Digital technologies supporting digitalization: a maturity model to manage their usage risks

Lamiae BENHAYOUN[1][0000-0003-4183-7205] and Imed BOUGHZALA[2][0000-0001-7362-8497]

[1] UIR Rabat Business School, Rabat, Morocco
[2] Institut Mines Telecom Business School, Evry, France
lamiae.benhayoun@uir.ac.ma

Abstract. Digital technologies in support of digitalization allows organizations to improve their strategic and operational performance, but also harbors risks of security, oversizing or loss of control, among others. While the management of these risks is essential to promote the success of digital transformation, no research offers an integrative framework to help monitor them. This study adopts a design science approach to conceive a maturity model evaluating the risks of using digital technologies. This framework is the initial step towards the supervision of these digital risks to succeed in digital transformation. We relied on an in-depth literature review and an empirical study using a Delphi approach and a focus group with 19 practitioners. Accordingly, we identify three dimensions of risks related to data, stakeholders and technology governance and distinguish them according to each digital technology in the spectrum of SMAC and DARQ technologies. We additionally define a maturity scale to assess these risks and a protocol to implement the maturity model. The paper concludes with its theoretical and practical implications as well as a research agenda.

Keywords: Digital technologies, Digital transformation, Risk management, Maturity, SMAC, DARQ

1 Introduction

To reap the benefits of the recent digital technologies, companies in all sectors are increasingly embracing deep digital transformation projects [1], for which expenditure will reach two trillion dollars by the end of 2022 [2]. Digital transformation or digitalization refers to changes in working methods, roles and behaviors of individuals, and commercial offers, that are induced by the intensive use of digital technologies in the organization and in its operational environment [3]. To accomplish a digital transformation process, companies rely on digitization by dematerializing information [1] and transforming their products, existing services and processes in digital variants [4]. This wave of transformation was driven by the advent of SMAC (Social, Mobile, Analytics, Cloud) technologies that enabled companies to improve their operational performance through the reduction of costs and execution times [3]. These technologies have also revolutionized the business models through which the company delivers value to customers, while providing them with an innovative user experience [5]. Today, being digital-first for a company is no longer an innovation or a competitive advantage, but a minimum condition for surviving in a constantly changing market. Successful companies are those that genuinely combine SMAC technologies with the new generation of DARQ technologies (Distributed ledger, Artificial intelligence, extended Reality, Quantum calculation) marking the post-digital era [6].

Over the past five years, digital transformation has aroused growing interest among practitioners and researchers in the Information Systems stream. Some scholars focused on identifying opportunities to improve operational and strategic performance offered by the use of digital technologies [7]. Others explored the changes in organizational practices that accompany the adoption and acceptance of these technologies [8], as they require different postures and capacities from previous technological waves [9]. Finally, few researchers took an interest in identifying the risks induced by

these technologies, in particular security risks [10], compliance with standards and regulations [11], relationships with third parties [7] and employee governance [12]. The exploration of such risks concerned specific sectoral contexts, often the military [13] and health [14], or specific technologies namely social networks [15] and artificial intelligence [16]. However, no study offers a model to monitor the risks related to the use of digital technologies as a whole, regardless of the organizational context. Designing such an integrative framework to manage these risks simultaneously rather than in isolation, would allow researchers to better understand the interconnected nature of digital technologies and the complexity that their risks add to existing operational problems. Also, this model would help firms implement preventive practices to better benefit from investments and efforts in deploying digital technologies.

In this respect, maturity models are often used to evaluate the organization's abilities, identify the most critical issues and initiate improvement activities [17]. They suggest that an enhanced action will lead to a better outcome [18]. Accordingly, we raise the following research question: *How to design a maturity model assessing the risks of using digital technologies in support to digital transformation* ? To answer this question, we follow a Design Science approach [19, 20] for maturity model development [21]. This approach relies on a thorough analysis of the literature, a Delphi method, and a focus group with 19 practitioners. The resulting maturity model constitutes the initial step in the successful monitoring of risks associated with the use of digital technologies. The paper is structured as follows. Section 2 presents our conceptual foundations, namely the technologies at the heart of digital transformation and the risks they entail. Section 3 explains the methodology adopted for this study. The results, consisting of the proposals made by the professionals with regards to the maturity model, are presented and discussed in Section 4. Finally, the conclusion highlights the study limitations and discusses the main directions of future research.

2 Literature review

2.1 Digital transformation: a change supported by digital technologies

To respond to a digitally disrupted environment, many companies joined the wave of digital transformation or digitalization over the past decade [22]. This phenomenon reflects a profound and intentional restructuring of their capacities, resources, and value creation pathways to benefit from the advantages offered by digital technologies [7; 23; 24]. This alteration aims to seize revolutionary opportunities in three major areas [9]. First, it seeks to improve the user experience by creating customized products and services and establishing a transparent and personalized digital relationship with clients [5]. Second, digital transformation offers opportunities for streamlining business processes that improve agility and responsiveness [3]. Finally, it allows the creation of new business models to increase the strategic benefits of using digital technologies [25].

Digital transformation is supported by digital technologies [26] encompassing all systems, tools, devices, and electronic resources used to generate, store and process data [27]. It was induced by the advent of SMAC technologies referring to Social, Mobile, Analytics and Cloud [1], and continues to intensify with the emergence of DARQ technologies (Distributed ledger, Artificial intelligence, extended Reality, Quantum computing) which are moving companies towards a post-digital era [6]. These technologies can quickly and severely alter the competitive dynamics of industries, that is why digitalization is now a priority for many organizations [7]. If digitalization represents undeniable advantages for companies, it nonetheless conceals major challenges. Scholars pointed out that digital transformation carries risks related to IS adoption [28], data governance [29], well-being at work [30], skills development [31], strategic alignment with IT [32], etc.

The term "transformation" expresses the entirety of actions to be taken when organizations are faced with a disruption. It goes beyond functional thinking and addresses the opportunities, but also

the risks associated with change [33]. Hence, identifying and managing the risks inherent in a transformation process is a prerequisite for its success [34]. However, unlike the grey literature such as reports from consulting firms and white papers from companies [e.g., 6; 35; 36], very few IS researchers characterized the risks associated with digital transformation [e.g., 7; 37]. Even fewer proposed approaches to monitor these risks [38]. This creates a real discrepancy: companies are increasingly implementing initiatives to manage the risks of digital transformation, while the academic literature does not scientifically explore these practices. Such research would promote the cross-fertilization of academic and practitioner knowledge.

