applied sciences

MDPI

Article

A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field

Fahad Mazaed Alotaibi [1], Arafat Al-Dhaqm [2,*], Wael M. S. Yafooz [3] and Yasser D. Al-Otaibi [4]

[1] Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Jeddah 21589, Saudi Arabia; fmmalotaibi@kau.edu.sa
[2] Faculty of Computing, Universiti Teknologi Malaysia, Skudai 81310, Malaysia
[3] Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 41477, Saudi Arabia; wyafooz@taibahu.edu.sa
[4] Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia; yalotaibi@kau.edu.sa
* Correspondence: mrarafat1@utm.my

Abstract: Information security policy (ISP) plays a crucial role in maintaining the availability, confidentiality, and integrity of sensitive data. However, it is of high complexity and heterogeneity due to the variety and redundancy of security policy practices and complexity of organisational systems. Various and duplicate ISP models and frameworks have been offered in the literature. The duplicate security policy practices, procedures, and processes in the existing models have made ISP disorganised, unstructured, and unclear to organisational users. As a result, there is still a need for a standardised and integrated model to make it simpler to share, manage, and reuse ISP practices amongst the organisations. The main objective of this study is to construct a metamodel to unify, organise, and structure ISP practices. By identifying, recognising, extracting, and combining the common information security policy practices from various ISP models in a built ISP metamodel called ISPM, we seek to make it simple for users and field specialists to derive/instantiate security policy models for their organisations. The development and validation process of the ISPM is based on the common security frameworks such as ISO 27001 frameworks. The developed ISPM consists of 19 common security practices: organisation, risk management, access control policy, edit, review, compliance, business management, backup and recovery, incident response, SETA program, security awareness, security training, security education, email security policy, cloud security policy, network security policy, website security policy, physical security policy, and privacy security policy. Each common security practice consists of several operations and attributes. The performance of the developed ISPM was compared to that of other models to evaluate its completeness and logicalness. Using ISO 27001 as a framework, the findings confirmed the comprehensiveness of ISPM. Therefore, it can contribute to organisations' security by helping them to develop their own security policy models.

Keywords: security policy; ISO 27001; metamodel; metamodeling approach; design science method

Citation: Alotaibi, F.M.; Al-Dhaqm, A.; Yafooz, W.M.S.; Al-Otaibi, Y.D. A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field. *Appl. Sci.* **2023**, *13*, 9703. https://doi.org/10.3390/app13179703

Academic Editors: Luis Javier Garcia Villalba, Anikó Costa and Remigiusz Wiśniewski

Received: 7 March 2023
Revised: 1 June 2023
Accepted: 20 June 2023
Published: 28 August 2023

1. Introduction

A security policy ensures sensitive information and information systems within an organisation are protected from unauthorised access and use [1]. These policies outline how sensitive information will be handled as well as the steps that will be taken to ensure data protection against unauthorised access, alteration, disclosure, or destruction. Organisations should tailor them to meet their specific needs and objectives as part of their overall security program. It should include guidelines for physical security, access control, data encryption, and user authentication. Furthermore, security policies should specify how to respond to security incidents, such as data breaches. A standard for cybersecurity management, ISO 27001 [2], should be considered when organising an ISP. Various guidelines and

effective practices (e.g., ISACA, ISO 27000, and NIST) are available to help companies apply their own security policies.

The ISO 27001 standard (ISECT, 2012) is part of the ISO 27,000 family of standards [2]. It represents a group of guidelines involved in security management systems. ISO 27001 is a British standard that was first established in October 2005. An example of a security management request is shown in Figure 1. An enterprise can apply a systematised and active approach to security risk management by selecting security processes to ensure the safety of vulnerable resources within a well-defined border.

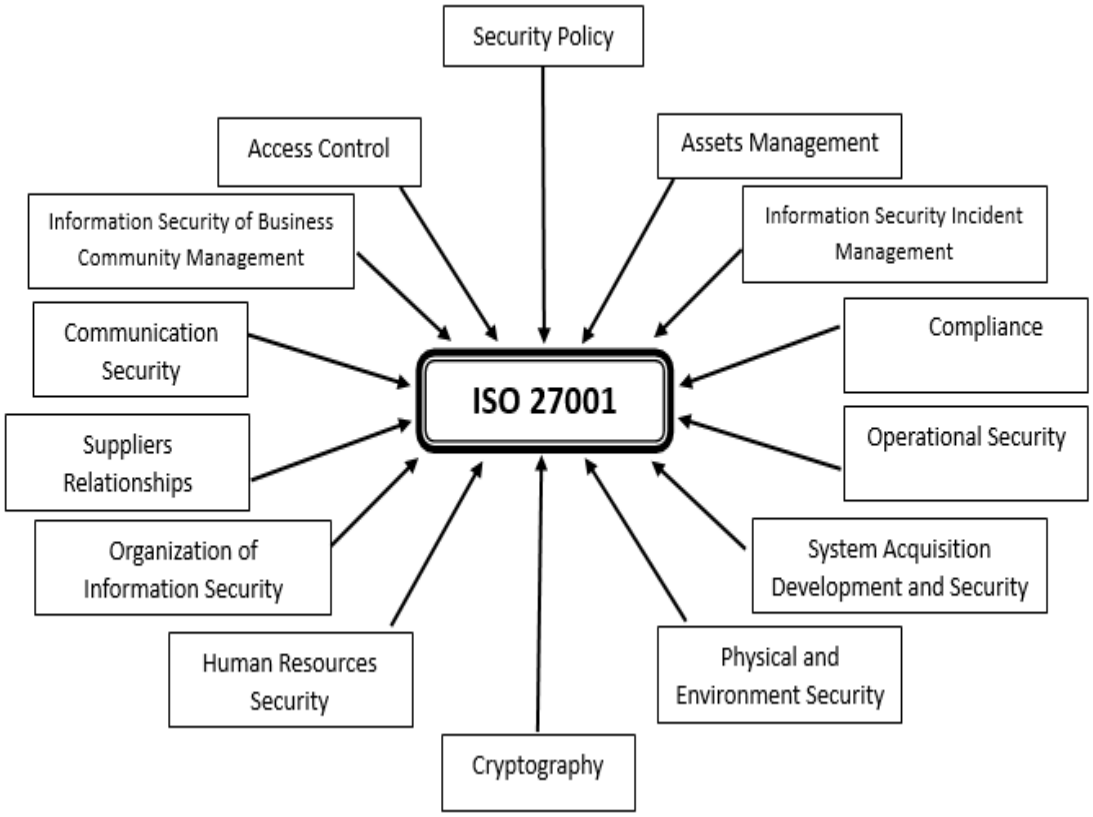

Figure 1. ISO 27001 international standard focused on information security.

Thus, the main purpose of this research is to develop a novel administration metamodel for managing and organising diverse security policy practices using a design science approach based on the ISO 27001 controls. The developed metamodel, which is called the information security policy metamodel (ISPM), aims to solve the redundancy, heterogeneity, and ambiguity of information security policy (ISP) practices by gathering and combining the common security practices into three high abstract levels. The three high levels of the developed metamodel control how the ISP practices behave. These modelling rules will be used to combine, structure, and organise all security practices in the ISP field into the developed ISPM. As a result, ISP users and experts will have access to organised, structured, managed, and shared ISP practices well-tailored to their organisations. This study developed and validated the ISPM using a metamodelling approach, which is a kind of design science method. Metamodelling is the process of creating a metamodel representing a particular domain. It is a way of understanding the concepts and relationships between the components of a system. It involves analysing the structure of the data, behaviour of the system, and component interactions [3].

