# Information Security Management Systems - A Maturity Model Based on ISO/IEC 27001

Diogo Proença[1,2](✉) and José Borbinha[1,2]

[1] Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal
{diogo.proenca,jlb}@tecnico.ulisboa.pt
[2] INESC-ID - Instituto de Engenharia de Sistemas e
Computadores Investigação e Desenvolvimento, Lisbon, Portugal

**Abstract.** An Information Security Management System, according with the ISO/IEC 27001 is the set of "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security". ISO/IEC 27001 defines the requirements and process for implementing an Information Security Management System. However, implementing this standard without a detailed plan can become a burden on organizations. This paper presents a maturity model for the planning, implementation, monitoring and improvement of an Information Security Management System based on ISO/IEC 27001. The purpose of this model is to provide an assessment tool for organizations to use in order to get their current Information Security Management System maturity level. The results can then be used to create an improvement plan which will guide organizations to reach their target maturity level. This maturity model allows organizations to assess their current state of affairs according to the best practices defined in ISO/IEC 27001. The maturity model proposed in this paper is evaluated through a multi-step perspective that is used to confirm that the maturity model makes a useful and novel contribution to the Information Security Management domain by taking in consideration the best practice of the domain.

**Keywords:** Information Security Management · Maturity model · Measurement Performance · Design

## 1 Introduction

In a growing and overly competitive world, only organizations that take advantage of the benefits the best information can deliver for decision-making are able to profit and thrive. Organizations should understand that information is such a valuable asset that it must be protected and managed properly. Information security should be used as a way to protect information against loss, exposure or destruction of its properties. [1] One of the goals of information security is to ensure business continuity while minimizing the impact of security incidents. In this sense, information is an asset that, like any other important asset, is essential to an organization and therefore needs to be adequately protected. This is especially important in the increasingly interconnected business

W. Abramowicz and A. Paschke (Eds.): BIS 2018, LNBIP 320, pp. 102–114, 2018.
https://doi.org/10.1007/978-3-319-93931-5_8

environment. As a result of this incredible increase in interconnectivity, information is now exposed to increasing numbers and a wide range of threats and vulnerabilities [2]. Information can exist in several forms. It can be printed or written on paper, electronically stored, transmitted by mail or by electronic means, presented in films or spoken in conversations. Whatever form is presented or the medium through which information is shared or stored, it is recommended that it be always adequately protected [2]. Information security is the protection of information from various types of threats to ensure business continuity, minimize risk to business, maximize return on investment and business opportunities. Information security is achieved by implementing a set of appropriate controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, deployed, monitored, critically reviewed and improved where necessary to ensure that the organization's business and security objectives are met. This should be done in conjunction with other business management processes [2]. Information security should always serve three elements [3]. The first is confidentiality, when we talk about confidentiality, we are talking about secrecy. Preserving the confidentiality of information means ensuring that only those who should have knowledge about it can access it. The second is integrity, the preservation of integrity involves protecting information against changes in its original state. These changes can be both intentional and accidental. The third and final one is availability, which ensures that information is accessible when someone who needs it tries to get it. The requested information must be provided as expected by the user.

The goal of this paper is to develop an artifact (a maturity model) by using an established approach to contribute to the Information Security Management body of knowledge. As a result, Design Science Research (DSR) was chosen as it combines the practical dimension and the scientific dimension. The maturity model focuses of the ISO/IEC 27001, which prescribes the requirements and process for implementing an Information Security Management System (ISMS), to define maturity model for ISMS. In this paper we target our attention in answering two research questions (RQ), as follows:

*RQ1 -* *What are key requirements for an Information Security Management System process according to the ISO/IEC 27001 relevant for the purpose of maturity assessment?*

*RQ2 -* *How could a maturity Model specific to ISMS be designed which targets the challenges of different organizations and industries?*

To address these research questions, this paper is structured in six sections. First, the key terms and concepts are explained in Sect. 2. This is Followed by Sect. 3, where the research methodology is outlines. Section 4, details the findings from a literature review in existing Information Security Management Maturity models and a comparison between the existing maturity models for the Information Security Management domain. Then Sect. 5, presents the ISMS Maturity model and the iterative development method used. The evaluation of the ISMS Maturity Model is presented in Sect. 6 which evaluates the mapping between the ISMS Maturity Model dimensions and the ISO/IEC 27001 requirements. This section also details the results of five assessments performed to five different organization using the proposed maturity model. Finally, Sect. 7 details the conclusions and the limitations of the ISMS maturity model.