2.2 Risks related to the use of digital technologies

Digital transformation involves a multitude of risks related, among others, to employee well-being [30], strategic alignment [32] and skills development [31]. The characterization and assessment of these risks constitutes a research gap that needs to be addressed in order to provide a better understanding and support of digital learning pathways and digital governance at individual, organizational and governmental levels. In this paper, we chose to focus on the risks that accompany a key dimension of digital transformation: the use of digital technologies. Their implementation forms the foundation of the digitalization process [39] and poses particular risks, as digital technologies require postures and capabilities different from the previous technological waves [9]. Indeed, due to the alterations in communication, work and more generally intellectual style induced by these digital technologies, it is crucial to understand them, know how to interact with them [40], and to manipulate the data they contain [41].

We therefore conducted a literature review to assess the state of scientific knowledge about the risks of using digital technologies. We relied on the reference platform "Web of Science" to explore articles in peer-reviewed journals and renowned conferences in the Information Systems' field. We limited our search to articles written in English and published since 2005, as this year marks the first scientific work on the digital transformation of companies [42]. To define our keywords, we were guided by the definition of digital technologies proposed by [27] and presented in the previous section, and that of the term "risk". According to [43], risk corresponds to something that can be lost and the probability of actually losing it. This concept reflects a hazard or a potential malfunction, more or less foreseeable, and which can cause damage [44]. Thus, we combined the terms "Digital transformation" or "Digitalization", with the keywords "Risk", "Threat" or "Danger", and with "Technology", "Digital technology" or one of the eight digital technologies (SMAC, DARQ) involved in digital transformation. In total, we selected 61 articles, the vast majority of which were published since 2016. Most of this research is based on case studies or exploratory interviews and none offers a classification of the risks associated with the use of digital technologies. To relate the risks identified in this state of the art, we relied on the 5W approach (Who, What, When, Where, Why) recommended by [45]. It delivers an exhaustive characterization of a phenomenon by classifying it according to its different dimensions. Table 1 explains these five classification criteria in the context of our study and provides examples of risks for each criterion resulting from our state of the art. These risks are detailed in the following paragraphs.

Who: The risks of using digital technologies have been analyzed at the levels of employees, companies and the government. Employee-specific risks mainly involve the lack of skills, leadership, creativity and of entrepreneurial spirit related to digital technologies [46]. They also include resistance to the change induced by these technologies [47] and the hampering of learning efforts following the misuse of artificial intelligence [48]. At the organizational level, the most critical risks refer to the non-alignment of IT and business strategies [32], the absence of a digital culture [49], and a low level of digital maturity in the case of SMEs [50]. Finally, the risks identified for government authorities concern the change in the structure of the labor market [51], the strengthening of

social inequalities [52] and the difficulty of interacting with citizens reliably and efficiently across the multitude of social networks [15].

Table 1. Analysis of the state of the art

Classification criterion	Explanation of criterion	Examples of results
Who	Categorizes the risks according to the level of analysis considered	• Individual: Degradation of skills, reluctance to change • Organization: Lack of alignment between IT and Business strategies, lack of digital culture • Government: Alteration of the job market, reinforcement of social inequalities
What	Classifies the risks according to the impacted transformation component	• Operational processes: Development costs, infrastructure instability, lack of competent actors • User experience: inappropriate use of technologies, confidentiality of data communicated • Business model: disruption of business activity, the institution's role in the socio-economic landscape
Where	Distinguishes the risks according to the sector of activity	• Bank-insurance: Fraud, huge flow of data that is hard to process • Military: Durability of technologies • Health: Data Privacy
Why	Qualifies the risks according to the technologies that cause them	• Artificial Intelligence: Ethical issues, limits of algorithms • Data Analytics: Data Privacy, Cybersecurity • Mobile: Network issues, device obsolescence • Blockchain: Lack of standards, lack of competent actors
When	Provides a reading of the risks according to the moment of their occurrence in the digitalization process	• Development of technology: Integration of Privacy by design, Inadequacy of certain digital project methods • Day-to-day use: Cybersecurity, data leakage

What: Although the existing theoretical corpus has addressed the risks associated with different aspects of digital transformation, most studies focused on the operational process aspect. Some authors pointed out that digitalization generates risks of substantial production and infrastructure development costs [53]. Others specified processual issues of data confidentiality [14], technology sustainability [13] and vulnerability [16], and lack of competent digital actors [54]. The literature also addressed the risks associated with the digital transformation of the user experience, namely miscontrol over their communicated data [55], citizen security in smart cities [56] and the difficulty of establishing an effective relationship with consumers through mobile marketing [57]. Finally, few studies underlined the risks of business model digitalization, particularly the difficulty to renew the strategies in light of new advanced technologies [58].

Where: Several authors emphasized process transformation risks in specific sectors. The health sector highlights the problem of data confidentiality [14], which results in the difficulty of establishing effective collaboration between healthcare providers and developers of specialized technologies [59]. The military sector is characterized by the concern of technology sustainability [13], while the agricultural sector presents risks of vulnerability and security of the connected objects used [16]. The digitalization of processes in the field of logistics is accompanied by significant development costs and a lack of experts with digital skills [54]. The financial and telecommunication sectors are mostly concerned by business model risks, namely the need to review the role of certain financial institutions [58] and telecommunications operators in the digital era [60].

Why: The 'Why' in our study qualifies the risks according to the originating technology among the SMAC/DARQ spectrum. Most studies focus on the risks generated by artificial intelligence, such

as the ethical issues of unemployment [61], and the limits of algorithms and their vulnerability [16]. A multitude of researchers also investigated the issues of mobile technologies in terms of data confidentiality [62], network vulnerability [63], and rapid obsolescence of devices [64]. The risks associated with Data analytics technologies are also very present, in particular fraud and cybersecurity [65], the difficulty of processing the volume of data which continues to increase [66], and data privacy [67]. This privacy issue also represents a significant risk when implementing Cloud technologies [67; 14] and social media [65]. These media additionally involve risks of inappropriate use to design an effective user experience [15] aligned with his expectations [57]. Numerous authors highlighted the risks of adopting Distributed ledger technology (e.g., Blockchain), in particular the immaturity of the technology, the absence of common standards [68], the scarcity of competent actors in this field, and the inefficiency of the institutional environment [69]. Finally, to our knowledge, no research deals with the risks of using extended reality and quantum technologies. Besides, some studies underlined the risks associated with digital technologies as a whole [e.g., 70; 51]. We discuss these risks in depth in Table 3.