The contribution of this study is to provide a comprehensive representation layer for the ISP field, which is called ISPM, to assist several organisations in identifying, preparing, managing, and developing security policy practices based on their own requirements. The developed metamodel also offers an approach to develop a policy framework compliant

with international standards such as ISO 27001. ISPM provides a detailed analysis of the different components of an ISPM framework, including the scope, objectives, roles, and responsibilities, as well as the security controls. Furthermore, it offers an overview of different types of security policies, as well as the importance of implementing them. Finally, it provides guidelines and best practices for organisations to ensure that their security policy is up-to-date and secure.

The remainder of this article is organised as follows: The related work is reviewed, and the problem is stated in Section 2; then, the methodology is described in Section 3. Afterward, the findings and discussion are provided in Section 4. Finally, the conclusion of the study and future work are provided in Section 5.

2. Related Work

Various studies conducted on ISPs have focused on several stages of ISP development. Each study in this domain has its own security processes, practises, tasks, procedures, and activities. In the following, some relevant studies previously carried out in this field are reviewed. In [4], the focus is on major challenges associated with Saudi Arabian enterprises, e.g., e-commerce agreement. In [5], the authors defined a scenario of ISP and examined it based on the perspectives of the information technology (IT) employees of Saudi businesses. Specifically, the ISP field in Saudi Arabia comprises 11 security policies that were introduced by [6] as: (1) risk documentation, (2) security awareness, (3) security insurance, (4) privacy, (5) reliability, (6) accessibility, (7) confidentiality, (8) verification, (9) permission, (10) access control, and (11) responsibility. The authors emphasised that employees should be aware of the ISP effectivity. However, their findings showed that most of the employees do not concern themselves with the existing policies and are often prone to non-compliance with and violate the policies; such violations often remain undetected methodically. In another research [7] the authors examined the ISP-related problems in Saudi Arabian companies, concentrating on an audit performed for a small Saudi company. In addition, the researchers investigated cyberattacks in Saudi Arabia. The motives and causes of these attacks were discussed as well. Following that, they prompted cybersecurity innovations to further resolve the risks. In [8], the authors presented approaches to identifying the changes and problems that could have negative impacts on employees' behaviour and goals. The report did not refer to the absence of a business-oriented information security policy providing adequate security measures. In [9], a framework was proposed for the development, implementation, and maintenance of security policies. The study emphasised the necessity of developing, implementing, and maintaining security strategies using methodical approaches. The policy formation model, however, is not entirely comprehensive since it does not explicitly address the development, dissemination, implementation, and review of policy documents [10,11]. The researchers suggested a limited approach that only considers the writing of policy documents and excludes all activities that should be done regarding the policy implementation and maintenance of the policy. The suggested approach consists of several steps: (1) asset identification, (2) formation of a team to establish draft policy, (3) review process on the drafted policy, and (4) the approval and publication of the draft of policy. Although a methodical process for developing security policies is provided in [12] the details regarding their publication, distribution, and enforcement are unavailable. Moreover, the authors neither addressed the issue of user compliance with the security policy nor the importance of user awareness and training. The policy formation model, however, is not entirely comprehensive since it does not explicitly address the development, dissemination, implementation, and review of policy documents [13]. The authors in [14] suggested a limited approach that only considers the writing of policy documents and exclude all activities bringing the policy implementation and the maintenance of the policy. The suggested approach consists of several steps which involves (1) asset identification, (2) formation of team to establish draft of policy, (3) review process on the drafted policy, (4) the approval and publication of the draft of policy. Although a methodical process for developing security policies is provided [15] details surrounding their publication,

distribution, and enforcement are unavailable. Additionally, [16] Neither addressed the issue of user compliance with the security policy nor the importance of user awareness and trainingSome aspects of policy making processes were duplicated in [17] it provided a more holistic perspective. In [18], three different perspectives were presented to demonstrate the efforts made by managers to ensure their employees are obeying the policies. Often, the establishment of security policies can cause the security practitioners to feel perplexed if one term is stated in three different ways or if different actions are listed under one category.

In [19], a recommended framework called Policy Framework for Information Security (PFIRES) was introduced, which consisted of four main phases: review, development, supply, and control, each of which with certain prerequisites for departure that must be met before proceeding to the following phase. The researchers in [20] introduced a model for development of security policy, which considers risk assessment, corporate culture, and knowledge, as well as security management, development, and protection. In [21] a five-stage model was presented for the development process, consisting of team building, risk assessment, policy formulation, implementation, and maintenance. The ISP development model proposed by [22] is divided into four primary phases: risk assessment, policy creation, policy implementation, and policy monitoring and maintenance. Each phase can be divided into stages that describe the actions conducted in each phase. The four steps recommended by [22]. In their study for creating and implementing information security policies are security policy formulation, security policy drivers, security policy guidance, and current concepts. In addition, the authors proposed a development process model of three phases: develop, implement, and evaluate. Their work engaged with variations of activities and practices. The findings indicated that the top three most important components in the structure of a security policy are asset management, security risk management, and defining the policy's scope. However, the security strategy controls were not included in their analysis. In [23] a model was proposed for ISP compliance, which consisted of self-efficacy (SE), awareness, and resource vulnerability. The authors in [24] developed a tool to evaluate how effectively workers internalised and followed information security standards and validate the accuracy and dependability of the tool. The findings were used as a foundation for establishing solutions for employees' poor compliance with information security policies as well as for encouraging information security policies that consistently place a strong emphasis on employee autonomy. In [25] a practical and reliable method was designed to determine the viability of the information security management framework to be used in small- and medium-sized organisations. However, it will not provide small- and medium-sized enterprises the flexibility they require. In [26], the researchers rigorously examined the factors influencing the compliance with information security policy. In [27], a taxonomy was developed to categorise diverse information security policy non-compliance behaviours. The authors revealed the factors that influence ISP compliance in growing economies involving small businesses. In general, the ISP field is deemed as heterogeneous, ambiguous, and unstructured. There is no standardised administration model or framework that allows the knowledge of information security regulations to be organised and maintained.

To sum up, the review of the relevant literature revealed that ISP is still an unstructured field suffering from ambiguity and heterogeneity. For the knowledge of ISP to be well organised and managed, this study plans to build a metamodel based on the ISO 27001 controls.

3. Research Methodology

In this study, a unique administration metamodel adopted from [28,29] was developed to manage and organise the heterogeneous ISP field. The developed metamodel was validated using two techniques. The first approach was used to identify and examine the problems with ISPs. The novel administration metamodel is developed and validated for managing and organising heterogeneous information security policy fields using the

second method, which was adapted from [29]. The modified research methodology is shown in Figure 2.

