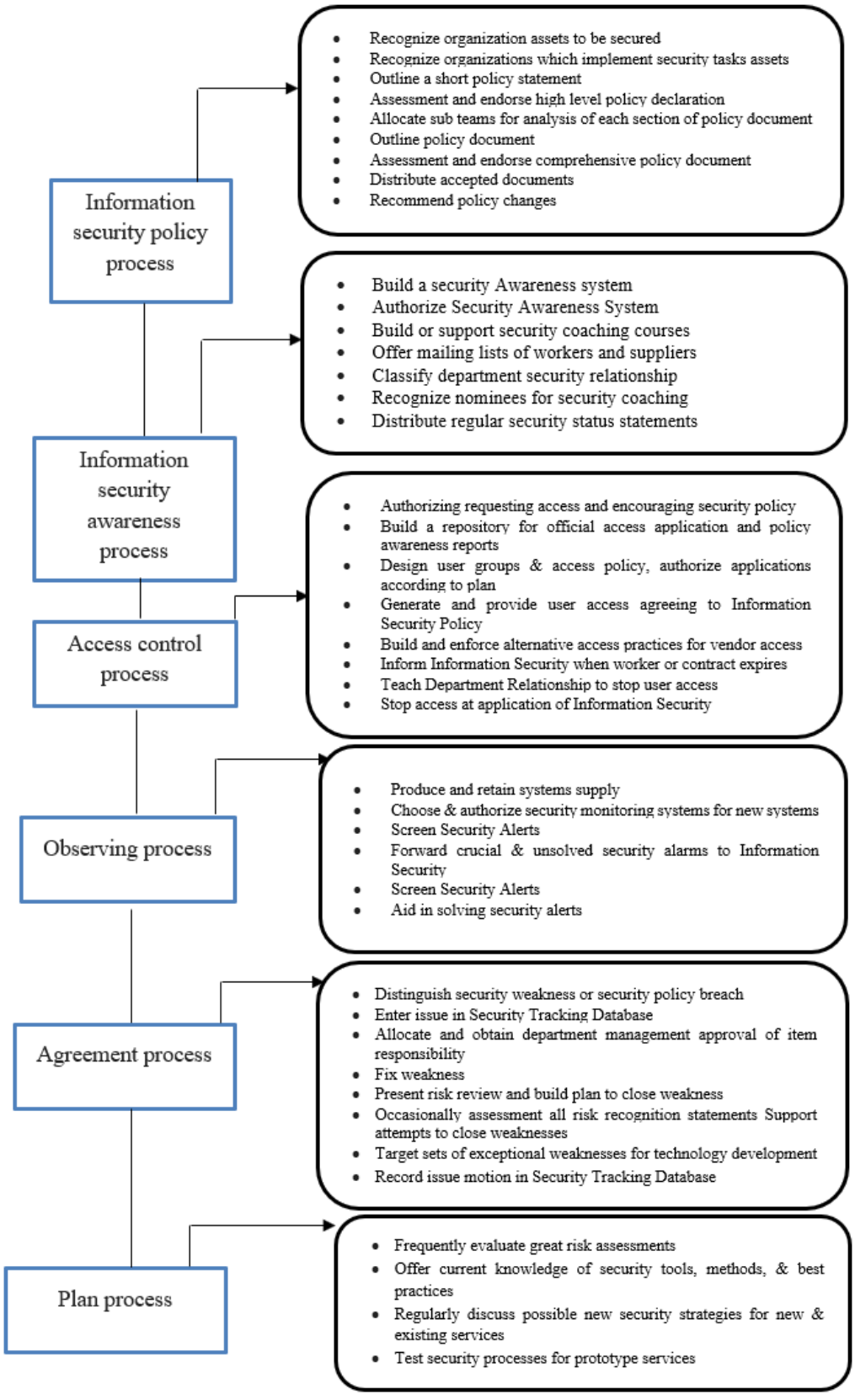

Fig. 3: Integrated information security policy model

The fourth proposed process is the observing process which is used to produce and retain systems supply, choose and authorize security monitoring systems for new systems, screen security alerts, forward crucial and unsolved security alarms to information security, screen security alerts, and assist in solving security alerts. The last two proposed processes are the agreement and plan processes. The agreement process is used for many purposes, for example, to distinguish security weaknesses or security policy breaches enter an issue in the security tracking database, allocate and obtain department management approval of item responsibility, fix weaknesses, present risk review, and build a plan to close weakness, occasionally assessment all risk recognition statements, support attempts to close weaknesses, target sets of exceptional weaknesses for technology development and record issue motion in the security tracking database. The last proposed process is the planning process which is used to frequently evaluate great risk assessments, offer current knowledge of security tools, methods, and best practices, regularly discuss possible new security strategies for new and existing services, and test security processes for prototype services.

Results and Discussion

Implementation of the Developed IISPM

The developed IISPM consists of six common processes which are: (1) Information security policy process, (2) Information security awareness process, (3) Access control process, (4) Observing process, (5) Agreement process, and (6) Plan process. Each process can apply separately by the organization based on its requirements. For example, the organization XXX needs to develop and implement an effective security policy that meets its specific needs. In this case, organization XXX should follow apply the first process which is the information security policy process. Is used to identify and recognize the organization's assets and assign the security team to assess the existing organization's security policy and then propose the proper information security policy for the organization. It consists of nine information security practices and is shown in Fig. 3:

- Recognized XXX organization assets to be secured: The security managers of the XXX organization should recognize the main assets of the XXX organization to avoid and mitigate an expected risk. This practice includes the following steps:

- ✓ Confidential information, including proprietary information, trade secrets, customer and employee data, and financial records
- ✓ Computer systems and networks, including hardware, software, and data
- ✓ Physical assets, such as buildings and equipment
- ✓ Intellectual property, such as patents and trademarks
- ✓ Access control systems, such as passwords, user authentication, and biometric scanners
