STRATEGIC MANAGEMENT, Vol. 28 (2023), No. 1, pp. 004-019

DOI: 10.5937/StraMan2200033F

Received: August 22, 2022
Revised: November 17, 2022
December 05, 2022
December 06, 2022
Accepted: December 08, 2022
Published online: January 23, 2023

Towards a readiness model derived from critical success factors, for the general data protection regulation implementation in higher education institutions

José Fernandes
School of Economics and Management, University of Minho, Campus de Gualtar, Braga, Portugal
https://orcid.org/0000-0001-7229-7884

Carolina Feliciana Machado
School of Economics and Management, University of Minho, Campus de Gualtar, Braga, Portugal
http://orcid.org/0000-0002-9685-1576

Luís Amaral
School of Engineering, University of Minho, Campus de Azurém, Guimarães, Portugal
https://orcid.org/0000-0002-9426-3834

Abstract
Background: Present the relevance of the study and highlights the key points of literature overview.
Purpose: As of May 25, 2018, General Data Protection Regulation (GDPR) has become mandatory for all organizations, public or private, that handle personal data of European citizens, regardless of their physical location. Higher education institutions (HEIs), namely public universities, are no exception to this requirement and, as in many other organizations, many HEIs begin the process of implementing the GDPR without meeting the minimum conditions necessary for implementation. The purpose of this study, therefore, is to present a model to determine the level of readiness of HEIs regarding the implementation of the GDPR.
Study design/methodology/approach: With the objective of designing a new artefact as a readiness model for the implementation of the GDPR, this study follows Design Science Research as an approach to be used to build the readiness model, based on a set of 16 critical success factors (CSFs) previously determined.
Findings/conclusions: A readiness model was designed, based on a set of 16 CSFs related to the implementation of GDPR in HEIs.
Limitations/future research: This is a new area of study that needs further development, namely through the practical application of the model, allowing the improvement of the measurement levels of the different CSFs.
Practical implications: The determined readiness model allows HEIs to realize a priori if they have the necessary conditions for the implementation of the GDPR, giving useful indications of the organizational dimensions and the CSFs that compose them where better performance is necessary to ensure a successful implementation.
Originality/Value: As far as we know, this is the first model of readiness based on CSFs related to the implementation of GDPR in HEIs, being therefore a first contribution to the development of this area.

Keywords
general data protection regulation; critical success factors; design science research; readiness model; maturity model; higher education institutions

Introduction

If it is true that the increasing use of information technologies has brought advantages by facilitating access to electronic services, provided by the State and by private organizations, it is also true that we can face a set of threats and risks here, namely, improper access to personal information. The themes of privacy and, consequently, that of data protection that concerns everyone, have been the subject of study for several decades, but they have never been as current as now due to the fact that every day, information is published, consulted, processed and stored our respect (Gstrein & Beaulieu, 2022; Staff, C.A.C.M., 2021; Wu, Vitak, & Zimmer, 2020). On the other hand, the collection and storage of personal information has become the basis of the commercial activity of many companies, being sometimes illegal because it is carried out without consent and without any type of control by the supervisory authorities.

In this scenario, it is critical to proceed with the application of the General Data Protection Regulation (GDPR), based on which the protection of the privacy of data subjects will be improved, allowing different organizations to work with clear rules and achievable requirements (Hoofnagle, van der Sloot & Borgesius, 2019; Li, Yu & He, 2019; Crutzen, Peters & Mondschein, 2019). As universities are institutions that constantly deal with personal data relating to students, teaching staff, technical, administrative and management workers, researchers and other workers, it is observed that there are many challenges that are posed to them with the entry into force of the GDPR. Namely, through the need for self-regulation, the need to demonstrate that they are carrying out the different data processing operations in accordance with what is advocated in the new regulation, the need to adapt to the new requirements, such as information portability, the right to be forgotten, the design of systems to guarantee the privacy from the moment they are built or even the need for a Data Protection Officer (DPO), all this will require a profound change in the way these institutions work (Habbabeh, Schneider & Asprion, 2019). To this extent, it is important to ensure, a priori, with an adequate level of performance, the factors that are critical for the successful implementation of the GDPR in national public universities (Fernandes, Machado & Amaral, 2022; Syed, Bandara, French & Stewart, 2018). These factors, called by Rockart (1979) CSFs, are "… areas of activity that should receive constant and careful attention from management" (Rockart, 1979, p.85).

The main aim of this paper is therefore to define a readiness model derived from CSFs, for the implementation of general data protection regulation in higher education institutions.

Beginning with a brief background analysis, in the following Section 2, the 16 CSFs that will be the basis for the construction of the readiness model will be presented. Section 3 sheds light on the research methodology adopted. In Section 4, the readiness model for the implementation of the GDPR will be presented. The main results, the final considerations, limitations and future work, will be discussed, respectively in Section 5 and in the conclusion session. Through the analysis of the performance level of the obtained 16 CSFs HEIs are able to understand which are the organizational areas that need more attention from management, reinforcing, this way, the allocation of resources and means to the process of implementation of the GDPR, contributing in a very positive way to the theoretical and practical development of this area of research, since it is the first model of readiness based on CSFs related to the implementation of GDPR in HEIs.

1. Background

The entry into force of the GDPR on May 25, 2018 made it mandatory for public and private organizations dealing with personal data to adapt to a new reality, where data subjects have new rights, and those responsible for data processing operations are required to demonstrate compliance with GDPR to national supervisory authorities. This new reality requires time for those responsible to adapt processes and technological infrastructure to support the organization's activity, as well as the financial and human resources necessary for its implementation (Tikkinen-Piri, Rohunen & Markkula, 2018).

Universities are organizations where there is typically an enormous amount and diversity of personal data, some of which are sensitive, concerning their students, teachers, researchers and staff, namely the academic records, the health records, the financial records, the site usage and searches records, the records of extracurricular activities, the records of donations, the photographs, the disciplinary processes, and other personal documents (Podnar, 2017; Marković,

Debeljak & Kadoić, 2019). Therefore, the application of GDPR is mandatory (Podnar, 2017).

This obligation to comply with the GDPR makes universities much more accountable for the data they have, having to justify to national supervisory authorities, their possession, the way they are collected, stored, disposed of and accessed by their teachers, researchers and staff (Cormack, 2017; Marković et al., 2019).

However, compliance with the GDPR causes great difficulties, constraints and challenges for organizations, in terms of the lack of implementation guides with practical orientations for the specific sector of activity, the need for investment in new hardware and software, in hiring specialized human resources, or in the education and training of workers (Gabriela, Cerasela & Alina, 2018).

Universities are no exception to this reality, being organizations that deal with personal data and that have a very specific organizational culture (Podnar, 2017), and in this sense, the legal need to demonstrate compliance with the GDPR causes its implementation to start many times without ensuring that the factors that are critical to the implementation have a level of performance appropriate (Teixeira, Silva & Pereira, 2019). These factors are, as we saw earlier, called by Rockart (1979) as CSFs. For Mufti, Niazi, Alshayeb and Mahmood (2018) readiness model can be defined "as a technique to assess an organization or team based on the specified criteria to represent their level of readiness" (Mufti et al., 2018, p.28613). For Schumacher, Erol, and Sihn (2016), a readiness model seeks to capture "… the starting-point and allow for initializing the development process" (Schumacher et al., 2016, p.161). Public and private organizations are in the process of implementing the GDPR, with some more advanced than others (Laybats & Davies, 2018). However, it is essential that they know the level of readiness they are on to successfully implement the new data protection regulation (Tikkinen-Piri et al., 2018; Privacy Culture, 2019; Lok, Opoku & Baldry, 2018; Dove, 2018). Thus, driven by the need to capture the starting point of the implementation process in the form of the necessary conditions to implement the new data protection regulation, a readiness model is presented, whose main objective is to determine the level of readiness of an HEI, and in particular, a university, to implement the GDPR successfully. This model, as well as the 16 CSFs that comprise it, related to the implementation of GDPR at universities, are some of the practical results of the research work carried out under the PhD in Business Sciences.