When: Regarding the moment of risk occurrence within the transformation process, our analysis of the literature showed that most of the risks are present during the development of technologies in support of digital transformation, for example the low quality of the Cloud developed in agile mode [71], the sustainability of digital engineering outputs in the military [13], the cost of developing digital technologies for warehousing [54], and the consideration of privacy issues in technology design [67]. A large part of the risks also takes place during the day-to-day use of digital technologies, for example resistance to change [47], skill degradation [48], alteration of social structures [52], leaks of sensitive data [62], and cybersecurity [55].

In short, no study offers an integrating framework or an overall classification of the risks associated with the use of digital technologies. To cover this gap and enrich the risks identified in our state of the art, we followed a design science approach to conceive a maturity model assessing these risks' management.

3 Research methodology

3.1 Data collection

Maturity models have been extensively investigated in several domains as an instrument for continuous improvement [17; 72]. They suppose that when activities are defined, managed, and executed effectively, they lead to better performance [18]. In this research, we follow the seminal design science methodology proposed by [21] to conceive a maturity model. Additional to the design stage, the authors suggest that the models should also undergo field applications and frequent updates for maintenance to comfort their continuous validity.

The construction of a maturity model requires determining the key process areas (KPAs), i.e., themes that are mutually exclusive and collectively exhaustive to describe the evaluated object [21]. Each KPA is defined through associated practices, implemented collectively to satisfy the goals of the area. These KPAs are described at a number of levels of performance [73; 74]. The highest maturity level is where the KPA's practices are efficiently applied and culturally rooted [75; 17].

To determinate the KPAs and the maturity scale, we relied on an in-depth literature review combined with a Delphi type approach. The Delphi method is generally used in Information Systems' research when the generation of ideas is necessary to convey a consensual opinion on a well-determined subject [76]. This approach is based on the remote surveying technique [77]. During our study, to collect a field reflection (bottom up) on the risks associated with the use of digital technologies, we set up an electronic survey system with 19 practitioners from 9 organizations. Table 2 summarizes the key characteristics of the participants and their organizations. The latter were chosen

because of their in-depth knowledge of the subject and the richness of points of view that they can provide based on their complementary profiles.

The survey was conducted in one-to-one sessions with participants and the entire process was recorded to circumvect any missing point. Each session was initiated by the introduction of the study objectives, namely to propose a structure of the maturity model and an assessment protocol. We also provided examples of risks associated with the use of digital technologies resulting from our 5W literature analysis. Subsequently, the participants reacted to questions structured according to three interaction times:

First, each participant had to refer to his digital transformation experience in order to propose risk management capabilities that are related to the use of digital technologies as a whole, and explain their components or items. These capabilities would ultimately represent the KPAs of our model.

Secondly, we asked them to provide us with a more detailed vision of these risks according to each of the SMAC/DARQ technologies in support of digital transformation.

Finally, we invited each participant to share with us the maturity assessment approaches he was knowledgeable of, and which could be suitable to the risks of using digital technologies. We mainly requested them to suggest a definition and criteria of maturity to be used in an evaluation scale.

Table 2. Characteristics of the participants and their organizations

Characteristics of the participants	
Number of participants	19
Youngest	31
Oldest	58
Average age	46
Male	14
Female	5
Education level	7 PhD, 10 Master, 2 Bachelor
Longest experience	25 years
Shortest experience	9 years
Average experience	15 years

Characteristics of the organizations				
Org	*Sector*	*Type*	*Size*	*Disciplines*
Org 1	IT consulting	Private	80	Analytics and AI expert
Org 2	Bank	Private	>50000	Analytics and AI expert, financial analyst
Org 3	Insurance	Private	≈10000	Analytics and AI expert, financial consultant
Org 4	University	Public	1000	Cybersecurity expert
Org 5	University	Public	1000	R&D managers
Org 6	Electricity	Private	300	CEO, R&D manager, Logistics manager
Org 7	Pharmaceutical	Private	500	CEO, Biotech researcher, R&D manager, Purchasing manager
Org 8	Automotive	Private	>50000	Purchasing manager, logistics manager, assembly manager
Org 9	Automotive	Private	>50000	R&D manager, logistics manager

3.2 Data analysis

To analyze the data collected from this panel, we proceeded according to the three themes addressed during the survey, namely the capabilities related to the risks of using digital technologies, the refinement of these risks according to the SMAC/DARQ spectrum, and finally the proposal of a maturity evaluation scale. To analyze each theme, we carried out a double purification as recommended by [78] which we explain below.

The first purification took place throughout the investigation process by relying on the system in support of our Delphi approach. Indeed, the latter makes it possible to collect feedback from participants following a structured and proven process. In addition, it facilitates the development of a summary document synthesizing their responses. As we implemented our data collection approach, we proceeded to clarify, reduce, and organize participant feedback.

The second purification took place at the end of all the sessions. The participants were invited to a full day focus group structured in two sessions of three hours each, moderated by the researchers. A focus group is a discussion of a particular topic under the direction of a moderator who promotes

group participation and communication and manages the discussion through a series of interactions [79]. During the first half-day, we presented the results of the Delphi survey and refined them. This refinement involved the reformulation, when necessary, of the answers, their consolidation, interpretation, and the verification of the proposals. In this step, we were guided by two criteria: the non-redundancy of ideas in the classification of participants' feedback, and the relatedness of each response to the topic of risks to use digital technologies.

During the second half-day, the developed maturity model was applied to a use case with the participation of the group members. An electricity firm taking part in the focus group was interested in implementing the model to assess the organization's maturity for managing the risks related to the use of digital technologies. This use case comforts the validity of the model as recommended by [21]. We present and discuss the field application in the findings' section.

4 Findings

4.1 The maturity model's KPAs

The maturity model developed in this research aims to assess the overall ability to manage the risks related to the use of digital technologies. It informs the firm on its strengths and weaknesses, that can serve on the definition of an action plan. To define the KPAs, we relied on an in-depth literature review combined with the insights of our Delphi approach. We asked the participants to refer to their experience of digital transformation to describe the main risks that characterize the use of digital technologies in general, and then each of the eight SMAC/DARQ technologies. This helped enrich our state of the art with new risks emerging from our study.