- ✓ Communications systems, such as telephone networks and wireless networks
- ✓ Backup and recovery systems, such as offsite data storage and disaster recovery plans
- ✓ Security systems, such as firewalls, intrusion detection systems, and antivirus software
- ✓ Employee training, policies, and procedures regarding security and privacy
- ✓ Third-party providers and vendors, such as cloud services, hosting providers, and managed service providers

- Recognize organizations that implement security tasks assets: This practice allows XXX organization to discover and recover the common organization which implement the security tasks assets, for example, the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), National Cyber Security Alliance (NCSA), Cybersecurity and Infrastructure Security Agency (CISA), United States Computer Emergency Readiness Team (US-CERT), Center for Internet Security (CIS), Federal Trade Commission (FTC), Electronic Frontier Foundation (EFF)
- Outline a short policy statement for XXX organization: This procedure provides a policy statement of the XXX organization. For example, this policy statement outlines the expectations for employees and contractors of XXX organization related to the responsible use of technology within the workplace. Employees and contractors are expected to use technology in an ethical, responsible, and lawful manner. This includes, but is not limited to, adhering to all applicable laws, respecting the privacy of others, protecting confidential information, and avoiding activities that could create liability for the organization. Unauthorized use of technology, including but not limited to, the installation of software, downloading of files, or unauthorized use of the company's networks, is strictly prohibited. Any violations of this policy may result in disciplinary action, up to and including termination. XXX reserves the right to audit and monitor employee or contractor technology use at any time. This policy is subject to change at any time with or without notice.
- Assessment and endorse high-level security policy declaration for XXX organization: Security policies should be endorsed by XXX organization's senior leadership and should be regularly reviewed and

updated in a timely manner. Endorsement of a security policy should include:

- ✓ A formal statement of commitment from senior leadership to the security policy
- ✓ A signature from the organization's executive officer or another senior-level manager
- ✓ A clear understanding of the roles and responsibilities of all stakeholders in the organization
- ✓ A communication plan to ensure that the security policy is effectively communicated to all personnel
- ✓ A process for monitoring, measuring, and evaluating the effectiveness of security policy
- ✓ A commitment to review, update and re-endorse the security policy on a regular basis