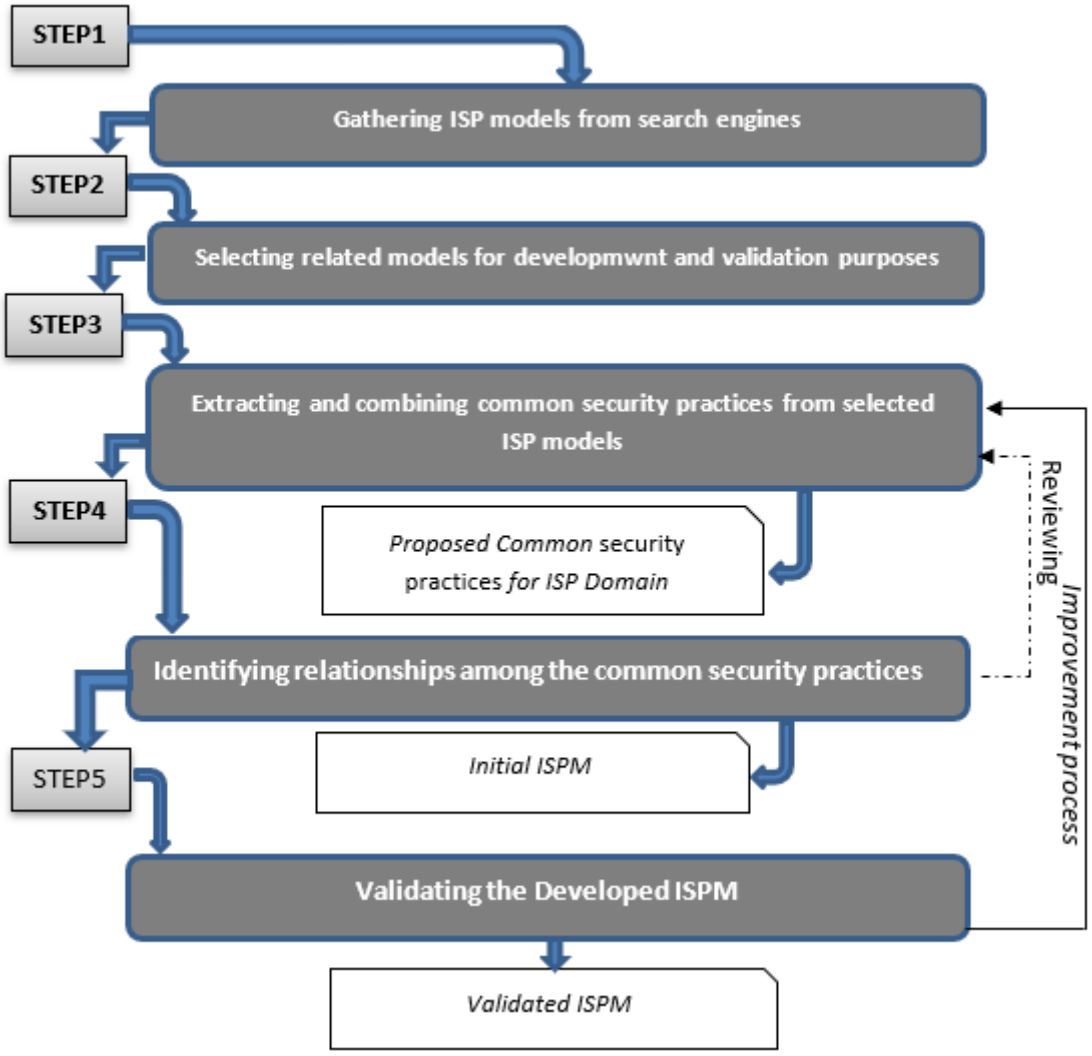

Figure 2. Development and validation method.

In the following, the steps illustrated in Figure 2 are explained in detail.

Step 1. Gathering ISP Models from Search Engines:

Five common search engines, i.e., Scopus, Web of Science, Springer, IEEE Xplore, and Google Scholar, were used to gather ISP models already existing in the literature. The keywords used in this study were "ISO 27001", " Security policy", and "Information Security Policy". Gathering ISP models was limited to papers published in the English language between 2010 and 2022. Table 1 presents the results of the search engines. Resources included journals, conference papers, books, book chapters, magazines, early access articles, and courses. Finally, a total of 15,714 articles were gathered from the search engines.

Step 2. Selecting related models for development and validation purposes:

The models gathered in the previous step were examined regarding their titles, abstracts, conclusions, and ultimately full texts. The models were tested to see whether they comply with our exclusion and inclusion criteria. The models that covered at least one ISO 27001 control were included, whereas the ones that did not cover at least one ISO 27001 control were excluded. After several iterations, 40 models were selected for the development and validation processes, as presented in Table 2. The purple colour in Table 2 represents the ISO 27001 controls covered by the existing ISP models.

Table 1. Findings of the search engines used in this study.

Search Engines	Articles
Scopus	201
Web of Science	385
Springer	1239
IEEE Xplore	89
Google Scholar	13,800
Total	15,714

Table 2. ISP models used for the development and validation processes in this paper.

ID	Year	Ref.	Security Policy	Organisation of Information Security	Human Resource Security	Assess Management	Access Control	Cryptography	Physical and Environmental Security	Operational Security	Communication Security	Systems Acquisition, Development, and Maintenance	Supplier Relationships	Information Security Incident Management	Business Continuity	Compliance
1.	2010	[30]														
2.	2011	[21]														
3.	2014	[22]														
4.	2014	[31]														
5.	2015	[7]														
6.	2015	[32]														
7.	2016	[4]														
8.	2016	[13]														
9.	2016	[33]														
10.	2017	[34]														
11.	2017	[35]														
12.	2017	[36]														
13.	2018	[6]														
14.	2018	[8]														
15.	2018	[9]														
16.	2018	[37]														
17.	2018	[1]														
18.	2018	[23]														
19.	2018	[38]														
20.	2018	[39]														
21.	2018	[40]														
22.	2018	[41]														

Table 2. *Cont.*

ID	Year	Ref.	Security Policy	Organisation of Information Security	Human Resource Security	Assess Management	Access Control	Cryptography	Physical and Environmental Security	Operational Security	Communication Security	Systems Acquisition, Development, and Maintenance	Supplier Relationships	Information Security Incident Management	Business Continuity	Compliance
23.	2018	[42]														
24.	2018	[43]														
25.	2018	[44]														■
26.	2018	[45]														■
27.	2019	[24]				■										
28.	2019	[46]														■
29.	2019	[47]														■
30.	2019	[48]														■
31.	2019	[49]			■											
32.	2020	[50]				■										
33.	2020	[51]	■											■		
34.	2021	[52]														■
35.	2021	[53]														■
36.	2022	[10]														■
37.	2022	[25]														■
38.	2022	[26]														■
39.	2022	[27]														■
40.	2022	[54]	■													

Notes: ■ refers to the ISO 27001 controls covered by the existing ISP models; ■ refers to the ISO 27001 controls which non covered by the existing ISP models.

This review revealed the importance of the ISO 27001 controls in the existing ISP studies. Figure 3 illustrates the significance of each ISO 27001 control in the existing ISP models. Only the top three most significant controls were considered by most existing studies. It is possible to assume that Compliance, Security policy, and System acquisition controls have larger significance. On the other hand, several security controls were shown to be of no significance. For example, 19 models covered compliance control, 12 models covered security policy control, 4 models covered system acquisition control, 3 models covered assess management, 2 models covered information security incident management control, and 1 model covered human resource security control.