Following the analysis of the collected data and the validation during the focus group, we distinguished three classes of risks that are exhaustive and exclusive to represent the KPAs of our maturity model. These risks are listed in Table 3, which mentions whether each has already been highlighted in the literature or whether it emerged solely from our empirical study. In the next paragraphs, we provide verbatim on the risks that were heavily discussed during the focus group.

Data sensitivity: Data sensitivity concerns information that should be protected from unauthorized access or disclosure due to its delicate nature. Participants underlined that "*digital technologies by nature generate data without the knowledge of the individual. The sharing of this data entails a risk in itself*". This is even more critical when it comes to "*personal data such as medical, financial or other sensitive data that could impact the reputation of the person*".

Relationships with third parties: According to the participants, "*digital technologies enable opening up to other stakeholders (customer, supplier, partner, competitor), and subsequently to more risks in terms of managing these relationships*". In particular, such technologies "*can cause a lot of formality in relationships, which harms the efficiency of partnerships*". Furthermore, some group members highlighted that "*the use of digital technologies makes the organization more exposed to the outside world, which can quickly put it at a disadvantage in the case of bad recommendations by customers*".

Governance of digital technologies: The group members insisted that "*the recent and constantly evolving nature of digital technologies poses challenges to the management of information systems within the company*". Indeed, "*these technologies require time to be mastered by the IT department and can quickly become obsolete*". The rapid mastery of these technologies is even more necessary to "*meet the instantaneous needs of the businesses in the organization. The digital age is precisely characterized by the culture of 'immediately'*". To meet their needs, businesses can "*resort to Shadow IT, which can pose a real governance problem for the IT Department. These technologies are increasingly accessible with the advent of digital. Apps and technologies developed yesterday are*

within everyone's reach!". Furthermore, the IT Department often encounters the problem of "*data overflow in case of poor management of the data generation and distribution channels"*.

Table 3. KPAs and their associated risks of using digital technologies

KPA	*Nature of the digital technology*	*Risks*
Data sensitivity	Digital technologies in general	Data generated without the knowledge of individuals
	Digital technologies in general	Access to unauthorized personal data (medical, financial, etc.)
	Digital technologies in general	Access to data that could damage the reputation of individuals
	Social	Exposure (fishing, harassment, grooming)
	Mobile	Access to private data
	Mobile	Cyberattacks
	Mobile	Identity theft
	Mobile	Data theft, Data alteration
	Analytics	Prohibited manipulation of data (fingerprints, genomes, etc.)
	Cloud	Lack of protection of private data
	Cloud	Security/ data leakage
	Distributed ledger (e.g., Blockchain)	Fraud
Relationships with third parties	Digital technologies in general	*Difficulty to manage digital relationships with a multitude of stakeholders**
	Digital technologies in general	*Rigid professional relations**
	Digital technologies in general	Risky outdoor exposure
	Social	Bad reputation and negative publicity resulting from social amplification
	Social	Professionalization of the means to harm the person
	Cloud	Pressure from the suppliers to implement inadequate Cloud
	Artificial Intelligence	Financial opportunism at the expense of other social classes
Governance of digital technologies	Digital technologies in general	Difficulty to align with the evolving nature of digital
	Digital technologies in general	Investments to master technologies that can quickly become obsolete
	Digital technologies in general	*Difficulty to meet the immediate needs of businesses**
	Digital technologies in general	Excessive use of Shadow IT
	Digital technologies in general	Overflow by large data flows
	Mobile	Poor technology design
	Analytics	Wrong measurement
	Analytics	Non-compliance with GDPR
	Cloud	Non-performance of technology
	Cloud	Data and country sovereignty
	Cloud	Loss of assets and their location
	Distributed ledger (e.g., Blockchain)	*Oversizing**
	Distributed ledger (e.g., Blockchain)	*Deployment by mimicry**
	Distributed ledger (e.g., Blockchain)	*Unnecessary investments**
	Artificial Intelligence	Algorithms not mastered
	Artificial Intelligence	Irresponsible innovation
	Artificial Intelligence	Inappropriate use
	Artificial Intelligence	*Poor choice of use cases**
	Artificial Intelligence	Misleading use
	Extended Reality	*Unnecessary investments to align with a fad**
	Quantum computing	*Overcapacity, oversizing to respond to simple problems**

**Risk emerging from the empirical study*

Regarding the risks associated to the particular use of a technology within the SMAC/DARQ spectrum, we note that a large part of the risks related to SMAC and Artificial Intelligence technologies have previously been identified in the literature, while the risks of using Distributed ledger, extended Reality and Quantum computing technologies have almost entirely emerged from our empirical approach.

4.2 The maturity scale adopted in our model

Most studies that designed maturity models rely on the definition of maturity and the scale proposed in the CMMI (Capability Maturity Model Integration), a seminal model developed by [80]. CMMI defines maturity as the degree to which processes are formally organized and executed to produce the desired results [74]. Most of the participants were aware of the CMMI and, consequently, responded in the Delphi questionnaire by referring to its definition of maturity and its scale composed of four levels namely ad hoc, exploring, managing, and optimizing.

However, when discussing with the group participants the adequacy of this scale to assess the risk management of using digital technologies, we concluded that it does not meet the peculiarities of this evaluated topic. Indeed, digital risk management does not correspond to institutionalized processes as is the case of CMMI-based models and additionally integrates a behavioral dimension of awareness. Thus, based on the practitioners' feedback, we propose to evaluate the maturity in our model not only in terms of the organization's ability to operationally implement practices dealing with the risks in Table 3, i.e. '*Capable to do'*, but also its propensity toward these practices, i.e. '*Willing to do'*.

To evaluate the organization's maturity according to these criteria, we adopted a hybrid descriptive approach as recommended by [21] for topics that were never operationalized from a maturity perspective. It consists of asking a question conveying the highest level of maturity for each evaluated item. In our case, for each risk, we ask two questions associated with the two maturity criteria. For the capability criterion, we evaluate if the organization is able to implement the methods and tools to prevent this risk and control it when it occurs. For the willingness criterion, we assess whether the organization perceives the relevance of managing the risk and is willing to implement the necessary practices in order to monitor it. After discussing with the focus group participants, we defined 4 levels of maturity associated with these two maturity criteria. A level of maturity is granted to the organization depending on its answers to the two questions on a scale of 1 to 4.

