applied sciences

Article

AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity

Jorge Hochstetter-Diez [1,2,3], Mauricio Diéguez-Rebolledo [1,2,3,4,*], Julio Fenner-López [1,4] and Cristina Cachero [3,5]

[1] Departamento Ciencias de la Computación e Informática (DCI), Universidad de La Frontera, Temuco 481-1230, Chile; jorge.hochstetter@ufrontera.cl (J.H.-D.); julio.fenner@ufrontera.cl (J.F.-L.)
[2] Centro de Estudios en Ingeniería de Software (CEISUFRO), Universidad de La Frontera, Temuco 481-1230, Chile
[3] Advanced Development and Empirical Research on Software (ALISoft), Universidad de Alicante, 03080 Alicante, Spain; ccachero@dlsi.ua.es
[4] CyberSecurity Workgroup, Centro de Modelación y Computación Científica (CEMCC), Universidad de La Frontera, Temuco 481-1230, Chile
[5] Departamento de Lenguajes y Sistemas Informáticos, Universidad de Alicante, 03080 Alicante, Spain
* Correspondence: mauricio.dieguez@ufrontera.cl

Abstract: In today's world, private and government organizations are legally obligated to prioritize their information security. They need to provide proof that they are continually improving their cybersecurity compliance. One approach that can help organizations achieve this goal is implementing information security maturity models. These models provide a structured framework for measuring performance and implementing best practices. However, choosing a suitable model can be challenging, requiring cultural, process, and work practice changes. Implementing multiple models can be overwhelming, if possible. This article proposes a prioritization strategy for public institutions that want to improve their information security maturity. We thoroughly analyzed various sources through systematic mapping to identify critical similarities in information security maturity models. Our research led us to create the AIM (Awareness, Infrastructure, and Management) Triad. This triad is a practical guide for organizations to achieve maturity in information security practices.

Keywords: maturity model; cybersecurity; information security

check for updates

Citation: Hochstetter-Diez, J.; Diéguez-Rebolledo, M.; Fenner-López, J.; Cachero, C. AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. *Appl. Sci.* **2023**, *13*, 8339. https://doi.org/10.3390/app13148339

Academic Editor: Gianluca Lax

Received: 12 June 2023
Revised: 12 July 2023
Accepted: 14 July 2023
Published: 19 July 2023

1. Introduction

Information security is a critical issue in organizational management and in government institutions. Public institutions associated with government entities often have access to a large amount of confidential information, including personal and financial data of citizens, national security information, and other sensitive information. Ensuring safeguarding citizens' privacy and security, and mitigating the risk of sensitive information exposure, are of utmost importance. Therefore, treating data information security with the utmost seriousness and responsibility is imperative.

Government entities have made various efforts to improve the management and security of their information systems [1]. Information management in public institutions must ensure that sensitive data is collected, stored, processed, and shared securely and confidentially [2]. Hence, many government entities use information security maturity models as guidelines or roadmaps for cybersecurity issues [3].

Maturity models are helpful because they provide systematic frameworks for measuring the performance of organizations in specific areas of work, though with a stronger focus on the technological aspect [4]. A maturity model is perceived as a roadmap that guides the organization towards implementing best practices, hence offering a starting point [5] in a path of evolutionary improvement from an initial stage of inconsistent processes up to the most mature processes of the organization [6]. Hence, it allows evaluation of the state of a given organization or business process's development while outlining improvement strategies to achieve desired objectives, as well as identifying areas on which the organization should focus to improve existing standards further and achieve some pre-defined goals [7].

Numerous authors have advocated Cybersecurity Maturity Models (CMMs) for diagnosing organizational progress and establishing measurement criteria in a broad spectrum of agencies: The tourism industry, health institutions, and e-government all rely on electronic processes, including public agencies and services, see [8–13]. However, the Oxford Cybersecurity Capacity Maturity Model (OC2M2) [14] stands out as one of the most comprehensive and widely adopted CMMs. Additionally, the Cybersecurity Capability Maturity Model (C2M2) developed by the United States Department of Energy [15], the NIST Cybersecurity Framework by the National Institute of Standards and Technology (NIST) [16], the Security and Privacy Capability Maturity Model (SP-CMM) created by the Carnegie Mellon Software Engineering Institute [17], and ISACA's CMMI Cybermaturity Platform [18] are all noteworthy models in this regard.

These models play a crucial role in helping organizations evaluate their current cybersecurity capabilities, identify areas for improvement, and prioritize actions and investments to meet their targets. However, adapting or modifying these models can be challenging due to their unique structures and varying categories for assessing cybersecurity maturity.

Recently, it has become apparent that public government entities face significant challenges in effectively addressing information security. The existing maturity models need to provide comprehensive guidance, making it arduous to implement a cohesive framework incorporating relevant models and standards. This lack of clear direction hampers the establishment of robust security policies, safeguarding of data, and efficient handling of security risks. This realization has emerged only in recent times; see for example [3,8,19,20].

We notice that it can be challenging to evaluate the effectiveness of security measures without proper maturity models for information security. However, having a clear reference framework can make it easier to determine if governmental entities meet security requirements and safeguard sensitive information. Hence, they need to prioritize [21], choose and adapt a maturity model from the point of view of ensuring data protection, as well as facilitating the implementation of relevant standards and best practices [22].

We observe that complying with any information security model (or standard) means addressing different organizational dimensions, which in some cases, are beyond the focus of a security administrator. For example, the ISO/IEC 27000 family includes practices such as incorporating information security clauses into administrator contracts or continuous training of technical teams. Committing to an information security standard means having an organizational structure that supports political and top management roles and technical and operational roles.

Using a maturity model suggests that the organization is taking a structured approach to improving its processes, procedures, or practices. It means that stakeholders and actors recognize the relevance of developing specific actions or practices, establish standards and norms with which they guide and evaluate their actions, methods, and strategies, and generate adjustments, changes, and innovations that enable improvements in procedures, techniques, technologies, capabilities, and efficacy.

In the literature, there are various proposals and applications of maturity models aimed at improving the information security of computer systems in organizations, which implies the need for qualified personnel in security assurance and protection, as well as continuous training and education in security matters [8,20]. However, the latter is difficult to implement, and many organizations may easily fall victim to attacks that materialize without having the necessary control and knowledge to isolate and counter such attacks on information assets [3]. Deciding on a maturity model for an organization can be complicated due to its multifaceted nature. It covers various areas within the organization, making it difficult to determine where to begin implementing it [23]. The organization may have to deal with multiple models simultaneously, which can be overwhelming and hinder the identification of critical areas needing improvement [24]. Moreover, each maturity model has its requirements, which may require significant changes in the organizational culture, processes, and work practices [25]. Therefore, determining where to start an implementation process of maturity models can be a highly complex task [25,26].

This article explores some challenges public or government entities face while seeking to implement Information Security Maturity Models. We identify some critical areas that should be considered in any attempt at prioritization while developing a plan considering each organization's specific resources and limitations. As a result, the maturity models implemented are relevant but also efficient and effective since prioritization for investment in information security resources, which supports improved decision-making at the institutional level, becomes an asset for those institutions.

A prioritization strategy that allows institutions to navigate the jungle of indicators associated with maturity models presents tangible benefits and adds value to the planning and design work in a subject as sensitive as Information Security. In order to propose a prioritization strategy regardless of a given maturity model, we adopted a procedure validated in the literature, in which we first consider the review of available maturity models through a systematic mapping, from which the common core elements specifically related to Information Security are extracted and grouped in a diagram to visualize the different possible paths in the process of improving the maturity levels.

The article is structured as follows: In Section 2, we explore some of the challenges that public or government entities face while seeking to implement Information Security Maturity Models. Section 3 presents some related work on maturity models for governmental institutions and presents relevant features of some internationally renowned maturity models. In Section 4, we adopt a general methodology for developing maturity models, which helps us identify the necessary characteristics for proposing the prioritization idea. In Section 5, we developed the stages defined in the methodology to generate our strategy. Finally, in Section 6, we describe our proposal for the prioritization strategy. We close this article with Section 7 in which we point out some of the limitations of our study, and in Section 8, we present our conclusions.

2. Background

Government entities are responsible for protecting the information they handle, as it often includes confidential data about citizens and government employees [27]. Information management must ensure that data is collected, stored, processed, and shared securely and confidentially [3,28], which is why organizations and government entities have adopted information security maturity models to ensure the adequate protection of data [24].

A maturity model is a roadmap that guides the organization in implementing good practices, providing a starting point [6,8], as well as providing systematic reference frameworks for measuring the performance of organizations in selected areas. They allow evaluating the state of development of a given organization or business process, identifying the areas in which the organization should focus to improve [29,30].

3. Maturity Models for Government Entities

In [31], the authors scrutinized the approaches used in evaluating information security and cybersecurity training and awareness programs for users with two objectives: First, to identify the measures used to evaluate the effectiveness of such programs, and second, to examine the use of maturity models for measuring their progress. While an extensive literature review was presented, a gap in the current literature regarding the evaluation of these programs was noticed, as only five articles and two maturity models focused on evaluation.

In [25], the authors aimed to conduct a comprehensive review of current cybersecurity capability maturity models through a systematic analysis of articles published from 2011 to 2019. They observed that most CMMs share similar elements, such as maturity levels and processes.

In another interesting analysis, the authors aimed to clarify the uncertainty reflected in the current information security maturity evaluation [20]. In this regard, a convergence to maturity has been assessed neither for a generic approach nor multiple specific approaches that would allow for a trend of adoption. Despite the existence of ISO 21827 standards, many security maturity models have been produced in the last decade that still need to be tested.

In [24], the authors aimed to identify the most widely used CMMs. For this purpose, they systematically reviewed studies published between 2012 and 2017, identifying 201 articles mentioning different maturity models. Of these, 12 primary articles identified the most used models, some specifically focused on cybersecurity.

In all these systematic reviews or mappings, the authors used rigorous methods to identify and analyze relevant scientific articles on information security maturity models for public institutions. Two common factors observed in these works are: (i) Evaluating information security and cybersecurity training and awareness programs for users is a field that needs more research, as only a few articles and maturity models are available in the current literature. (ii) Despite the existence of various information security and CMMs, there still needs to be validation in processes. Each model has a specific purpose and different organization sizes and application domains. There needs to be more consensus on the best way to evaluate information security maturity.

3.1. The Oxford Cybersecurity Capacity Maturity Model (OC2M2)

The OC2M2 was created in 2012 with stakeholders from the energy and cybersecurity industries, focusing on evaluating the electricity industry's security posture. In 2014, it included three versions targeting users in the electricity, oil, and natural gas sectors, among others. In June 2022, the model was unified into a version adapted to include the energy sector and made significant updates to reflect changes in technology, threats, and security approaches [14].

The OC2M2, as explained by [32], is a valuable tool for evaluating the governance of cybersecurity capacity. The measurement encompasses five dimensions applicable for evaluating and establishing qualitative and quantitative benchmarks and improving cybersecurity awareness, which, in turn, helps institutions enhance their management and situational awareness of cybersecurity issues.

Indeed, OC2M2 proposes different levels of maturity of cybersecurity, which are expressed in the following five dimensions:

- Developing cybersecurity policy and strategy.
- Encouraging responsible cybersecurity culture within society.
- Building cybersecurity knowledge and capabilities.
- Creating effective legal and regulatory frameworks.
- Controlling risks through standards and technologies.

While these dimensions encompass essential areas that must be present for a comprehensive evaluation of cybersecurity capabilities, there are also various factors, aspects, stages of development, and indicators of cybersecurity capabilities within each dimension, together with some domains, as follows:

Dimension: A representation of the (different) frameworks through which an organization can self-determine its own cybersecurity maturity status. Hence they are the most important, or top-level, structure in a CMM. In turn, the dimensions are composed of factors.

Factor: They describe what each dimension of the maturity model implies or means concerning cybersecurity capabilities inside a dimension. These elements aim to improve the level of development of these capabilities, incorporating holistically all the features that make it possible to determine each level. On the other hand, factors are dynamic in that they should be continuously reviewed and updated based on the information gathered in the application of the model. Notice that most factors contain certain aspects that structure or detail them into more concise parts (indicators). However, there may be factors of a more limited scope that do not require these more specific aspects.

Aspect: They group or organize indicators for each factor into smaller, more easily understood classes. The number of aspects depends upon the context and complexity of the parent factor. Each aspect comprises a series of indicators within the five levels of development proposed by a CMM.