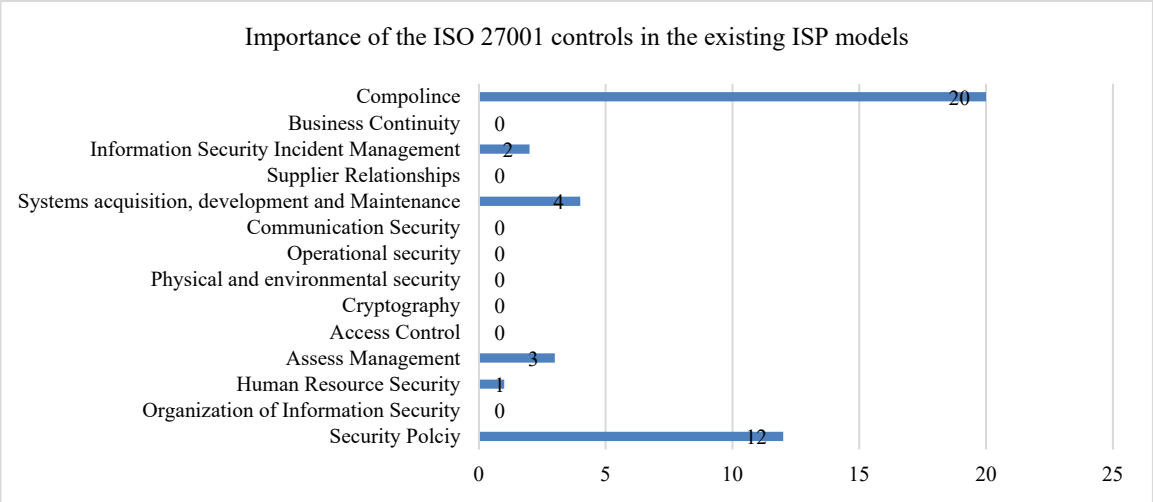

Figure 3. Significance of each ISO 27001 control in the existing ISP models.

Step 3. Selecting related models for development and validation purposes:

The common security practices were obtained from the selected 40 models based on the following criteria [55–57]:

(i) Excluding the articles' title, abstract, introduction, related work, and conclusion: the security practices must be extracted from the major body of a textual or graphical model.

(ii) Excluding any security practice that is not associated to the field: the best rule for extracting security practices, according to [57], is: "if it is not relevant to the field, then do not include it in the case field model".

(iii) Excluding particular security practices related to specific fields: the security practices with specific meaning or functioning must be excluded. The reason is that a security practice name that is more common is easier to reuse than a security practice name that is more specific. According to [57], "it is important, to begin with, a very comprehensive list of security practices and gradually eliminate security practices that are irrelevant".

Therefore, this study extracts security practices manually similar to previous studies [3,56,58]. This is a hard process whereby every model is used in order to identify potential security practices required in this study. Selection and filtering of the number of security practices from the selected ISP models were selected one by one based on their meaning and functioning.

Furthermore, combining common security practices with extracted security practices is based on their similar meanings or functions [55–57]. Candidate common security practices that differ in naming, synonyms, definitions, and meaning is therefore laborious and may result in incorrect results. From the extracted security practices, two techniques were applied to filter and propose common security practices. Wordnet2 and Thesaurus.com are used for synonym checking. These techniques are used in the selection process to identify common security practices from the extracted security practices.

Therefore, security practices that have the same meaning or are equally effective regardless of their names or synonyms are categorised under the same name. As an example, security policy practice is also known as security protection practice, as well as security authentication practice. Accordingly, Table 3 presents 19 common security practices with their definitions based on the techniques described above. In either semantic or functional terms, each proposed common security practice is like an existing common security practice.

Table 3. Common security policy practices.

Proposed Common Security Practices	Definition
Organisation	It is the owner of the ISP model.
Risk Management	Risk management is assuming the unanticipated. It is a tool that helps monitor risks in building projects. Its aim is to create a simple, useful method of recognising, assessing, examining, and controlling risks in an educated and organised way.
Access control policy	An access control policy is a set of rules that defines who or what is allowed to access a computer system, network, or other physical or virtual resource. The policy should define who is authorised to access the system, what actions they are allowed to perform, and what measures should be taken to protect the resources. The policy should also specify the consequences of unauthorised access or misuse of the system.
Security Policy Practice	Security policy practice is a process of establishing and implementing policies, procedures, and controls, which governs the use of technology, data, and information systems within an organisation. Security policy practice involves identifying and addressing potential risks, vulnerabilities, and threats to an organisation's data and systems, as well as developing and managing processes and procedures to ensure the security of the organisation's information. Security policy practice also involves developing, implementing, and enforcing security measures to protect the organisation's data and systems from unauthorised access, use, and misuse. Additionally, security policy practice involves monitoring the effectiveness of security procedures and controls and ensuring the security of the organisation's data and systems.
Edit Practice	It is an important security practice through which the security policies are edited and improved.
Review Practice	It is an important security practice through which the security policies are reviewed and improved.
Security Compliance Practice	Security compliance is the set of procedures for permanent examining and assessment of systems. These procedures involve the interaction, documents, and automation of security compliance rules and practices.
Business Management Practice	Business management practice is a broad term that encompasses the range of activities and processes used to manage and coordinate the activities of an organisation. It involves the use of strategic, operational, and financial tools to ensure that the organisation meets its goals and objectives. The practice of business management involves a variety of disciplines such as accounting, finance, human resources, marketing, operations management, and organisational development. Business management also involves the use of technology, such as software and data analytics, to improve organisational efficiency and effectiveness. Business management practices are essential for any organisation to succeed in today's competitive market.
Backup and Recovery Practice	Backup and recovery define the method of producing and keeping copies of data, which can safeguard organisations against data loss.
Incident Response Practice	Incident Response Practice is a set of procedures, plans, and processes organisations use to respond to cyber incidents. It involves the identification, analysis, containment, and recovery from malicious activities or security incidents, as well as the reporting of such incidents. The practice also includes preparation activities such as the development of incident response plans and policies, the implementation of security controls, and the training of staff in incident response procedures.
SETA Program Practice	A SETA (Security education, Training, and Awareness) plan encourages the fundamental cybersecurity experience of an organisation's members and should be compulsory for both existing members and future new hires.
Security Awareness Practice	Security awareness is the experience and attitude employees of an organisation have in regard to the safeguard of the physical, and particularly informational, resources of that organisation.
Security Training Practice	Security training is a tactic employed by IT and security experts to prevent and lessen user threat. This program is aimed at assisting users and workers in realising the task they participate to prevent information security violations.
Security Education Practice	Security education is a kind of SETA program that offers workers with awareness on IT security, frequently as part of their primary education to a corporation. Each worker of the business should be informed of the risks of weak IT security and the procedures necessary to safeguard important data against both inside and outside threats.

Table 3. *Cont.*

Proposed Common Security Practices	Definition
Email Security Policy Practice	An email security policy is a sequence of practices controlling the usage of emails within a system or an organisation. It describes how a group of users interacts with emails that are sent and received through email.
Cloud Security Policy Practice	A cloud security policy is a recognised policy under which a corporation manages in the cloud. These guidelines describe the security strategy and manage all assessments regarding the protection of cloud assets.
Network Security Policy Practice	Network security policy practice is the development and implementation of policies, procedures, and technologies designed to protect an organisation's computer networks, systems, and data from unauthorised access, misuse, and destruction. It involves several processes such as risk assessment, security awareness, encryption, access control, firewalls, and intrusion detection. It also includes measures to protect against viruses, worms, and other malicious software. The goal of network security policy practice is to ensure the security, integrity, and availability of corporate data and resources.
Website Security PolicyPractice	Website security policy is an extra layer of security that helps to discover and relieve some types of attacks, e.g., data injection attacks and Cross-Site Scripting (XSS).
Physical Security Policy Practice	Physical security is the way of guarding components of an organisation's infrastructure, assets, and employees against risks or compromises in the real environment.
Privacy Security Policy Practice	This practice helps users to control their contacts and personal data and to safeguard their data from moving into the wrong parts, through a violation, leak, or cyber threats.