For capability, if the organization states that it perfectly masters the methods and tools to monitor the risk, it is considered (4)*expert*. If it feels capable but needs more formalization, the maturity level is (3)*capable*. If the organization has some ideas but does not know how to proceed to mitigate the risk, it is (2)*novice*. If it does not have any idea, method or tool to proceed with the risk, it is (1)*not capable*.

As for willingness, the organization is a (4)*firm believer* if it is fully convinced with the benefits of managing the risk and is inclined to implement all the necessary practices. It is (3)*culturally rooted* if it perceives the interest of managing the risk and would eventually agree to implement some practices in this respect. The organization is (2)*potentially receptive* if it is not against managing the risk but is not convinced with the interest of this action. Finally, it is (1)*culturally resistant* if it does not find any relevance in monitoring the risk.

4.3 Feedback from the field application

4.3.1. Presentation of the case application

We performed a field application during the second half-day of the focus group to improve the designed maturity model and evaluate its usability, usefulness, and completeness [74]. The CEO of the

company "Org 6", expressed his interest to assess the maturity of his organization with respect to the management of risks related to the use of digital technologies. This SME operates in the electricity sector. It proposed solutions for electrical mobility and energy storage that respect the principle of planned sustainability, in contrast to planned obsolescence.

This principle aims to face the uncertainties related to health, financial and ecological crises, by adopting a design and manufacturing mode that fosters sharing, reuse and cooperation. Sustainability is at the heart of this organization's activities: from the design, production, maintenance of its products and the logistical choices, to the management of its employees. Org 6 relies on digital technologies to implement this planned sustainability principle. Therefore, it found extreme relevance in evaluating its maturity in terms of digital use, considering the importance of this dimension for its activities and performance.

4.3.2. The maturity evaluation protocol

During the second half-day of the focus group, the 3 participating members of Org 6 (CEO, R&D manager, Logistics manager) applied our maturity model. The model was implemented in a VBA tool prior to the focus group and was adjusted as we discussed with the practitioners during the first half-day. The evaluation was split into four phases. After each one, a debriefing was performed with these 3 actors as well as with the rest of the focus group members.

The first phase consisted in an introduction to the maturity tool's structure and functionalities. The participants were invited to browse a one-page documentation which recalls the objectives of the model and the instructions to guide its implementation. Following the debriefing, the content of this introductory page was improved according to the participants' comments to make it a frame of reference enabling future firms to use the model without the presence of the researcher as an external moderator.

During the second phase, the 3 firm actors proceeded to self-assessment by completing a questionnaire adapted from the Delphi survey to assess the organization's maturity according to the established maturity scale. The discussion with the participants following this stage enabled to clarify some maturity items by reformulating them or illustrating them with examples.

In the third phase, participants scrolled, together with the moderator, the assessment results that are automatically generated in a summary report. It depicts an aggregated score for each KPA accompanied with detailed results for each risk according to the two maturity criteria. Participants unwrapped their results from the least to the most performant KPA and discussed the reasons for the maturity gap of each KPA's items. Accordingly, recommendations for improvement were formulated with the help of the focus group members to enable cross fertilization of best practices.

The fourth phase aimed at verifying the success related to the usage of the model by asking all the focus group members to answer a set of questions assessing its usability, completeness, and utility [74]. Also, the participants could fill blank spaces to provide any further feedback that was not delineated through the proposed questions. Besides collecting their comments and propositions in writing, the researchers made sure to record the oral, gestural, and visual reactions of the participants throughout the evaluation session which had served to improve the content of the model.

4.3.3. Results of the maturity assessment

The assessment showed that Org 6 was very mature regarding the relationships with third parties. It was using digital technologies efficiently with its suppliers, particularly the Cloud and AI, while controlling for their risks. Org 6 applies these technologies to monitor the supply and demand and enable more flexibility on its partnerships. It also harnesses the power of social media to observe the trends and collect the users' feedback on its products. Regarding this topic, we noted a difference of understanding among the three evaluating members. While the CEO was aware of the digitalization projects within the company aiming at fully benefitting from the potential of social media, the R&D

and logistics' manager thought that Org 6 is still immature regarding these aspects. After deep discussions, they agreed that the organization is mindful that social media could eventually harm its reputation and was implementing an AI based scanning to spot any negative tweets or comments and resolve the related issue.

This firm depicted several maturity problems regarding the KPA of Data sensitivity. In fact, it was in the process of implementing GDPR principles in its organization, such as the assignment of a chief digital officer and the collection of consent when personal data is eventually extracted. This firm was also lacking cybersecurity protocols and protective actions for its Cloud. Nevertheless, all these issues concerned the capability maturity criterion and not the willingness. Org 6 was convinced with the necessity to act on these risks and had indeed started an internal reflection on the actions to put in place.

4.3.4. Evaluation of the model's utility, completeness, and usability

In the fourth phase of the model's application underlined in the evaluation protocol (section 4.3.2), we asked the focus group members to answer a set of questions regarding the model's completeness, usability, and utility. A debriefing was then performed to understand the pros and cons of our operationalized model and enhance it accordingly.

Regarding the model's **completeness**, we asked the participants to compare the accuracy of its content with classifications or frameworks of risks associated with the use of digital technologies that they were aware of. None of the participants was knowledgeable of such risks' classification. Nevertheless, they were informed of some tools to assess digital maturity, for instance the DQ framework by the DQ institute [81], the European Digital Competence Framework for Citizens by the European Commission [82], and the Digital Quotient by McKinsey & company [83]. A participant from the insurance sector stated the existence of a risk management process in a concurrent organization, entirely designed in-house, and built according to the life cycle of data in the insurance world. However, it only deals with the risks related to data. Compared to all these tools, the participants stressed that the maturity model developed in this study was "*more accurate in comparison to well-known generic tools. It follows a rigorous scientific approach far from any speculation and is co-constructed with practitioners to align with their frame of reference*". Also, the fact that its design involved organizations from different sectors made it an integrative framework that "*would promote mutual learning between organizations from a variety of sectors, especially as it is difficult for each company to have individual access to constructive feedback about these emerging technologies*".