Stage: Stages map the organization's progress against a given factor/aspect of the CMM. The model proposes five stages of development that serve as a snapshot or evidence of the level of cybersecurity achieved. This evidence helps, in turn, as a baseline to determine the impact of the measures adopted from this point onward. Each stage defines a set of indicators helping to visualize progress towards a higher state of maturity.

Indicator: An indicator represents an essential element of the structure of a Cybersecurity Maturity Model. The evaluation of an indicator makes it possible to describe the state of development within an aspect, factor, and dimension. In other words, compliance or non-compliance with each indicator is evidence of the organization's status or degree of progress concerning maturity.

3.2. Cybersecurity Capability Maturity Model (C2M2)

The C2M2 uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments that allow organizations to self-evaluate both their cybersecurity capabilities and their Security investments optimization strategies, see [15].

It contains about 350 cybersecurity practices, grouped by objectives into ten logical domains. Each of the practices has a maturity indicator level that indicates the progression of practices within a domain; these domains are:

- Asset, Change, and Configuration Management.
- Threat and Vulnerability Management.
- Risk Management.
- Identity and Access Management.
- Situational Awareness.
- Event and Incident Response, Continuity of Operations.
- Third-Party Risk Management.
- Workforce Management.
- Cybersecurity Architecture.
- Cybersecurity Program Management.

3.3. NIST Cybersecurity Framework (NIST-CSF)

The NIST-CSF defines a proposal of four categories and five maturity levels for the security assessment of organizations. This proposal seeks to support organizations continuously assessing and monitoring their security levels [16].

The categories guide assessors regarding the organization's cybersecurity and operational risk performance to protect the organization, identify, detect, respond to threats, and recover from incidents. Furthermore, the maturity levels aim to evaluate the extent of progress the organization has made in these categories [33]. See Table 1.

Table 1. Categories and Maturity labels of NIST-CSF.

Categories:	**Maturity Levels:**
– Identify. – Protect. – Detect. – Respond. – Recover.	– Level 1—Initial. – Level 2—Repeatable. – Level 3—Defined. – Level 4—Managed. – Level 5—Optimized.

3.4. Security and Privacy Capability Maturity Model (SP-CMM)

The SP-CMM is mainly oriented to the establishment of objective criteria for the evaluation of cybersecurity and privacy controls [17].

One of the main characteristics of this model is that it considers both cybersecurity and the privacy of information.

This proposal provides security advisors with support in three specific aspects:

1. Defining the expectations of a security and privacy program.
2. Planning and budgeting the activities of the security and privacy program.
3. Establishing minimum criteria for evaluating supplier controls.

The SP-CMM proposes six levels of maturity:

- CMM 0—Not Performed: This level is defined as "non-existence practices".
- CMM 1—Performed Informally: This level is defined as "ad hoc practices".
- CMM 2—Planned and Tracked: This level is defined as "requirements-driven practices".
- CMM 3—Well-Defined: This level is defined as "enterprise-wide standardization".
- CMM 4—Quantitatively Controlled: This level is defined as "metrics-driven practices".
- CMM 5—Continuously Improving: This level is defined as "world-class practices".

This model contemplates over 1000 cybersecurity and privacy controls grouped into 32 domains. These controls cover more than 100 legal, regulatory, and contractual frameworks. The domains considered by the model can be seen in Table 2:

Table 2. SP-CMM Domains.

Domains	
1. Security and Privacy Governance	17. Assurance
2. Asset Management	18. Maintenance
3. Business Continuity and Disaster Recovery	19. Mobile Device Management
4. Capacity and Performance Planning	20. Network Security
5. Change Management	21. Physical and Environmental Security
6. Cloud Security	22. Privacy
7. Compliance	23. Project and Resource Management
8. Configuration Management	24. Risk Management
9. Continuous Monitoring	25. Secure Engineering and Architecture
10. Cryptographic Protections	26. Security Operations
11. Data Classification and Handling	27. Security Awareness and Training
12. Embedded Technology	28. Technology Development and Acquisition
13. Endpoint Security	29. Third-Party Management
14. Human Resources Security	30. Threat Management
15. Identification and Authentication	31. Vulnerability and Patch Management
16. Incident Response	32. Web Security

3.5. ISACA's CMMI Cybermaturity Platform

Companies must consider their people, processes, and technologies when implementing cybersecurity capabilities to ensure a comprehensive and reliable program. Many companies focus primarily on technology practices since they often provide tangible results and can be automated to simplify workflows [18].

ISACA's CMMI cybersecurity platform is an industry-leading platform that seeks to assess, manage, and mitigate cybersecurity risk and build cyber enterprise maturity.

It offers a redefinition through practical recommendations on specific standards. Notable among its recommendations are: (i) Providing a single cybersecurity risk assessment framework to simplify security gap analysis. (ii) Suggesting a risk-based action plan to help prioritize projects and close cybersecurity gaps. (iii) Providing an evidence-based approach to assess, optimize and report on cyber capabilities. (iv) Helping to implement key frameworks and keep up with the cybersecurity landscape through regular updates.

The cybersecurity platform offered by CMMI identifies and prioritizes gaps between maturity objectives determined by the target industry profile and current capabilities determined by self-assessment. Its business model offers specific recommendations based on real-world differences and positions consumers on a comparative edge with the best practices.

4. A Methodology for Developing a Prioritization Strategy

We now focus on proposing a strategy that allows public institutions to implement an ad hoc maturity model that responds to the characteristics and goals of each organization.

For this, we needed to identify, classify, and prioritize the relevant variables of the information security context. However, most of these variables were already present in the maturity models discussed. Given that our objective was not to create a new maturity model but to integrate the available models and propose a prioritization scheme for their implementation. We followed an adaptation of Becker's methodology [34], which proposes a process for designing and validating maturity models, specifically for information systems.

The methodology consists of two main phases: Generation and Transfer. Our work focused mainly on the Generation phase, which has four sub-phases: Problem Definition, Comparison of Existing Maturity Models, and Determination of a Development Strategy. Nonetheless, we did not consider the iterative maturity model development phase because it is at this stage that a maturity model comes in. Thus its development exceeds the purposes of this work.

Figure 1 depicts a simplified road map to developing a maturity model, as described in [8]. We used this for our design since, as already explained, it was not our intention to propose a new maturity model but rather to focus on an ad-hoc strategy that prioritizes the implementation of some of the elements of a maturity model. Hence we propose the application of the first three phases of the methodology for the identification, classification, and prioritization of these elements. The following section describes our approach to the development within these three sub-phases: Problem Definition, Comparision (of existing maturity models), and the Determination of a Development Strategy.

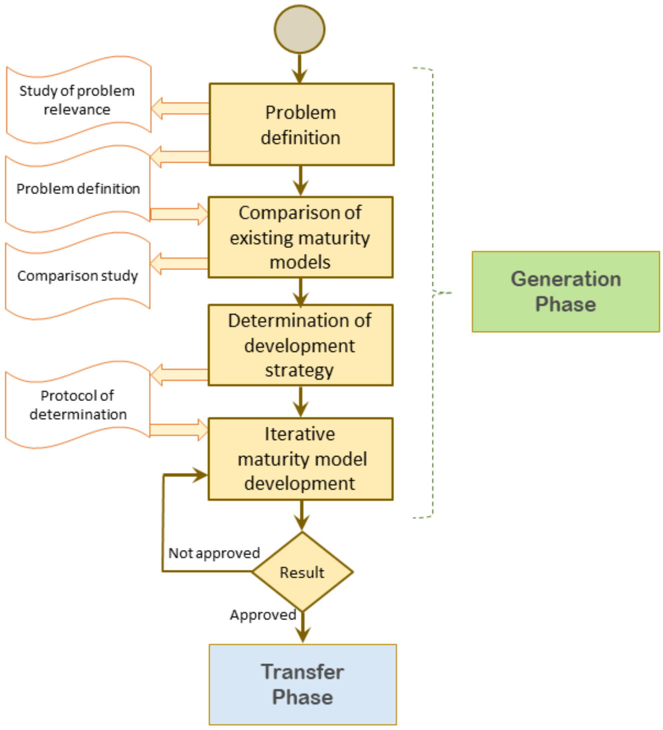
Study of problem relevance
Problem definition
Comparison study
Protocol of determination
Problem definition
Comparison of existing maturity models
Determination of development strategy
Iterative maturity model development
Generation Phase
Not approved
Result
Approved
Transfer Phase

Figure 1. Stages adopted from the methodology for developing maturity models [8].

5. Towards an Information Security Roadmap

5.1. Problem Definition

According to Becker [34], establishing relevance also requires the exact definition of the problem, which—in our context—as been already identified: we address the difficulties of state institutions in implementing the necessary procedures and cultural changes that are relevant for the improvement of their information systems and associated information security.

These challenges gain further relevance when considering that public institutions or organizations often face the necessity of defining and implementing protective measures for their information assets due to the vulnerability of their IT infrastructure. However, these measures are proving insufficient in light of the increasing frequency of cyber-attacks globally. Consequently, it is imperative for organizations to systematically establish security policies that comprehensively address the wide array of threats they encounter [3].

5.2. Systematic Mapping

During this sub-phase, we examined maturity models within information security in government entities, similar to how we outlined related studies in the preceding section. As mentioned earlier, the purpose of a maturity model is to provide an organizational roadmap for implementing best practices, primarily focusing on the technological domain as a starting point [4]. Some disciplines use these models to diagnose and define measures of progress [7,9,10,13,35].

For establishing the principles for our systematic mapping procedure, the contributions of different authors [36–38] were considered as a reference in regard to their methodology for systematic mappings. The PRISMA's systematic mapping study (SMS) technique [39] provides a means for validating, examining, and categorizing findings related to a specific subject or area of interest. This enables the determination of the research's extent and the classification of the knowledge gained.

As Petersen [40] points out, the mapping merely verifies the abstract, results, and conclusions. Therefore, we followed the protocol for a systematic mapping defined by Petersen [40]. To carry out a systematic mapping study, the phases represented in Figure 2 were followed sequentially.

The approach used in systematic mapping is that the generated report has as its main objective to catalog and categorize the evidence found in the literature, pointing out areas where knowledge is lacking. At the same time, in addition to providing a full description of the articles [41]. The components of the systematic mapping process are detailed in the subsequent sections.

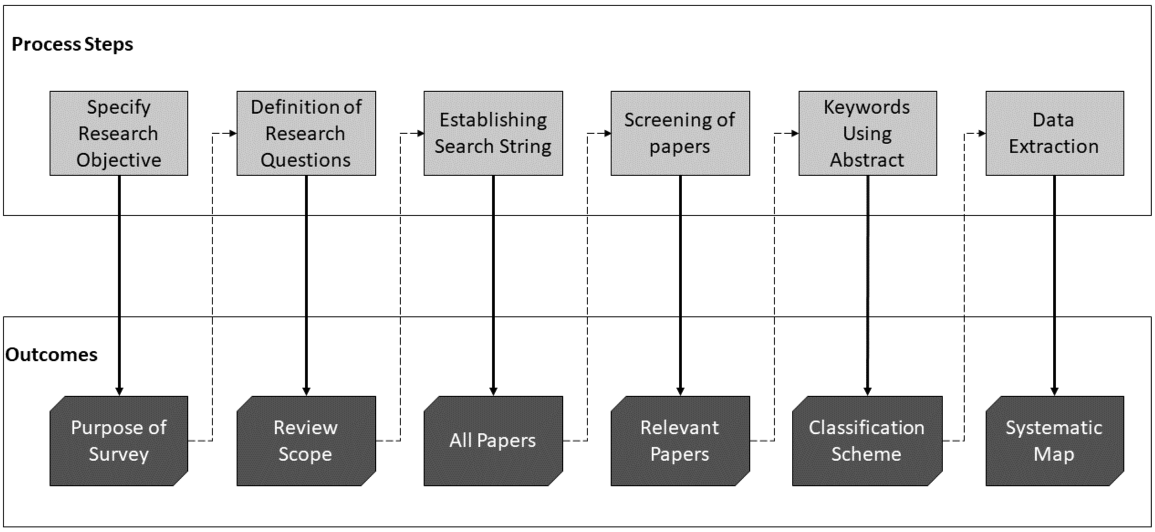

Figure 2. Stages of the systematic mapping.

5.2.1. Goal and Research Questions

General guidelines: We aim to have a comprehensive view of related work on maturity models as tools to assess information security or cybersecurity. The objective of this proposal is to provide an updated guide to assist government entities in implementing information security maturity models in priority areas.

The second step of systematic mapping, as outlined by [38], involves defining the research question(s) (RQ). Table 3 presents each of the research questions and their rationale. These questions were used to select, analyze, and categorize the information found in the study area.

Table 3. Research question and motivating.

