Addressing SME Characteristics for Designing Information Security Maturity Models

Bilge Yigit Ozkan, Marco Spruit

Addressing SME Characteristics for Designing Information Security Maturity Models

Bilge Yigit Ozkan[1[0000-0001-6406-356X]] and Marco Spruit[1[0000-0002-9237-221X]]

[1] Utrecht University, Department of Information and Computing Sciences, Princetonplein 5, 3584 CC Utrecht, Netherlands
b.yigitozkan@uu.nl, m.r.spruit@uu.nl

Abstract. This paper identifies the effects of small and medium-sized enterprises' (SME) characteristics on the general design principles for maturity models in the information security domain. The purpose is to guide the research on information security maturity modelling for SMEs that will fit in form and function for their capability assessment and development purposes, and promote organizational learning and development. This study reviews the established frameworks of general design principles for maturity models and projects the design requirements of our envisioned information security maturity model for SMEs. Maturity models have different purposes of uses (descriptive, prescriptive and comparative) and design principles with respect to these purposes of uses. The mapping of SME characteristics and design principles facilitates the development of an information security maturity model that systematically integrates the desired qualities and components addressing SME characteristics and requirements.

Keywords: Information Security, Maturity Model, Assessment, Process Improvement, Organisational Learning, SME

1 Introduction

Small and medium-sized enterprises (SMEs), which are the predominant form of enterprise and make up 99.8% of European enterprises in the Organisation for Economic Co-operation and Development (OECD) area [1], are ill-prepared for cyberattacks [2].

One way of tackling the challenges of managing and implementing information security is through the use of maturity models [2]. Originating from software engineering, maturity modelling is a method for representing domain specific knowledge in a structured way in order to provide organizations with an evolutionary process for assessment and improvement [3] [4].

Previous research shows that maturity models promote greater levels of organisational learning [5]. Organisational capabilities are developed through organisational learning processes [6]. From a socio-technical perspective, since information security domain is quite complex [7], the value of maturity models is indisputable for developing the necessary information security capabilities. Addressing the characteristics and the requirements of the target organisation will yield to more effective individual and organizational learning and development.

From the perspective of information security maturity models (ISMM), there is a need to facilitate SMEs with tailor-made models that are more situation aware and that can adapt to their specific needs [8]. In a recent study for adaptive information security modelling for SMEs, the authors state that utilisation of maturity models for self-assessing information security capabilities can be a remedy for SMEs [2].

There have been studies conducted on the development and design of maturity models. Mettler [9] investigated maturity models as a subject of design science. Becker et al. considering maturity models as design science artifacts, propose a procedure model that distinguishes eight phases in the development of maturity models [4]. De Bruin et al. propose a methodology to generalize the phases of developing a maturity model and outlined the main phases of generic model development [10]. Pöppelbuß and Röglinger propose a framework of general design principles for maturity models [11].

The utilisation of maturity models in different organisational structures has been another aspect that has been studied in the literature. Mettler and Rohner present a first design proposition of a situational maturity model [12]. In the information security domain, there have been several studies addressing the effect of organisational characteristics. Mijnhardt et al. investigated organisational characteristics influencing SME information security maturity [8]. In this study, they focused on four different categories of characteristics (General, in and out sourcing, IT dependency and IT complexity). These categories include 11 characteristics such as size, revenue, number of employees, time an organization can run without IT support.

Baars et al. conclude that a maturity framework should consider the differences between the characteristics of their target organizations [13]. There have also been cluster based approaches to SME information security [14] [2].

The design principles applied during the development and design of the maturity models affect their applicability in several ways. For example, designing a situational-aware maturity model enables its adaption to different organisational contexts. Being inspired by the studies investigating the maturity models as design artifacts [4] [9] and those providing guidance on the design and development of maturity models [10] [11], the research question this paper addresses is formulated as follows.

"How can SME characteristics be addressed for designing information security maturity models?"

The purpose is to support the development of SME aware ISMMs as design artifacts that will promote greater levels of individual and organisational learning.