Step 4. Identifying relationships amongst common security practices:

A survey of ISP models showed various UML relationships amongst security practices, which were common amongst all such models; these relationships were Association, Specialisation/Generalisation, and Aggregation. The Association relationship typically indicates that one class retains a relationship to another class to achieve a mission [59]. The Specialisation/Generalisation relationship connects a subclass to its superclass. It denotes an inheritance of attributes and operations from the superclass to the subclass [59]. Finally, the aggregation relationship typically implies ownership [59]. This study illustrates the relationships amongst security practices, based on the semantic UML relationship that was discovered and identified during the survey of the ISP field.

Therefore, three kinds of relationships were identified, namely Association, Specialisation, and Aggregation. The output of this step is the development of the information security policy metamodel (ISPM), as shown in Figure 4.

The developed ISPM consists of 19 common security practices: organisation, risk management, access control policy, edit, review, compliance, business management, backup and recovery, incident response, SETA program, security awareness, security training, security education, email security policy, cloud security policy, network security policy, website security policy, physical security policy, and privacy security policy.

Therefore, this study developed a comprehensive metamodel called ISPM that is able to reconcile and recognise the diverse characteristics of the ISP field. The redundant security practices were combined in the developed ISPM. Figure 5 shows the three primary layers of the developed ISPM, which are utilised to control how the ISP field behaves. For instance, Level 2 of the developed ISPM is the abstract layer that unifies all the ISP field's common security practices. The behaviour of the Level-1 objects is governed by Level 2. The primary ISP field model, Level 1, represents the key characteristics, functions, and connections of the ISP field model. Additionally, it controls how the Level-0 ISP user model behaviour should be. Level 0 represents the ISP's actual data. As a result, the Level-2 metamodel will use modelling blocks to express the knowledge of the ISP field. The primary building components that are frequently reused are the modelling blocks [32]. In many instances of the ISP field, the metamodel blocks are a collection of properties and operations that are reused [33]. In this study, an ISP's operations and properties are contained in a model

block. Table 4 illustrates the availability of a model block at three levels of metamodel: Level 2-Metamodel, Level-1-ISP Field Model, and Level-0-ISP User Data Model. The M1-Block is used to represent an example of security practices in the M1-ISP Model, whereas the M0-Block is used to represent the data of the example of a common security practice in the M0-ISP User Data Model, and the M2-Block is used to represent a portion of the common security practices in the Level 2-Metamodel. As a result, the building blocks of the metamodel common security practices that were previously discussed are represented as the activities, tasks, responsibilities, processes, information, and plans of the ISP field. Each metamodel common security practice is therefore represented by a UML class as shown in Table 4. These are the following fields in each ISPM Class:

ISPM Class ID is a unique identifier for the common security practice.

ISPM Class Name represents an ISP common security practice name.

ISP Class Terminology represents an ISP common security practice definition.

ISPM Class Attribute represents an ISP requirement.

ISPM Class Operation represents an ISP task.

ISPM Class Relationship represents the relationship with another common security practice.

Each ISPM common security practice has unique M2-Blocks that together make up the common security practice's true meaning. As an illustration, Table 4 shows an example of the M2-Blocks of the incident responding concept, including incident responding name, incident responding team, perform live response, perform interview, perform source seize, incident responding tools, and incident responding plan.

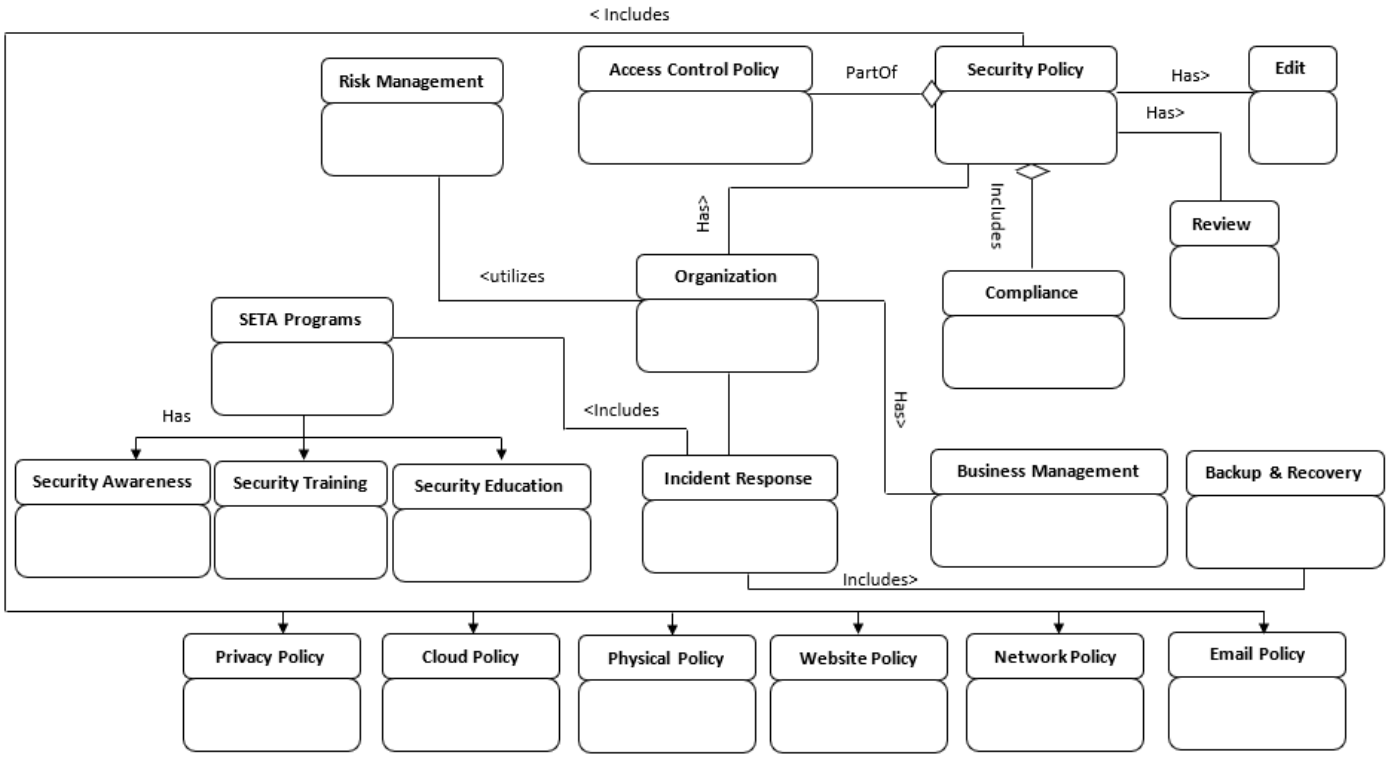

Figure 4. Developed ISPM based on ISO 27001.