Research Question	Motivating 2
RQ1: How many studies focus on maturity models for evaluating information security or cybersecurity?	Data
RQ2: How many of those studies propose maturity models specifically for assessing information security or cybersecurity in governmental/public institutions?	Data

5.2.2. Generating a Search String

To generate a search string, the keywords of the research questions were identified, along with the objectives, and then concatenated with logical connectors. This search string was applied to search engines and validated by us. The resulting string was: (*Cybersecurity OR "Information security") AND ("maturity model").*

5.2.3. Data Extraction

For the data search and extraction process, databases and websites with access to digital libraries were included. These would contain search engines that would allow searches using search strings to download many related works. The selected data sources were WoS and Scopus. For both databases, two searches were applied: (i) included search in only titles and (ii) only in abstracts, both for the last five years.

5.2.4. Inclusion and Exclusion Criteria

The selection of the studies found through the aforementioned academic search engines was based on the following inclusion/exclusion criteria:

Inclusion criteria:

- Papers published in English from journals and conferences.
- Complete works related to maturity models to measure cybersecurity or information security.
- Works from 2017 onwards were included.

Exclusion Criteria:

- Technical reports, summaries, editor comments, states of the art.
- Studies before 2017.
- Studies without an author.
- Documents that do not include maturity models to measure cybersecurity or information security.
- Duplicate studies in different databases.
- Documents that do not come from traceable journals or procedures.

5.2.5. Search Execution

The search string was applied to the selected sources, and an initial quantity of 114 works was obtained. The information was extracted using export tools from each of the digital libraries. We then applied the exclusion criteria for double-indexed works, reducing the number of results to 83. The next stage was reading the titles and abstracts; the most relevant papers were selected, totaling 60 documents (see Figure 3).

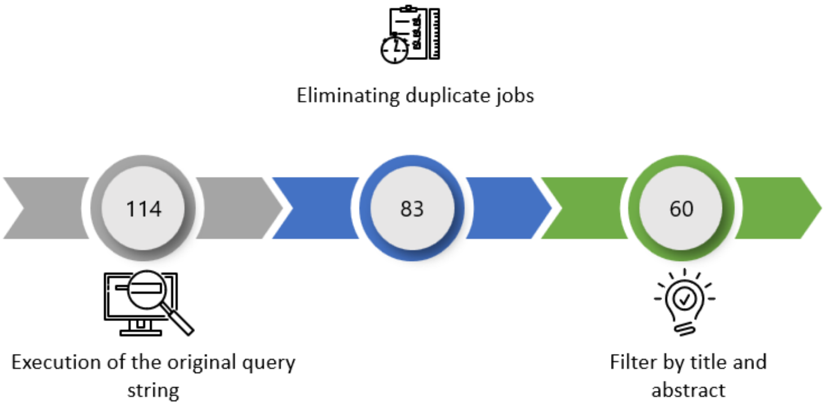
Eliminating duplicate jobs
114
83
60
Execution of the original query string
Filter by title and abstract

Figure 3. Search execution and filtering summary.

5.2.6. Classification Scheme

Publications were classified into three dimensions: time, category, and type of proposal. The temporal dimension classified the works into bands by year of publication between 2017–2022.

We organized the publications into various groups: health, consumer data protection, training programs, organizations, e-services government, pymes, critical infrastructure, cybersecurity models, incident response and cyber-defense, IS management and cybersecurity governance, big data, and software industry. We assigned the works to different categories based on their similarities. Hence, some of the publications belong to more than one category. We classified the articles found into three types:

(i) Analysis: Studies or literature reviews of the field of maturity models information security.

(ii) Use: Works that apply maturity models to information security and evaluate their results.

(iii) Implementation: Works that propose a maturity model for and or information security for a specific context.

5.2.7. Map Construction

After categorizing and classifying the works, we summarized the information for more accessible representation and analysis, as is common practice in systematic mappings. See Figure A1 in Appendix A for details.

5.2.8. Results and Analysis

The following is a solution to the research questions posed above.

RQ1: How many studies address maturity models as tools for assessing information security or cybersecurity?

We found sixty papers discussing Information Security maturity models from 2017 to 2022. All sixty papers discuss the use of maturity models to evaluate cybersecurity or information security, with thirty-four proposing a maturity model for a specific context in cybersecurity or information security, twenty-three applying maturity models to evaluate cybersecurity or information security, and twenty-nine being studies or literature reviews of maturity models in cybersecurity or information security (see Figure 4). None of the papers provided prioritization strategies. Table A1 in Appendix A depicts and summarizes the articles selected for review.

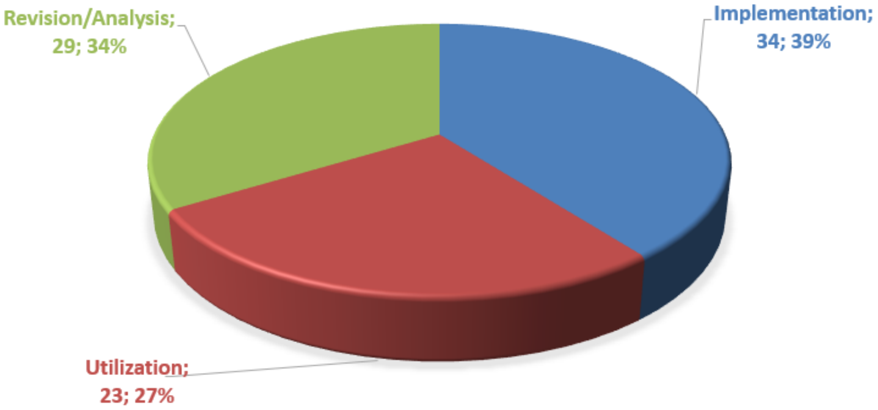

Figure 4. Article classification into three types.

RQ2: How many of them develop proposals in the field of governmental (public) institutions?

We have identified only three works that propose a maturity model for cybersecurity or information security in e-government services, which we review below.

In [42], the authors propose a maturity model for the existing e-services of Himachal Pradesh to provide a basis for developing improved electronic services for citizens to access. The authors present a classification of four maturity levels. However, the model lacks a clear description of the dimensions considered and indicators used to conceptualize maturity levels, indicating a need for improvement in terms of usability.

In [43], the authors propose a risk assessment framework and a related workflow that can be used semi-automatically in the organization to create an audit report and assess security risks. The proposed framework aims to use the ISO 27001 model and its technical implementations. The study's objective is to analyze the vulnerability assessment methods in information security and propose an effective model after analyzing existing maturity models.

In [44], the authors present a CMM for the federal public administration agencies of Brazil, adapted from three internationally recognized maturity models: C2M2 [15], NIST SCF [16], and Community Cybersecurity Maturity Model (CCSMM) [45]. Their model proposes the following levels (N's) and Domains (D's):

N0: Does not present any practices for a domain.
N1: Presents a set of initial practices for a domain.
N2: Presents a level of institutionalization of activities.

- Documented practices.
- Stakeholders are identified and participate.
- Necessary resources are provided to support the processes.
- Guidelines guiding the application of practices are identified.

N3: Guidelines guiding the application of practices are identified.

- Governance exists to guide activities.
- Policies include compliance requirements.
- Activities are periodically reviewed.
- Responsibilities and authority to execute practices are defined.
- The team performing the practices has adequate skills and knowledge.

D1. Risk Management.
D2. Asset Management.
D3. Access Management.
D4. Threat and Vulnerability Management.
D5. Continuity Management.
D6. Information Exchange.

D7. Training, Awareness, and Culture.
D8. Technological Infrastructure.
D9. Cybersecurity Governance.

In summary, from the results of the systematic mapping, we conclude that only three articles meet the criteria for their inclusion in our study; however, of these, we decided that only the model proposed by Azambuja and Neto [44] was worth considering more closely, as it is the only one of the three that presents a detailed description of the domains and levels presented. Please note that our decision to analyze the Azambuja and Neto model solely does not indicate that the other models are not valuable or noteworthy. Instead, we determined that this particular model was better suited for achieving the specific objectives of our study.

As we examined the articles in the Systematic Mapping process and the Related Works section, we came across diverse maturity models that organizations, including government institutions, can choose. However, none of these options provides guidance that prioritizes their implementation according to the organization's needs. Instead, it is the organizations themselves that must adjust to the structure of the model.

While it is true that this situation allows many organizations to organize and align themselves to a security structure proposed by the maturity model, it only sometimes lets organizations define their growth path according to their objectives, needs, or resources.

Table 4 summarises the domains the selected maturity models proposed and the number of maturity levels they present. Note that all of them (except [44]) can be considered general purpose, i.e., they are not designed to adapt to particular situations or the particular needs of specific organizations, making them less flexible and forcing organizations to adjust to the requirements of the models, which then require support in deciding how to achieve given levels of the information security maturity models. To ensure success, an implementation strategy should be developed that incorporates the elements from various maturity models. However, these elements should be prioritized based on the organization's specific needs.

Table 4. Comparative table of revised maturity models.

Characteristics	**SP-CMM**	**OC2M2**	**C2M2**	**NIST CSF**	**[44]**
Purpose	General	General	General	General	Specific
Domains	24	6	12	10	9
Levels	6	5	4	5	4

6. Development of a Prioritization Strategy

Our strategy for developing our approach to maturity models consists now of the integration of relevant features extracted from a set of maturity models into a new model that public institutions can adopt step-wise, taking into account the institution's best practices, development time, and regulatory requirements, thus providing a basis for customization.

The models that form the basis for the definition of our proposal are OC2M2, C2M2, SP-CMM, NIST CSF, and the Azambuja and Neto models.

We consider 13 dimensions comprising the concepts defined in the reviewed proposals. Table 5 contains the dimensions proposed for the maturity model and their respective definitions. We included the five dimensions of the Cybersecurity Capability Maturity Model, as they cover the organization holistically, from the organization's perspective, not only considering the technical perspective but also covering aspects such as organizational culture, risk management, and compliance.

However, some domains within information security are essential and hidden within the Oxford model. To give more importance to these domains, we defined eight other dimensions in our proposal. These integrate the dimensions proposed by the different approaches and must be detailed to better support organizations' maturity analyses. Table A2 in the Appendix B summarize the domains found. The columns represent the domains of the proposed model, while the rows correspond to the domains defined in the models analyzed. Each mark indicates in which domain of our model the domains of the models studied in the systematic mapping are present.

It is important to remember that each organization has its own Information Security needs and challenges. Hence, assessing a wide range of dimensions is necessary to obtain a complete and accurate picture of its security maturity level. Selecting the correct dimensions ensures that the model is broad enough to cover all essential areas but, at the same time, specific enough to provide a detailed and accurate assessment.

Our proposal examines 13 dimensions of information security to assess an organization's security maturity level fully. Including the dimensions proposed by the Oxford model and other additional dimensions can provide a more detailed and precise assessment to better support organizations' maturity analyses.

Our proposal, which is illustrated in Figure 5, summarizes the dimensions and domains of the Oxford and C2M2 Information Security Maturity Models. This framework can be used by public institutions, particularly those with limited budgets, to prioritize their efforts and improve their maturity level in Information Security.

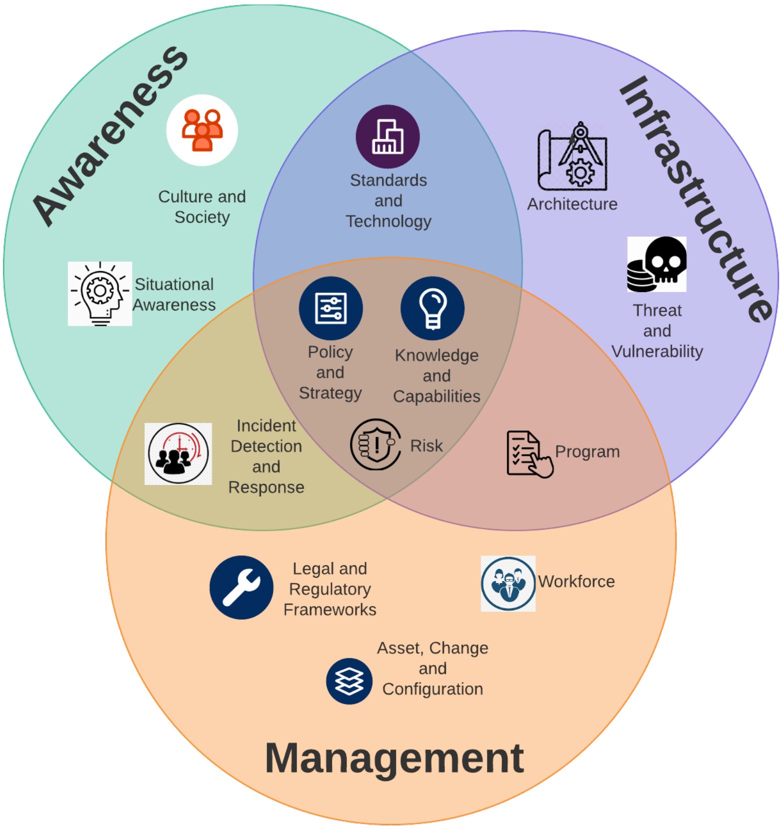

Figure 5. Awareness—Infrastructure—Management (AIM) Triad.