For the model's **usability**, the participants appreciated the content of the introductory page which methodically explains how to use the model at each step. They then insisted that "*a collective evaluation involving key actors of the organization and representatives of its trades is crucial to capture the firm maturity profile and identify trouble spots*", and "*discern differences of understanding within the same firm that could hinder the implementation of any change management initiative*". Such interactivity would even foster "*actions to correct behavioral issues regarding digital technologies*". Indeed, "*a collective feedback based on the implicit recommendations of the model would guide the firm toward a better distribution of responsibilities with respect to the governance and use of digital technologies*".

As for the **utility** of the model, two key findings of the focus group discussion and the field application should be underlined. The first one was the participants' ability to clearly distinguish digital technologies from other types of Information Technologies. In fact, the group now understood that "*digital technologies are more 'data' oriented and involve a new cognitive framework".* These technologies *"alter our ways of communicating and working and require capacities and postures different from IT*". The respondents explained that "*classical IT is more closed, internal to the company*" while "*digital technologies involve the generation and exchange of data between several internal and external actors, whose volume and speed are important*". In addition, "*digital extends*

information and communication technologies and leads to new practices such as Do It Yourself and Bring Your Own Device".

The second utility finding was particularly highlighted by Org 6. The CEO stressed that the model "*clearly ascertains the risks to be managed. It helped us take a step back on our abilities and pointed out our weaknesses and strengths of which we were not necessarily aware. This makes it easier to initiate targeted improvement actions to manage the alarming risks*". However, a participant underlined that "*this risk management should extend to all dimensions of digital transformation and not only to the use of technologies*". In this regard, another group member explained that "*digitalization involves risks of different kinds: legal risk, image risk, financial risk, ethical risk, time to market risk, usage risk, security risk, risk of non-availability, risk of monitoring, etc*.". Finally, the group participants argued that an adjustment phase of the model prior to its use "*can make the results more significant and concise by focusing the evaluation on the risks that are most relevant to the firm*". This scoping step could address "*all the key individuals within the organization and external experts to revise the model according to the firm's strategic and operational concerns and then apply it*".

5 Conclusion

The advent of digital technologies has induced a wave of transformation within organizations. The latter aims to redefine operational processes, business models, and user experiences to capitalize on the potential offered by digital technologies. However, this digitalization also harbors risks, among others, ethical, technical, and intellectual, of which companies must be aware in order to manage them throughout the transformation process. In this sense, this paper focused on the risks associated with a particular dimension of digital transformation, the use of digital technologies, as it constitutes the foundation of the digitalization process.

Our results combine both the insights of the literature and of an empirical study with practitioners following a Delphi approach and a focus group. From a theoretical standpoint, they contribute to defining the concept of digital risk capability by characterizing its dimensions and components. In this respect, they underline the existence of three classes of risks for using digital technologies, namely risks related to data sensitivity, relationships with third parties, and the governance of digital technologies. In addition, this research brings out new risks specific to the SMAC/DARQ spectrum and accordingly enhances our understanding of these technologies' common and different properties. Furthermore, our findings provide a definition of maturity specific to digital risks that is aligned with the conceptual nature of these items and the practitioners' cognition. From a managerial standpoint, the present study answers a contemporary practical need of firms who embrace digital transformation projects to prosper in this post-digital era. It raises managers' awareness of the risks they should prevent and monitor and provides them with a user-friendly tool to accompany the implementation of digital technologies within their organizations and initiate the necessary improvement actions to capture digital benefits in a secure manner.

This study, however, has some limitations that represent promising research perspectives. First, this paper focused only on the dimension of using digital technologies. It would be relevant to address in depth the risks related to the other aspects of the digitalization such as the alignment between the business strategy and the digital one or the development of employee skills. This would enable a better understanding of the interconnection between digital technologies, but also their relation to the different aspects of organizational performance. Second, the panel of respondents was limited to some specific sectors and, thus, was not statistically representative of the various industries that possess disparate levels of digital maturity. Further case studies would enrich our results and evaluate their applicability in other organizational contexts. Such studies can also inform the digital learning pathways and governance at the individual, organizational and governmental levels. Finally, this research was limited to the design of a maturity model for managing the risks associated to the use

of digital technologies, without addressing the most appropriate way to manage them through concrete actions. Future field applications across different sectors could help build a framework of actions to be undertaken with respect to the maturity deficiency of each risk. Also, a quantitative study can help build a predictive model to prioritize the risks according to their probability of occurrence in an organization considering its contextual peculiarities.

References

1. Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., ... & Ahlemann, F. (2017). Digitalization: opportunity and challenge for the business and information systems engineering community. Business & information systems engineering, 59(4), 301-308.
2. IDC. (2018). Worldwide Digital Transformation Spending Guide. Retrieved from https://www.idc.com/getdoc.jsp?containerId=IDC_P32575
3. Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalization challenge: How to benefit from digitalization in practice. International journal of information systems and project management, 5(1), 63-77.
4. Gassmann, O., Frankenberger, K., & Csik, M. (2014). The business model navigator: 55 models that will revolutionize your business. PearsonUK.
5. Reis, J., Amorim, M., Melão, N., & Matos, P. (2018, March). Digital transformation: a literature review and guidelines for future research. In World Conference on Information Systems and Technologies (pp. 411-421). Springer, Cham.
6. Accenture. (2019). The Post-Digital Era is Upon Us: ARE YOU READY FOR WHAT'S NEXT?. Retrieved from https://www.accenture.com/_acnmedia/pdf-94/accenture-techvision-2019-tech-trends-report.pdf
7. Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. MIS Quarterly Executive, 15(2).
8. Majchrzak, A., Markus, ML, & Wareham, J. (2016). Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges. MIS quarterly, 40(2), 267-277.
9. Singh, A., & Hess, T. (2017). How Chief Digital Officers Promote the Digital Transformation of their Companies. MIS Quarterly Executive, 16(1).
10. Ardolino, M., Rapaccini, M., Saccani, N., Gaiardelli, P., Crespi, G., & Ruggeri, C. (2018). The role of digital technologies for the service transformation of industrial companies. International Journal of Production Research, 56(6), 2116-2132.
11. Preece, R. (2018). The GDPR accountability principle and the use of scenario workshops in the digital age. Journal of Data Protection & Privacy, 2(1), 34-40.
12. Garmann-Johnsen, NF, Helmersen, M., & Eikebrokk, TR (2018). Digital Transformation in Healthcare: Enabling Employee Co-Creation through Web 2.0.
13. Zimmerman, P., Gilbert, T., & Salvatore, F. (2017). Digital engineering transformation across the Department of Defense. The Journal of Defense Modeling and Simulation.
14. Yang, L., Zheng, Q., & Fan, X. (2017, May). RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks. In IEEE INFOCOM 2017-IEEE Conference on Computer Communications (pp. 1-9). IEEE.
15. Dneprovskaya, N., Bayaskalanova, T., Shevtsova, I., Urintsov, A. (2018). Digital Transformation Of Communication Between Government Authorities And Citizens. Proceedings of the International Conference on Research Paradigms Transformation in Social Sciences
16. Barreto, L., & Amaral, A. (2018, September). Smart Farming: Cyber Security Challenges. In 2018 International Conference on Intelligent Systems (IS) (pp. 870-876). IEEE.
17. Van Looy, A., Poels, G., & Snoeck, M. (2017). Evaluating business process maturity models. Journal of the Association for Information Systems, 18(6), 1.
18. Dooley, K., Subra, A., & Anderson, J. (2001). Maturity and its impact on new product development project performance. Research in Engineering Design, 13(1), 23-29.
19. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS quarterly, 75-105.
20. Hevner, A., & Gregor, S. (2020). Envisioning entrepreneurship and digital innovation through a design science research lens: A matrix approach. Information & Management, 103350.