## 2 Foundation

This section explains the key terns and concepts within this paper, such as, "maturity models" and "information security management system" to ensure a common understanding.

In 1986, the US Department of Defense needed a method to assess the capabilities of the software companies with whom it worked, so Watts Humphrey, the SEI team and Miter Corporation were tasked with this task. In 1991 was released the first version, the CMM maturity model of capabilities. This model has achieved remarkable success and has been revised and improved having evolved into CMMI, the currently integrated capability maturity model integration version 1.3 [4].

Due to the success obtained, the principles used to develop the SEI maturity models served as inspiration to other authors, both academics and practitioners, and there are now hundreds of models applied to different domains [2]. Currently, the two major references of maturity models are CMMI and ISO/IEC 15504, both of which are related to Software Engineering processes.

In general, maturity can be defined as "an evolutionary progression in the demonstration of a specific skill or in the achievement of an objective from an initial state to a desired final state" [5]. In addition to the general definitions, there are many definitions of maturity that are directly related to the domain to which this term refers. As this work will develop a maturity model applied to a process of ISMS, it is also important to define maturity applied to a process. Maturity can then be defined as the "degree to which an organization executes processes that are explicitly and consistently documented, managed, measurable, controlled, and continuously improved. Maturity can be measured through appraisals" [4]. According to Loon [15], a maturity model is a sequence of maturity levels for certain objects, usually people, organizations or processes. In these models is represented the evolutionary path, anticipated, desired or typical, through discrete levels. In addition to the above, these models provide the necessary criteria to reach each of the model's maturity levels. Thus, maturity models allow us to see at what level of the evolutionary process certain objects meet. The maturity levels are organized from an initial level of lower capacity to an advanced level corresponding to the maximum capacity of the reality in question. In order to reach higher maturity levels, it is necessary that there is a continuous progression of the capability of a given object.

ISO/IEC 27001 was based on the British standard BS7799 and ISO/IEC 17799. It was prepared to provide the requirements to establish, implement, operate, monitor, critically analyze, maintain and improve an ISMS [2]. An ISMS as defined by this standard is "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security" [2]. This standard is used around the world by all types of organizations as the basis for the organization's policy management and implementation of information security. It is being used by small, medium and large organizations. In fact, ISO/IEC 27001 is designed to be flexible enough to be used by any type of organization. This standard adopts the Plan-Do-Check-Act (PDCA) model, as depicted in Fig. 1, which is applied to structure all the ISMS processes.

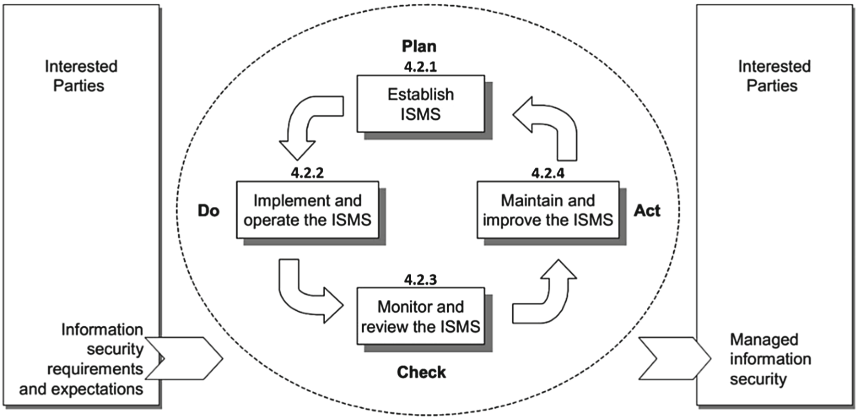
Interested Parties
Information security requirements and expectations
Plan
4.2.1
Establish ISMS
4.2.2
Implement and operate the ISMS
Do
4.2.4
Maintain and improve the ISMS
Act
4.2.3
Monitor and review the ISMS
Check
Interested Parties
Managed information security