Design Science Research was used as a research methodology for generating the readiness model, justified by the fact that the generation of a model while still an artifact fits into one of the possible results of this type of methodology (Hevner & Chatterjee, 2010; Hevner, March, Park, & Ram, 2004; Peffers, Tuunanen, Rothenberger & Chatterjee, 2007; Vaishnavi & Kuechler, 2004).

2. Critical success factors to GDPR implementation in HEIs

As previously mentioned, the readiness model that will be presented in the following sections is based on a set of 16 CSFs related to the implementation of GDPR in HEIs, in particular at public universities. These 16 CSFs, as well as the readiness model presented, are both empirical results of a Ph.D. in Business Administration. Before proceeding to the description of the readiness model, it is therefore important to present the list of 16 CSFs on which the model is based. The research strategy used in its identification was based on a multiple holistic case study focused on Portuguese public universities. In Portugal, the public university higher education system consists of 14 universities (excluding the Military University Institute), each with a Data Protection Officer (DPO).

To determine the 16 CSFs, an invitation was made to the DPOs of the 14 universities to participate in the study, with 8 accepting the invitation with the condition that their participation be made anonymously. Several research methods were used, predominantly qualitative, namely the method of Caralli, Stevens, Willke and Wilson (2004). Thus, when applying the method by Caralli et al. (2004), semi-structured interviews were conducted with 8 DPOs from 14 Portuguese public universities, who agreed to participate in the study. The interviews lasted a total of 10 hours, 30 minutes and 20 seconds. Then, according to the criteria defined by Azevedo et al. (2017), transcripts of the interviews were carried out, resulting in 100,588 characters. After this, the method of Caralli et al. (2004) was applied in the analysis of the transcriptions, resulting in 440 activity statements, which according to Caralli et al. (2004) represent what the organization is doing or what it should be doing in any activity or project to achieve success. These 440 activity statements were then grouped into 30 affinity groups with

some similarity to each other, with each set being assigned a designation named of the support theme, which characterizes all the activity statements contained in that group. The list of 30 CSFs was then derived from the 30 supporting themes.

Then, another research method was applied, more specifically, the Delphi method (Keeney, McKeena & Hasson, 2011; Okoli & Pawlowski, 2004) to prioritize the 30 CSFs previously obtained, having been selected as panel of experts, the 8 DPOs of the national public universities who agreed to continue participating in the study. In order to reach consensus among the panel members (Schmidt, 2007) regarding the ranking to be attributed to the 30 CSFs, two rounds were necessary to complete the process, namely, when a Kendall coefficient of agreement of 0.788 was obtained, and one stability coefficient between rounds measured by Spearman's RHO coefficient of 0.977, complemented by a Kendall tau b of 0.899.

As the 30 CSFs were placed in a global ranking, it was now important to determine the subset of CSFs of greatest importance for the DPOs who were part of the panel of experts of the Delphi method. Thus, the hierarchical cluster analysis technique was used as a way to detect, in the set of 30 CSFs, groups or clusters of CSFs with some statistical homogeneity between them. For the use of this technique, the mean and the respective standard deviation were used as a statistical measure of the proximity between cases or CSFs as they fully characterize each of the 30 CSFs that integrate the ranking with the final 30 CSFs obtained by applying the method of Delphi. The quadratic Euclidean distance was used as a measure of distance between the cases or CSFs under analysis, as well as Ward's connection algorithm to group the cases or CSFs into clusters. In this way, as a result of the application of the hierarchical cluster analysis technique, a list of 16 CSFs related to the implementation of GDPR at universities was obtained, which is presented below, and which will be the basis of the readiness model presented in the following sections.

Table 1 List of 16 CSFs related to the implementation of the GDPR in Universities

	List of 16 CSFs related to the implementation of GDPR in Portuguese public Universities
CSF-1	Empower workers on the GDPR.
CSF-2	Commit top management, with the GDPR.
CSF-3	Implement the GDPR with the involvement of management and workers.
CSF-4	Create a culture for data protection.
CSF-5	Ensure the security of information held by the HEI.
CSF-6	Adapt the Information Systems to the GDPR.
CSF-7	Implement the GDPR with the least negative impact on the HEI.
CSF-8	Use a progressive approach in the implementation of the GDPR.
CSF-9	Start the implementation of the GDPR, by surveying the process network.
CSF-10	Adapt data processing operations to the GDPR, with minimal impact on the HEIs mission.
CSF-11	Conduct security audits generating evidence of the degree of GDPR compliance.
CSF-12	Guarantee the necessary resources and means for the DPO.
CSF-13	Create a decentralized team of pivots for data protection.
CSF-14	Create institutional communication channels dedicated to the GDPR.
CSF-15	Adopt a computer application that allows integrated management of the GDPR operationalization.
CSF-16	Implement a change management process around the GDPR.

Source: the authors

Analyzing the list of 16 CSFs in the table above, it is possible to organize them in 6 organizational dimensions. Thus, we find that 4 CSFs are related to the Human Resources Dimension (CSF 1, 2, 3 and 13), 1 CSF to the Organizational Culture Dimension (CSF 4), 1 CSF to the Financial Dimension (CSF 12), 6 CSFs to the Procedural Dimension (CSF 7, 8, 9, 10, 14 and 16), 3 CSFs to the Information Systems and Technologies Dimension (CSF 5, 6 and 15) and 1 CSF with the Quality Dimension (CSF 11).

3. Research methodology

For the design of the readiness model, this study uses Design Science Research as an approach to research, following the guidelines defined by Hevner et al. (2004) as well as the sequence of processes defined by Peffers et al. (2007). According to Hevner and Chatterjee (2010), Design Science Research is a research paradigm that, through the creation of useful and innovative artifacts, seeks to answer practical questions posed

to people in their daily lives. Thus, according to Ojo, Curry, Janowski and Dzhusupova (2015), Design Science Research "creates and evaluates artifacts that define ideas, practices, technical capabilities, and products through which the analysis, design, implementation and use of information systems can be effectively accomplished" (p.4).

In this study, the domain of application of Design Science Research is related to the creation of an artifact as a model that allows identifying the level of readiness of universities for the implementation of GDPR in HEIs. The problem to be solved involves people, structures, processes, implementation strategies and aspects related to the organizational culture; therefore, the space where the study phenomenon resides is properly framed in the Design Science Research framework defined by Hevner et al. (2004). The following table details the type of Design Science Research (Hevner et al., 2004; Ojo, Curry & Janowski, 2014).