- ➢ Allocate sub-teams for analysis of each section of the security policy document of XXX organization: This procedure should include three main teams:

- ✓ Network security team
- ✓ Network administrator
- ✓ Network security engineer
- ✓ Cyber security analyst
- ✓ Security architect
- ✓ Physical security team
- ✓ Security guard
- ✓ Physical security officer
- ✓ Facility manager
- ✓ Surveillance technician
- ✓ System security team
- ✓ System administrator
- ✓ System security engineer
- ✓ Security analyst
- ✓ Security architect

- ➢ Outline security policy document: A security policy document outlines the XXX organization's security policies and procedures. It outlines the steps XXX organization must take to protect its data, employees, and customers. It also describes the roles and responsibilities of each party involved in the security process. The security policy document for the XXX organization should include:

- ✓ Overview: A high-level overview of the XXX organization’s security policies and procedures
- ✓ Security principles: The core principles that guide the XXX organization’s security policies and procedures
- ✓ Access controls: The types of access controls used to protect data and systems
- ✓ Authentication and authorization: The procedures for authenticating users and authorizing access to systems
- ✓ Network security: The measures taken to protect the XXX organization’s networks from external threats
- ✓ Data security: The steps taken to secure data, including encryption and data backup
- ✓ Incident response: The procedures for responding to security incidents
- ✓ Compliance: The steps taken to ensure compliance with applicable laws and regulations
- ✓ Monitoring and auditing: The measures taken to monitor and audit the XXX organization’s security posture
- ✓ Education and awareness: The training and awareness programs are used to educate employees and customers about security policies
- ✓ Business continuity: The steps taken to ensure continuity of operations in the event of a disaster

The security policy document of the XXX organization should be reviewed and updated regularly to ensure it is up to date with the latest security best practices. It should also be reviewed by all stakeholders to ensure they understand the security measures in place.

- ➢ Assessment and endorse comprehensive security policy document for XXX organization: A comprehensive security policy document should include a set of security measures that are designed to protect an organization's information and physical assets from unauthorized access, use, disclosure, disruption, modification, or destruction. It should also define a set of procedures and guidelines that help to ensure that information and physical assets are protected. To assess and endorse a comprehensive security policy document for the XXX organization, the following steps should be taken:

- ✓ Review the document and ensure that it covers all security objectives, such as authentication and authorization, access control, incident response, data protection, and physical security
- ✓ Assess the document against industry standards such as ISO 27001 and NIST 800-53
- ✓ Ensure that the policy is written in clear and simple language that is easy to understand
- ✓ Ensure that the policy is regularly updated to reflect changes in technology, laws, and regulations
- ✓ Get the policy endorsed by the XXX organization’s senior leadership
- ✓ Monitor and track the implementation of the policy and ensure that it is enforced consistently
- ✓ Evaluate the effectiveness of the policy and make necessary changes as needed

- ➢ Distribute accepted security policy documents to users in XXX organization: Once security policy documents have been accepted, they should be distributed to all users who need to be aware of the policies in the XXX organization. This can be done

in a variety of ways, including email, hardcopy documents, intranet postings, or employee handbooks. It is important to ensure that all users have access to the documents and understand the policies before they are expected to follow them. Additionally, it is important to provide periodic reminders and updates to the users to ensure that they stay up to date on security policies

- Recommend security policy changes for XXX organization: Several steps and practices should be followed to recommend the security policy change for the XXX organization:

- ✓ Implement a two-factor authentication system for all users, with regular password changes
- ✓ Implement a comprehensive email security system to prevent malicious attachments, links, and malware from being sent to users
- ✓ Enforce stringent access control policies that include regular reviews of user accounts, privileges, and roles
- ✓ Implement a comprehensive patch management system to ensure all systems and applications are regularly updated
- ✓ Implement a strong data backup and recovery system to ensure business continuity
- ✓ Establish a data encryption system to protect sensitive data
- ✓ Implement a system to detect and respond to any suspicious activity
- ✓ Implement a system to monitor the network perimeter for any suspicious activity
- ✓ Establish and enforce a Bring Your Own Device (BYOD) policy to ensure personal devices are secure
- ✓ Establish and enforce a company-wide security awareness program to ensure employees are educated in proper security practices
- ✓ The implementation of the developed IISPM is based on the organization's perspective

This section discusses how the developed IISPM applying by organizations to develop their specific security policies.