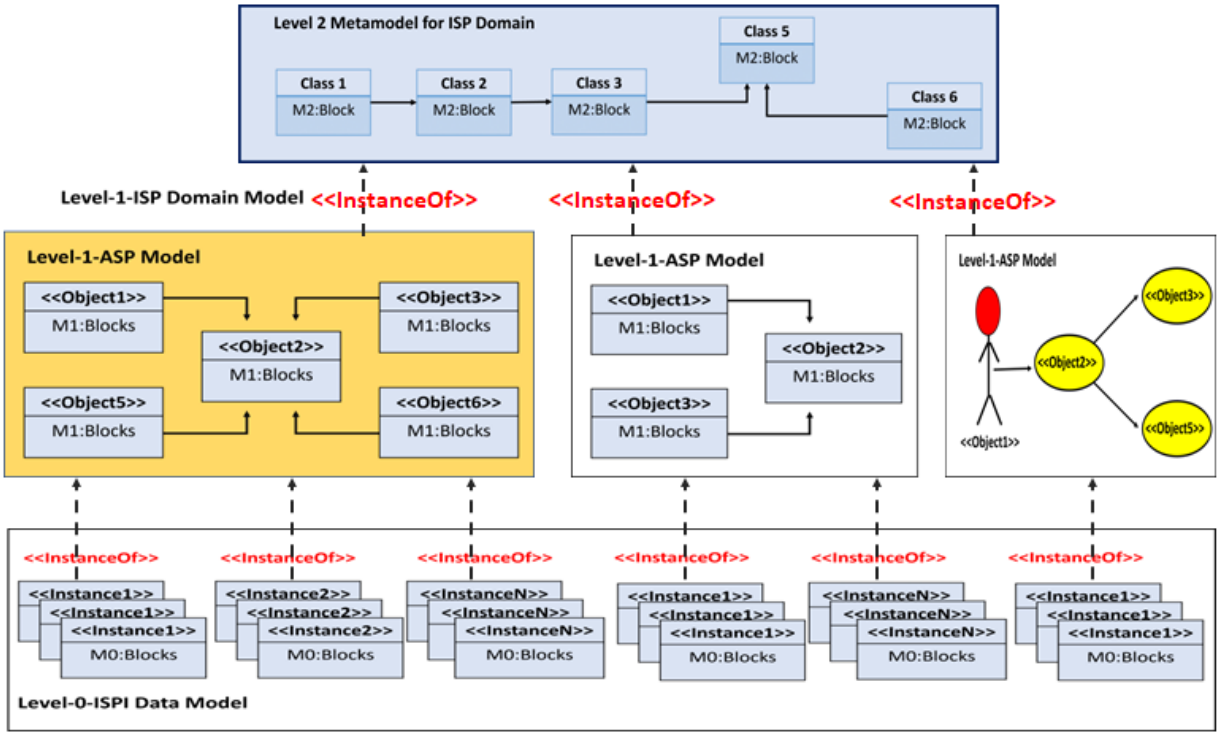

Figure 5. Architecture layers of the developed ISPM.

Step 5. Validating the Developed ISPM:

This is the final step of the development and validation process of ISPM. It is used to validate the completeness and logicalness of the developed metamodel through comparing it with other models [60]. Comparison with other models helps to identify any missing security practices in the developed ISPM and ensures it has sufficiently broad coverage. To do this, the security practices of ISPM were validated and compared to those of other models existing in the same field [60]. Specifically, ISPM was used to generate all security practices found in the ISP models gathered and combined in Step 2, that is, each ISPM security practice was examined in this study. Therefore, and based on the results of this step, the developed ISPM was found to be comprehensive and capable of covering most of the ISO 27001 practices, as shown in Table 5. The purple colour in this table represents the ISO 27001 security controls covered by the developed ISMP practices.

Based on the validation process above, the developed ISPM covered eight security controls of ISO 27001. Compared to the existing ISP models (which were reviewed in Section 2 and Table 2), the developed ISPM is a comprehensive metamodel. ISPM covers all the security controls in the ISO 27001 standard, including physical security, personnel security, access control, cryptography, system security, network security, incident management, and compliance. In addition, it provides detailed guidance on the implementation of each control, as well as detailed recommendations on how to measure and report on progress. Furthermore, ISPM also provides a framework for assessing the security posture of an organisation, which can be used to identify gaps in their security posture and address them. Overall, ISPM is comprehensive and broadly applicable, and also provides guidance on how to implement, measure, and report on security controls.

Table 4. M2-Blocks of The Incident Responding Concept.

ISPM Concept Name	**Incident Responding**	
Concept ID _	INSR-01	
ISPM Terminology	Incident responding is a planning process that used to gather incident details such as any information about incident events and known timelines, the parties involved thus far in the investigation, and the size and number of databases involved. The credential is required to login in high level for investigation. Also responding to an incident required avoiding any roadblock such windows firewall, network access control, IDS, IPS and versus	
	capture	Relation type: Specialization, Relation name: "Is Akind Of"
	interview	Relation type: Specialization, Relation name: "Is Akind Of"
	Live Response	Relation type: Specialization, Relation name: "Is Akind Of"
Attribute i. ID ii. Name iii. Description	Attribute ID (Unit Fragment)	Class Attribute: (Name and Description)
	AINSR-01	Incident Responding Name: The name of the process (e.g.,: SONY database Incident Responding)
	AINSR-01	Incident Responding Type: type of incident responding that must perform by incident responders (e.g.,: live response for volatile data, capture investigation sources, or conduct interview along with CEO or Corporation team)
	AINSR-01	Incident Responding Team: the name of the incident responder that achieve the mission
	AINSR-01	Incident Responding Plan: The plan of incident responding that needs to be followed by all incident responder involved (e.g.,: "Isolate SONY Network Database Plan)
	AINSR-01	Incident Place: The location where the incident took place which has one or more places (e.g.,: S SONY Corporation);
	AINSR-01	Incident Responding Tools: the forensic and techniques tools that may use by incident responders to conduct incident responding
	AINSR-01	Incident Responding Authority: incident responders who have the authority to make incident responding
	AINSR-01	Incident Responding Date: the date and time of the start and end of the incident responding
	AINSR-01	Incident Responding Result: the output of the incident responding (e.g.,: compromised, destroyed, changed or clean)
	AINSR-01	Data At Risk: data that reside in victim database served Areas that must be protected
Operation i. ID ii. Name iii. Description	Operation ID (Unit Fragment)	Class Operation: (Name and Description)
	OINSR-01	Perform Seize Source (): A process to seize whole investigation source (e.g.,: capture volatile and non-volatile artefact of the victim database)
	OINSR-01	Perform Live Response (): A process to capture volatile data from volatile artefacts
	OINSR-01	Perform interview (): A process to gather information from IT managers, and Security managers. Also gather information from high level managements (CEO)
	OINSR-01	Perform Protect Data (): A process to preserve the organization database data from tampering and move it to safe place to conduct further investigation
	OINSR-01	Check incident (): Incident responding team must ensure about database incident (e.g.,: check the critical and nature of the incident)
	OINSR-01	Return Report (): submit report to the Organization manages about incident responding task.

Table 5. Comparison of the developed ISPM practices with the ISO 27001 security controls.

Developed ISPM	Security Policy	Organisation of Information Security	Human Resource Security	Assess Management	Access Control	Cryptography	Physical and Environmental Security	Operational Security	Communication Security	Systems Acquisition, Development, and Maintenance	Supplier Relationships	Information Security Incident Management	Business Continuity	Compliance
Organisation		■												
Risk Management				■										
Access Control Policy					■									
Security Policy	■													
Edit														
Review														
Compliance														■
Business Management													■	
Backup and Recovery								■						
Incident Response												■		
SETA Program												■		
Security Awareness												■		
Security Training												■		
Security Education												■		
Email Policy	■													
Cloud Policy	■													
Network Policy	■													
Website Policy	■													
Physical Policy	■													
Privacy Policy	■													

4. Finding and Discussion

Information Security Policy (ISP) can be defined as a set of rules, regulations, and guidelines that protect information systems from unauthorised access, use, modification, and destruction. It may also address other issues related to information security, such as computer security, data security, and network security. There are several ISP models and frameworks in the literature that are duplicated, resulting in a disorganised, unstructured, and unclear ISP field due to the duplicate policies, procedures, and processes described in these models. As a result of reviewing and analysing the literature, the authors of the present paper gained a deeper understanding of security policy practices from an ISO 27001 perspective. Then, key areas where improvements are needed were identified to ensure security policies are compliant with ISO 27001 standards and best practices. Specifically, the review conducted in this study identified the need for better policy implementation, more detailed policy documentation, improved risk assessment processes, and improved internal and external communication. Additionally, authors recognised the importance

of developing a culture of security in organisations and providing adequate training and guidance to staff.