Table 2 Type of Design Science Research

Guideline	Description	Readiness Model Instance
1 – Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.	We developed and artifact, in the form of a readiness model prototype to the implementation of the GDPR at universities.
2 – Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	The prototype of the readiness model, aims to solve the problem of organizations, namely in HEIs that start the implementation of GDPR without having guaranteed a good performance of the CSFs that are necessary for the implementation to be successfully completed. On the other hand, it will also allow to assess, a priori, the existence and good performance of these CSFs, and if they do not exist or are not performing adequately, it will allow the necessary conditions to be created so that they can be adjusted to the necessary level.
3 – Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	The adequacy of the prototype of the GDPR readiness model to the intended purpose, should be assessed, in subsequent stages, namely in the scope of future research, through a case study. The comments that may be collected regarding the performance of the prototype of the readiness model, will be useful for it to be improved, thus increasing its suitability to reality. The prototype of the model as a developed artifact can be evaluated in terms of its fidelity to real-world phenomena, integrity, level of detail, robustness and internal consistency (March & Smith, 1995).
4 – Research Contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	The prototype of the readiness model, with the different CSFs and levels of evaluation, translates into an effective contribution to the domain of study, related to the issue of the implementation of GDPR in the University context, thus increasing the existing knowledge base.
5 - Research Rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.	The prototype of the model built will serve as a knowledge base the 16 CSFs that were previously obtained through the application of rigorous data collection and analysis procedures, previously described. The prototype of the readiness model will be built based on the 16 determined CSFs, using different levels to assess the degree of performance of the CSFs.
6 – Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	The prototype of the model will be built based on a set of information collected in previous stages of the process. The execution of the design cycle, as the central cycle of Design Science Research, will allow, in consecutive stages of design and evaluation, the improvement of the prototype of the readiness model until the desired level is reached (Hevner et al., 2004).
7 – Communications of Research	Design science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The prototype of the readiness model will be presented in the doctoral thesis, in scientific journals, conferences of the specialty, as well as in the DPOs of universities.

Source: Adapted from Hevner et al. (2004, p.83) and Ojo et al. (2014, p.4).

It is now important to present the research framework adopted for the development of the readiness model, which is an instantiation of the framework defined by Hevner et al. (2004). In developing the research framework, the work already done by Habbabeh et al. (2019) was taken in account.

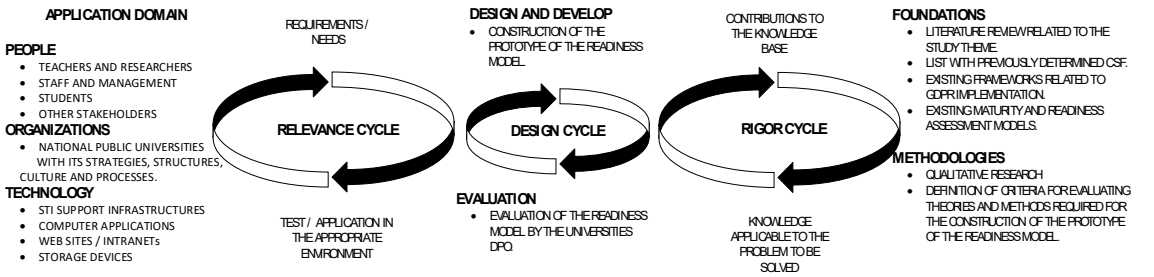

Figure 1 Research Framework for the development of the readiness model
Source: Adapted from Hevner et al. (2004) and Habbabeh et al. (2019, p.224)

On the left side, we can find the space where the phenomenon of interest centered on HEIs resides and where the requirements for the prototype of the readiness model as an artefact are defined as a problem to be solved. The definition of requirements and the assessment of their conformity should be carried out in a continuous relevance cycle, until the readiness model fully responds to the requirements initially identified. In this context, it incorporates people as workers from different professional classes, students and other stakeholders who interact with the university and on whom there is a need to proceed with data protection, applying GDPR conveniently. Then there is the organization, with its data protection strategies, with its structures, culture and processes that shape it. And finally, we have the technology, with the infrastructures, websites, intranets, and other information storage, which allow the operationalization of the strategy defined, superiorly, for the implementation of the GDPR.

On the right side, we have the base where the knowledge necessary to build the artefact as a readiness model is found, being this diversified. More specifically, it will resort to the literature review already carried out related to the study theme, to existing frameworks already analyzed and that also relate to the subject of study, to existing models that allow the assessment of the readiness levels and, mainly, to the 16 CSFs that were previously obtained through the application of rigorous data collection and analysis procedures involving the use of different techniques. What is being sought now is the construction of a readiness model as an artefact, which can be, in the scope of future research, improved through the evaluation and contribution of the DPOs of Portuguese public universities. We also have the methodologies used in the justification and evaluation phase of the created artefact. The rigor cycle is executed continuously, through a process that allows the acquisition of new knowledge, with later incorporation in the model of readiness, until, it is considered that it fully complies with the requirements initially determined.

Finally, we have the central cycle, the most critical one, where in successive interactions, the design and development of the readiness model is carried out. This cycle is being fed with the requirements and tests carried out by the relevance cycle, and for the knowledge obtained continuously through the cycle of rigor.

Based on the research framework in figure 1 as well as steps 1 - Identify a problem, 2 - Define objectives as a Solution, 3 - Design and Development an Artifact and 6 - Communication, from de process model defined by Peffers et al. (2007), the readiness model was designed. Like in other studies (Brendel, Zapadka, & Kolbe, 2018), Steps 4 - Evaluation and 5 - Demonstration, were not implemented, being considered for the next phase, in future work.

4. Readiness model for the implementation of the GDPR

The 16 CSFs previously defined will be the basis for the development of the readiness model. Therefore, it is necessary to assess the performance

level of each of the 16 CSFs. To proceed with the evaluation, the following structure was chosen (Nur Mardhiyah 2013; Tapia, 2009):

- Type of evaluation: The evaluation of each CSF is carried out individually and sequentially, from CSF 1 to CSF 16.
- Levels of the evaluation system: A scale with 5 evaluation levels (level 1 to level 5) will be used to measure the level of performance of each CSF. Models with 5 evaluation levels are widely used in CMM-related maturity models (Eadie, Perera, & Heaney, 2012), as well as in readiness models (Olszak & Mach-Król, 2018; Akbar, Mahmood, Huang, Khan & Shameem, 2020).
- Assessment system: A cumulative assessment system (or measuring model) will be used (Nur Mardhiyah, 2013), meaning that when assessing a CSF at level *n*, one must ensure that level *n-1* is already met.
- Assessment structure: The assessment structure consists of 5 levels, starting with the lowest level - level 1, which determines the allocation of 1 point, progressing to the highest level - level 5, which determines the allocation of 5 points.

Having defined the rules to be used in the assessment of the 16 CSFs as a basis for the readiness model, it is now important for each CSF to indicate the respective assessment structure. For that, different maturity and readiness models that already exist were considered as a starting point. The following table summarizes the proposed evaluation structure for the 16 CSFs.