**Fig. 1.** PDCA model applied to ISMS processes and ISO/IEC 27001 mapping [2]

## 3 Research Methodology

In order to address the research questions of this paper, we selected the DSR paradigm [17, 19]. DSR is described by "a designer answering questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The designed artifacts are both useful and fundamental in understanding that problem" [19]. The major benefit of DSR is the fact that it addresses real-world problems and simultaneously contributes to the body of knowledge [17]. However, the development of maturity models within the Information Security Management domain is not new but has been popular for quite some time [6]. Mettler, et al. [12] count more than 100 models in the information systems domain, Poeppelbuss et al. [14] counts even many more. One significant fault within this research area is the lack of specific contributions regarding how to develop maturity models. Moreover, most authors rarely describe their development process. Up to our knowledge there are only a few development procedure models for maturity models. The models of Becker et al. [16] and De Burin et al. [13] seem to be quite popular among the community based their citation counts. We decided to apply the model of Becker et al. [16] to develop our maturity model because it is based on DSR and therefore provides a methodological foundation very suitable for application in our research approach. Furthermore, Becker et al. provide a stringent and consistent development process according to the DSR guidelines of Hevner et al. [17].

Becker et al. [16] argue that maturity models are artifacts that serve to solve the problem of appreciating capacity and obtain improvement measures. According to [19] design science allows you to create artifacts such as constructs, models, methods, and instantiations that help improve problem-solving capabilities. Thus, the authors state that design science research is appropriate for the development of maturity models.

In the same study [16], the author proposes a procedure for the development of maturity models composed of eight steps. All steps should be documented. As depicted in the procedure model in Fig. 2 the first steps focus on the problem identification (step 1). In this step the research problem is identified and detailed, the practical relevance of the problem is specified and the value of the artifact is justified. This step is followed by the comparison with existing maturity models (step 2). This second step is based on the problem identification of the first step and analysis of existing maturity model in the Information Security Management domain, which leads to the identification of weaknesses in these models. We conducted a literature analysis, which was based on an extensive online search to find existing maturity models focused on the Information Security Management domain. Thus, the analysis of the maturity models was performed according to their functionality, as well as, their capability to address the ISO/IEC 27001 requirements.

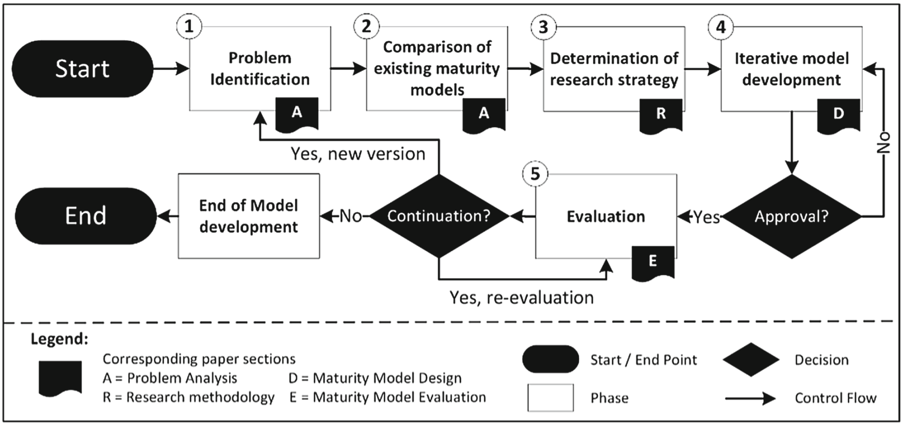

**Fig. 2.** Procedure model of the research approach (adopted from Becker et al. [16])

The next step deals with the determination of the research strategy (step 3) outlined in this section of the paper. This is followed by the iterative maturity model development (step 4). In this step, we used model adoption techniques, such as, configuration, instantiation, aggregation, specialization and analogy [18] to incorporate the ISO/IEC 27001 in the maturity model. This allowed us to create a rigorous maturity model regarding both the structure and content. In the last step, evaluation (step 5), we combined the steps of Becker et al. [16], conception of transfer and evaluation, implementation of transfer media, and evaluation. All steps will be conducted, but to match the structure of this paper we made this change.