For this purpose, the Information Security Policy Metamodel (ISPM) was developed in this study. The developed metamodel allows for the comprehensive examination of various components of ISP and development of a holistic view of the policy. It provides a structured view of the policy structure and helps to identify relationships amongst various elements. The ISPM also aids in the development of a comprehensive understanding of policies, as well as the development of more detailed policies. Furthermore, it helps to develop a more effective security posture by allowing for the identification of potential security vulnerabilities. ISPM was designed in a way to be flexible and extensible, allowing for the integration of additional security practices and the continual improvement of policies. Additionally, it was designed in a way to be easily integrated into existing information security frameworks. ISPM can help organisations develop their own effective security strategies.

From the ISO 27001 perspective, the developed ISPM is more comprehensive than the existing information security policy models in Section 2 and Table 2. It provides a structured approach, with a detailed set of steps, which can help organisations to develop a secure information security policy, covering all important aspects of information security. It covers risk assessment, threat identification and risk management, data protection and privacy, access control and authentication, audit and logging, encryption and other security measures, and incident response. In addition, the metamodel can be used to develop a comprehensive security framework that covers all aspects of information security.

5. Conclusions

The purpose of this study was to develop a comprehensive metamodel for ISPs. By reviewing and analysing the literature, a deeper understanding of security policy practices from an ISO 27001 perspective was gained. Based on this analysis, an ISP metamodel was developed. The developed metamodel covered 10 common security practices: Organisation, risk management, access control policy, edit, review, compile, manage, backup and recovery, incident response, SETA program, security awareness, security training, security education, email security policy, cloud security policy, network security policy, website security policy, physical security policy, and privacy security policy. There are several operations and attributes involved in each common security practice. Experts and researchers can benefit from the developed ISPM in many ways. Using the metamodel, organisations will be able to structure and manage security policy according to security policy management practices. Additionally, the metamodel will enable experts to benchmark their security policies against it to gain a better understanding of security practices. Metamodels provide a solid foundation for future research. Future work could involve empirically refining and validating the metamodel through expert interviews, case studies within such organisations, and finally focus groups. For refinement of the proposed metamodel, experts will be interviewed in future work to provide comments. Considering the metamodel, case studies can be used to assess the implementation of security practices. Metamodel validation will be carried out by focus groups.

Author Contributions: Conceptualization, F.M.A., W.M.S.Y., A.A.-D., W.M.S.Y.; methodology, A.A.-D., Y.D.A.-O.; formal analysis, A.A.-D.; investigation, A.A.-D.; data curation, A.A.-D.; writing—original draft preparation, A.A.-D., W.M.S.Y.; writing—review and editing A.A.-D., F.M.A., Y.D.A.-O.; visualization, F.M.A.; supervision, Y.D.A.-O., F.M.A.; project administration, F.M.A., W.M.S.Y.; validation A.A.-D. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was funded by Institutional Fund Projects under grant no. (IFPIP: 1056-830-1443). The authors gratefully acknowledge the technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research work was funded by Institutional Fund Projects under grant no. (IFPIP: 1056-830-1443). The authors gratefully acknowledge the technical and financial support provided by the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Moody, G.D.; Siponen, M.; Pahnila, S. Toward a unified model of information security policy compliance. *MIS Q.* **2018**, *42*, 285–311. [CrossRef]
2. Brenner, J. ISO 27001 risk management and compliance. *Risk Manag.* **2007**, *54*, 24–29.
3. Abdullah, A.; Othman, S.H.; Razali, M.N. Structuring knowledge on house Price Volatility through a metamodel. *ARPN J. Eng. Appl. Sci.* **2006**, *10*, 17785–17795.
4. Thakur, K.; Ali, M.L.; Gai, K.; Qiu, M. Information Security Policy for E-commerce in Saudi Arabia. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 187–190.
5. Alzamil, Z.A. Information security practice in Saudi Arabia: Case study on Saudi organizations. *Inf. Comput. Secur.* **2018**, *26*, 568–583. [CrossRef]
6. Talib, A.M.; Alomary, F.O.; Alwadi, H.F.; Albusayli, R.R. Ontology-Based Cyber Security Policy Implementation in Saudi Arabia. *J. Inf. Secur.* **2018**, *9*, 315. [CrossRef]
7. Alsaif, M.; Aljaafari, N.; Khan, A.R. Information Security Management in Saudi Arabian Organizations. *Procedia Comput. Sci.* **2015**, *56*, 213–216. [CrossRef]
8. Almubayedh, D.; Al Khalis, M.; Alazman, G.; Alabdali, M.; Al-Refai, R.; Nagy, N. Security Related Issues In Saudi Arabia Small Organizations: A Saudi Case Study. In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC), Riyadh, Saudi Arabia, 25–26 April 2018; pp. 1–6.
9. Aljuryyed, A. 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*; Dawson, M., Tabona, O., Maupong, T., Eds.; IGI Global: Hershey, PA, USA, 2022; pp. 62–82.
10. AlGhamdi, S.; Win, K.T.; Vlahu-Gjorgievska, E. Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Gov. Inf. Q.* **2022**, *39*, 101721. [CrossRef]
11. Evers, M.M. Discovering the prize: Information, lobbying, and the origins of US–Saudi security relations. *Eur. J. Int. Relat.* **2022**, *29*, 104–128. [CrossRef]
12. Ølnes, J. Development of security policies. *Comput. Secur.* **1994**, *13*, 628–636. [CrossRef]
13. Alshaikh, M.; Maynard, S.B.; Ahmad, A.; Chang, S. Information security policy: A management practice perspective. *arXiv* **2016**, arXiv:1606.00890.
14. Bayuk, J.; Waterhouse, L.L.P.P. *Security through Process Management*; Price Waterhouse: London, UK, 1997.
15. Tipton, H.F.; Krause, M. *Information Security Management Handbook*; CRC Press: Boca Raton, FL, USA, 2007.
16. Pierson, P. The Study of Policy Development. *J. Policy Hist.* **2005**, *17*, 34–51. [CrossRef]
17. Cavusoglu, H.; Cavusoglu, H.; Son, J.; Benbasat, I. Institutional pressures in security management: Direct and indi-rect influences on organizational investment in information security control resources. *Inf. Manag.* **2015**, *52*, 385–400. [CrossRef]
18. Rees, J.; Bandyopadhyay, S.; Spafford, E.H. PFIRES: A policy framework for information security. *Commun. ACM* **2003**, *46*, 101–106. [CrossRef]
19. Karyda, M.; Kiountouzis, E.; Kokolakis, S. Information systems security policies: A contextual perspective. *Comput. Secur.* **2004**, *24*, 246–260. [CrossRef]
20. Diver, S. Information Security Policy-A Development Guide for Large and Small Companies. Available online: https://www.sans.org/reading-room/whitepapers/policyissues/information-securitypolicy-development-guide-large-small-companies-1331 (accessed on 25 October 2018).
21. Tuyikeze, T.; Pottas, D. An Information Security Policy Development Life Cycle. In Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth, South Africa, 17–18 May 2010; pp. 165–176.
22. Tuyikeze, T.; Flowerday, S. Information Security Policy Development and Implementation: A Content Analysis Approach. In Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014); Plymouth University: Plymouth, UK, 2014; pp. 11–20.
23. Park, M.; Chai, S. Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 3–6 January 2018.
24. Proença, D.; Borbinha, J. Information security management systems—A maturity model based on ISO/IEC 27001. In Proceedings of the Lecture Notes in Business Information Processing; Springer: Berlin/Heidelberg, Germany, 2018; Volume 320, pp. 102–114.
25. White, G.B.; Sjelin, N. The NIST Cybersecurity Framework. In *Research Anthology on Business Aspects of Cybersecurity*; IGI Global: Hershey, PA, USA, 2022; pp. 39–55.