21.Maier, A. M., Moultrie, J., & Clarkson, P. J. (2012). Assessing organizational capabilities: reviewing and guiding the development of maturity grids. IEEE transactions on engineering management, 59(1), 138-159.
22.Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems.
23.Sebastian, IM, Ross, JW, Beath, C., Mocker, M., Moloney, KG, & Fonstad, NO (2017). How Big Old Companies Navigate Digital Transformation. MIS Quarterly Executive.
24.Svahn, F., Mathiassen, L., Lindgren, R., & Kane, GC (2017). Mastering the digital innovation challenge. MIT Sloan Management Review, 58(3), 14.
25.Lepore, D., Nambisan, S., Tucci, CL, & Zahra, SA (2019, July). Digital Transformation & Firms' Innovative Strategies: Capabilities, Ecosystems, and Business Models. In Academy of Management Proceedings (Vol. 2019, No. 1, p. 14623). Briarcliff Manor, NY 10510: Academy of Management.
26.Stolterman, E., & Fors, A. C. (2004). Information technology and the good life. In Information systems research (pp. 687-692). Springer, Boston, MA.
27.Strachan, R., & Aljabali, S. (2015). Investigation into Undergraduate International Students' Use of Digital Technology and Their Application in Formal and Informal Settings. International Association for Development of the Information Society.
28.Gombault, A., Allal-Chérif, O., & Décamps, A. (2016). ICT adoption in heritage organizations: Crossing the chasm. Journal of Business Research, 69(11), 5135-5140.
29.Earley, S., & Maislin, S. (2016). Data governance and digital transformation: Using the customer journey to define a framework. Applied Marketing Analytics, 2(1), 25-40.
30.Koffer, S. (2015). Designing the digital workplace of the future–what scholars recommend to practitioners.
31.Muller, E., & Hopf, H. (2017). Competence center for the digital transformation in small and medium-sized enterprises. Procedia Manufacturing, 11, 1495-1500.
32.Masuda, Y., Shirasaka, S., Yamamoto, S., & Hardjono, T. (2018). Architecture board practices in adaptive enterprise architecture with digital platform: a case of global healthcare enterprise. International Journal of Enterprise Information Systems (IJEIS), 14(1), 1-20.
33.Karimi, J., & Walter, Z. (2015). The role of dynamic capabilities in responding to digital disruption: A factor-based study of the newspaper industry. Journal of Management Information Systems, 32(1), 39-81.
34.McDaniels, T., & Small, M. (Eds.). (2004). Risk analysis and society: an interdisciplinary characterization of the field. Cambridge University Press.
35.Capgemini. (2019). Digital Transformation Review: 12th Edition. Retrieved from https://www.capgemini.com/fr-fr/etudes/digital-transformation-review-12/
36.Deloitte. (2018). Managing Risk in Digital Transformation. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-managing-risk-in-digital-transformation-1-noexp.pdf
37.Sambamurthy, V., & Zmud, RW (2012). Guiding the digital transformation of organizations. Lightness Digital Press.
38.Carcary, M., & Doherty, E. (2016, September). 'The Digital Wild West': Managing the Risks of Digital Disruption. In The European Conference on Information Systems Management (p. 29). Academic Conferences International Limited.
39.Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. Business & Information Systems Engineering, 57(5), 339-343.
40.Kineshanko, MK, & Jugdev, K. (2018). Enhancing Digital Intelligence Through Communities of Learning. In On the Line (pp. 111-125). Springer, Cham.
41.Adams, NB (2004). Digital intelligence fostered by technology. Journal of Technology Studies, 30(2), 93-97.
42.Zhu, K., Dong, S., Xu, SX, & Kraemer, KL (2006). Innovation diffusion in global contexts: determinants of post-adoption digital transformation of European companies. European journal of information systems, 15(6), 601-616.
43.Merriam Webster (2001). Merriam-Webster's collegiate dictionary. Advocate [Internet][cited 31 Jan 2013]. Available from: www. merriam-webster. com/dictionary.
44.Mili, A., Bassetto, S., Siadat, A., & Tollenaere, M. (2009). Dynamic risk management unveil productivity improvements. Journal of Loss Prevention in the Process Industries, 22(1), 25-34.
45.Szostak, R. (2004). Classifying science (pp. 1-22). Springer Netherlands.
46.Tekic, Z., & Koroteev, D. (2019). From disruptively digital to proudly analog: A holistic typology of digital transformation strategies. Business Horizons, 62(6), 683-693.
47.Dasi, A., Elter, F., Gooderham, PN, & Pedersen, T. (2017). New Business Models In-The-Making in Extant MNCs: Digital Transformation in a Telco. In Breaking up the Global Value Chain: Opportunities and Consequences (pp. 29-53). Emerald-Publishing Limited.