Table 3 Evaluation structure for the 16 CSFs based on different maturity and readiness models that already exist

CSF	CSFs Assessment Levels	Measurement Model of CSF Performance Level – Adapted from
CSF-1	Level 5 - Continuous training; Level 4 - Structured training; Level 3 - Focused training; Level 2 - Informal training; Level 1 - No training.	Nur Mardhiyah (2013); Thomson and Von Solms (2006)
CSF-2	Level 5 - Commitment, with monitoring and evaluation; Level 4 - Commitment, with frequent interaction; Level 3 - With commitment; Level 2 - With minimal commitment; Level 1 - No commitment.	Nur Mardhiyah (2013)
CSF-3	Level 5 - Permanent involvement; Level 4 - Effective involvement; Level 3 - Informal involvement; Level 2 - Symbolic involvement; Level 1 - No involvement.	Ives and Olson (1984)
CSF-4	Level 5 – Optimized; Level 4 – Embedded; Level 3 – Defined; Level 2 – Development; Level 1 - Ad hoc.	The Department of Internal Affairs (2014)
CSF-5	Level 5 - Total compliance; Level 4 - Acceptable compliance; Level 3 - Basic compliance; Level 2 - Initial compliance; Level 1 - Non-compliant.	Saleh (2011)
CSF-6	Level 5 - Optimized; Level 4 - Managed; Level 3 - Defined; Level 2 - Repeatable; Level 1 - Initial.	Woodhouse (2008)
CSF-7	Level 5 - Optimized; Level 4 - Managed; Level 3 - Defined; Level 2 - Repeatable; Level 1 - Initial.	Domingus (2017)
CSF-8	Level 5 - Adaptable; Level 4 - Adoptive; Level 3 - Defined; Level 2 - Exploratory; Level 1 - Unaware.	Morgan (2011)
CSF-9	Level 5 - Optimized; Level 4 - Managed; Level 3 - Defined; Level 2 - Repeatable; Level 1 - Ad hoc.	AICPA/CICA (2011)
CSF-10	Level 5 - Optimized; Level 4 - Managed; Level 3 - Defined; Level 2 - Repeatable; Level 1 - Initial.	MetaCompliance (2017)
CSF-11	Level 5 - Optimized; Level 4 - Mature; Level 3 - Compliant; Level 2 - Managed; Level 1 - Initial.	Uttam, Kumar & Sujoy (2013)
CSF-12	Level 5 - Optimized; Level 4 - Predictable; Level 3 - Defined; Level 2 - Managed; Level 1 - Initial.	Curtis, Hefley and Miller (2009)
CSF-13	Level 5 - Adaptable; Level 4 - Adoptive; Level 3 - Defined; Level 2 - Exploratory; Level 1 - Nonexistent.	Morgan (2011)
CSF-14	Level 5 - Continuous improvement; Level 4 - Managed and focused; Level 3 - Structured and proactive; Level 2 - Reactive; Level 1 - Initial.	UNECE (2019); Kolomiyets (2020)
CSF-15	Level 5 - Optimized; Level 4 - Integrated; Level 3 - Defined; Level 2 - Development; Level 1 - Initial.	PAHO (2020)
CSF-16	Level 5 - Organizational competence; Level 4 - Organizational standards; Level 3 - Multiple projects; Level 2 - Isolated projects; Level 1 - Ad-hoc or absent.	Prosci (2004)

Source: the authors' own elaboration

In the previous table for the 16 CSFs, and considering that the 16 CSFs are ranked in descending order in relation to their degree of relevance, it was understood to weigh the different CSFs differently. The calculation of the level of readiness for each CSF follows the following principles:

- A first weighting is carried out for each CSF according to its position or relevance. In this way, CSF 1, the most important CSF will have an added weight of 100% in relation to the number of points assigned to it, CSF 2 will have an added weight of 87.5% in relation to the number of points assigned to it, the CSF 3 will have an added weight of 81.25% in relation to the number of points assigned to it, and so on until we reach CSF 16 (least important CSF), which has no added weight in relation to the number of points assigned to it.
- With a second weighting, it is guaranteed that the increase previously attributed is different, depending on whether the CSF has been assessed at level 1, 2, 3, 4 or 5. Thus, for example, for CSF 1 which is the most relevant CSF , has a score increase of 100% distributed as follows: if the level at which it was assessed is level 1, the score awarded is 1 point (its value); if the level at which it was assessed was level 2, the score awarded is 2.5 points (its value plus 25%); if the level at which it was assessed was level 3, the score awarded is 4.5 points (its value plus 50%); if the level at which it was assessed was level 4, the score awarded is 7 points (its value plus 75%), if the level at which it was assessed was level 5, the score awarded is 10 points (its value increased by 100%).

In the following table (Table 4), we can see the different scores that each CSF can obtain, considering the aforementioned weights.

Table 4 Weighting attributed to the 16 CSFs

	SCALE WEIGHTING EVALUATION															
Increased weight of CSF		**Increased weight Level 1**	**Points allocated**	**Weighted rating**	**Increased weight Level 2**	**Points allocated**	**Weighted rating**	**Increased weight Level 3**	**Points allocated**	**Weighted rating**	**Increased weight Level 4**	**Points allocated**	**Weighted rating**	**Increased weight Level 5**	**Points allocated**	**Weighted rating**
FCS 1	100.00%	0.00%	1	1	25.00%	2	2.50	50.00%	3	4.50	75.00%	4	7.00	100.00%	5	10.00
FCS 2	87.50%	0.00%	1	1	21.88%	2	2.44	43.75%	3	4.31	65.63%	4	6.63	87.50%	5	9.38
FCS 3	81.25%	0.00%	1	1	20.31%	2	2.41	40.63%	3	4.22	60.94%	4	6.44	81.25%	5	9.06
FCS 4	75.00%	0.00%	1	1	18.75%	2	2.38	37.50%	3	4.13	56.25%	4	6.25	75.00%	5	8.75
FCS 5	68.75%	0.00%	1	1	17.19%	2	2.34	34.38%	3	4.03	51.56%	4	6.06	68.75%	5	8.44
FCS 6	62.50%	0.00%	1	1	15.63%	2	2.31	31.25%	3	3.94	46.88%	4	5.88	62.50%	5	8.13
FCS 7	56.25%	0.00%	1	1	14.06%	2	2.28	28.13%	3	3.84	42.19%	4	5.69	56.25%	5	7.81
FCS 8	50.00%	0.00%	1	1	12.50%	2	2.25	25.00%	3	3.75	37.50%	4	5.50	50.00%	5	7.50
FCS 9	43.75%	0.00%	1	1	10.94%	2	2.22	21.88%	3	3.66	32.81%	4	5.31	43.75%	5	7.19
FCS 10	37.50%	0.00%	1	1	9.38%	2	2.19	18.75%	3	3.56	28.13%	4	5.13	37.50%	5	6.88
FCS 11	31.25%	0.00%	1	1	7.81%	2	2.16	15.63%	3	3.47	23.44%	4	4.94	31.25%	5	6.56
FCS 12	25.00%	0.00%	1	1	6.25%	2	2.13	12.50%	3	3.38	18.75%	4	4.75	25.00%	5	6.25
FCS 13	18.75%	0.00%	1	1	4.69%	2	2.09	9.38%	3	3.28	14.06%	4	4.56	18.75%	5	5.94
FCS 14	12.50%	0.00%	1	1	3.13%	2	2.06	6.25%	3	3.19	9.38%	4	4.38	12.50%	5	5.63
FCS 15	6.25%	0.00%	1	1	1.56%	2	2.03	3.13%	3	3.09	4.69%	4	4.19	6.25%	5	5.31
FCS 16	0.00%	0.00%	1	1	0.00%	2	2.00	0.00%	3	3.00	0.00%	4	4.00	0.00%	5	5.00

Source: the authors' own elaboration

Considering the previous definitions, the execution level of each CSF (M_{CSF}) and the readiness level of the HEI (Vnp) is calculated as follows:

The execution level of each CSF:

$$M_{CSF} = N + (N * pn)$$

M_{CSF} = Number of points related to the level of execution of the CSF.

N = Number of points at which the CSF was assessed.

pn = Weight of the level at which the CSF was assessed.

HEI's readiness level:

$$Vnp = \sum_{i=1}^{16} M_{CSF}$$

Vnp = Value of the organization's readiness level
M_{CSF} = Execution level of each of the 16 CSFs

In this way, the HEI's readiness level is identified according to the range of points in the following table.

Table 5 Criterion for assessing HEI's readiness level

Range of points	Readiness Levels
16 – 35 points	N1 - Initial
36 – 55 points	N2 – Repeatable
56 – 76 points	N3 – Defined
77 – 97 points	N4 – Managed
98 – 118 points	N5 - Optimized

Source: Adapted from Paulk, Curtis, Chrissis, & Weber (1993)

In the table above, each qualitative level relative to the HEI's readiness level, can be analyzed as follows:

- N1 – Initial - The implementation of the GDPR has started, without the organization having created and maintained the necessary conditions for this purpose. The implementation process is based on informality and ad-hoc procedures carried out in the units and services. The DPO does not have the necessary visibility in the organization, nor is it involved in all processes where there is a need to ensure that data protection complies with the GDPR. In this state, the organization focuses on the need to demonstrate that it is acting in accordance with the GDPR, without, however, having any practical evidence of this conformity, resulting from security audits.
- N2 – Repeatable - Top management is minimally committed to the implementation process, providing minimal training to workers, facilitating the connection between the units and services with the DPO, temporarily allocating resources to the implementation process, providing communication channels that are not yet comprehensive. There are no comprehensive policies or procedures to ensure information security, nor are the necessary investments made to increase Information Systems and Technologies (ITS) security levels. The organization's culture is still indifferent to information security. The processes and procedures are not fully documented, and do not cover all areas of the organization's business. Data from data processing operations are collected only in some of the most critical units; however, they are not aggregated, shared or used to support decision making.
- N3 – Defined - There is an effective commitment from top management, with respect for the technical autonomy of the DPO that interacts autonomously and regularly with the units and services.
There are minimum resources allocated to the DPO, and workers are provided with training geared to specific situations, with workers focused and aware of the information security practices that they must consider in all situations. The university reviews its security policies and procedures regularly and in accordance with the good practices of an information security management system (ISMS), however, its monitoring is carried out in an ad-hoc manner. Investment in ITS is planned according to cost / benefit. There is a standardized data protection procedure, being communicated to the entire organization, which knows what is expected of it at this level. The processes and procedures necessary for the functioning of the university are documented and critical functions have been assessed. Data from data processing operations are collected electronically, however, their integration is still manual.
- N4 – Managed - Top management has a strong commitment to the implementation of the GDPR, allocating permanent resources and conducting frequent interactions with the DPO, in order to monitor and investigate the status of the process, while respecting the technical independence of the DPO. Training is provided to workers oriented to real and concrete situations where it is necessary to deal with personal data. The protection of personal data is present in the design of processes and in Information Systems (IS) to support the organization's mission. Information security is treated in a centralized manner, with the interaction of users with ITS seen as a vulnerability. The

organization reviews its information security practices in accordance with the recommendations of an ISMS. The need to guarantee the privacy of all stakeholders is no longer seen as a threat, but as a way for the organization to be transparent in the way it deals with personal data. There is a central register of data processing operations in progress in the organization. Security and GDPR compliance audits are carried out on a regular basis by internal experts. There is a strong use of the available communication channels to disseminate information about the GDPR. Data on data processing operations are collected from all units and services and are integrated in real time.

- N5 – Optimized - Top management often interacts with the DPO in order to assess its performance and the state of implementation of the GDPR. Continuous training is available to all workers in order to promote updating and professional development in areas related to data protection. Information security is permanently monitored by operating an ISMS at the university. There is regular investment in ITS, according to well-defined cost-benefit criteria. The confidentiality, integrity and availability of information is guaranteed, with minimal risk to information security. The organization uses the GDPR as a way to mark a distinctive position in relation to the competition, having a culture strongly oriented towards data protection. The process network is regularly reviewed, allowing for continuous improvement of processes, with data protection policies and updated privacy notices, with the process of conducting audits centered on the areas of activity critical to the organization. The recording of data processing operations is performed automatically in all units and services, with data being made available in an integrated manner.

Based on the OAWSP Maturity Model, we can see in Figure 2 below how the execution level of each of the 16 CSFs should evolve. What is expected is that all 16 CSFs have an assessment that allows them to be as much as possible within the cycle.

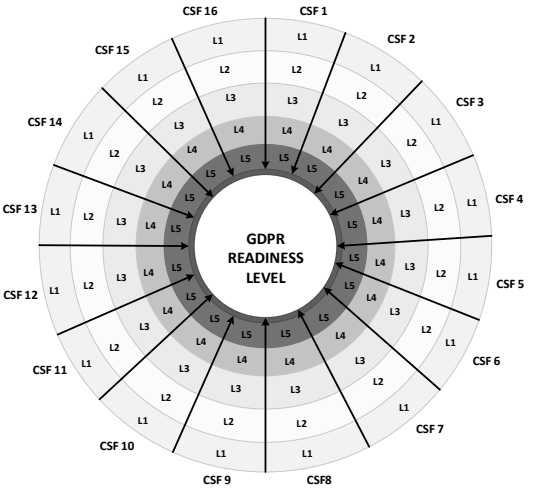

Figure 2 Identification of the readiness level for the GDPR implementation
Source: the authors

Considering that the 16 CSFs are organized in dimensions, it is possible to check the execution level of each of the dimensions: D1 - Human Resources, D2 - Organizational Culture, D3 - Financial, D4 - Processes, D5 - Information Systems and Technologies and D6 - Quality, for the level of readiness of the organization. The following table indicates the weight of each dimension as well as the number of maximum points that it can have, if each of the CSF that compose it is assessed at level 5 with the weighting referred to in Table 4.

Table 6 Weight and maximum number of points by dimension

Organizational Dimensions	Nº of CSFs that are part of the organizational dimension	Relative weight of the organizational dimension (PR_D)	Maximum number of points of the organizational dimension ($NPmax_D$)
Dimension 1 - Human Resources	4 (CSF 1; CSF 2; CSF 3; CSF 13)	25% (4/16)	34,98 (10+9,38+9,06+5,94)
Dimension 2 - Organizational Culture	1 (CSF 4)	6,25% (1/16)	8,75
Dimension 3 – Financial	1 (CSF 12)	6,25% (1/16)	6,25
Dimension 4 – Processes	6 (CSF 7; CSF 8; CSF 9; CSF 10; CSF 14; CSF 16)	37,5% (6/16)	40,00 (7,81+7,5+7,19+6,88+5,63+5)
Dimension 5 - Information Systems and Technologies	3 (CSF 5; CSF 6; CSF 15)	18,75% (3/16)	21,88 (8,44+8,13+5,31)
Dimension 6 – Quality	1 (CSF 11)	6,25% (1/16)	6,56

Source: the authors' own elaboration

The absolute level of execution of each of the Dimensions (NAE_D) is obtained by adding the execution level (M_{CSF}) of the CSFs that compose it, dividing this value by the number of maximum points ($NP_{Max\,(D)}$) that each of the dimensions can have. The following formulas illustrate what has just been mentioned.

$$NAE_{D1}= \frac{M_{FCS(CSF1)}+ M_{CSF(CSF2)}+ M_{CSF(CSF3)}+ M_{CSF(CSF13)}}{NP_{Max\,(D1)}}$$

$$NAE_{D2}= \frac{M_{CSF(CSF4)}}{NP_{Max\,(D2)}}$$

$$NAE_{D3}= \frac{M_{CSF(CSF12)}}{NP_{Max\,(D3)}}$$

$$NAE_{D4}= \frac{M_{CSF(CSF7)}+ M_{CSF(CSF8)}+ M_{CSF(CSF9)}+ M_{CSF(CSF10)}+ M_{CSF(CSF14)}+M_{CSF(CSF16)}}{NP_{Max\,(D4)}}$$

$$NAE_{D5}= \frac{M_{CSF(CSF5)}+ M_{CSF(CSF6)}+ M_{CSF(CSF15)}}{NP_{Max\,(D5)}}$$

$$\boldsymbol{NAE_{D6}= \frac{M_{CSF(CSF11)}}{NP_{Max\,(D6)}}}$$

Considering that each dimension has, as we saw in table 6, a certain relative weight (PR_D), in relation to the other dimensions, it is possible to calculate the relative contribution of execution of each dimension to the level of readiness of the organization. The relative level of execution of each of the Dimensions (NRE_D) is obtained by multiplying the absolute level of execution of each of the Dimensions (NAE_D), by its relative weight ($\boldsymbol{PR_D}$) indicated in the previous table. The following formulas illustrate what has just been mentioned.

$$NRE_{D1}= (NAE_{D1} * PR_{D1})$$
$$NRE_{D2}= (NAE_{D2} * PR_{D2})$$
$$NRE_{D3}= (NAE_{D3} * PR_{D3})$$
$$NRE_{D4}= (NAE_{D4} * PR_{D4})$$
$$NRE_{D5}= (NAE_{D5} * PR_{D5})$$
$$NRE_{D6}= (NAE_{D6} * PR_{D6})$$

The readiness model shown in the following figure (Figure 3) follows the principles listed by Khan, Niazi and Ahmad (2008), fulfilling the requirement of having to be useful for users and having to be simple to use, avoiding the need for complexification.

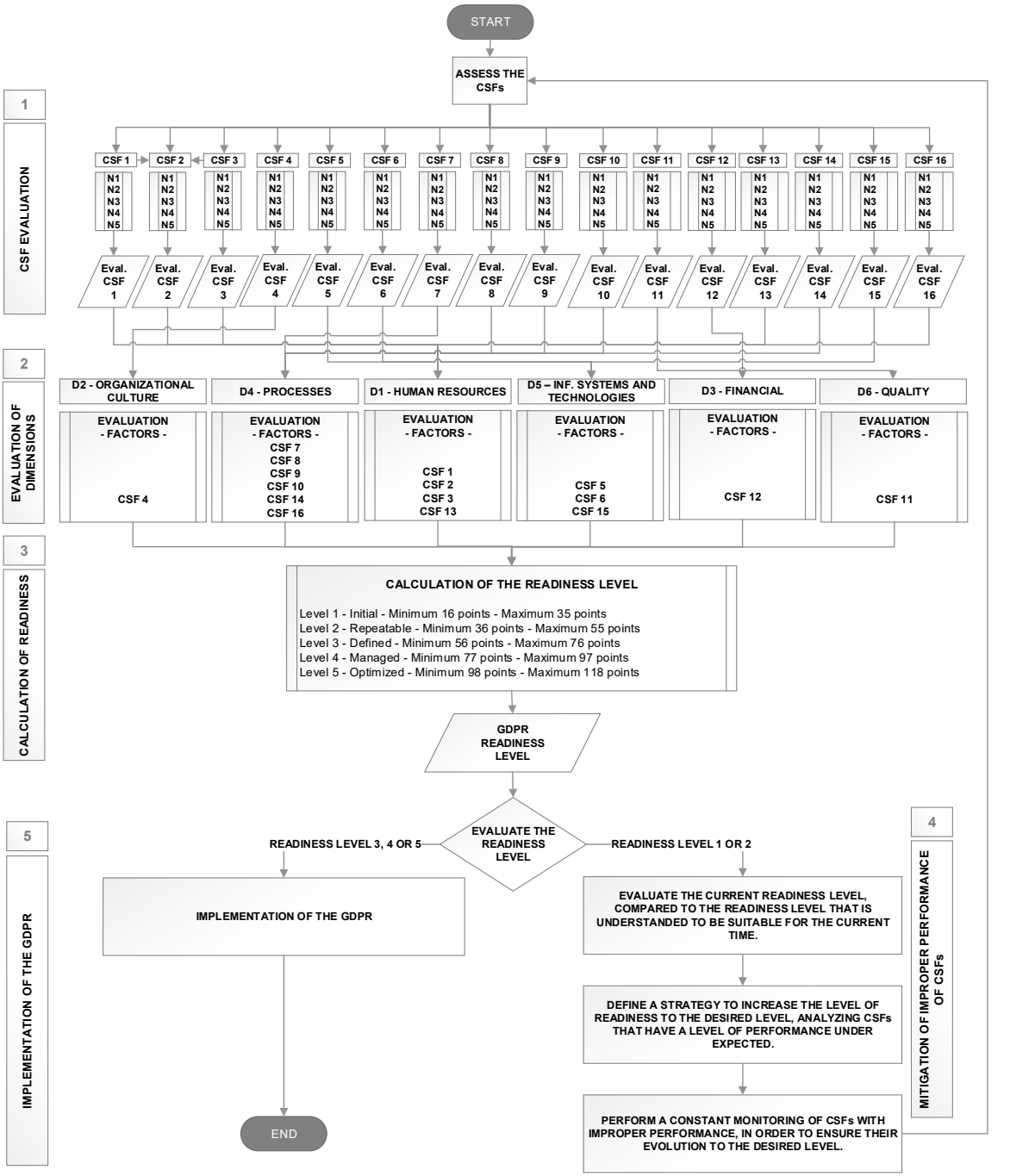

Figure 3 Readiness model proposed for the implementation of GDPR, based on CSFs
Source: the authors

5. Discussion

The readiness model presented in the previous figure (Figure 3) consists of 6 phases. Thus, in the first phase, the performance level of each of the 16 CSFs is assessed individually and sequentially. For this purpose, each CSF must be evaluated using the evaluation structure shown in table 3. This way, we obtain the level of execution (M_CSF) of each of the 16 CSFs. The evaluation of the performance level of each of the 16 CSFs allows knowing which CSFs are performing poorly for the GDPR implementation process, thus allowing HEI managers to make the necessary adjustments at any time.

Then, at the level of organizational functioning, the performance level of the 6 organizational dimensions in the model is assessed - D1 - Human Resources, D2 - Organizational Culture, D3 - Financial, D4 - Processes, D5 - Information Systems and Technologies and D6 - Quality. For this purpose, based on the individual assessment of the 16 CSFs previously carried out, we obtain the absolute (NAE_D) and relative (NRE_D) contribution of each organizational dimension using the formulas identified in the previous section. With this evaluation, it is possible to perceive the organizational dimensions with an inadequate performance level for the process of implementation of the GDPR.

Next, we move on to the third stage of assessing HEI's readiness level for the implementation of the GDPR. The HEI readiness level (Vnp), is obtained by adding the execution level of the 16 CSFs, which, when mapped in the intervals defined in Table 5, allows the identification of the HEI's readiness level for the implementation of the GDPR.

With the achievement of the HEI's level of readiness for the implementation of the GDPR, the model presents two distinct paths. For a readiness level 1 or 2, in a continuous improvement cycle, it is intended that HEI will evaluate the results obtained, and that it will implement the necessary remediation strategies, in order to increase the performance of CSFs that are underperforming. This process must be carried out continuously until it is verified that the HEI's readiness level is already at levels 3, 4 or 5 and in that case, the institution has the conditions to enter the GDPR implementation phase.

The use of this model as a management tool allows HEI to have a broad view of the factors that are critical for the implementation of the GDPR, mapping them into different organizational dimensions, with special emphasis on those that relate to the procedural component, as well as for the management of human resources, as absolutely critical dimensions for the implementation process. On the other hand, it also allows the institution, in moments after the start of the implementation process, to be able, due to the implementation of internal control mechanisms, as well as in the scope of continuous improvement processes, to check the CSFs that may be showing signs decrease in performance. In this way, it is possible to correct and act proactively in these CSFs, avoiding compromising in the medium term the quality of the implementation process already carried out.

Conclusions, limitations and future work

Design Science Research was used, as a research methodology in information systems, to proceed with the design of a model (artifact) of readiness for the implementation of the GDPR in HEIs. The developed model consists of 5 distinct phases. Thus, in phase 1, each of the 16 CSFs is evaluated on a scale with 5 levels of readiness, from 1 to 5, in which level 1 represents the initial or preparatory level of readiness, continuing growing up to level 5 of optimized, where the organization is considered to have the 16 CSFs with a high level of execution.

In phase 2, the dimensions that fit the different CSFs are evaluated, in order to understand the organizational dimensions that need to be worked on better in order to obtain a better performance in the CSF that constitute them. Next, we move on to phase 3, where the organization's readiness level is calculated, measured once again on a scale of 1 to 5, with the organization being classified in each of the different levels, according to the score obtained at the end – between 16 and 35 points at level 1, between 36 and 55 points at level 2, between 56 and 76 points at level 3, between 77 and 97 points at level 4 and between 98 and 118 points at level 5. In phase 4, a mitigation or remediation cycle is carried out for the worst performing CSF, whenever the organization obtains a score that places it at levels 1 or 2. Phase 5 of GDPR implementation is carried out whenever the organization obtains a readiness level of 3,4 or 5.

This model is a practical contribution to the development of the study area related to the implementation of GDPR in HEIs. With this model, HEIs are able to quickly understand, through the analysis of the performance level of the 16 CSFs, which are the organizational areas that need more attention from management, with a possible reinforcement in the allocation of resources and means to the process of implementation of the GDPR. The constant measurement of the CSFs performance level and the consequent calculation of the HEI's readiness level for the GDPR also allows, in the context of a process of continuous improvement, a proactive action to correct aspects that may be degrading the organizational performance in the field of data protection.

This is not an easy task for any medium/large organization, and much less for HEIs, where in a very complex academic culture, thousands of students, professors, researchers and non-teaching

workers interact daily in the most various activities. In this sense, the problem that we propose to solve, with the design and development of a readiness model for the implementation of the GDPR in Universities, involves aspects related to people who deal with personal data every day, within the scope of their functions and roles, making use of a set of skills acquired for this purpose. In addition to people, it also involves the strategy, structures, processes and culture of universities, as well as technology in the form of their infrastructures and applications. In this way, it is considered that the availability of a readiness model will allow knowing the different activities of the HEIs where a reinforcement of resources may be necessary, increasing this the existing knowledge about the performance of the CSFs essential to the implementation of the GDPR.

As a limitation, there is the fact that the model presented has not been tested, therefore it was not possible to comply with steps 4 and 5 of the process model defined by Peffers et al. (2007) for the design of artifacts using the Design Science Research approach.

These two steps are considered for the scope of future work, where they can be carried out by conducting a multiple case study. In that manner, the model can be applied and contributions can be obtained from the HEIs DPOs. These contributions allow the improvement of the readiness model, namely, in the CSFs assessment structure, as well as in the tuning of the intervals related to the 5 levels of readiness in which a given HEI may be.

References

AICPA/CICA. (2011). *Privacy Maturity Model*. American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants. Retrieved February 6, 2020, from https://vvena.nl/wp-content/uploads/2018/04/aicpa_cica_privacy_maturity_model.pdf

Akbar, M. A., Mahmood, S., Huang, Z., Khan, A. A., & Shameem, M. (2020). Readiness model for requirements change management in global software development. *Journal of Software: Evolution and Process, 32*(10), e2264,1-32. https://doi.org/10.1002/smr.2264

Azevedo, V., Carvalho, M., Fernandes-Costa, F., Mesquita, S., Soares, J., Teixeira, F., & Maia, Â. (2017). Interview transcription: conceptual issues, practical guidelines, and challenges. *Revista de Enfermagem Referência, 4*(14), 159-167. https://doi.org/10.12707/RIV17018

Brendel, A.B., Zapadka, P., & Kolbe, L.M. (2018). Design science research in green IS - analyzing the past to guide future research. *ECIS*.

Caralli, R. A., Stevens, J. F., Willke, B. J., & Wilson, W. R. (2004). *The critical success factor method: establishing a foundation for enterprise security management*. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst. https://doi.org/10.1184/R1/6585107.v1

Cormack, A. (2017). *A year to get your act together: How universities and colleges should be preparing for new data regulations.* FE News. Retrieved March 25, 2020, from https://www.fenews.co.uk/fe-voices/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations/

Crutzen, R., Peters, G.-J. & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, *34*(11), 1347-1357. https://doi.org/10.1080/08870446.2019.1606222

Curtis, B., Hefley, B., & Miller, S. (2009). *People capability maturity model (P-CMM) version 2.0*. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst. https://doi.org/10.21236/ADA512354

Domingus, M. (2017). *Capability Maturity Model for Safeguarding Privacy in Academic Research.*

Dove, E. S. (2018). The EU General Data Protection Regulation: implications for international scientific research in the digital era. *Journal of Law, Medicine & Ethics, 46*(4), 1013-1030. https://doi.org/10.1177/1073110518822003

Eadie, R., Perera, S. and Heaney, G. (2012). Capturing maturity of ICT applications in construction processes. *Journal of Financial Management of Property and Construction,17*(2),176-194. https://doi.org/10.1108/13664381211246624

Fernandes, J., Machado, C. & Amaral, L. (2022). Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions. *Digital Policy, Regulation and Governance*, *24*(4), 355-379. https://doi.org/10.1108/DPRG-03-2021-0041

Gabriela, G., Cerasela, S. E., & Alina, C. A. (2018). The EU General Data Protection Regulation *implications* for Romanian *small* and *medium-sized enterprises*. *Ovidius University Annals (Economic Sciences Series), 18*(1), 88-91.

Gstrein,O. & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, *35*(3), open-access. https://doi.org/10.1007/s13347-022-00497-4

Habbabeh, A., Schneider, B., & Asprion, P. M. (2019). Data privacy assessment: an exemplary for higher education institutions. *International Journal of Management, Knowledge and Learning, 8*(2), 221-241.

Hevner, A., & Chatterjee, S. (2010). Design science research in information systems in design research in information systems. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_2

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Hoofnagle, C., van der Sloot, B. & Borgesius, F. (2019) The European Union general data protection regulation: what it is and what it means, *Information & Communications Technology Law*, *28*(1), 65-98. https://doi.org/10.1080/13600834.2019.1573501

Ives, B., & Olson, M. H. (1984). User involvement and MIS success: a review of research. *Management Science, 30*(5), 586-603. https://doi.org/10.1287/mnsc.30.5.586

Khan, S., Niazi, M., & Ahmad, R. (2008, August). *A readiness model for software development outsourcing vendors*. In 2008 IEEE International Conference on Global Software Engineering (273-277). IEEE. https://doi.org/10.1109/ICGSE.2008.37

Keeney, S., McKenna, H., & Hasson, F. (2011). *The Delphi technique in nursing and health research*. United Kingdom, Wiley-Blackwell. https://doi.org.10.1002/9781444392029

Kolomiyets T. (2020). The United Nations Economic Commission for Europe (UNECE) - *Internal Communications and Employee Engagement Maturity Model*. Retrieved May, 25, 2020, from https://statswiki.unece.org/display/SCFP/Maturity+model

Laybats, C., & Davies, J. (2018). GDPR: Implementing the regulations. *Business Information Review*, *35*(2), 81-83. https://doi.org/10.1177/0266382118777808

Li, H., Yu, L. & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1),1-6. https://doi.org/10.1080/1097198X.2019.1569186

Lok, K. L., Opoku, A., & Baldry, D. (2018). Design of sustainable outsourcing services for facilities management: critical success factors. *Sustainability, 10*(7), 2292. https://doi.org/10.3390/su10072292

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems, 15*(4), 251-266. https://doi.org/10.1016/0167-9236(94)00041-2

Marković, M. G., Debeljak, S., & Kadoić, N. (2019). Preparing students for the era of the General Data Protection Regulation (GDPR). *TEM Journal, 8*(1), 150-156. http://doi.org/10.18421/TEM81-21

MetaCompliance (2017). *GDPR Best Practices Implementation Guide - Transforming GDPR Requirements into Compliant Operational Behaviours*. Asociación Española de empresas de Seguridad (AES). Retrieved February 6, 2020, from https://www.aesseguridad.es/wp-content/uploads/2020/09/CBS360A.pdf

Mufti, Y., Niazi, M., Alshayeb, M., & Mahmood, S. (2018). A readiness model for security requirements engineering. *IEEE Access, 6*, 28611-28631. https://doi.org/10.1109/ACCESS.2018.2840322

Morgan, J. (2011). *The Five-Step Maturity Model for Building a Collaborative Organization*. Chess Media Group. Retrieved May 21, 2020, from https://www.cloudave.com/27679/the-five-step-maturity-model-for-building-a-collaborative-organization/

The Department of Internal Affairs (2014). *User guide for the Privacy Maturity Assessment Framework (version 1.0)*. Published by Department of Internal Affairs on behalf of the New Zealand Government. Retrieved May 21, 2020, from https://psi.govt.nz/privacyleadership/

Nur Mardhiyah, A. (2013). *A model for organisational readiness in information technology (IT) project implementation in the Malaysian construction industry/Nur Mardhiyah Aziz*, Unpublished doctoral dissertation, University of Malaya, Kuala Lumpur.

Ojo, A., Curry, E., Janowski, T., & Dzhusupova, Z. (2015). Designing next generation smart city initiatives: The SCID framework. *In Transforming city governments for successful smart cities* (pp. 43-67). Springer, Cham. https://doi.org/10.1007/978-3-319-03167-5_4

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & management, 42*(1), 15-29. https://doi.org/10.1016/j.im.2003.11.002

Olszak, C. M., & Mach-Król, M. (2018). A conceptual framework for assessing an organization's readiness to adopt big data. *Sustainability, 10*(10), 3734. https://doi.org/10.3390/su10103734

PAHO (2020). *Pan American Health Organization* - IS4H Maturity Model Assessment Tool: Data Management and Information Technologies. Retrieved May 21, 2020, from https://www.paho.org/ish/images/docs/about-IS4H-mm.pdf?ua=1

Paulk, M., Curtis, W., Chrissis, M., B., & Weber, C. (1993). *Capability Maturity Model for Software (Version 1.1)* (CMU/SEI-93-TR-024). Software Engineering Institute, Carnegie Mellon University. Retrieved June 6, 2020, from http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=11955

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Podnar, K. (2017). Is your university ready to pass the GDPR exam? Kristina Podnar. Retrieved February 6, 2020, from https://www.kpodnar.com/post/is-your-university-ready-to-pass-the-gdpr-exam

Privacy Culture (2019). *The GDPR Maturity Framework*. IAPP. Retrieved June 9, 2020, from https://iapp.org/media/pdf/resource_center/PrivacyCulture_GDPR_Maturity_Framework.pdf

Prosci (2004). *Change Management Maturity Model.* PROSCI People, Change, Results. Retrieved June 6, 2020, from https://www.prosci.com/blog/the-five-areas-that-define-your-organizational-change-capability

Rockart, J. F. (1979). Chief executives define their own data needs. *Harvard Business Review, 57*(2), 81-93.

Saleh, M. F. (2011). Information security maturity model. *International Journal of Computer Science and Security (IJCSS), 5*(3), 21.

Schmidt, R. C. (2007). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences*, *28*(3), 763-774. https://doi.org/10.1111/j.1540-5915.1997.tb01330.x

Schumacher, A., Erol, S., & Sihn, W. (2016). A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises. *Procedia CIRP, 52*(1), 161-166. https://doi.org/10.1016/j.procir.2016.07.040

Staff, C.A.C.M. (2021). Differential privacy: the pursuit of protections by default. *Communications of the ACM*, *64*(2), 36-43. https://doi.org/10.1145/3434228

Syed, R., Bandara, W., French, E., & Stewart, G. (2018). Getting it right! Critical success factors of BPM in the public sector: a systematic literature review. *Australasian Journal of Information Systems, 22*(0), 1-39. https://doi.org/10.3127/ajis.v22i0.1265

Tapia, S. (2009). *Assessing business-IT alignment in networked organizations*. Unpublished doctoral dissertation, University of Twente. Enschede, Holland.

Teixeira, G., Silva, M. and Pereira, R. (2019). The critical success factors of GDPR implementation: a systematic literature review. *Digital Policy, Regulation and Governance, 21*(4), 402-418. https://doi.org/10.1108/DPRG-01-2019-0007

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Thomson, K. L., & von Solms, R. (2006). Towards an information security competence maturity model. *Computer fraud & security, 2006*(5), 11-15. https://doi.org/10.1016/S1361-3723(06)70356-6

UNECE (2019). *Economic Commission for Europe. Conference of European Statisticians* - Strategic Communications Framework for Statistical Institutions. Retrieved May 22, 2020, from https://www.unece.org/fileadmin/DAM/stats/documents/ece/ces/2019/7_Strategic_commmunication_framework_for_consultation.pdf

Uttam, B., Kumar, R. A., & Sujoy, D. (2013*). Audit Maturity Model. Cognizant Technology Solutions*, 155-161. https://doi.org/10.5121/csit.2014.4115

Vaishnavi, V., & Kuechler, W. (2004). *Design research in information systems.* Design science research in information systems and technology. Retrieved May 21, 2020, from http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf

Woodhouse, S. (2008). An isms (im)-maturity capability model. In *2008 IEEE 8th International Conference on Computer and Information Technology Workshops* (pp. 242-247). IEEE. https://doi.org/10.1109/CIT.2008.Workshops.46

Wu, P., Vitak, J. & Zimmer, M. (2020). A contextual approach to information privacy research. *Journal of the Association for Information Science and Technology*, *71*(4), 485-490. https://doi.org/10.1002/asi.24232

Ojo, A., Curry, E., & Janowski, T. (2014). *Designing next generation smart city initiatives - Harnessing findings and lessons from a study of ten smart city programs*. Proceedings of the European Conference on Information Systems (ECIS) 2014, Tel Aviv, Israel. Retrieved September, 4, 2020, from https://aisel.aisnet.org/ecis2014/proceedings/track15/12

✉ Correspondence

José Manuel Machado Fernandes

University of Minho, School of Economics and Management
Largo do Paço, 4704-553 Braga, Portugal

E-mail: jf@reitoria.uminho.pt