Protecting organization assets from external and internal risks is the priority of security departments in organizations. Several information security policy models and frameworks have been developed for this purpose. However, the unified and structured model used to organize and manage the ISP is still missing (Bakreski *et al*., 2022). There are many organizations and individuals working on developing such a model, but no single model has been accepted yet. The development of such a model requires a detailed understanding of the various aspects of information security, such as identity and access management, data protection, risk management, and incident response. Additionally, the model must be flexible enough to accommodate the different needs of organizations of different sizes and complexity. As such, it is likely to take some time before a unified and structured model is available for organizations to use.

Therefore, this study developed an Integrated Information Security Policy Model (IISPM) to organize and structure the whole information security policies processes and practices. The developed model consists of six abstract information security policy processes and 42 common practices.

The author selected one abstract process which is the information security policy process for the implementation.

Conclusion

Information Security Policy (ISP) is an essential topic to protect the confidentiality, integrity, and availability of precise data. Though, the ISP is still an ambiguous and varied field due to the variety of security policies and the multiplicity nature of organization systems. Several specific and generic ISP models have been presented for various purposes. The suggested models have numerous redundant procedures, concepts, activities, processes, and tasks that make the ASP domain unorganized, unstructured, and ambiguous among domain experts and users. Thus, the structured and integrated model to simplify sharing, managing, and reusing ISP activities and tasks is still missing. This study applied the design science method to provide a unified model for the ISP domain called the Integrated Information Security Policy Model (IISPM). This aims to identify, recognize, extract, and match different ISP processes, concepts, activities, and tasks from different ISP models in a developed IISPM, thus, allowing domain experts and users to derive/instantiate solution models easily. The proposed IISPM consists of six main abstract processes: (1) Information security policy process, (2) Information security awareness process, (3) Access control process, (4) Observing process, (5) Agreement process, and (6) Plan process. Each proposed process has specific security practices. The future work on this study is to demonstrate the effectiveness of the proposed model in terms of compliance.

Acknowledgment

I would like to express our sincerest gratitude to the researchers who contributed to this study. Their invaluable contributions enabled us to make this study a success. I appreciate their efforts and support, and thank them for their time and dedication.

Funding Information

The authors have not received any financial support or funding to report.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Al-Dhaqm, A., Abd Razak, S., Dampier, D. A., Choo, K. K. R., Siddique, K., Ikuesan, R. A., ... & Kebande, V. R. (2020a). Categorization and organization of database forensic investigation processes. *IEEE Access*, *8*, 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Al-Dhaqm, A., Abd Razak, S., Dampier, D. A., Choo, K. K. R., Siddique, K., Ikuesan, R. A., ... & Kebande, V. R. (2020b). Categorization and organization of database forensic investigation processes. *IEEE Access*, *8*, 112846-112858. https://doi.org/10.1109/ACCESS.2020.3000747

Al-Dhaqm, A., Abd Razak, S., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020c). Towards the development of an integrated incident response model for the database forensic investigation field. *IEEE Access*, *8*, 145018-145032. https://doi.org/10.1109/ACCESS.2020.3008696

Al-Dhaqm, A., Bakhtiari, M., Alobaidi, E., & Saleh, A. (2013). Studding and Analyzing Wireless Networks Access points.