## 4 Problem Analysis

In order to provide a consistent and precise problem definition, we gathered the ISMS process requirements from ISO/IEC 27001. According to the ISO/IEC 27001, the activities for ISMS Processes can be summarized as follows:

- A1: Establish the ISMS – “Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.” [2];
- A2: Implement and operate the ISMS – “Implement and operate the ISMS policy, controls, processes and procedures.” [2];
- A3: Monitor and Review the ISMS – “Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.” [2];
- A4: Maintain and Improve the ISMS – “Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.” [2].

**Table 1.** ISO/IEC 27001 activities reference matrix fit assessment

| Maturity model | A1 | A2 | A3 | A4 | Σ |
|---|---|---|---|---|---|
| O-ISM3 | 2 | 3 | 4 | 4 | **13** |
| SSE-CMM | 2 | 4 | 4 | 2 | **12** |
| ISF MM | 2 | 2 | 3 | 3 | **10** |
| COBIT 5 | 4 | 2 | 4 | 2 | **12** |
| ONG C2M2 | 3 | 2 | 2 | 3 | **10** |
| BSIMM | 3 | 4 | 4 | 4 | **15** |
| Average | **2,6** | **2,8** | **3,5** | **3** | **12** |

These are the activities that the ISMS process must perform in order to be in line with the recommendations of the ISO/IEC 27001. The activities are used as a reference baseline to assess the appropriateness of several existing Information Security Management Maturity Models. Based on the results of the literature review we conducted within the Information Security Management domain, we identified several papers dealing with maturity models. We selected maturity models that used different methodological approaches. Then, each maturity model was analyzed according to the degree to which they cover and fit to the previously defined reference baseline. Each maturity model was ranked for every requirement according to the degree of matching, using a Likert-scale, from 1 (very low) to 5 (very high). After this analysis, we concluded that only six maturity models scored an aggregate of at least 10 points according to the defined ISO/IEC 27001 activities baseline: (1) Open Information Security Management Maturity Model (O-ISM3) [6]; (2) Systems Security Engineering – Capability Maturity Model (SSE-CMM) [7]; (3) ISF Maturity Model Accelerator (ISF MM) [8]; (4) Control Objectives for Information and Related Technologies - Version 5 (COBIT 5) [9]; (5) Cyber Security Capability Maturity Model (C2M2) [10], and (6) Building Security in Maturity Model

(BSIMM) [11]. Table 1 presents the assessment results of the above as the most significant identified maturity model in detail. Based on this set an average total score of 12 was achieved (maximum score 20).

## 5 Maturity Model Design

In accordance to the maturity model development approach of Becker et al. [16] a new maturity model has to be developed, if no existing or the advancement of an existing one is capable of addressing the identified problem. So, based on the findings of our analysis there is no maturity model which satisfactorily fulfill the entire ISO/IEC 27001 activities baseline. Therefore, we will develop a new maturity model. The newly developed maturity model presented in Table 2 adopts established structural elements, domains and functions of the best practice in ISO/IEC 27001. As detailed within the research methodology, we applied an iterative process for the maturity model development. In total we needed two iterations which can be detailed as follows:

*First iteration:* As a first step, we defined the characteristics and structure of the maturity model. We started by proposing five maturity levels, Initial, Managed, Defined, Quantitively Managed, and Optimizing. These maturity levels can be found in various established maturity models, such as, CMMI [4]. In this initial iteration, we focused in just a part of the ISO/IEC 27001 ISMS process namely the Plan step. For each criterion of the maturity model we modeled what was the manifestation of that criterion at the different maturity levels.

*Second Iteration:* In the second iteration we completely overhauled the definition of the maturity levels by proposing five new maturity levels, Initial, Planning, Implementation, Monitoring, and Improvement. These maturity levels are based on the PDCA cycle used within the ISO/IEC 27001 as depicted in Fig. 1. Table 3 details the activities on which our maturity model is based, along with a mapping to the ISO/IEC 27001 ones they were derived from. This made it easier for a user accustomed with the ISO/IEC 27001 to understand the maturity model and make a connection between what was being asked in each assessment criterion and the requirements specified in the ISO/IEC 27001, which resulted in an easily understandable maturity model that is presented in Table 2. Finally, this leads to the following maturity levels: (Level 1) Initial Stage; (Level 2) Planning Stage; (Level 3) Implementation Stage; (Level 4) Monitoring Stage; (Level 5) Improvement Stage.

To improve from level X to level X + 1, the organization must comply with all the criteria from level X, which makes this maturity model follow a “stages” approach. What an organization can expect from progressing through the maturity levels is that their ISMS process will become increasingly managed, defined and optimized.

**Table 2.** ISMS maturity model

| Maturity level | Assessment criterion |
|---|---|
| Level 1: initial | *No criteria* |
| Level 2: planning | 2.1 - Define scope and boundaries of the ISMS |
| | 2.2 - Define ISMS policy |
| | 2.3 - Define risk assessment approach |
| | 2.4 - Perform risk identification |
| | 2.5 - Perform risk analysis and evaluation |
| | 2.6 - Define risk treatment options |
| | 2.7 - Define risk treatment control objectives and controls |
| | 2.8 - Obtain management approval for residual risks |
| | 2.9 - Obtain management authorization to implement and operate the ISMS |
| | 2.10 - Prepare a statement of applicability |
| Level 3: implementation | 3.1 - Formulate risk treatment plan |
| | 3.2 - Implement risk treatment plan |
| | 3.3 - Implement controls to meet control objectives |
| | 3.4 - Define effectiveness measurement procedure of the selected controls |
| | 3.5 - Implement training and awareness programmes |
| | 3.6 - Manage operation of the ISMS |
| | 3.7 - Manage resources for the ISMS |
| | 3.8 - Implement procedures and controls for detection and response to security events |
| Level 4: monitoring | 4.1 - Execute monitoring and reviewing procedures and other controls |
| | 4.2 - Undertake regular reviews of the effectiveness of the ISMS |
| | 4.3 - Measure the effectiveness of controls |
| | 4.4 - Review risk assessments |
| | 4.5 - Review residual risks |
| | 4.6 - Review identified acceptable levels of risks |
| | 4.7 - Conduct internal ISMS audits |
| | 4.8 - Undertake management review of the ISMS |
| | 4.9 - Update security plans |
| | 4.10 - Record actions and events |
| Level 5: improvement | 5.1 - Implement the identified improvements in the ISMS |
| | 5.2 - Take appropriate corrective and preventive actions |
| | 5.3 - Communicate actions and improvements to all interested parties |
| | 5.4 - Ensure that improvements achieve their objectives |

## 6 Maturity Model Evaluation

The evaluation step is a main element of DSR. It is necessary to show the "utility, quality, and efficacy of a design artifact" [19]. To be compliant with these requirements we evaluated the ISMS Maturity Model by using a multi-perspective approach which consists of three stages: (1) Evaluation of the mapping using the Wand and Weber

**Table 3.** Mapping of the ISMS maturity model and ISO/IEC 27001 requirements, and the resulting evaluation using the Wand and Weber (W&W) ontological deficiencies.

| PCDA cycle | ISMS maturity model activities | ISO/IEC 27001 requirements | W&W ontological deficiencies |
|---|---|---|---|
| Plan | *Maturity level: planning* | | |
| | Define scope and boundaries of the ISMS | 4.2.1 – (a) | Complete |
| | Define ISMS Policy | 4.2.1 – (b) | Complete |
| | Define risk assessment approach | 4.2.1 – (c) | Complete |
| | Risk identification | 4.2.1 – (d) | Complete |
| | Risk analysis and evaluation | 4.2.1 – (e) | Complete |
| | Risk treatment options | 4.2.1 – (f) | Complete |
| | Risk treatment control objectives and controls | 4.2.1 – (g) | Complete |
| | Obtain management approval for residual risks | 4.2.1 – (h) | Complete |
| | Obtain management authorization to implement and operate the ISMS | 4.2.1 – (i) | Complete |
| | Prepare a statement of applicability | 4.2.1 – (j) | Complete |
| Do | *Maturity level: implementation* | | |
| | Formulate risk treatment plan | 4.2.2 - (a) | Complete |
| | Implement risk treatment plan | 4.2.2 - (b) | Complete |
| | Implement controls to meet control objectives | 4.2.2 - (c) | Complete |
| | Define effectiveness measurement procedure of the selected controls | 4.2.2 - (d) | Complete |
| | Implement training and awareness programmes | 4.2.2 - (e) | Complete |
| | Manage operation of the ISMS | 4.2.2 - (f) | Complete |
| | Manage resources for the ISMS | 4.2.2 - (g) | Complete |
| | Implement procedures and controls for detection and response to security events. | 4.2.2 - (h) | Complete |
| Check | *Maturity level: monitoring* | | |
| | Execute monitoring and reviewing procedures and other controls | 4.2.3 – (a) | Complete |
| | Undertake regular reviews of the effectiveness of the ISMS | 4.2.3 – (b) | Complete |
| | Measure the effectiveness of controls | 4.2.3 – (c) | Complete |
| | Review risk assessments | 4.2.3 – (d) | Overload |
| | Review residual risks | 4.2.3 – (d) | Overload |
| | Review identified acceptable levels of risks | 4.2.3 – (d) | Overload |
| | Conduct internal ISMS audits | 4.2.3 – (e) | Complete |
| | Undertake management review of the ISMS | 4.2.3 – (f) | Complete |
| | Update Security Plans | 4.2.3 – (g) | Complete |
| | Record Actions and Events | 4.2.3 – (h) | Complete |
| Act | *Maturity level: improvement* | | |
| | Implement the identified improvements in the ISMS | 4.2.4 – (a) | Complete |
| | Take appropriate corrective and preventive actions | 4.2.4 – (b) | Complete |
| | Communication | 4.2.4 – (c) | Complete |
| | Ensure that improvements achieve their objectives | 4.2.4 – (d) | Complete |

Ontological Deficiencies; (2) an assessment of the fit of the ISMS Maturity Model against the ISO/IEC 27001 requirements used to compare existing ISMS maturity models in Sect. 4; and (3) assess five organizations using the ISMS Maturity Model.

To evaluate the mapping between our maturity model and ISO/IEC 27001, regarding completeness and clarity, we performed an analysis according to the Wand and Weber method [20]. Wand and Weber define an ontological evaluation of the grammars method, where two sets of concepts are compared in order to identify four ontological deficiencies, as depicted in Fig. 3:

- **Incompleteness -** Can every element in the first set be mapped to an element in the second set? If there is not a total mapping, it is considered incomplete;
- **Redundancy -** Are there elements in the first set mapped to more than one element in the second set? If so, the mapping is considered redundant;
- **Excess -** Is every element from the second set mapped to an element in the second set? The mapping is considered excessive if there are elements from the second set without a relationship;
- **Overload -** Is every element of the second set mapped to only one element in the first set? The mapping is considered overloaded if any element in the second set has more than one mapping to the first set.

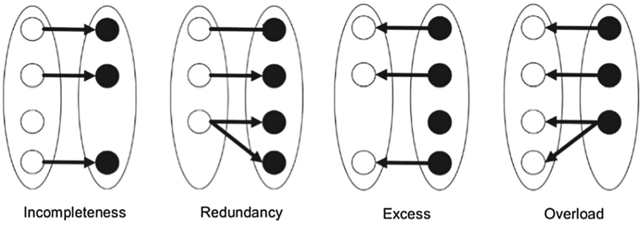

**Fig. 3.** Wand and weber ontological deficiencies [20]

The ontological evaluation of the mapping between the ISMS Maturity Model and ISO/IEC 27001 chapters (see Fig. 1) and requirements is detailed in Table 3. A first observation is that the mapping is complete, since every proposed activity can be mapped to an ISO/IEC 27001 requirement. As for the other attributes, there is no redundancy and excess. However, regarding overload, the ISO/IEC 27001 "4.2.3 - (d)" requirement was overloaded as in our understanding it defines a requirement for three different activities. As a result, we created three different assessment criteria for this requirement. Finally, the ISMS Maturity Model covers all the requirements detailed in Sect. 4, which means that the total score using the same scale is 20.

Following the first two evaluation steps, we assessed five real organizations by following an assessment method, anonymized due to consent issues. Organization Alpha is the public institute responsible for promoting and developing administrative modernization in its country. Its operation is in three axes: customer service, digital transformation and simplification. Organization Beta is part of the business sector in its country government that produces and supplies goods and services that require high security standards, namely: coins, banknotes, and documents, such as, citizen's card and passports. Organization Gamma is a public higher education institution that has approximately 11.500 students being the largest school of engineering, science and technology in its country. Organization Delta is a public institution for scientific and technological research and development whose purpose is to contribute to the creation, development and diffusion of research in fields related to civil engineering. Organization Omega is a private organization which focus on software development and maintenance providing services all over the globe with various offices in Europe.

For each of these five organizations we took the role of assessors, assessed the organization collecting objective evidence for the assessment criteria defined in the maturity model. Then, the results were analyzed which resulted in the assessment results depicted in Table 4. In this table, "Y" stands for criterion satisfied, an empty cell stands for criterion not satisfied, and the last columns shows the final maturity level for each of the assessed organizations.

**Table 4.** ISMS maturity assessment results

| | Criterion | 2.1 | 2.2 | 2.3 | 2.4 | 2.5 | 2.6 | 2.7 | 2.8 | 2.9 | 2.10 | 3.1 | 3.2 | 3.3 | 3.4 | 3.5 | 3.6 | 3.7 | 3.8 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | ALPHA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| | BETA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| | GAMMA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | | | | | Y | Y | Y | |
| | DELTA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |
| | OMEGA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y |

| | Organization | 4.1 | 4.2 | 4.3 | 4.4 | 4.5 | 4.6 | 4.7 | 4.8 | 4.9 | 4.10 | 5.1 | 5.2 | 5.3 | 5.4 | Maturity Level |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization | ALPHA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 5 |
| | BETA | | | | | | Y | Y | Y | | | | | | | 3 |
| | GAMMA | | | Y | | | | | Y | | | | | | | 2 |
| | DELTA | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | | | | | 4 |
| | OMEGA | Y | Y | Y | | Y | | | | | | Y | Y | | | 3 |

In order to achieve a certain maturity level, the organization must comply with all the criteria for that specific level and the levels below, which means that an organization at maturity level 3 complies with all the criteria for maturity levels 2 and 3.

As can be perceived from Table 4, we were able to assess each of the assessment criteria, which in turn allowed us to determine the ISMS maturity level for each of the five organizations. From our analysis, the assessment results shown that the maturity model correctly determined the maturity levels and these in fact correspond to our perception of the maturity of the ISMS implemented in the organization. These results were then used by the organizations to create improvement plans specially tailored to their organizational context.

## 7 Conclusions

The aim of this paper is to detail the development of a maturity model for the ISMS process based on the ISO/IEC 27001 standard. The latter can serve as a governance instrument that could be used by the Information Security Management function to analyze and evaluate the current strengths and weaknesses of the ISMS process.

However, the model is not restricted to analytical purposes only. It can also be used to derive a roadmap towards an evolutionary improvement of the Information Security Management function regarding its capabilities and its effectiveness and efficiency.

The first part of the paper elaborates the ISMS activities requirements which were used as a reference baseline to investigate whether existing maturity models are capable of holistically assessing an ISMS process (RQ1). The findings revealed that existing maturity models cover the entire reference baseline insufficiently, since they only selectively address the activities. Hence, no existing maturity model is able to solve the identified problem. Finally, we decided to design a new maturity model in consistency to the defined research strategy.