For instance, a public university or educational institution may need to prioritize Awareness in the CySec-AIM Triad. The process of achieving information security is a journey that begins with developing knowledge, capabilities, policies, strategies, and risk assessment. By allocating resources to improve in these areas, one can achieve a higher level of maturity in information security. Then, in the subsequent stage, the institution can focus on Incidence Detection and Response and compliance with Standards and Technology while advancing maturity in the Management and Infrastructure clusters. Finally, the institution can attain Awareness maturity by following the path towards Situational Awareness, along with the impact on Culture and Society. Thus, the model offers an ordered adaptation of maturity models that aligns more closely with the institution's unique characteristics, which could differ from those of an entity focused on Infrastructure. If a public institution dealing with Critical Infrastructure needs to improve its maturity levels, it will follow a different path. Governmental institutions such as ministries would be more inclined toward the Management aspects of their mission, hence requiring a different prioritization.

Table 5. Dimensions and their definitions of the proposed Maturity Model.

Dimensions	**Description**
Culture and Society	Refers to the culture and values of an organization and its impact on cyber security. It is about how an organization promotes and fosters cyber security awareness among its employees, suppliers, and customer.
Situational Awareness	Ability of an organization to detect, analyze and understand cybersecurity risks and threats in real-time and at different levels of the organization.
Standards and Technology	Use of established cybersecurity standards and technologies to protect an organization's systems and data.
Architecture	Refers to designing and implementing a secure and robust technology infrastructure to protect an organization's assets and data. Security architecture ranges from network and system protection to data and application security.
Threat and Vulnerability	An organization's ability to identify, assess and mitigate the security risks associated with the threats and vulnerabilities it faces.
Program	Refers to an organization's cybersecurity strategy and planning. An effective cyber security program should be aligned with the organization's business objectives, identify critical assets and associated risks, and establish policies and procedures for cyber security management. It should also include the designation of a cybersecurity team and the assignment of clear roles and responsibilities.
Workforce	The set of employees and contractors of an organization who have access to systems and data critical to the operation of the business. This includes workers who handle information technology and security and employees who do not work directly in those areas but still have access to confidential systems and data.
Asset, Change, and Configuration	Refers to the management and control of an organization's information technology assets, as well as the management of changes and configurations of these assets. Assets include all systems, applications, data, and network components critical to an organization's business. Asset management involves the identification, classification, and prioritization of assets, as well as the ongoing monitoring and maintenance of assets. In addition, asset management also includes the safe disposal of assets at the end of their life cycle.
Legal and regulatory Framework	Refers to laws and regulations governing information security and data privacy in a particular jurisdiction. These laws and regulations may come from various sources, such as government, industry, or the private sector, and compliance with them is mandatory for organizations operating in that jurisdiction.
Incident detection and response	An organization's ability to detect, respond to, and recover from cybersecurity incidents. This includes early identification of potential security threats, rapid and effective response to incidents, and recovery of affected systems and data.
Policy and Strategy	Refers to an organization's ability to establish clear and effective policies and strategies for information security and cybersecurity management. This includes defining security objectives, identifying risks and threats, and creating policies and procedures to manage and mitigate these risks. The importance of "Policy and Strategy" in a CMM is that well-defined and communicated policies and strategies are the foundation for effective information security and cybersecurity management.
Knowledge and capabilities	Refers to an organization's ability to have a thorough understanding of information security and cybersecurity and to develop and maintain the skills and capabilities necessary to protect the organization's systems and data. The importance of "Knowledge and capabilities" in a CMM lies in the fact that an organization can only be as secure as its personnel's cybersecurity skills and knowledge.
Risk	Refers to an organization's ability to identify, assess and manage the risks associated with information security and cybersecurity. The importance of "Risk" in a CMM is that risk management is essential to ensure that the organization can adequately protect its information assets and minimize the impact of potential security breaches.

As shown in Figure 5, our proposal provides a grouping of domains into three main groups: (i) Awareness, (ii) Infrastructure, and (iii) Management. This grouping allows the institution to have a first approximation of the domains it should emphasize, depending on its need to advance in any aspects defined by these three classifications. In other words, if the organization must or wishes to progress in Infrastructure according to its particular conditions, then the domains in this classification should be prioritized.

On the other hand, if the organization wishes to consider progress in more than one category, e.g., Awareness and Management, the domains at the intersection of the two classifications should be prioritized. Therefore, if the organization wishes to advance in an integrated way in all three classifications, the domains at the intersection of the three categories should be prioritized.

To apply our proposal, we present below a general approach to the process an organization should follow to prioritize its progress in achieving a Security Maturity Model. As shown in Figure 6, the proposal is presented as a process of continuous improvement, which is defined in three major stages in an iterative manner, in such a way as to generate partial progress, if necessary, until the overall goal established by the organization is achieved.

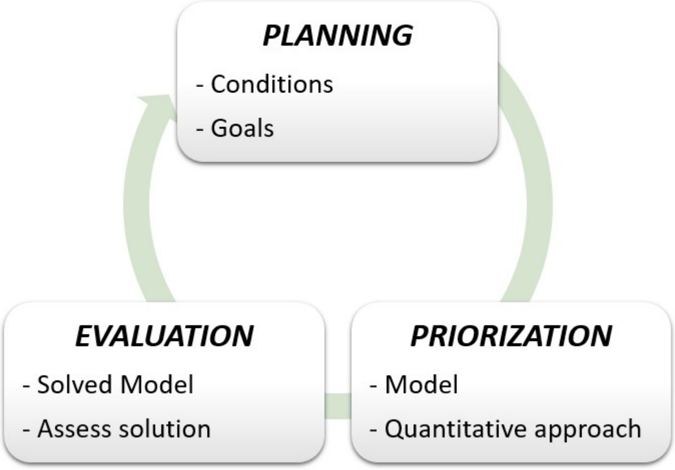

Figure 6. Prioritization cycle.

This iterative process can then be described as follows:

- Planning: At this stage, the organization must define a baseline regarding its current situation regarding its subscribed model. In addition, the organization needs to identify the goals they want to accomplish through the prioritization project. These objectives must be realistic and achievable, i.e., consistent with the characteristics and constraints to which the organization is subject. These objectives should reflect the organization's goal, defining the areas or categories in which it wishes to progress. Similarly, the organization should identify its constraints in implementing the actions the maturity model recommends.
  At this point, when the organization sets the expected objectives to be achieved, the categories of the AIM Triad must be prioritized, and the levels of importance or relative weights of each element to be considered in the subsequent analysis must be determined. This first prioritization approach should consider the organization's particular characteristics and goals that should be considered for the following prioritization.
- Prioritization: In this stage, the prioritization model is determined to achieve the objectives described and consider the constraints and the organization's current baseline. The model is supported by the definitions made in the previous stage, taking into account the first prioritization approach based on the selection of the elements of the AIM Triad. The construction of this model can be supported by quantitative mathematical prioritization techniques such as those proposed in [46]. This model reflects what the organization wants to achieve, and its resolution will determine the recommended priorities according to the conditions of the organization.

There are several quantitative mathematical techniques for dealing with a prioritization problem. Each method tackles issues with distinctive characteristics and applies to various contexts and problems. For this case, we propose maintaining the classification of prioritization scenarios proposed in [46]. As shown in Table 6, we detail the two possible scenarios that the organization may face. Each scenario establishes a prioritization model to be implemented and solved.

The first scenario is related to those cases in which the organization wishes to establish levels of prioritization of security elements without defining any restriction or limitation of resources. In this case, the cost of implementing the controls and the benefits reported by this implementation correspond to the sums of all the individual components without considering the synergies between them. In this case, the problem consists of classifying the security elements according to their characteristics to help the decision-maker choose the ones he wants to implement. Then, the classification problem is multidimensional because each control has several associated factors, such as investment, operational cost, duration and difficulty of implementation, and the resulting benefits.

The second scenario corresponds to a situation in which organizations not only wish to determine a prioritized ranking of security elements but also seek to determine a sequence of implementation. This second scenario can be divided into three possible situations: (i) In the first case, implementation is sequential, i.e., one security element at a time. In this case, the implementation time of each element is not relevant since the total time is independent of them, i.e., the total time will always be the same regardless of the order of implementation of the controls; (ii) A second case considers sequential implementation but now the implementation times are relevant, so the order of implementation is important; (iii) a third case considers parallel implementation, not sequential.

- Evaluation: Finally, the model is solved at this stage, and the prioritization recommendation is obtained. In addition, the answer received is reviewed, and the relevance of the recommendation about the proposed objectives is evaluated. If this answer is inconsistent with the goals, the model can be re-evaluated, and a new recommendation can be executed.

Table 6. Prioritization scenarios and their solution methods.

Scenario	Method	Objective
Multidimensional ranking of controls	[47,48]	Prioritization
Sequencing of independent controls	[49–51]	Prioritization—Sequencing

7. Limitations of the Study

The approach presented in this study follows a well-established methodology in the literature for developing maturity models. Its objective was to create a validated procedure to establish a prioritization strategy for attaining Information Security maturity in Public Institutions. This strategy considers the unique characteristics of these institutions in terms of management and resources. However, it is important to acknowledge that the proposed procedure may have limitations as it might need to be more specific and address the specific challenges faced by individual public or governmental organizations.

The effectiveness of the suggested prioritization strategy may be affected by the variety of traits and individual situations in Public Institutions. While we have tried to account for variations in management and resources, it is crucial to identify any institutions that may require additional support or specific attention to fully address their needs within this proposal.

Our proposed strategy for information security may not cover all necessary aspects for evaluating a public organization, as a more thorough research and review process could have identified additional critical dimensions. Therefore, it is crucial to recognize the limitations of our proposal and continue exploring and updating it as new research and technologies emerge.

To ensure the accuracy and impartiality of our findings, we sought to minimize interpretation errors and biases in our study by adopting measures that involve multiple validation stages and criteria to identify potential inconsistencies or mistakes in the data.

Furthermore, we created visual aids to help analyze and comprehend the results. These aids allowed us to identify patterns and relationships that may have been missed during individual data reviews, eventually leading to the design of the AIM Triad.

In conclusion, we employed various methods to reduce errors in interpreting the data and study outcomes, including our research group's individual assessments and visual aids to facilitate information analysis.

8. Conclusions and Future Work

Information security maturity, as assessed by any available maturity model, can be a hard target to reach since the needs and constraints of a given public institution can significantly differ from another, thus resulting in the need to follow different paths toward maturity. As a result, while maturity models provide snapshots of the information security status at a given moment, as well as identifying areas of improvement, the journey to maturity may vary substantially from one institution to another if the characteristics of the institution subject to evaluation is considered. Thus, the AIM Triad provides an overview of the possible paths that may be taken along this road. Since we did not introduce metrics for evaluating the impact of different choices, a comprehensive quality assessment cannot be derived yet at this stage. This aspect will be the subject of a forthcoming article that considers the use of quantitative mathematical models to support recommendations for prioritization.

In this sense, we intend to formalize a methodological proposal for prioritizing the implementation of an information security maturity model in the context of public organizations, by customizing this implementation according to their particular characteristics. This formalization will seek to systematize the prioritization strategy, detailing the artifacts, tools, actors, and products. Secondly, we expect to validate our proposal through quantitative and qualitative techniques, such as expert judgment and adoption studies. Finally, the applicability and effectiveness of the strategy will be tested through case studies in authentic contexts, with data from different public institutions.

Author Contributions: J.H.-D. contributed to the writing and development of the manuscript in all its phases. M.D.-R. contributed to the methodology and discussions. J.F.-L. contributed to the analysis of the results and limitations of the study. C.C. contributed to the review of articles. All authors have read and agreed to the published version of the manuscript.

Funding: This work received partial support from Proyecto DIUFRO DI21-0079 and Proyecto DIUFRO DI22-0043, Universidad de La Frontera, Temuco. Chile.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are extremely grateful to the reviewers for their kind suggestions for improving the overall quality and readability of the paper.