To answer this research question, we used the SME characteristics resulting from a literature review [15]. These characteristics guided us to identify the "boundary/context" as discussed by Cronholm & Göbel in their study on guidelines supporting the formulation of design principles [16]. We discuss the effects of the SME characteristics' [15] on the general design principles [11] and propose 16 design requirements for an ISMM for SMEs.

The rest of the paper is organised as follows. First, background and related research are presented. Second, the general design principles for maturity models [11] are investigated with respect to SME characteristics and the findings are presented. Third, the associations between the SME characteristics and the design principles are presented by including the proposed design principles as a summary. Finally, conclusions are drawn.

2 Background and Related Research

2.1 Design Principles

To date, several studies have investigated the phenomenon of *"Design Principles"*. According to Hevner and Chatterjee, a principle is a clear statement of truth that guides or constrains action. A principle can also be formed as a rule or a standard of conduct [17]. Jones and Gregor state that design principles "… define the structure, organization, and functioning of the design product or design method" [18]. Chandra et al. focused on the characteristics of effective design principle formulation [19]. A recent study by Cronholm & Göbel proposed guidelines supporting the formulation of design principles [16].

2.2 Design Principles for Maturity Models

In the literature, the maturity models are distinguished by their purpose of use as descriptive, prescriptive and comparative. The maturity models for descriptive purpose of use focus on the assessment of the as-is capabilities of an organisation. The maturity models for prescriptive purpose of use provide guidance on how to proceed on the evolutionary path of the maturity levels. The maturity models for comparative purpose of use enables internal and external benchmarking through the assessment results [4, 10, 20]. De Bruin et.al. argue that even though maturity model types (descriptive, prescriptive and comparative) can be seen as distinct types, they actually represent evolutionary phases of a model's lifecycle. In the final phase of this lifecycle, to be used comparatively the model must be applied in a wide range of organizations in order to attain sufficient data to enable valid comparison [10].

Pöppelbuß and Röglinger proposed general design principles (DPs) for maturity models grouped according to typical purposes of use and justified on the foundation of maturity modelling literature [11]. It is important to note that Pöppelbuß and Röglinger states that they deliberately omitted the comparative purpose of use as the fact of whether corresponding DPs can be met largely depends on external factors [11].

2.3 SME Characteristics

Several studies in the literature suggest that SMEs may be differentiated from larger companies by a number of key characteristics [15] [21] [22]. Different approaches to the phenomena of organisational characteristics were taken in the literature. Yu et al. abstract organisations as organic entities similar to humans and investigate organisational characteristics in categories theoretically rooted in psychology [23]. Mijnhardt et al. use an indicator-based approach to distinguish between a wide variety of different organizations [8].

In this paper, we focus on the characteristics present in the literature related to SME research. Cocca and Alberti conducted a literature review and analysed many papers focusing on SMEs in different fields of science [15]. Their findings were grouped into two main categories: external and internal. The factors related to external environment are typically outside the control of organisation [16]. As the implementation of maturity models (MM) is often considered as part of improvement initiatives [24], they primarily depend on the internal environment of the organisations [25].

In **Table 1**, we present the internal characteristics that we investigated in regard to their effects to general design principles proposed by Pöppelbuß and Röglinger [11]. To increase the readability and to enable more comprehensible referral, the third column in **Table 1** presents the keywords used for the corresponding internal characteristics. Internal characteristics are related to resources, structure, and management practices. The keywords were selected in a way that we consider they represent the characteristic in a recallable manner.

Table 1. Internal characteristics and whether they affect the design of information security MMs for SMEs [15].

#	Internal Characteristics (IC)	Keyword
1	Flexible and adaptable to changes, innovative	Flexible
2	Loose and flat structure, lack of bureaucracy	Structure
3	Skills shortages	Skills
4	Lack of management expertise	Management
5	Risk of personal assets	Personal Assets
6	Limited resources: time, human, financial	Resources
7	Lack of organizational capabilities	Capabilities
8	Specialist and tacit knowledge	Knowledge
9	Poor strategic planning	Strategic
10	Reliance on financially based performance measures	Performance
11	Control and decision-making rest primarily with one or a few people	Control
12	Reactive, fire-fighting strategy	Reactive
13	Intuition-based decision making	Decision
14	Learning-by-doing processes	Learning-by-doing
15	Short term vision and orientation	Short-term
16	Incremental improvements and adjustments	Improvements
17	Poor human resource management	HRM
18	Focus on technical aspects and production	Technical
19	Misconception of performance measurement	Performance

3 Addressing SME Characteristics for Designing Information Security Maturity Models

In order to answer the research question, we investigated each design principle proposed by Pöppelbuß and Röglinger [11] and analysed the effect of the internal SME characteristics proposed by Cocca and Alberti [15] on the design principles. The authors of the paper did this analysis thus the findings need to be validated. We further elaborate on the constraints of validity in the conclusion section.

In this section, we present descriptive and prescriptive design principles proposed by Pöppelbuß and Röglinger [11] and we discuss the effect of SME characteristics, requirements and needs on these design principles. Additionally, we present our insights for the comparative

type maturity models. For each design principle, we discuss the SME characteristics' effect on the design principle and we propose design requirements for an ISMM for SMEs. **Table 2**, **Table 3** and **Table 4** present basic, descriptive and prescriptive design principles respectively. To increase the readability and to enable a more comprehensible referral, the third column in these tables presents the keywords used for the corresponding design principles. The keywords were selected in a way that we consider they represent the characteristic in a recallable manner.

3.1 Basic Design Principles

The basic design principles proposed by Pöppelbuß and Röglinger [11] are given in **Table 2**.

Table 2. Basic design principles [11]

#	Principle	Keyword
1.1	Basic Information	Information
1.2	Definition of central constructs related to maturity and maturation	Maturity
1.3	Definition of central constructs related to the application domain	Domain
1.4	Target group-oriented documentation	Users

For an information security model for SMEs, we elaborate on the basic design principles given in **Table 2** as follows.

Regarding Information (DP1.1), the domain coverage and prerequisites for applicability of the maturity model should be provided by possibly referring SMEs to some resources. The prerequisites for applications might be confusing for SMEs who have skill shortages (Skills-IC3), lack of organisational capabilities (Capabilities-IC7) and lack of management expertise (Management-IC4). Regarding the target group, in the case of SMEs, the employees or managers who have the most experience in the information security domain should be addressed (Knowledge-IC8) but poor human resources management might make this difficult to accomplish (HRM-IC17). The results should be reported in an easily understandable way. Since SMEs have short-term vision and orientation (Short-term-IC15) and information security is a continuous initiative, it should be made clear to the target group how the ISMM would be beneficial for their business in the long term (Strategic-IC9). SMEs that are aiming at using the ISMM might not have heard of any other maturity models (Skills-IC3, Capabilities-IC7, Reactive-IC12). Therefore, the differences in the ISMM at hand from the other models available should be made clear. The differences might occur in the domain coverage, the purpose of use, target group, design process and the extent of empirical validation.

DR1 – The information on security domain coverage and prerequisites for applicability of the ISMM should be accompanied by extra resources for SMEs.

DR2 – The long-term benefits of utilising the ISMM should be made clear.

DR3 – The differences in the ISMM at hand from the other models available should be made clear.

Regarding Maturity (DP1.2), as information security is a complex domain [7], a low level of abstraction would provide more granularity and help better realisation of improvement

steps to be taken by the SMEs. This design principle is related to IC14, "Learning-by-doing processes", IC16, "Incremental improvements and adjustments" and IC18 "Focus on technical aspects and production". Having these characteristics in nature, SMEs will benefit from a low-level granularity in an ISMM.

DR4 – Low-level granularity should be provided to help better realisation of improvement steps to be taken by the SMEs.

Regarding Domain (DP1.3), it is needed to provide the definitions of central constructs related to the information security domain. The utilisation of any well-known frameworks in the information security domain will increase the understandability of the maturity model [22]. Well-known standards published by Standard Developing Organisations (SDOs) in the information security domain (e.g. ISO/IEC 27002 [26]) might be a good reference to facilitate the usage of adequate language and understandability of the maturity model. This design principle is related to Skills-IC3, Resources-IC6, and Capabilities-IC7. SMEs having these internal characteristics will benefit by being provided with central constructs that are recognised and well-perceived by their stakeholders.

DR5 – The central constructs that are recognised and well-perceived by SMEs' stakeholders (i.e. standards) should be provided to facilitate the usage of adequate language and understandability of the maturity model.

Regarding Users (DP1.4), given the complexity of information security and the internal characteristics of SMEs (Skills-IC3, Capabilities-IC7, Learning-by-doing-IC14, Improvements-IC16), the documentation of the ISMM should be self-explanatory and easy to understand. Poor human resources management (HRM-IC17) should be considered here as a factor. The risk of Personal Assets (IC5) increases the importance of the ISMM for SMEs. Managing the information security risks reduces the risk of assets which is a direct positive effect for the target group. Providing SMEs with some guidance on how to estimate the cost of efforts with respect to capabilities and maturity levels should be considered (Performance-IC10).

DR6 – The documentation of the ISMM should be self-explanatory and easy to understand.

DR7 – The benefit of using the ISMM for protecting the assets should be made explicit.

DR8 – The documentation of the ISMM should include guidance on how to estimate the cost of efforts with respect to capabilities and maturity levels.

3.2 Design Principles for a Descriptive Purpose of Use

The design principles for a descriptive purpose of use are proposed by Pöppelbuß and Röglinger [11] as follows (**Table 3**).

Table 3. DPs for a Descriptive Purpose of Use [11]

#	Principle	Keyword
2.1	Intersubjectively verifiable criteria for each maturity level and level of granularity	Criteria
2.2	Target group-oriented assessment methodology	Assessment

Regarding Criteria (DP2.1), assessment criteria should be concise, precise and clear as defined by [11] as a general principle, specifically for information security maturity modelling for SMEs, the information source [20] for the criteria should be also be provided. The SME characteristics Skills-IC3, Capabilities-IC7, Learning-by-doing-IC14 and Improvements-IC16 are related to this principle. SMEs would benefit from well-founded assessment criteria as they rather plan for small steps of improvements (Learning-by-doing-IC14 and Improvements-IC16) and they have a lack of expertise and capabilities.

DR9 – The assessment criteria should be concise, precise and clear and the information source for the assessment criteria should be provided.

As a consequence of several SME characteristics related to lack of expertise and skills (Skills-IC3, Resources-IC6, Capabilities-IC7), SMEs might prefer to outsource the management and implementation of information security. Outsourcing information technology infrastructure is also an identifier in the decision to outsource the security of this infrastructure. Regarding Assessment (DP2.2), outsourcing decisions should be one of the parameters to consider for the applicability of assessment criteria.

DR10 – The assessment methodology should enable the configuration of the criteria according to SMEs' outsourcing decisions.

The European Digital SME Alliance has recently published a position paper on the EU Cybersecurity Act and the role of standards for SMEs [27]. In this paper, the need for distinction between different types of SMEs is emphasized. The reason of this differentiation is presented as to make sure that cybersecurity solutions and standards are tailored to them. Regarding Assessment (DP2.2), the SME categories proposed by the Digital SME Alliance can be considered to configure the assessment criteria provided by the maturity model (Knowledge-IC8).

DR11 – The assessment methodology should enable the configuration of the criteria according to different categories of SMEs' according to their role in the digital ecosystem.

The assessment methodology should be reusable to allow multiple assessments and comparisons over the time of the assessment results to present and observe the improvement [28].

3.3 Design Principles for a Prescriptive Purpose of Use

The design principles for a prescriptive purpose of use are proposed by Pöppelbuß and Röglinger [11] as follows (**Table 4**).

Table 4. DPs for a prescriptive purpose of use [11]

#	Principle	Keyword
3.1	Improvement measures for each maturity level and level of granularity	I-Measures
3.2	Decision calculus for selecting improvement measures	D-Calculus
3.3	Target group-oriented decision methodology	D-Methodology

Regarding I-Measures (DP3.1), prescriptive maturity models must include improvement measures that enable the development of a road-map for improvement [11] [10]. In consideration of information security as the application domain and SMEs as the target group for maturity modelling, the improvement measures should be organised in small and achievable

steps which could be facilitated by lack of bureaucracy (Structure-IC2, Learning-by-doing-IC14, Improvements-IC16).

DR12 – The improvement measures should be organised in small and achievable steps.

DR13 – The improvements required to progress to the next maturity level should be explicit.

D-Calculus (DP3.2) is related to decision alternatives and prioritization for improvement planning. Improvement objectives may stem from different sources e.g. internal (management) or external (customers). Given the limited skills, resources, capabilities and management expertise of SMEs (Skills-IC3, Management-IC4, Resources-IC6 and Capabilities-IC7), the decisions for choosing amongst different improvement road-maps is more critical and needs to be justified thus should be further supported to be clear and rational.

DR14 – Clear and rational guidelines should be provided for selecting the improvement measures.

In addition to providing a well-grounded decision for improvement, regarding D-Methodology (DP3.3), a maturity model should also provide SMEs with the tailored advice for adapting the improvement measures considering their role in the digital ecosystem [27], flexibility, control and decision-making mechanisms (Flexibility-IC1, Knowledge-IC8, Control-IC11, Decision-IC13).

DR15 – Tailored advice for adapting the improvement measures should be provided for different categories of SMEs.

3.1 Design Principles for a Comparative Purpose of Use (CPoU)

As stated earlier, our reference study for the general design principles, Pöppelbuß and Röglinger deliberately omitted the principles for the comparative purpose of use [11]. De Bruin et al. states that for a model to be used comparatively it must be applied in a wide range of organizations in order to attain sufficient data to enable valid comparison. Cholez and Girard presented a framework that allows multiple assessments and successive comparisons over the time of the assessment results in their study on information security maturity assessment in SMEs. The exemplar assessment result in this study presents a radar graphic depicting the enterprise profile [28]. We recognize that the utilisation of this kind of visuals to present the assessment results for comparative purposes can assist SMEs for better understanding and presenting their as-is and to-be positions. This will help to reduce “Misconception of performance measurement” in regards to Performance-IC19 (**Table 1**). As stated in Section 3.1, SMEs may gain strategic advantage by comparatively using the assessment results (Strategic-IC9).

DR16 – Visual presentation of the assessment results for comparative purposes should be utilized to assist SMEs to better understand and present their as-is and to-be positions.

4 Mapping of SME Characteristics and Design Principles

In this section, the mapping of internal characteristics given in **Table 1** and design principles given in respective tables (**Table 2**, **Table 3**, **Table 4**) are presented here as a summary

in **Table 5**. This table shows the associations between the SME characteristics and the design principles by specifying the corresponding design requirements as discussed in this paper.

Table 5. Mapping of SME characteristics and design principles.

Internal Characteristics	Design Principles									
	Information DP1.1	Maturity DP1.2	Domain DP1.3	Users DP1.4	Criteria DP2.1	Assessment DP2.2	I-Measures DP3.1	D-Calculus DP3.2	D-Methodology DP3.3	CPoU
Flexibility (IC1)									DR15	
Structure (IC2)							DR12, DR13			
Skills (IC3)	DR1, DR3		DR5	DR6	DR9	DR10		DR14		
Management (IC4)	DR1							DR14		
Personal Assets (IC5)				DR7						
Resources (IC6)			DR5			DR10		DR14		
Capabilities (IC7)	DR1, DR3		DR5	DR6	DR9	DR10		DR14		
Knowledge (IC8)	DR1					DR11			DR15	
Strategic (IC9)	DR2									DR16
Performance (IC10)				DR8						
Control (IC11)									DR15	
Reactive (IC12)	DR3									
Decision (IC13)									DR15	
Learning-by-doing (IC14)		DR4		DR6	DR9		DR12, DR13			
Short-term (IC15)	DR2									
Improvements (IC16)		DR4		DR6	DR9		DR12, DR13			
HRM (IC17)	DR1			DR6						
Technical (IC18)		DR4								
Performance (IC19)										DR16

5 Conclusion

In this paper, we investigated the SME characteristics [15] that may affect the general design principles of maturity models for SMEs [10] [11]. We discuss the possible effect of the SME characteristics on the general design principles and propose 16 design requirements for an ISMM for SMEs.

We present the mapping of the internal SME characteristics and the design principles by specifying the corresponding design requirements as a summary. Since the mapping of the internal SME characteristics and the design principles was done by the authors, it is important to bear in mind the possible bias in these. This limitation stimulates further research to assess the validity of the proposed design requirements by means such as evaluation by SMEs and maturity model developers. Another possibility for future research is a review of a set of existing ISMMs concerning the proposed design principles.

We believe that if the proposed design principles are taken into account from the very start of ISMM development for SMEs, one can systematically account for diverse SME characteristics profiles, thereby significantly increasing the potential usability and applicability of the resulting maturity model. This will yield a better individual and organisational learning with respect to information security.

References

1. Digital SME Alliance: Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem, https://www.digitalsme.eu/digital/uploads/20170731-DIGITAL-SME-Cybersecurity-Position.pdf, (2017).
2. Bilge Yigit Ozkan, Marco Spruit, Roland Wondolleck, Verónica Burriel Coll: Modelling adaptive information security for SMEs in a cluster. JIC. ahead-of-print, (2019). https://doi.org/10.1108/JIC-05-2019-0128.
3. Yigit Ozkan, B., Spruit, M.: A Questionnaire Model for Cybersecurity Maturity Assessment of Critical Infrastructures. In: Fournaris, A.P., Lampropoulos, K., and Marín Tordera, E. (eds.) Information and Operational Technology Security Systems. pp. 49–60. Springer International Publishing, New York, USA, Heraklion, Crete, Greece (2019). https://doi.org/10.1007/978-3-030-12085-6_5.
4. Becker, J., Knackstedt, R., Pöppelbuß, J.: Developing Maturity Models for IT Management. Bus. Inf. Syst. Eng. 1, 213–222 (2009). https://doi.org/10.1007/s12599-009-0044-5.
5. Bititci, U.S., Garengo, P., Ates, A., Nudurupati, S.S.: Value of maturity models in performance measurement. International Journal of Production Research. 53, 3062–3085 (2015). https://doi.org/10.1080/00207543.2014.970709.
6. Curado, C.: Organisational learning and organisational design. The Learning Organization. 13, 25–48 (2006). https://doi.org/10.1108/09696470610639112.
7. Tisdale, S.M.: Architecting a Cybersecurity Management Framework: Navigating and Traversing Complexity, Ambiguity, and Agility - ProQuest, https://search.proquest.com/openview/0934ecf7a7afd537d2f2307843e1fdb3/1?cbl=18750&diss=y&pq-origsite=gscholar, (2016).
8. Frederik Mijnhardt, Thijs Baars, Marco Spruit: Organizational Characteristics Influencing SME Information Security Maturity. Journal of Computer Information Systems. 56, 106–115 (2016). https://doi.org/10.1080/08874417.2016.1117369.
9. Tobias Mettler: A Design Science Research Perspective on Maturity Models in Information Systems - Alexandria. Institute of Information Management, Universtiy of St. Gallen, Switzerland (2009).
10. de Bruin, T., Freeze, R., Kulkarni, U., Rosemann, M.: Understanding the Main Phases of Developing a Maturity Assessment Model. In: ACIS 2005 Proceedings. p. 11. , Sydney (2005).
11. Pöppelbuß, J., Röglinger, M.: What makes a useful maturity model? a framework of general design principles for maturity models and its demonstration in business process management. In: ECIS (2011).

12. Mettler, T., Rohner, P.: Situational Maturity Models As Instrumental Artifacts for Organizational Design. In: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. p. 22:1–22:9. ACM, New York, NY, USA (2009). https://doi.org/10.1145/1555619.1555649.
13. Thijs Baars, Frederik Mijnhardt, Kevin Vlaanderen, Marco Spruit: An analytics approach to adaptive maturity models using organizational characteristics. Decis. Anal. 3, 1–26 (2016). https://doi.org/10.1186/s40165-016-0022-1.
14. Mayer, N.: A Cluster Approach to Security Improvement according to ISO/IEC 27001. In: Proceedings of the 17th European Systems & Software Process Improvement and Innovation Conference (EUROSPI'10). , Grenoble, France (2010).
15. Cocca, P., Alberti, M.: SMEs' Three-step Pyramid: A new Performance Measurement Framework for SMEs. Presented at the 16th International Annual EurOMA Conference , Göteborg, Sweden June 14 (2009).
16. Cronholm, S., Göbel, H.: Guidelines Supporting the Formulation of Design Principles. In: Australasian Conference on Information Systems 2018. University of Technology, Sydney (2018). https://doi.org/10.5130/acis2018.ak.
17. Hevner, A., Chatterjee, S.: A Science of Design for Software-Intensive Systems. In: Hevner, A. and Chatterjee, S. (eds.) Design Research in Information Systems: Theory and Practice. pp. 63–77. Springer US, Boston, MA (2010). https://doi.org/10.1007/978-1-4419-5653-8_6.
18. Jones, D., Gregor, S.: The Anatomy of a Design Theory. Journal of the Association for Information Systems. 8, (2007). https://doi.org/10.17705/1jais.00129.
19. Chandra, L., Seidel, S., Gregor, S.: Prescriptive Knowledge in IS Research: Conceptualizing Design Principles in Terms of Materiality, Action, and Boundary Conditions. In: 2015 48th Hawaii International Conference on System Sciences. pp. 4039–4048. IEEE, HI, USA (2015). https://doi.org/10.1109/HICSS.2015.485.
20. Maier, A.M., Moultrie, J., Clarkson, P.J.: Assessing Organizational Capabilities: Reviewing and Guiding the Development of Maturity Grids. IEEE Trans. Eng. Manage. 59, 138–159 (2012). https://doi.org/10.1109/TEM.2010.2077289.
21. Storey, D.J.: Understanding The Small Business Sector. 48 (1994).
22. Hudson, M.: Introducing integrated performance measurement into small and medium sized enterprises, https://pearl.plymouth.ac.uk/handle/10026.1/400, (2001).
23. Yu, D., Xiao, H., Bo, Q.: The Dimensions of Organizational Character and Its Impacts on Organizational Performance in Chinese Context. Frontiers in Psychology. 9, (2018).
24. Helgesson, Y.Y.L., Höst, M., Weyns, K.: A review of methods for evaluation of maturity models for process improvement. Journal of Software: Evolution and Process. 24, 436–454 (2012). https://doi.org/10.1002/smr.560.
25. Rainer, A., Hall, T.: Key success factors for implementing software process improvement: a maturity-based analysis. Journal of Systems and Software. 62, 71–84 (2002). https://doi.org/10.1016/S0164-1212(01)00122-4.
26. ISO/IEC: ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls, https://www.iso.org/standard/54533.html, (2013).
27. The European Digital SME Alliance: The EU Cybersecurity Act and the Role of Standards for SMEs. , Brussels (2020).
28. Cholez, H., Girard, F.: Maturity assessment and process improvement for information security management in small and medium enterprises. Journal of Software: Evolution and Process. 26, 496–503 (2014). https://doi.org/10.1002/smr.1609.