26. Hengstler, S.; Nickerson, R.C.; Trang, S. Towards a Taxonomy of Information Security Policy Non-Compliance Behavior. In Proceedings of the 55th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2022; pp. 4826–4835.
27. Kabanda, S.; Mogoane, S.N. A Conceptual Framework for Exploring the Factors Influencing Information Security Policy Compliance in Emerging Economies. In *International Conference on e-Infrastructure and e-Services for Developing Countries*; Springer International Publishing: Cham, Switzerland, 2022; pp. 203–218.
28. Wolfswinkel, J.F.; Furtmueller, E.; Wilderom, C.P.M. Using grounded theory as a method for rigorously reviewing literature. *Eur. J. Inf. Syst.* **2013**, *22*, 45–55. [CrossRef]
29. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Choo, K.-K.R.; Glisson, W.B.; Ali, A.; Abrar, M. CDBFIP: Common Database Forensic Investigation Processes for Internet of Things. *IEEE Access* **2017**, *5*, 24401–24416. [CrossRef]
30. Bulgurcu, B.; Cavusoglu, H.; Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Q.* **2010**, *34*, 523–548. [CrossRef]
31. Sommestad, T.; Hallberg, J.; Lundholm, K.; Bengtsson, J. Variables influencing information security policy compliance: A systematic review of quantitative studies. *Inf. Manag. Comput. Secur.* **2014**, *22*, 42–75.
32. Osho, O.; Onoja, A.D. National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *Int. J. Cyber Criminol.* **2015**, *9*, 120.
33. Safa, N.S.; Von Solms, R.; Furnell, S. Information security policy compliance model in organizations. *Comput. Secur.* **2016**, *56*, 70–82. [CrossRef]
34. Ismail, W.B.W.; Widyarto, S.; Ahmad, R.A.T.R.; Ghani, K.A. A Generic Framework for Information Security Policy Development. In Proceedings of the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 19–21 September 2017; pp. 1–6.
35. Irfan, S.; Junseok, H. The application of AHP to evaluate information security policy decision making. *Int. J. Simul. Syst. Sci. Technol.* **2014**, *10*, 46–50.
36. Alqahtani, F.H. Developing an Information Security Policy: A Case Study Approach. *Procedia Comput. Sci.* **2017**, *124*, 691–697. [CrossRef]
37. Almeida, F.; Carvalho, I.; Cruz, F. Structure and Challenges of a Security Policy on Small and Medium Enterprises. *KSII Trans. Internet Inf. Syst.* **2018**, *12*, 747–763.
38. Amankwa, E.; Loock, M.; Kritzinger, E. Establishing information security policy compliance culture in organizations. *Inf. Comput. Secur.* **2018**, *26*, 420–436. [CrossRef]
39. Alshare, K.A.; Lane, P.L.; Lane, M.R. Information security policy compliance: A higher education case study. *Inf. Comput. Secur.* **2018**, *26*, 91–108.
40. Barrera, D.; Molloy, I.; Huang, H. Standardizing IoT Network Security Policy Enforcement. In Proceedings of the Workshop on Decentralized IoT Security and Standards (DISS), San Diego, CA, USA, 5 February 2018; p. 6.
41. Chen, X.; Chen, L.; Wu, D. Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. *J. Comput. Inf. Syst.* **2016**, *58*, 312–324.
42. Kovács, L. Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Acad. Rev.* **2018**, *23*, 16–24.
43. Calzavara, S.; Rabitti, A.; Bugliesi, M. Semantics-Based Analysis of Content Security Policy Deployment. *ACM Trans. Web* **2018**, *12*, 1–36.
44. Adi, K.; Hamza, L.; Pene, L. Automatic security policy enforcement in computer systems. *Comput. Secur.* **2018**, *73*, 156–171. [CrossRef]
45. Alzahrani, A.; Johnson, C.; Altamimi, S. Information Security Policy Compliance: Investigating the Role of Intrinsic Motivation Towards Policy Compliance in the Organisation. In Proceedings of the 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 25–27 May 2018; pp. 125–132.
46. Sharma, S.; Warkentin, M. Do I really belong?: Impact of employment status on information security policy compliance. *Comput. Secur.* **2018**, *87*, 101397.
47. Alotaibi, M.J.; Furnell, S.; Clarke, N. A framework for reporting and dealing with end-user security policy compliance. *Inf. Comput. Secur.* **2019**, *27*, 2–25. [CrossRef]
48. Kim, H.L.; Choi, H.; Han, J. Leader power and employees' information security policy compliance. *Secur. J.* **2019**, *32*, 391–409. [CrossRef]
49. Zellhofer, D. Information Security Policies in Organizations. In *Organizing for the Digital World*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 49–62.
50. Siemiatkowski, P.; Tomaszewski, P.; Marszalek-Kawa, J.; Polcikiewicz, Z. The Assessment of the Local Security Policy Efficiency. *Eur. Res. Stud. J.* **2020**, *23*, 217–237. [CrossRef]
51. Wu, Y.C.; Sun, R.; Wu, Y.J. Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability* **2020**, *12*, 2916. [CrossRef]
52. Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]
53. Koohang, A.; Nord, J.H.; Sandoval, Z.V.; Paliszkiewicz, J. Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. *J. Comput. Inf. Syst.* **2020**, *61*, 99–107. [CrossRef]

54. Onyema, E.M.; Kumar, M.A.; Balasubaramanian, S.; Bharany, S.; Rehman, A.U.; Eldin, E.T.; Shafiq, M. A Security Policy Protocol for Detection and Prevention of Internet Control Message Protocol Attacks in Software Defined Networks. *Sustainability* **2022**, *14*, 11950. [CrossRef]
55. Caro, M.F.; Josyula, D.P.; Cox, M.T.; Jiménez, J.A. Design and validation of a metamodel for metacognition support in artificial intelligent systems. *Biol. Inspired Cogn. Arch.* **2014**, *9*, 82–104. [CrossRef]
56. Al-Dhaqm, A.; Razak, S.; Othman, S.H.; Ngadi, A.; Ahmed, M.N.; Mohammed, A.A. Development and validation of a Database Forensic Metamodel (DBFM). *PLoS ONE* **2017**, *12*, e0170793.
57. Bogen, A.C.; Dampier, D.A. Preparing for Large-Scale Investigations with Case Domain Modeling. In Proceedings of the 5th Annual Digital Forensic Research Workshop (DFRWS 2005), New Orleans, LA, USA, 17–19 August 2005.
58. Ali, A.; Razak, S.A.; Othman, S.H.; Mohammed, A.; Saeed, F. A metamodel for mobile forensics investigation domain. *PLoS ONE* **2017**, *12*, e0176223. [CrossRef]
59. Pilone, D.; Pitman, N. *UML 2.0 in a Nutshell*; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2005.
60. Sargent, R.G. Model Verification and Validation. In *Modeling and Simulation in the Systems Engineering Life Cycle*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 57–65.