Al-Dhaqm, A., Razak, S., & Othman, S. H. (2018, November). Model derivation system to manage database forensic investigation domain knowledge. In *2018 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 75-80). IEEE. https://doi.org/10.1109/AINS.2018.8631468

Al-Dhaqm, A., Ikuesan, R. A., Kebande, V. R., Abd Razak, S., Grispos, G., Choo, K. K. R., ... & Alsewari, A. A. (2021a). Digital forensics subdomains: The state of the art and future directions. *IEEE Access*, *9*, 152476-152502. https://doi.org/10.1109/ACCESS.2021.3124262

Al-Dhaqm, A., Razak, S., Ikuesan, R. A., R. Kebande, V., & Hajar Othman, S. (2021b). Face validation of database forensic investigation metamodel. *Infrastructures*, *6*(2), 13. https://doi.org/10.3390/infrastructures6020013

Al-Dhaqm, A., Razak, S., Othman, S. H., Choo, K. K. R., Glisson, W. B., Ali, A., & Abrar, M. (2017a). CDBFIP: Common database forensic investigation processes for Internet of Things. *IEEE Access*, *5*, 24401-24416. https://doi.org/10.1109/ACCESS.2017.2762693

Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Ali Mohammed, A. (2017b). Development and validation of a Database Forensic Metamodel (DBFM). *PloS One*, *12*(2), e0170793. https://doi.org/10.1371/journal.pone.0170793

Al-Dhaqm, A., Razak, S., Othman, S. H., Ngadi, A., Ahmed, M. N., & Ali Mohammed, A. (2017c). Development and validation of a database forensic metamodel (DBFM). *PloS One*, *12*(2), e0170793. https://doi.org/10.1371/journal.pone.0170793

Alghamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organizations. *Government Information Quarterly*, *39*(4), 101721. https://doi.org/10.1016/j.giq.2022.101721

Alhussan, A. A., Al-Dhaqm, A., Yafooz, W. M., Emara, A. H. M., Bin Abd Razak, S., & Khafaga, D. S. (2022). A Unified Forensic Model Applicable to the Database Forensics Field. *Electronics*, *11*(9), 1347. https://doi.org/10.3390/electronics11091347

Ali, A., Abd Razak, S., Othman, S. H., Mohammed, A., & Saeed, F. (2017). A metamodel for mobile forensics investigation domain. *PloS One*, *12*(4), e0176223. https://doi.org/10.1371/journal.pone.0176223

Aljuryyed, A. (2022). Cybersecurity Issues in the Middle East: Case Study of the Kingdom of Saudi Arabia. In *Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security* (pp. 62-82). IGI Global. https://doi.org/10.4018/978-1-7998-8693-8.ch004

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems (TIIS)*, *12*(2), 747-763. https://doi.org/10.3837/tiis.2018.02.012

Almubayedh, D., Alazman, G., Alabdali, M., Al-Refai, R., & Nagy, N. (2018, April). Security related issues in Saudi Arabia small organizations: A Saudi case study. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-6). IEEE. https://doi.org/10.1109/NCG.2018.8593058

Alsaif, M., Aljaafari, N., & Khan, A. R. (2015). Information security management in Saudi Arabian organizations. *Procedia Computer Science*, *56*, 213-216. https://doi.org/10.1016/j.procs.2015.07.201

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2016). Information security policy: A management practice perspective. *arXiv preprint arXiv:1606.00890*. https://arxiv.org/abs/1606.00890

Alzamil, Z. A. (2018). Information security practice in Saudi Arabia: case study on Saudi organizations. *Information & Computer Security*. https://doi.org/10.1108/ICS-01-2018-0006

Bakreski, O., Cvetkovski, S., & Bardjieva Miovska, L. (2022). Forecasting as a Function of Security Management. In *Proceedings of the Economics & Finance Conferences*. International Institute of Social and Economic Sciences (IISES). https://doi.org/10.20472/EFC.2022.016.003

Barkhiya, R. K. (2014). *Optimized Algorithms of Vertical Handoff Management using Filtering Model in Heterogeneous Wireless Network* (Doctoral dissertation).

Bayuk, J., & Price Waterhouse, L. L. P. (1997). Security through process management. *Price Waterhouse*.

Connolly, L. Y., Lang, M., & Tygar, D. J. (2018). Employee security behaviour: The importance of education and policies in organisational settings. In *Advances in Information Systems Development: Methods, Tools and Management* (pp. 79-96). Springer International Publishing. https://doi.org/10.1007/978-3-319-74817-7_6

Evers, M. M. (2023). Discovering the prize: Information, lobbying and the origins of US-Saudi security relations. *European Journal of International Relations*, *29*(1), 104-128. https://doi.org/10.1177/13540661221115961

Ghabban, F. M., Alfadli, I. M., Ameerbakhsh, O., AbuAli, A. N., Al-Dhaqm, A., & Al-Khasawneh, M. A. (2021, June). Comparative analysis of network forensic tools and network forensics processes. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 78-83). IEEE. https://doi.org/10.1109/ICSCEE50312.2021.9498226

Hengstler, S., Nickerson, R. C., & Trang, S. (2022, January). Towards a Taxonomy of Information Security Policy Non-Compliance Behavior. In *Proceedings of the 55th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2022.588

Ismail, W. B. W., Widyarto, S., Ahmad, R. A. T. R., & Abd Ghani, K. (2017, September). A generic framework for information security policy development. In *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* (pp. 1-6). IEEE. https://doi.org/10.1109/EECSI.2017.8239132

Kabanda, S., & Mogoane, S. N. (2022, May). A Conceptual Framework for Exploring the Factors Influencing Information Security Policy Compliance in Emerging Economies. In *e-Infrastructure and e-Services for Developing Countries: 13th EAI International Conference, Africomm 2021, Zanzibar, Tanzania, December 1-3, 2021, Proceedings* (pp. 203-218). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-06374-9_13

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & Security*, *24*(3), 246-260. https://doi.org/10.1016/j.cose.2004.08.011

Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). *Information security management framework suitability estimation for small and medium enterprise*. Infinite Study. https://doi.org/10.20334/2019-027-M

Ksibi, S., Jaidi, F., & Bouhoula, A. (2022). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mobile Networks and Applications*, 1-21. https://doi.org/10.1007/s11036-022-02042-1

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

Ofori, K. S., Anyigba, H., Ampong, G. O. A., Omoregie, O. K., Nyamadi, M., & Fianu, E. (2022). Factors influencing information security policy compliance behavior. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 213-232). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch010

Olnes, J. (1994). Development of security policies. *Computers and Security*, *13*(8), 628-636. https://doi.org/10.1016/0167-4048(94)90042-6

Panda, S. K., & Jana, P. K. (2015, January). A multi-objective task scheduling algorithm for heterogeneous multi-cloud environment. In *2015 International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV)* (pp. 82-87). IEEE. https://doi.org/10.1109/EDCAV.2015.7060544

Park, M., & Chai, S. (2018). Internalization of information security policy and information security practice: A comparison with compliance. https://doi.org/10.24251/HICSS.2018.595

Pierson, P. (2005). The study of policy development. *Journal of Policy History*, *17*(1), 34-51. https://doi.org/10.1353/jph.2005.0006

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A policy framework for information security. *Communications of the ACM*, *46*(7), 101-106. https://doi.org/10.1145/792704.792706

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping process of digital forensic investigation framework. *International Journal of Computer Science and Network Security*, *8*(10), 163-169.

Talib, A. M., Alomary, F. O., Alwadi, H. F., & Albusayli, R. R. (2018). Ontology-based cyber security policy implementation in Saudi Arabia. *Journal of Information Security*, *9*(4), 315-333. https://doi.org/10.4236/jis.2018.94021

Thakur, K., Ali, M. L., Gai, K., & Qiu, M. (2016, April). Information security policy for e-commerce in Saudi Arabia. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 187-190). IEEE. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.14

Tipton, H. F., & Krause, M. (2007). *Information security management handbook*. CRC press. https://doi.org/10.1201/9781439833032

Tuyikeze, T., & Flowerday, S. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. In *HAISA* (pp. 11-20). ISBN-10: 9781841023755.

Tuyikeze, T., & Pottas, D. (2011). An information security policy development life cycle. In *Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa* (pp. 165-176). ISBN-10: 9781841022567.

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. *European Journal of Information Systems*, *22*(1), 45-55. https://doi.org/10.1057/ejis.2011.51