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

Appendix A

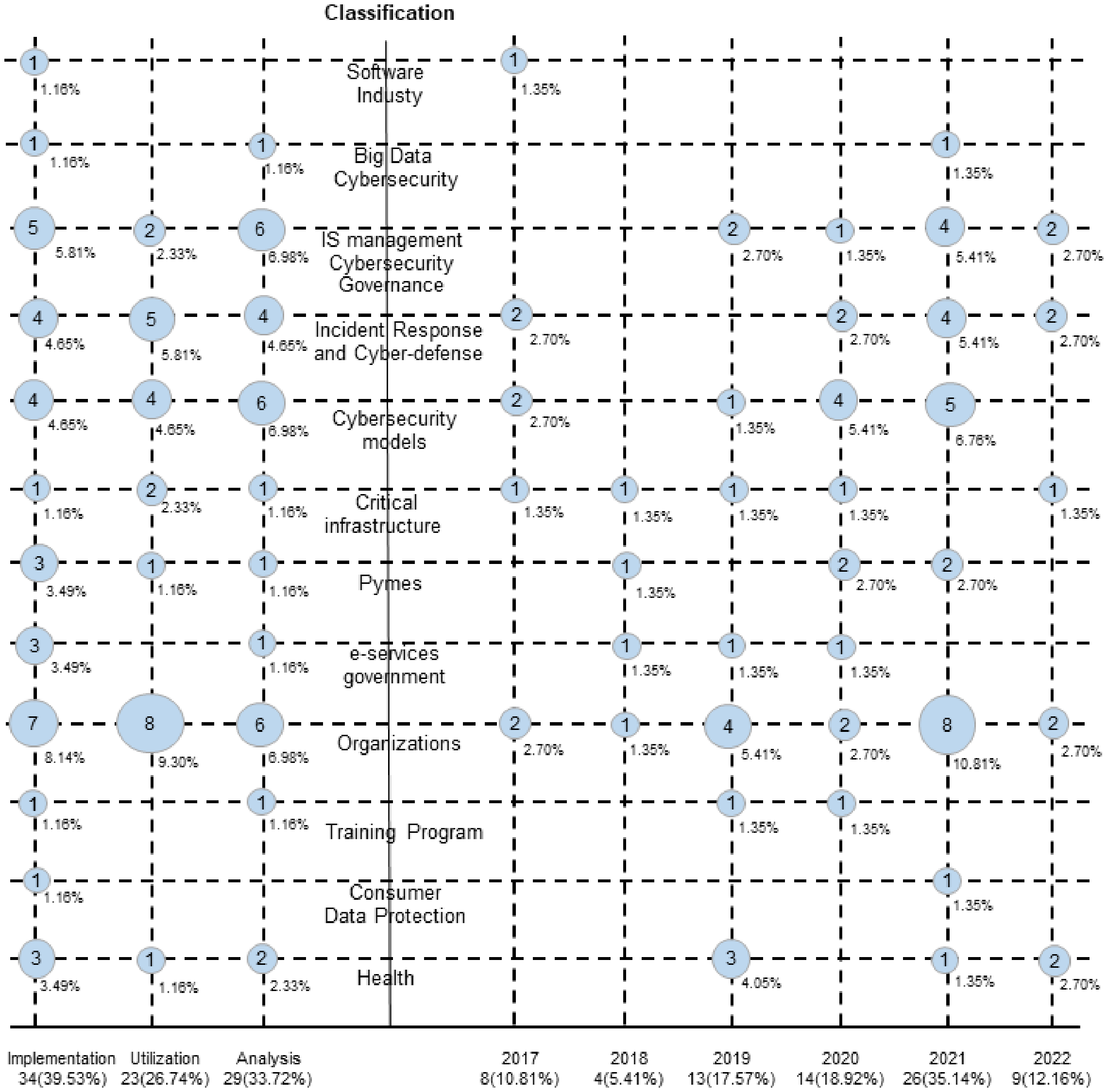

Figure A1. Representation of the systematic mapping.

Table A1. Articles used for analysis and results of systematic mapping.

Num.	Article	Cite	Brief Description
1	A Big Data Maturity Model for Electronic Health Records in Hospitals	[52]	The article discusses the unique security risks of Electronic Health Record (EHR) systems and proposes a new maturity model to assess the security of EHR in hospitals. The proposed approach was evaluated through a case study and received positive results.
2	A Conceptual Consumer Data Protection Maturity Model for Government Adoption: South African Context	[53]	The article proposes a Consumer Data Protection Maturity Model (CDPMM) to help the South African government evaluate the progress of their Consumer Data Protection Framework (CDPF) implementation. The CDPF aims to improve Information Security (IS) compliance awareness among consumers through government-led training initiatives. The CDPMM was developed based on literature and evaluated through expert reviews. The article was published in 2021 by Springer Nature Switzerland AG.

Table A1. *Cont.*

Num.	Article	Cite	Brief Description
3	A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom	[54]	The article suggests a cybersecurity assessment framework for Higher Education Institutes in the UK, which integrates all security and privacy regulations and best practices. The framework can be used for self-assessment or audit purposes and is web-based for benchmarking. Published by MDPI in 2020.
4	A Maturity Model for IT-Related Security Incident Management	[55]	In this study published by Springer Nature Switzerland AG in 2019, a maturity model is validated to measure an organization's ability to escalate IT-related security incidents. Three Swedish health organizations use a self-assessment tool and incident managers are interviewed. The study finds that the model corresponded well with the organization's ability to handle incidents for low and medium maturity levels.
5	A New Adaptive Cybersecurity Capability Maturity Model	[56]	The article proposes a framework using maturity models to evaluate organizational performance and improve the level of security. Maturity models determine the level of maturity achieved using specific criteria and are commonly used to measure an organization's security level. The proposed framework focuses on information security and technology maturity to help organizations achieve their desired state.
6	A proposed maturity model for Himachal Pradesh government e-Services	[42]	The paper proposes a maturity model for the e-services of the Himachal Pradesh government in India, with a focus on accessibility and functionality. It also addresses the major concerns of information security in the e-service portal and provides a proposed solution. The model and solution are intended to help the government improve its e-services and portal security.
7	A structured comparison of the corporate information security maturity level	[57]	This article suggests using a maturity model to measure the level of information security controls in organizations, as a direct measurement is not possible. The analytic hierarchy process (AHP) can be used to compare the level of maturity of information security controls and rank companies. Real data from a large international media and technology company was used to validate the approach.
8	A technological analysis of Colombia's cybersecurity capacity: a systemic perspective from an organizational point of view	[58]	The paper examines Colombia's cybersecurity capacity, specifically incident response and critical infrastructure protection, using a dynamics system paradigm and simulation model. It proposes policies for organizational sensitivity to cybersecurity risks and aims to assist decision-makers in investing in cybersecurity development. However, the study is limited to one organization.
9	Addressing SME Characteristics for Designing Information Security Maturity Models	[59]	The article proposes using maturity models to assess organizational performance and progress towards a desired state, specifically in the area of information security. It suggests a framework for evaluating organizational maturity based on information security and technology maturity. The aim is to help organizations improve their level of security.
10	Adopting security maturity model to the organizations' capability model	[60]	The paper proposes a security maturity model that classifies organizations into five levels based on their technology and process capability. The model helps bridge cybersecurity gaps and assists auditors in measuring the organization's security level and developing automated countermeasures. The authors applied the model in two case studies in Yemen.
11	Advanced approach to information security management system utilizing maturity models in critical infrastructure	[61]	The article proposes an information security maturity model for critical infrastructure, as current methods lack connectivity. The model was tested on the thermal power sector in the Republic of Korea and can provide useful insights for future research or practical application of infrastructure ISMSs.
12	An Analysis of Assessment Approaches and Maturity Scales Used for Evaluation of Information Security and Cybersecurity User Awareness and Training Programs: A Scoping Review	[31]	This study aims to identify the approaches used to assess information security and cybersecurity user awareness and training programs, with a focus on two objectives: identifying the measurements used to assess program effectiveness and studying the use of maturity models to measure program progress. A Scoping Literature Review was conducted, revealing a gap in the current literature on program assessment, with only five papers and two maturity models addressing the issue.
13	An explanatory review on cybersecurity capability maturity models	[25]	The article discusses the need for updated cybersecurity measures in public and private sectors due to growing cyber threats. CMMs are used to measure an organization's cybersecurity readiness, but the review found that most models lack a validation process and are designed for specific purposes and organization sizes.
14	An extended digital forensic readiness and maturity model	[62]	The study develops a digital forensic maturity assessment model (DFMM) for enterprises by utilizing feedback from forensic experts. The DFMM model was validated through semi-structured interviews, and key changes were introduced to enhance the model. The study provides access to a non-proprietary DFMM maturity model for practitioners, academics, and organizations.

Table A1. *Cont.*

Num.	Article	Cite	Brief Description
15	Application of a fuzzy analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems	[63]	The study proposes a fuzzy analytic hierarchy process (AHP) approach to determine the cyber resilient capability maturity level in the digital supply chain. The proposed method is applied in 9 SME companies to test the assessments, and the result indicates that the identify factor is the most important, followed by protect, detect, respond, recover, and continuity.
16	Assessing information security performance of enterprise internal financial sharing in a cloud computing environment using analytic hierarchy process	[64]	The aim of this work is to improve enterprise efficiency by addressing issues such as high financial costs and low management efficiency. The study proposes an information security maturity model with four indicators: information security strategy, technology, organization, and operation.
17	Assessing the maturity of national cybersecurity and resilience	[65]	Article overview of maturity levels and assessment methodologies for evaluating cybersecurity and resilience. Different maturity models and assessment frameworks are compared and analyzed for their usefulness in designing national cybersecurity strategies and programs to achieve cyber resilience.
18	Assessment of national cybersecurity capacity for countries in a transitional phase: The spring land case study	[66]	The paper discusses the importance of cybersecurity capacity building and presents the results of two qualitative studies using the Cybersecurity Capacity Maturity Model (CCMM) for nations to analyze Spring Land's cybersecurity capacity.
19	Building a Maturity Framework for Big Data Cybersecurity Analytics	[67]	The article proposes a maturity framework for big data cybersecurity analytics. This framework has seven dimensions across five stage levels: organization, human, infrastructure, data management, analytics application, governance, and security.
20	Comparative study of cybersecurity capability maturity models	[68]	The article discusses the common elements among these models and notes that each model has its own unique fields of application. This article aims to provide a comprehensive overview of the most widely used cybersecurity capability maturity models. © Springer International Publishing AG 2017.
21	CTI-SOC2M2-The quest for mature, intelligence-dr iven secur ity operations and incident response capabilities	[69]	This article discusses the importance of cyber threat intelligence (CTI) and its sharing to cope with advanced threats and strongly influence security capabilities.
22	Current cybersecurity maturity models: How effective in the healthcare cloud?	[70]	The study presents a literature review of maturity models for cloud security assessment in healthcare and argues the need for a cloud security maturity model for healthcare organizations.
23	Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios	[71]	The article describes the Secure and PrivatE smArt gRid (SPEAR) Horizon 2020 project's development of a Cyber Hygiene Maturity assessment Framework (CHMF) for Smart Grids. The CHMF is designed to evaluate the Cyber Hygiene Level (CHL) of Smart Grids against common and unexpected threats, and to provide a cyber-health check for Smart Grid operator organizations.
24	Cybercrimes and defense approaches in vehicular networks	[72]	The chapter focuses on the challenges of securing defense systems and identifying information leakage and sharing points. It discusses the expansion of defense networks, the resulting security challenges, and various cyberattacks commonly found in defense networks.
25	Cybercriminal approaches in big data models for automated heavy vehicles	[73]	The chapter provides a comparative analysis of cybersecurity maturity models and introduces major classes of automated heavy vehicles, recent trends, driver assistance facilities, wireless networks, and cyberattacks on vehicle infrastructure.
26	Cybersecurity for railways – A maturity model	[74]	The chapter highlights the increasing frequency and severity of cyber-attacks in various sectors, including railways, and the need to move towards advanced security analytics and automation to prevent security breaches.
27	Cybersecurity for the Smart Grid	[75]	This article provides an overview of cybersecurity principles for the smart grid, including cyber-physical security and specific models such as the Electricity Subsector Cybersecurity Capability Maturity Model.
28	Cybersecurity maturity assessment of a critical infrastructure organisation—approach and obsvervations	[76]	The paper presents an assessment approach that includes semi-structured interviews, NIST cybersecurity framework, responsibility assignment matrix, and maturity model to collect and analyze data on people, process, and technology aspects of cybersecurity.

Table A1. *Cont.*

Num.	Article	Cite	Brief Description
29	Cybersecurity maturity model for providing services in the financial sector in Peru	[77]	The paper proposes a CMM for the financial sector, including cloud security and privacy capabilities, measured on a 5-level maturity scale. It was validated with pilot studies in two financial entities, showing an average acceptance level of 4.3 and maturity level of 3. Preliminary results were used to propose activities to eliminate gaps and improve capabilities.
30	Cybersecurity maturity model for the Brazilian Federal Government Agencies	[44]	This paper presents a CMM for Brazilian Federal Public Administration agencies. The model was developed through qualitative research analyzing existing models and using content analysis to set the model domains. An online questionnaire was used to apply the model to 35 agencies, revealing low cybersecurity maturity.
31	Cybersecurity workforce in railway: its maturity and awareness	[78]	This research paper evaluates cybersecurity maturity and awareness risk in railway transportation using two models: Railway-Cybersecurity Capability Maturity Model (R-C2M2) and Information Security Awareness Capability Model (ISACM).
32	Developing a cyber counterintelligence maturity model for developing countries	[79]	The paper proposes designing a cyber counterintelligence maturity model specifically for developing countries by discussing basic concepts of frameworks and maturity models and how they are utilized in developed countries for cybersecurity.
33	Development of Cyber Resilient Capability Maturity Model for Cloud Computing Services	[80]	This research aimed to develop a cyber resilient model and maturity model, as well as a self-assessment model for the cyber resilient capability of cloud computing services. The researchers used NIST cybersecurity concepts and conducted in-depth interviews, focus-group discussions with experts, and data collection from cloud service providers.
34	Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems	[81]	This paper proposes a cybersecurity capability readiness level system to assess the readiness status of cybersecurity systems for use. It compares and contrasts the existing readiness level systems and the CMM and proposes a new system based on the Technology Readiness Level (TRL) system. The paper defines and discusses the new system's levels.
35	Evaluation model of the access control domain of the ISO 27002 standard applied to the database management process	[82]	This study analyzed the vulnerabilities of the Database Management process in two institutions using the ISO 27002 access control domain and ISM3 maturity model. Four categories with 14 questions were established and evaluated through interviews, observations, and technical tests.
36	Incorporating Systems Thinking into a Cyber Resilience Maturity Model	[83]	The authors propose a systems thinking approach to cyber resilience, considering critical infrastructure and services as a system of systems.They suggest exploring cyber resilience as a system property and discuss dimensions of operation and domains of practice that are embedded in a sectoral cyber resilience maturity model.
37	Information and cybersecurity maturity models: a systematic literature review	[20]	This paper addresses the lack of maturity and convergence in information security maturity evaluation by using a systematic literature review to identify gaps in existing research. The authors highlight the influence of ISO/IEC 27001/27002 and the need for further investigation into ISO 21827.
38	Information security management systems—A maturity model based on ISO/IEC 27001	[84]	This paper proposes a maturity model for ISMS planning, implementation, monitoring, and improvement based on ISO/IEC 27001. The model is an assessment tool for organizations to determine their current ISMS maturity level and develop an improvement plan based on best practices to reach their target maturity level. The model's effectiveness is evaluated through a multi-step perspective.
39	Information Security Maturity Model for Healthcare Organizations in the United States	[85]	This article presents a maturity model for improving information security in healthcare organizations in the US. The model includes specific performance metrics with relative importance measures to prioritize resources and mitigate the most significant security threats.
40	Information Security Multiprofile Maturity Model (ISM3)	[86]	This paper presents the Multiple Profile Model of Information Security Maturity (ISM3) which generates Individual Information Security Profiles (PISI). ISM3 is flexible and based on best practices and regulatory frameworks such as NIST, ISO, COBIT, and ITIL. The accompanying software tool generates PISIs for specific industries, entities, and subdivisions, with target values and specific metrics for criteria measurement.
41	Information Systems Maturity Level Assessment using the HISMM Framework: Case Study of State Hospital in Jakarta	[87]	This study evaluates the maturity level of the Information System in a hospital using the Healthcare Information System Maturity Model (HISMM) framework. The investigation was conducted by analyzing six relevant dimensions: Data Analysis, Strategy, People, Electronic Medical Records, Information Security, and IT Infrastructure System.

Table A1. *Cont.*

Num.	Article	Cite	Brief Description
42	Internet financial security based on big data	[88]	The paper aims to analyze internet financial enterprises' internal and external security challenges, identify information security risks and protection strategies to help improve information security construction. The authors use H Internet financial enterprises as a case study to assess the information security status and shortcomings and derive an optimization protection strategy.
43	ISFAM 2.0: Revisiting the information security assessment model	[89]	The paper discusses the importance of having an information security maturity model tailored to each organization's organizational profile. It highlights the need for a well-fitted information security maturity model to support an organization fully.
44	Maturity Concept and Model Review	[90]	The paper discusses the importance of measuring and evaluating activities and processes to manage and improve them, particularly in information security management. It introduces the concept of a maturity model and briefly reviews existing models.
45	Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities	[91]	The use of maturity models to measure information security is widespread, but the quality of maturity level assessments has not been adequately investigated. This study aimed to analyze the accuracy of security managers' ability to assess maturity levels of security controls using the COBIT maturity levels.
46	Maturity Model of Information Security for Software Developers	[92]	The paper discusses the need for software developers to protect their own information and their customers' information. ISO 27001 is currently the most widely recognized standard for information security procedures. The paper presents an information security maturity model based on ISO 27001 designed for software developers.
47	Maturity models in cybersecurity: A systematic review [Modelos de Madurez en Ciberseguridad: una revisión sistemática]	[24]	Based on a systematic review of studies published from 2012 to 2017, this study aimed to determine the most commonly used CMM. Out of 201 articles found that mentioned different maturity models, 12 primary articles were selected to identify the most used models.
48	Maturity of information systems security in selected private Banks in Ethiopia	[93]	The paper discusses the importance of information system security in organizations and the need to determine the maturity level of information security governance. It focuses on a study to measure the information system security maturity level of private banks in Ethiopia using the SSE-CMM maturity model and ISO/IEC 27001 information security control areas.
49	Method for Designing Countermeasures for Crypto-Ransomware Based on the NIST CSF	[94]	This paper proposes a method for designing countermeasures to address the growing problem of crypto-ransomware attacks. The proposed model is based on the NIST 800-53 revision 4 standard and the Information Security Maturity Model published by ISACA in the COBIT Focus magazine.
50	Modelling adaptive information security for SMEs in a cluster	[95]	The paper presents a method for adapting an Information Security Focus Area Maturity (ISFAM) model to the organizational characteristics (OCs) of a small- and medium-sized enterprise (SME) cluster.
51	Novel Maturity Model for Cybersecurity Evaluation in Industry 4.0	[96]	This paper focuses on the need for adequate IT security measures in the manufacturing industry in the context of Industry 4.0. As networking in the production environment increases, the number of attack surfaces also increases, making cybersecurity a critical concern for companies.
52	Organisational Information Security Management Maturity Model	[97]	The paper discusses the importance of Information Security Management (ISM) in protecting the confidentiality, integrity, and availability of information in organizations. Despite compliance with ISM requirements, many organizations continue to suffer from security incidents, indicating low maturity levels in ISM implementation.
53	Personal data protection maturity model for the micro financial sector in Peru	[98]	The microfinance sector is crucial for the economic development of developing countries, as it promotes the integration and growth of all social classes. With the increasing volume of data generated by transactions and operations in this sector, it is important to manage personal data privacy policies effectively to comply with regulations, make informed decisions, and improve processes.
54	Security maturity model of web applications for cyber attacks	[99]	Given the projected increase in cyberattacks on the healthcare sector and the lack of widely available security maturity models with post-evaluation monitoring, there is a need to propose a simple and applicable security maturity model for web applications against cyberattacks in the healthcare sector. This proposed model will be based on the International Professional Practice Framework.

Table A1. *Cont.*

Num.	Article	Cite	Brief Description
55	Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level	[43]	The weakness of employees in organizations remains a significant vulnerability despite millions spent on high-level security systems. Lack of training and expertise can result in cybercrime, and a shortage of qualified cyber-security staff further exacerbates the problem. A semi-automated risk assessment framework and security maturity model based on ISO 27001 and relevant standards are proposed to address this issue, which can help auditors, security officers and managers.
56	Smart Secure: A Novel Risk-based Maturity Model for Enterprise Risk Management during Global Pandemic	[100]	The authors propose a CMM called 'Smart Secure' to guide security leaders in risk-based cybersecurity management. The model helps distribute resources based on the criticality of the application, resulting in efficient cybersecurity funding and improved overall cybersecurity posture for the organization.
57	Steps to design a maturity model with an agile framework for the implementation of IT security management systems aligned to the policies of the Colombian government for the public sector	[101]	Currently, public sector companies may struggle with implementing and measuring the maturity of their information security and privacy models, despite having them in place. This proposal offers guidelines and steps to design a maturity model based on an agile framework that can be adapted to their specific needs and resources. The process follows an exploratory methodology in phases to achieve the proposed outcome.
58	The cybersecurity governance in changing the security psychology and security posture: Insights into e-procurement	[102]	This study aims to identify effective practices for cybersecurity governance by examining and synthesizing existing CMMs and frameworks from the literature and industry. The study analyzed and compared prominent cybersecurity maturity models, such as the Cybersecurity Governance Maturity Model (CSGMM) and Cyber Preparedness (Cyber Prep) framework, and identified 12 practical measures for effective cybersecurity governance for manufacturing firms.
59	Towards a cyber counterintelligence maturity model	[103]	This paper argues for a new approach to cyber security that incorporates Cyber Counterintelligence (CCI) as a core component. The paper explores the need for CCI practices in both government and private business, and argues for the effectiveness of a multi-disciplinary and integrated CCI approach. It discusses the need for a CCI maturity model and proposes an appropriate CCI framework as the underlying basis for such a model.
60	Towards an information security awareness maturity model	[104]	The continuous improvement of Information Security Awareness (ISA) is important and can be assessed using Maturity Models (MM). The Integrated Behavioral Model (IBM), which includes knowledge, attitude, and habit, was used as a definition of ISA in a research project. A systematic literature review was conducted to determine if a MM based on the IBM can be defined to assess ISA maturity. However, no existing MM for information security considers all aspects of the IBM, unlike MM in other fields that deal with human factors.

Appendix B

Table A2. Classification of the maturity models domains.

	Goal	**Culture and Society**	**Situational Awareness**	**Standards and Technology**	**Architecture**	**Threat and Vulnerability**	**Program**	**Workforce**	**Asset, Change, and Configuration**	**Legal and Regulatory Framework**	**Incident Detection and Response**	**Policy and Strategy**	**Knowledge and Capabilities**	**Risk**
SP-CMM	Secure Engineering and Architecture				✓									
	Asset Management			✓					✓					
	Business Continuity and Disaster Recovery				✓		✓				✓			
	Change Management								✓					
	Configuration Management								✓					
	Continuous Monitoring								✓		✓			
	Incident Response										✓			
	Compliance			✓						✓				
	Security and Privacy Governance			✓						✓		✓		
	Security Awareness and Training	✓	✓					✓					✓	
	Risk Management													✓
	Vulnerability and Patch Management					✓					✓			
	Human Resources Security	✓	✓					✓						
	Assurance					✓			✓					
	Capacity and Performance Planning						✓							
	Cloud Security				✓									
	Cryptographic Protections					✓								
	Data Classification and Handling								✓					
	Embedded Technology			✓					✓					
	Endpoint Security					✓			✓					
	Identification and Authentication					✓		✓	✓					
	Maintenance						✓							
	Mobile Device Management								✓					
	Network Security					✓			✓					
	Physical and Environmental Security								✓	✓				✓
	Privacy							✓		✓				
	Project and Resource Management						✓	✓	✓					
	Security Operations			✓			✓	✓	✓					
	Technology Development and Acquisition			✓					✓	✓				
	Threat Management					✓			✓					
	Third-Party Management					✓			✓	✓				
	Web Security				✓	✓			✓					
OC2M2	Cybersecurity Policy and Strategy											✓		
	Cybersecurity Culture and Society	✓												
	Cybersecurity Knowledge and Capabilities												✓	
	Legal and Regulatory Frameworks									✓				
	Standards and Technologies			✓										

Table A2. *Cont.*

	Goal	Culture and Society	Situational Awareness	Standards and Technology	Architecture	Threat and Vulnerability	Program	Workforce	Asset, Change, and Configuration	Legal and Regulatory Framework	Incident Detection and Response	Policy and Strategy	Knowledge and Capabilities	Risk
C2M2	Cybersecurity Architecture				✓									
	Asset, Change and Configuration Management								✓					
	Event and Incident Response, Continuity of Operations										✓			
	Situational Awareness		✓											
	Risk Management													✓
	Third-Party Risk Management													✓
	Threat and Vulnerability Management					✓								
	Workforce Management							✓						
	Identity and Access Management					✓		✓	✓					
	Cybersecurity Program Management						✓							
NIST CSF	Asset Management			✓										
	Governance						✓			✓		✓		
	Awareness and Training	✓	✓										✓	
	Risk Assessment													✓
	Risk Management													✓
	Access Control					✓		✓	✓					
	Business Environment									✓		✓		
	Data Security			✓		✓				✓		✓		
	Information Protection Processes and Procedures			✓	✓									
[44]	Asset Management								✓					
	Continuity Management										✓			
	Cybersecurity Governance											✓		
	Training, Awareness, and Culture	✓	✓										✓	
	Risk Management													✓
	Threat and Vulnerability Management					✓								
	Access Management					✓		✓	✓					
	Information exchange					✓				✓		✓		
	Technological Infrastructure			✓	✓									

References

1. AlGhamdi, S.; Win, K.T.; Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review. *Comput. Secur.* **2020**, *99*, 102030. [CrossRef]
2. Yang, L.; Elisa, N.; Eliot, N. Privacy and security aspects of E-government in smart cities. In *Smart Cities Cybersecurity and Privacy*; Elsevier: Amsterdam, The Netherlands, 2019; pp. 89–102.
3. Diéguez, M.; Cares, C.; Cachero, C.; Hochstetter, J. MASISCo—Methodological Approach for the Selection of Information Security Controls. *Appl. Sci.* **2023**, *13*, 1094. [CrossRef]
4. Andersen, K.V.; Henriksen, H.Z. E-government maturity models: Extension of the Layne and Lee model. *Gov. Inf. Q.* **2006**, *23*, 236–248. [CrossRef]
5. Canetta, L.; Barni, A.; Montini, E. Development of a digitalization maturity model for the manufacturing sector. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; pp. 1–7.
6. Lemke, F.; Taveter, K.; Erlenheim, R.; Pappel, I.; Draheim, D.; Janssen, M. Stage models for moving from e-government to smart government. In Proceedings of the International Conference on Electronic Governance and Open Society: Challenges in Eurasia; Springer: Berlin/Heidelberg, Germany, 2019; pp. 152–164.

7. Goncalves Filho, A.P.; Waterson, P. Maturity models and safety culture: A critical review. *Saf. Sci.* **2018**, *105*, 192–211. [CrossRef]
8. Hochstetter, J.; Díaz, J.; Diéguez, M.; Espinosa, R.; Arango-López, J.; Cares, C. Assessing Transparency in eGovernment Electronic Processes. *IEEE Access* **2021**, *10*, 3074–3087. [CrossRef]
9. Valdés, G.; Solar, M.; Astudillo, H.; Iribarren, M.; Concha, G.; Visconti, M. Conception, development and implementation of an e-Government maturity model in public agencies. *Gov. Inf. Q.* **2011**, *28*, 176–187. [CrossRef]
10. Luna-Reyes, L.F.; Gil-Garcia, J.R.; Romero, G. Towards a multidimensional model for evaluating electronic government: Proposing a more comprehensive and integrative perspective. *Gov. Inf. Q.* **2012**, *29*, 324–334. [CrossRef]
11. Ifenthaler, D.; Egloffstein, M. Development and implementation of a maturity model of digital transformation. *TechTrends* **2020**, *64*, 302–309. [CrossRef]
12. Proença, D.; Borbinha, J. Maturity models for data and information management. In Proceedings of the International Conference on Theory and Practice of Digital Libraries, Porto, Portugal, 10–13 September 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 81–93.
13. Gouscos, D.; Kalikakis, M.; Legal, M.; Papadopoulou, S. A general model of performance and quality for one-stop e-government service offerings. *Gov. Inf. Q.* **2007**, *24*, 860–885. [CrossRef]
14. Bilak, S.; Brennan, K. *Cybersecurity Capability Maturity Model (C2M2)-Cybersecurity Maturity Model Certification (CMMC) Supplemental Guidance (Draft)*; Technical Report; Carnegie-Mellon University: Pittsburgh, PA, USA, 2022.
15. U.S. Department of Energy. *Cybersecurity Capability Maturity Model (C2M2)*; U.S. Department of Energy: Washington, DC, USA, 2020.
16. National Institute of Standards and Technology. NIST Cybersecurity Framework. 2022. Available online: https://www.nist.gov/cyberframework/framework (accessed on 10 July 2023).
17. Carnegie Mellon University Software Engineering Institute. *Security & Privacy Capability Maturity Model (SP-CMM)*; Version 2.0; Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA, USA, 2001.
18. ISACA. *CMMI Cybermaturity Platform*; ISACA: Schaumburg, IL, USA, 2023.
19. Hochstetter, J.; Vairetti, C.; Cares, C.; Ojeda, M.G.; Maldonado, S. A transparency maturity model for government software tenders. *IEEE Access* **2021**, *9*, 45668–45682. [CrossRef]
20. Rabii, A.; Assoul, S.; Touhami, K.O.; Roudies, O. Information and cyber security maturity models: A systematic literature review. *Inf. Comput. Secur.* **2020**, *28*, 627–644. [CrossRef]
21. Pazmiño Vallejo, L.M. Calidad de la Gestión en la Seguridad de la Información Basada en la Norma ISO/IEC 27001, en Instituciones Públicas, en la Ciudad de Quito DM. Master's Thesis, PUCE, Quito, Ecuador, 2015.
22. Moumen, M.; Elaoufir, H. An integrated management system: From various aspects of the literature to a maturity model based on the process approach. *Int. J. Product. Qual. Manag.* **2018**, *23*, 218–246. [CrossRef]
23. Lin, T.C.; Wang, K.J.; Sheng, M.L. To assess smart manufacturing readiness by maturity model: A case study on Taiwan enterprises. *Int. J. Comput. Integr. Manuf.* **2020**, *33*, 102–115. [CrossRef]
24. Rea-Guamán, A.M.; Sanchez-Garcia, I.; San Feliu, T.; Calvo-Manzano, J. Maturity models in cybersecurity: A systematic review. In Proceedings of the 2017 12th Iberian Conference on Information Systems and Technologies (CISTI), Lisbon, Portugal, 14–17 June 2017; pp. 1–6.
25. Garba, A.A.; Siraj, M.M.; Othman, S.H. An explanatory review on cybersecurity capability maturity models. *Adv. Sci. Technol. Eng. Syst. J.* **2020**, *5*, 762–769. [CrossRef]
26. Lopes, D.; Carvalho, J.V.; Gonçalves, C.T. Maturity Models as Instruments for the Optimization of Electronic Business in the Tourism Industry. In Proceedings of the International Conference on Tourism, Technology and Systems, Cartagena, Colombia, 29–31 October 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 278–287.
27. Kettl, D.F. The transformation of governance: Globalization, devolution, and the role of government. *Public Adm. Rev.* **2000**, *60*, 488–497. [CrossRef]
28. Ismagilova, E.; Hughes, L.; Rana, N.P.; Dwivedi, Y.K. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Inf. Syst. Front.* **2020**, *24*, 393–414. [CrossRef]
29. Poeppelbuss, J.; Niehaves, B.; Simons, A.; Becker, J. Maturity models in information systems research: Literature search and analysis. *Commun. Assoc. Inf. Syst.* **2011**, *29*, 27. [CrossRef]
30. Gollhardt, T.; Halsbenning, S.; Hermann, A.; Karsakova, A.; Becker, J. Development of a digital transformation maturity model for IT companies. In Proceedings of the 2020 IEEE 22nd Conference on Business Informatics (CBI), Antwerp, Belgium, 22–24 June 2020; Volume 1, pp. 94–103.
31. Muronga, K.; Herselman, M.; Botha, A.; Da Veiga, A. An analysis of assessment approaches and maturity scales used for evaluation of information security and cybersecurity user awareness and training programs: A scoping review. In Proceedings of the 2019 Conference on Next Generation Computing Applications (NextComp), Balaclava, Mauritius, 19–21 September 2019; pp. 1–6.
32. von Solms, B.; Upton, D. Cyber security capacity governance. *Bus. Manag. Rev.* **2016**, *7*, 34.
33. Foster, C. Why NIST CSF Maturity Is Important for All Organizations. 2022. Available online: https://blog.charlesit.com/why-nist-csf-maturity-is-important-for-all-organizations (accessed on 10 July 2023).
34. Becker, J.; Knackstedt, R.; Pöppelbuß, J. Developing maturity models for IT management. *Bus. Inf. Syst. Eng.* **2009**, *1*, 213–222. [CrossRef]

35. Sandoval-Almazan, R.; Gil-Garcia, J.R. Are government internet portals evolving towards more interaction, participation, and collaboration? Revisiting the rhetoric of e-government among municipalities. *Gov. Inf. Q.* **2012**, *29*, S72–S81. [CrossRef]
36. García-González, A.; Ramírez-Montoya, M.S. Systematic mapping of scientific production on open innovation (2015–2018): Opportunities for sustainable training environments. *Sustainability* **2019**, *11*, 1781. [CrossRef]
37. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Keele, UK; University of Durham: Durham, UK, 2007.
38. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic mapping studies in software engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), Bari, Italy, 26–27 June 2008; pp. 1–10.
39. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. RESEARCH METHODS and REPORTING-Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement-David Moher and colleagues introduce PRISMA, an update of the QUOROM guidelines for reporting systematic reviews and meta-analyses. *BMJ CR-Print* **2009**, *338*, 332.
40. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [CrossRef]
41. James, K.L.; Randall, N.P.; Haddaway, N.R. A methodology for systematic mapping in environmental sciences. *Environ. Evid.* **2016**, *5*, 7. [CrossRef]
42. Kakkar, A.; Rawat, S.; Gupta, P.; Khatri, S.K. A Proposed Maturity Model for Himachal Pradesh Government e-Services. In *Intelligent Computing and Information and Communication*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 643–652.
43. Abazi, B.; Kő, A. Semi-automated Information Security Risk Assessment Framework for Analyzing Enterprises Security Maturity Level. In Proceedings of the Research and Practical Issues of Enterprise Information Systems: 13th IFIP WG 8.9 International Conference (CONFENIS 2019), Prague, Czech Republic, 16–17 December 2019; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 141–152.
44. Azambuja, A.J.; Neto, J.S. Cybersecurity maturity model for the Brazilian Federal Government Agencies. *Rev. Serv. Público* **2020**, *71*, 660–712 . [CrossRef]
45. The Community Cybersecurity Maturity Model (CCSMM). *Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM)*; IGI Global: Hershey, PA, USA, 2021; pp. 1–31. [CrossRef]
46. Diéguez, M.; Bustos, J.; Cares, C. Mapping the variations for implementing information security controls to their operational research solutions. *Inf. Syst. Bus. Manag.* **2020**, *18*, 157–186. [CrossRef]
47. Gass, S.I.; Saaty, T.L. Parametric Objective Function (Part 2)—Generalization. *J. Oper. Res. Soc. Am.* **1955**, *3*, 395–401. [CrossRef]
48. Wierzbicki, A.P. The Use of Reference Objectives in Multiobjective Optimization. In *Lecture Notes in Economics and Mathematical Systems*; Springer: Berlin/Heidelberg, Germany, 1980; pp. 468–486. [CrossRef]
49. Cheng, T.; Ng, C.; Yuan, J.; Liu, Z. Single machine scheduling to minimize total weighted tardiness. *Eur. J. Oper. Res.* **2005**, *165*, 423–443. [CrossRef]
50. Koulamas, C. The single-machine total tardiness scheduling problem: Review and extensions. *Eur. J. Oper. Res.* **2010**, *202*, 1–7. [CrossRef]
51. Edis, E.B.; Oguz, C.; Ozkarahan, I. Parallel machine scheduling with additional resources: Notation, classification, models and solution methods. *Eur. J. Oper. Res.* **2013**, *230*, 449–463. [CrossRef]
52. Daraghmeh, R.; Brown, R. A Big Data maturity model for electronic health records in hospitals. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 826–833.
53. Bredenkamp, I.E.; Kritzinger, E.; Herselman, M. A Conceptual Consumer Data Protection Maturity Model for Government Adoption: South African Context. In *Software Engineering Application in Informatics: Proceedings of 5th Computational Methods in Systems and Software 2021*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 1, pp. 820–834.
54. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
55. Wahlgren, G.; Kowalski, S. A maturity model for IT-related security incident management. In Proceedings of the Business Information Systems: 22nd International Conference (BIS 2019), Seville, Spain, 26–28 June 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 203–217.
56. Ghaffari, F.; Arabsorkhi, A. A new adaptive cyber-security capability maturity model. In Proceedings of the 2018 9th International Symposium on Telecommunications (IST), Tehran, Iran, 17–19 December 2018; pp. 298–304.
57. Schmid, M.; Pape, S. A structured comparison of the corporate information security maturity level. In Proceedings of the ICT Systems Security and Privacy Protection: 34th IFIP TC 11 International Conference (SEC 2019), Lisbon, Portugal, 25–27 June 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 223–237.
58. Patino, A.M.S.; Ramirez, D.P.G. A technological analysis of Colombia's cybersecurity capacity: A systemic perspective from an organizational point of view/Analisis de la capacidad de ciberseguridad para la dimension tecnologica en Colombia: Una mirada sistemica desde la organizacion/Analise da capacidade de seguranca cibernetica para a dimensao tecnologica na Colombia: Uma visao sistemica da organizacao. *Rev. Ing. Solidar.* **2019**, *15*, 1f.
59. Yigit Ozkan, B.; Spruit, M. Addressing SME characteristics for designing information security maturity models. In Proceedings of the Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium (HAISA 2020), Mytilene, Greece, 8–10 July 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 161–174.

60. Al-Matari, O.M.; Helal, I.M.; Mazen, S.A.; Elhennawy, S. Adopting security maturity model to the organizations' capability model. *Egypt. Inform. J.* **2021**, *22*, 193–199. [CrossRef]
61. You, Y.; Oh, J.; Kim, S.; Lee, K. Advanced approach to information security management system utilizing maturity models in critical infrastructure. *KSII Trans. Internet Inf. Syst.* **2018**, *12*, 4995–5014.
62. Taiwo, A.; Claims, I. An extended digital forensic readiness and maturity model. *Forensic Sci. Int. Digit. Investig.* **2022**, *40*, 301348.
63. Uraipan, N.; Praneetpolgrang, P.; Manisri, T. Application of an analytic hierarchy process to select the level of a cyber resilient capability maturity model in digital supply chain systems. *ECTI Trans. Comput. Inf. Technol.* **2021**, *15*, 198–207. [CrossRef]
64. Zhou, X.; Weng, H. Assessing information security performance of enterprise internal financial sharing in cloud computing environment using analytic hierarchy process. *Int. J. Grid Util. Comput.* **2022**, *13*, 256–271. [CrossRef]
65. Sharkov, G. Assessing the maturity of national cybersecurity and resilience. *Connect. Q. J.* **2020**, *19*, 5–24. [CrossRef]
66. Tallón-Ballesteros, A. Assessment of National Cybersecurity Capacity for Countries in a Transitional Phase: The Spring Land Case Study. In *Modern Management Based on Big Data II and Machine Learning and Intelligent Systems III: Proceedings of MMBD 2021 and MLIS 2021*; IOS Press: Amsterdam, The Netherlands, 2021; Volume 341, p. 144.
67. Pham, C.M. Building a maturity framework for big data cybersecurity analytics. In *Research Anthology on Privatizing and Securing Data*; IGI Global: Hershey, PA, USA, 2021; pp. 365–385.
68. Rea-Guaman, A.M.; San Feliu, T.; Calvo-Manzano, J.A.; Sanchez-Garcia, I.D. Comparative study of cybersecurity capability maturity models. In Proceedings of the Software Process Improvement and Capability Determination: 17th International Conference (SPICE 2017), Palma de Mallorca, Spain, 4–5 October 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 100–113.
69. Schlette, D.; Vielberth, M.; Pernul, G. CTI-SOC2M2–The quest for mature, intelligence-driven security operations and incident response capabilities. *Comput. Secur.* **2021**, *111*, 102482. [CrossRef]
70. Akinsanya, O.O.; Papadaki, M.; Sun, L. Current cybersecurity maturity models: How effective in healthcare cloud? In Proceedings of the CERC, Darmstadt, Germany, 29–30 March 2019; pp. 211–222.
71. Skarga-Bandurova, I.; Kotsiuba, I.; Velasco, E.R. Cyber Hygiene Maturity Assessment Framework for Smart Grid Scenarios. *Front. Comput. Sci.* **2021**, *3*, 614337. [CrossRef]
72. Singh, A.; Chawla, P.; Krishnamurthi, R.; Kumar, A. Cybercrimes and defense approaches in vehicular networks. In *Autonomous and Connected Heavy Vehicle Technology*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 37–63.
73. Kaushik, K.; Bathla, G.; Naeem, U.; Kumar, A. Cybercriminal approaches in big data models for automated heavy vehicles. In *Autonomous and Connected Heavy Vehicle Technology*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 303–333.
74. Kour, R.; Karim, R.; Thaduri, A. Cybersecurity for railways—A maturity model. *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit* **2020**, *234*, 1129–1148. [CrossRef]
75. Sorin, A.; Staroswiecki, E. *Cybersecurity for Smart Grid Systems: Fundamentals and Challenges*; Wiley-IEEE Press: Hoboken, NJ, USA, 2018.
76. Katta, V.; Simensen, J.E.; Reegård, K.; Houmb, S.H.; Engum, E.A. Cybersecurity maturity assessment of a critical infrastructure organisation–approach and observations. In Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 779–785.
77. Alayo, J.G.; Mendoza, P.N.; Armas-Aguirre, J.; Molina, J.M. Cybersecurity maturity model for providing services in the financial sector in Peru. In Proceedings of the 2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI), Bogota, Colombia, 29 September–1 October 2021; pp. 1–4.
78. Kour, R.; Karim, R. Cybersecurity workforce in railway: Its maturity and awareness. *J. Qual. Maint. Eng.* **2021**, *27*, 453–464. [CrossRef]
79. Jaquire, V.; von Solms, S. Developing a cyber counterintelligence maturity model for developing countries. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, 31 May–2 June 2017; pp. 1–8.
80. Baikloy, E.; Praneetpolgrang, P.; Jirawichitchai, N. Development of cyber resilient capability maturity model for cloud computing services. *TEM J.* **2020**, *9*, 915. [CrossRef]
81. Straub, J. Evaluating the Use of Technology Readiness Levels (TRLs) for Cybersecurity Systems. In Proceedings of the 2021 IEEE International Systems Conference (SysCon), Vancouver, BC, Canada, 15 April–15 May 2021; pp. 1–6.
82. Patino, S.; Caicedo, A.; Guaña, E.R. Modelo de evaluación del dominio control de acceso de la norma ISO 27002 aplicado al proceso de gestión de bases de datos. *RISTI-Rev. Ibérica Sist. Tecnol. Inf.* **2019**, *2019*, 230–241.
83. Shaked, A.; Tabansky, L.; Reich, Y. Incorporating systems thinking into a cyber resilience maturity model. *IEEE Eng. Manag. Rev.* **2020**, *49*, 110–115. [CrossRef]
84. Proença, D.; Borbinha, J. Information security management systems-a maturity model based on ISO/IEC 27001. In Proceedings of the Business Information Systems: 21st International Conference (BIS 2018), Berlin, Germany, 18–20 July 2018; Springer: Berlin/Heidelberg, Germany, 2018; pp. 102–114.
85. Barnes, B.; Daim, T. Information Security Maturity Model for Healthcare Organizations in the United States. *IEEE Trans. Eng. Manag.* **2022**. [CrossRef]
86. Briceag, V. Model Multiprofil de Maturitate a Securității Informației (M3SI). *Rom. J. Inf. Technol. Autom. Control* **2022**, *32*, 99–112. [CrossRef]
87. Lubis, M.; Putri, I.I.; Izzati, B.M. Information Systems Maturity Level Assessment using the HISMM Framework: Case Study of State Hospital in Jakarta. In Proceedings of the 2022 International Conference on Science and Technology (ICOSTECH), Batam, Indonesia, 3–4 February 2022; pp. 1–6.

88. Hu, S.; Huang, M. Internet Financial Security Based on Big Data. In Proceedings of the International Conference on Applications and Techniques in Cyber Intelligence (ATCI), Fuyang, China, 19–21 June 2021; Volume 1244, pp. 485–490.
89. Spruit, M.; Slot, G. ISFAM 2.0: Revisiting the Information Security Assessment Model. In *Security Risks: Assessment, Management and Current Challenges*; Springer: Cham, Switzerland, 2017; pp. 87–108.
90. Miloslavskaya, N.; Tolstaya, S. Maturity Concept and Model Review. In *Lecture Notes in Networks and Systems, Proceedings of the 10th World Conference on Information Systems and Technologies (WorldCIST 2022), Budva, Montenegro, 12–14 April 2022*; Springer: Berlin/Heidelberg, Germany, 2022; Volume 468, pp. 182–191.
91. Schmitz, C.; Schmid, M.; Harborth, D.; Pape, S. Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Comput. Secur.* **2021**, *108*, 102306. [CrossRef]
92. da Silva, M.P.; de Barros, R.M. Maturity model of information security for software developers. *IEEE Lat. Am. Trans.* **2017**, *15*, 1994–1999. [CrossRef]
93. Shimels, T.; Lessa, L. Maturity of information systems security in selected private Banks in Ethiopia. In Proceedings of the 2021 International Conference on Information and Communication Technology for Development for Africa (ICT4DA), Bahir Dar, Ethiopia, 22–24 November 2021; pp. 184–189.
94. Torres-Calderon, H.; Velasquez, M.; Mauricio, D. Method for Designing Countermeasures for Crypto-Ransomware Based on the NIST CSF. In *Networking, Intelligent Systems and Security*; Smart Innovation, Systems and Technologies; Springer: Cham, Switzerland, 2021; Volume 237, pp. 251–260.
95. Ozkan, B.Y.; Spruit, M.; Wondolleck, R.; Burriel Coll, V. Modelling adaptive information security for SMEs in a cluster. *J. Intellect. Cap.* **2020**, *21*, 336–354.
96. Kreppein, A.; Kies, A.; Schmitt, R.H. Novel Maturity Model for Cybersecurity Evaluation in Industry 4.0. In Proceedings of the 3rd International Conference on Advances in Cyber Security (ACeS 2021), Penang, Malaysia, 24–25 August 2021; Springer: Berlin/Heidelberg, Germany, 2021; Volume 1487, pp. 198–210.
97. Zammani, M.; Razali, R.; Singh, D. Organisational Information Security Management Maturity Model. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 668–678 . [CrossRef]
98. García, A.; Calle, L.; Raymundo, C.; Domínguez, F.; Moguerza, J.M. Personal data protection maturity model for the micro financial sector in Peru. In Proceedings of the 2018 4th International Conference on Computer and Technology Applications (ICCTA), Istanbul, Turkey, 3–5 May 2018; pp. 20–24.
99. Rojas, R.; Muedas, A.; Mauricio, D. Security maturity model of web applications for cyber attacks. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019; pp. 130–137.
100. Deshpande, V.M.; Desai, A. Smart Secure: A Novel Risk based Maturity Model for Enterprise Risk Management during Global Pandemic. In Proceedings of the 2021 6th International Conference for Convergence in Technology (I2CT), Maharashtra, India, 2–4 April 2021; pp. 1–7.
101. Villalba, K.M.; Donado, S.A. Steps to design a maturity model with an agile framework for the implementation of IT security management systems aligned to the policies of the Colombian government for the public sector. *RISTI—Rev. Iber. Sist. Tecnol. Inf.* **2022**, *2022*, 501–507.
102. Gani, A.B.A.; Fernando, Y. The cybersecurity governance in changing the security psychology and security posture: Insights into e-procurement. *Int. J. Procure. Manag.* **2021**, *14*, 308–327. [CrossRef]
103. Jaquire, V.; von Solms, S. Towards a cyber counterintelligence maturity model. In Proceedings of the 12th International Conference on Cyber Warfare and Security, Dayton, OH, USA, 2–3 March 2017; Academic Conferences International Limited: Montreal, QC, Canada, 2017; pp. 432–440.
104. Fertig, T.; Schütz, A.E.; Weber, K.; Müller, N.H. Towards an Information Security Awareness Maturity Model. In *Learning and Collaboration Technologies. Human and Technology Ecosystems, Proceedings of the 7th International Conference, LCT 2020, Held as Part of the 22nd HCI International Conference (HCII 2020), Copenhagen, Denmark, 19–24 July 2020*; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 22, pp. 587–599.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.