In the second part of the paper, we described the development of a maturity model for ISMS, including the model itself as well as its evaluation to address the second research question (RQ2). The developed model is based on existing maturity model structures and inherits concepts and methodologies of the ISO/IEC 27001. The researchers took care during the development to provide a consumable research result. Moreover, the ISMS maturity model benefited from the multi-perspective evaluation approach by further advancements.

Naturally, the applied research approach comes along with certain limitations. This paper presents the assessment results for five organizations using the ISMS Maturity Model. However, in order to extend usefulness of the maturity model, as well as, provide additional validation scenarios and further improve the research aspect, we suggest evaluating (and refining) the ISMS maturity model within different industry sectors, this would lead to a more generic ISMS maturity model and would enable cross-industry benchmarking.

**Acknowledgements.** This work was supported by national funds through Fundação para a Ciência e a Tecnologia (FCT) with reference UID/CEC/50021/2013.

## References

1. Dubois, E., Heymans, P., Mayer, N., Matulevicius, R.: A systematic approach to define the domain of information system security risk management. In: Nurcan, S., Salinesi, C., Souveyet, C., Ralyté, J. (eds.) Intentional Perspectives on Information Systems Engineering, pp. 289–306. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12544-7_16
2. ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements (2013)
3. Miller, H., Murphy, R.: Secure cyberspace: answering the call for intelligent action. IT Professional (2009)
4. CMMI Product Team: CMMI for Development, Version 1.3, Carnegie Mellon Univ., no. November, p. 482 (2010)
5. Mettler, T.: A design science research perspective on maturity models in information systems. Institute of Information Management, University of St. Gallen, St. Gallen (2009)
6. The Open Group: Open Information Security Management Maturity Model (O-ISM3) (2011)
7. Carnegie-Mellon-University: Systems Security Engineering Capability Maturity Model (SSE-CMM) - Model Description Document. Version 3.0 (2003)

8. ISF: Time to grow using maturity models to create and protect value, in Information Security Forum ISF (2014)
9. IT Governance Institute: COBIT 5 – A business Framework for the Governance and Management of Enterprise IT (2012)
10. Department of Energy, U.S. Department of Homeland Security, Cybersecurity Capability Maturity Model (C2M2 v1.1) (2014)
11. McGraw, G., Migues, S., West, J.: Building Security in Maturity Model (BSIMM) Version 8 (2015)
12. Mettler, T., Rohner, P., Winter, R.: Towards a classification of maturity models in information systems. In: D'Atri, A., De Marco, M., Braccini, A., Cabiddu, F. (eds.) Management of the Interconnected World. Physica-Verlag, Heidelberg (2010). https://doi.org/10.1007/978-3-7908-2404-9_39
13. De Bruin, T., Freeze, R., Kaulkarni, U., Rosemann, M.: Understanding the main phases of developing a maturity assessment model. In: Proceedings of the Australasian Conference on Information Systems (ACIS) (2005)
14. Poeppelbuss, J., Niehaves, B., Simons, A., Becker, J.: Maturity models in information systems research: literature search and analysis. In: Communications of the Association for Information Systems, vol. 29 (2011)
15. van Loon, H.: Process Assessment and Improvement: A Practical Guide. Springer, New York (2015)
16. Becker, J., Knackstedt, R., Pöppelbuβ, J.: Developing maturity models for IT management: a procedure model and its application. Bus. Inf. Syst. Eng. **3**, 213–222 (2009)
17. Hevner, A., Ram, S., March, S., Park, J.: Design science in information systems research. MISQ **28**, 75–105 (2004)
18. Vom Brocke, J.: Design principles for reference modeling-reusing information models by means of aggregation, specialization, instantiation, and analogy. In: Fettke, P., Loos, P. (eds.) Reference Modeling for Business Systems Analysis. Idea Group Inc., Hershey (2007)
19. Hevner, A., Chatterjee, S.: Design Research in Information Systems: Theory and Practice. Springer, Heidelberg (2010). https://doi.org/10.1007/978-1-4419-5653-8
20. Wand, Y., Weber, R.: On the ontological expressiveness of information systems analysis and design grammars. Inf. Syst. J. **3**(4), 217–237 (1993)