48.Sulkowski, Ł., & Kaczorowska-Spychalska, D. (2018, July). Internet of Things-New Paradigm of Learning. Challenges for Business. In International Conference on Applied Human Factors and Ergonomics (pp. 307-318). Springer, Cham.
49.Romero, D., Flores, M., Herrera, M., & Resendez, H. (2019, June). Five Management Pillars for Digital Transformation Integrating the Lean Thinking Philosophy. In 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-8). IEEE.
50.Riera, C., & Iijima, J. (2019). The Role of IT and Organizational Capabilities on Digital Business Value. Pacific Asia Journal of the Association for Information Systems, 11(2).
51.Sushko, VA, Dekhanova, NG, & Kholodenko, UA (2019). Employment policy in the conditions of the digital revolution. Dilemmas Contemporáneos: Education, Política y Valores, 7(1).
52.Lopes, N., Rao, HR, McKenna, SA, Yang, S., Estevez, E., & Nielsen, M. (2019, April). Panel: Digital Transformation Impact on Society. In 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 19-21). IEEE.
53.Kushzhanov, NV & Mahammadli, D. (2019). The digital transformation of the oil and gas sector in Kazakhstan: Priorities and problems. News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences.
54.Borisova, V., Taymashanov, K., & Tasueva, T. (2019). Digital Warehousing as a Leading Logistics Potential. In Sustainable Leadership for Entrepreneurs and Academics (pp. 279-287). Springer, Cham.
55.Kushzhanov, NV, & Aliyev, UZ (2018). Digital space: changes in society and security awareness. Bulletin of the National Academy Of Sciences of the Republic of Kazakhstan, (1), 94-101.
56.Medapati, PK, Tejo Murthy, PHS, & Sridhar, KP (2019). LAMSTAR: For IoT-based face recognition system to manage the safety factor in smart cities. Transactions on Emerging Telecommunications Technologies, e3843.
57.Kaczorowska-Spychalska, D. (2018). Shaping Consumer Behavior in the Fashion Industry by Interactive Communication. Fibers & Textiles in Eastern Europe.
58.Lindman, J., Tuunainen, VK, & Rossi, M. (2017). Opportunities and risks of Blockchain Technologies–a research agenda.
59.Dugstad, J., Eide, T., Nilsen, ER, & Eide, H. (2019). Towards successful digital transformation through co-creation: a longitudinal study of a four-year implementation of digital monitoring technology in residential care for persons with dementia. BMC health services research, 19(1), 366.
60.Cave, M. (2018). How disruptive is 5G?. Telecommunications Policy, 42(8), 653-658.
61.Arntz, M., Gregory, T., & Zierahn, U. (2017). Revisiting the risk of automation. Economics Letters, 159, 157-160.
62.Harshanath, SB (2018, October). Detection and Protection Related to Data Sharing Technologies. In TENCON 2018-2018 IEEE Region 10 Conference (pp. 0156-0161). IEEE.
63.Kartit, Z., & Diouri, O. (2019, March). Security Extension for Routing Protocols in Ad hoc Mobile Networks: A comparative Study. In Proceedings of the 2nd International Conference on Networking, Information Systems & Security (p. 69). ACM.
64.Prioteasa, AL., Chicu, N., & and Ciocoiu, CN. (2018). Implications of Digitization on Risk Management in Romanian Companies. Proceedings of the 31st IBIMA Conference, Milan, Italy
65.Shah, S., Shah, B., Amin, A., Al-Obeidat, F., Chow, F., Moreira, FJL, & Anwar, S. (2019). Compromised user credentials detection in a digital enterprise using behavioral analytics. Future Generation Computer Systems, 93, 407-417.
66.Mitra, A., & Munir, K. (2019). Influence of big data in managing cyber assets. Built Environment Project and Asset Management.
67.Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2016, September). Data protection compliance regulations and implications for smart factories of the future. In 2016 12th International Conference on Intelligent Environments (IE) (pp. 40-47). IEEE.
68.Malyavkina, LI, Savina, AG, & Parshutina, IG (2019, May). Blockchain technology as the basis for digital transformation of the supply chain management system: benefits and implementation challenges. In 1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth"(MTDE 2019). AtlantisPress.
69.Grigoryeva, EE, & Sentizova, NR (2019, May). Features of the Russian raw and cut diamonds business digitalization. In 1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth"(MTDE 2019). AtlantisPress.
70.Tekic, Z., & Koroteev, D. (2019). From disruptively digital to proudly analog: A holistic typology of digital transformation strategies. Business Horizons, 62(6), 683-693.
71.Muntés-Mulero, V., Ripolles, O., Gupta, S., Dominiak, J., Willeke, E., Matthews, P., & Somosköi, B. (2018). Agile risk management for multi-cloud software development. IET Software, 13(3), 172-181.
72.Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. Information and software technology, 54(12), 1317-1339.

73.Akhlaghpour, S., & Lapointe, L. (2018). From Placebo to Panacea: Studying the Diffusion of IT Management Techniques with Ambiguous Efficiencies: The Case of Capability Maturity Model. Journal of the Association for Information Systems, 19(6), 441-502.
74.Fraser, P., Farrukh, C., & Gregory, M. (2003). Managing product development collaborations—a process maturity approach. Proceedings of the Institution of Mechanical Engineers, Journal of Engineering Manufacture, 217(11), 1499-1519.
75.Moultrie, J., Clarkson, P. J., & Probert, D. (2007). Development of a design audit tool for Technology SMEs. Journal of Product Innovation Management, 24(4), 335-368
76.Keil, M., Tiwana, A., & Bush, A. (2002). Reconciling user and project manager perceptions of IT project risk: a Delphi study 1. Information systems journal, 12(2), 103-119.
77.Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. Journal of management information systems, 17(4), 5-36.
78.Gioia, DA, Corley, KG, & Hamilton, AL (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational research methods, 16(1), 15-31.
79.McDonald, W. J. (1994). Provider perceptions of focus group research use: A multicountry perspective. Journal of the Academy of Marketing Science, 22(3), 265-273.
80.SEI. (2006). Software for development, Version 1.2. Software Engineering Institute
81.Digital Intelligence (DQ). (2017). A Conceptual Framework & Methodology for Teaching and Measuring Digital Citizenship. https://www.dqinstitute.org/wp-content/uploads/2017/08/DQ-Framework-White-Paper-Ver1-31Aug17.pdf (DQ Institute, 2017).
82.European Commission. (2018). How European Education Keeps up Nowadays. URL: https://eavi.eu/how-europeaneducation-keeps-up-nowadays-e-learning-and-e-education.
83.McKinsey & Company. (2015). Raising your Digital Quotient. https://www.mckinsey.com/businessfunctions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient