Bakos, Levente; Dumitrașcu, Dănuț Dumitru

Article

Decentralized enterprise risk management issues under rapidly changing environments

Risks

Provided in Cooperation with:
MDPI – Multidisciplinary Digital Publishing Institute, Basel

Suggested Citation: Bakos, Levente; Dumitrașcu, Dănuț Dumitru (2021) : Decentralized enterprise risk management issues under rapidly changing environments, Risks, ISSN 2227-9091, MDPI, Basel, Vol. 9, Iss. 9, pp. 1-18,
https://doi.org/10.3390/risks9090165

This Version is available at:
https://hdl.handle.net/10419/258249

risks

MDPI

Article

Decentralized Enterprise Risk Management Issues under Rapidly Changing Environments

Levente Bakos [1,*] and Dănuț Dumitru Dumitrașcu [2]

[1] Mechanical Engineering Department, Faculty of Technical and Human Sciences Târgu Mureș, Sapientia Hungarian University of Transylvania, 400112 Cluj-Napoca, Romania
[2] Industrial Engineering and Management Department, Faculty of Engineering, Lucian Blaga University of Sibiu, 550024 Sibiu, Romania; dan.dumitrascu@ulbsibiu.ro
* Correspondence: bakos@ms.sapientia.ro; Tel.: +40-265-206-201

Abstract: Under the growing complexity of manufacturing processes, supply chains, markets and stakeholder expectations, enterprise risk management (ERM) has become an extremely important, probably yet still underdeveloped, management function. Enterprise risk management theory and practice should keep pace with the changes of rapidly changing environments, through new, more adaptive approaches. The article presents some of the results of a longitudinal survey at Eastern-European manufacturing organizations made on risk management techniques. The goal of the research was the study of risk management techniques under rapidly changing environments in highly standardized industries (pharmaceutical and automotive). The research was focused on the role of human resources in handling technology-related/operational risks and to what extent a decentralized risk management is present. Multidisciplinary cooperation, the selection of the teams, communication and the decision making within the team was analysed. During our research few common risk analysis routines were identified at the studied organizations. Through an interview-based qualitative survey, possible weaknesses of common risk identification techniques were identified. The article presents three risk evaluation methods with the same features. The answers provided during the interviews indicate that risk assessment techniques are mostly centralized (coordinated by a single person/unit), linear (based on If-Then construct) and rigid, definitively not suitable when quick changes are in the organization environment.

Keywords: enterprise risk management; decentralized risk assessment; linear thinking

Citation: Bakos, Levente, and Dănuț Dumitru Dumitrașcu. 2021. Decentralized Enterprise Risk Management Issues under Rapidly Changing Environments. *Risks* 9: 165. https://doi.org/10.3390/risks9090165

Academic Editor: Mogens Steffensen

Received: 4 August 2021
Accepted: 7 September 2021
Published: 10 September 2021

1. Introduction

Organizations under rapidly changing environments are becoming more exposed to unpredicted situations. The preparedness for the future challenges depends on the efficiency of their risk assessment techniques. Uncertainty is part of each organization's life. "Risks are fraught with uncertainty due largely to their prospective nature. Each facet of risk—events, outcomes, and effects—involves uncertainty" (Sobel and Reding 2012). Under the growing complexity of manufacturing processes, supply chains, markets and stakeholder expectations, enterprise risk management (ERM) became an extremely important, probably yet still underdeveloped, management function. Global financial crises, pandemics, terrorism, the blast of new technologies, major geo-political changes are only a few but strong challenges from the external environment that each organization must face. Technological disturbances, human errors, ever changing customer demands, uncertain resources (human, financial, material) are further concerns in risk management. Most of these factors existed decades ago; the major difference comparatively even up to 5–6 years ago consists of the speed at which these changes are happening. We are witnessing an emerging new infrastructure and communication environment turning into complex systems that mankind has never experienced before. Enterprise risk management

(ERM) theory and practice should keep pace with these changes through new, more adaptive approaches.

The goal of our research is to study risk management techniques under rapidly changing environments in highly standardized industries. The research presents some of the results of a longitudinal survey at Eastern-European manufacturing organizations made on risk management techniques.

The research method in this qualitative phase consisted of a semi-structured face-to-face interview. The research questions were related to the human resource management side of the studied risk management methods, tools and processes. Beside what kind of risk identification tools/methods are in use, a major concern was about who sets the procedures and make decisions, how the teams are selected, how the teams work under rapidly changing conditions and finally, to what extent a decentralized risk management is present. We investigated the professional background of the risk assessment teams (multidisciplinary teams vs. homogenous staff) and also the decision making rules within the teams (centralized vs. decentralized). During the survey, how the explicit knowledge is gained during the management of risks, how the knowledge-transfer is carried out and if there is a conciliation of divergent professional goals were investigated.

While researching the manner in which the risk assessment teams are handled, some disadvantages of common risk assessment techniques were discovered which makes these procedures definitively not suitable when there are quick changes. In this article three weaknesses of some common risk identification techniques used in risk management are presented: (1) centralized approach, (2) linear thinking and (3) time as constraint avoided. These might become obstacles in adaptive risk management under rapidly changing environments.

The first issue represents the centralized approach. Risk management, if it exists as an intentional process within the organization, represents a high importance activity. As such, it usually is coordinated by the top management level. As consequence, the risk management by default is centralized, rigid and linear.

Beside centralization, the second issue underlined here as a possible weakness of common risk identification techniques is the linear thinking. Linear thinking it is typical for the technical environments, being the "preference for attending to external data and facts and processing this information through conscious logic and rational thinking to form knowledge, understanding, or a decision for guiding subsequent action" as it was defined in (Vance et al. 2007) On the other hand, nonlinear thinking is the "preference for attending to internal feelings, impressions, and sensations when comprehending and communicating information" (Vance et al. 2007), and is not really the usual way in which things are done in technical risk evaluation. Still, in risk management the intuition, creativity and concentration on internal factors are key issues, and these characteristics by definition are related to non-linear thinking. In our non-linear world, complex systems (as the organizations) are definitively characterized by non-linearity (Rihani 2002), and our digitalized era demands for non-linear thinking (Osterman et al. 2013).

The third issue about possible weaknesses of the common risk identification techniques is that mostly there are scarce recommendations of how time as a constraint should be handled. The speed at which things in our environments change is much higher than was expected. The quick transformations are fuelled by digital technology, power of networks (of any type) and increasing information processing power. Time became a key parameter in most of the processes. The traditional static, timely unconstrained conditions are proper to have a clear image about the present, but this instant picture is very soon outdated. Similar to most of the scientific domains, in industry the existing risk management models, methods and techniques should be reconsidered under the increasing rate of change. Innovation cycles are shortened, and the success or failure of an efficient risk evaluation is closely connected to ability to take in consideration the variation of the initial conditions. Innovation, adaptability and resilience are the new metrics for success.

During our research, few common risk technical analysis routines were identified at the studied organizations. That is the reason why among the plenitude of concepts, methods and techniques only three common risk assessment tools were chosen: risk management based on standards, the PDCA (Plan-Do-Check-Act) cycle and FMEA (Failure Mode and Effects Analysis). The present article aims to call attention to the weaknesses of these techniques under rapidly changing environments. These weaknesses are: centralized approach, linear thinking, and unfocused on time as a constraint.

2. Literature Review

Risk management is an extremely wide notion. Wherever there are uncertainties there are risk management processes. There is no scientific discipline without intense academic research on risks and without a plethora of guidelines, frameworks, and tools. Our survey is focused on the borderline of technical risk assessment of industrial manufacturing processes (approached through risk standards and specific evaluation techniques) and the company-focused risk analysis topic (represented by the holistic ERM approach). Accordingly, in order to frame our survey, the literature review will present some references related to ERM, in the first part, and also some relevant achievements of risks assessment tools used in industrial environments in the second part.

2.1. ERM vs. Traditional Risk Management

There several domains of management science dealing with the enterprise level risk: enterprise risk management, corporate risk management, integrated risk management or business risk management are just few of the concepts found in literature. Although they are different in name, industry and region, nevertheless, they all share a common theme: the identification, prioritization and quantification of risks in order to help corporations effectively manage their exposure. (Daud et al. 2010). Among these concepts it seems ERM represents the most suitable approach to our research topic.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defined ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (CCOSO 2004). According to the ERM frameworks all risks occurring in the entity must be combined and managed in enterprise approach. (Razali and Tahir 2011). This holistic approach of the ERM is widely discussed in the scientific literature, several reviews present this topic in detail CCOSO (2004), Gates (2006), Gordon et al. (2009), Ching and Colombo (2014), Bromiley et al. (2015), Fraser et al. (2015), Wu et al. (2015), Lackovic (2017), and more recently Anton and Nucu (2020), Kerraous (2020). The holistic approach to managing risk can enable organizations to deal with risks and opportunities more effectively, enhancing the organization's capability to create and preserve value for stakeholders (CCOSO 2004).

Kumar, in a recent article (Kumar 2021), posits several arguments about the differences between the risk management and enterprise risk management. Risk management on the one hand is the process of risk identification and risk mitigation, ERM on the other hand is a risk management architecture that binds the risk management across the organization. It can be said that ERM is enabler of Companywide risk management (Kumar 2021).

In spite of the fact that our survey focuses on risk assessment tools mostly related to technologies, the article emphasizes the importance of a companywide holistic approach and opposes the silo approach of some traditional risk management routines. In manufacturing environments, very often the risk management is a fragmented approach followed in silos by few departments. This approach might become an enterprise level threat with major consequences. Silo risk management does not work because risks are highly correlated and cannot be managed independently. (Kumar 2021). The implementation of the ERM system improves organizational performance Paape and Speklé (2012), Mensah and Gottwald (2016), COSO (2017). A proper risk management strategy can grow in competi-

tive advantage, supporting firms to grow (Blanco-Mesa et al. 2019). A recent review based on a large sample from 2008–2019 literature indexed on the ISI Web of Science has revealed that the most frequently investigated topic of ERM is firm performance. (Anton and Nucu 2020).

2.2. Decentralization and Non-Linear Thinking

Traditionally, organizations have a hierarchical structure. The top of hierarchy have overall responsibility for all activities and procedures. Risk management is not an exception. As argued above, a companywide holistic approach is essential, the fragmented silo approach is not efficient. Still, the holistic, enterprise wide approach does not necessarily mean a centralized, CEO-based rigid structure. Most of the ERM frameworks suggest that for a company with good risk management embedding, a separate risk management function is required, headed by the CRO (Chief Risk Officer). (COSO 2017; Kumar 2021). The "quality" of CROs has a strong influence on how the level of adoption risk management policies, and company performance (Beasley et al. 2005; Daud et al. 2010; Razali et al. 2011; Paape and Speklé 2012; Baxter et al. 2013; Waweru and Kisaka 2013; Kerraous 2020; Mensah and Gottwald 2016). Furthermore, the results of (Baxter et al. 2013) show that the existence of a risk committee has a positive result on the ERM's integration (Baxter et al. 2013). The existence of risk commitees, risk management teams, leads to a decentralized approach. In this case, the decisions are not made by a single person, and the traditional top-down chain of command is not present. In rapidly changing complex environments, decentralized risk management approaches might provide the single solutions.

Concepts like cloud technology, smart factory, organic computing and Industry 4.0 point to decentralized organizations. (Qin et al. 2016; Wang Shiyong et al. 2016) There is already a rich scientific literature regarding the new types of less-hierarchical organizations. Teal organizations (Laloux 2014), "organic-computing" concept (Müller-Schloer and Tomforde 2017), the emerging integrative concept of self-managing organizations (Lee and Edmondson 2017) are just few of the concepts recently emerged. Brian Robertson's holacracy (Robertson 2015), in which employees have the freedom to take actions within their roles of responsibility, an organization (almost) without managers, apparently skipped the scientific debate phase and was directly put in practice at several organizations. Some of the most cited examples, the Amazon-owned Zappos or the Morning Star, are analysed in the scientific literature and are supported by theoretical findings (Hamel 2011; Lee and Edmondson 2017). All of these initiatives and theories have as a common goal to create a better organized adaptive, innovative structure which can handle the challenges of our era. The problems of the third decade of the XXI century cannot be solved with management solutions developed for the problems of the first industrial revolution.

The decentralized risk management is not a new approach. There are many domains in which decentralized risk management is the standard; let us mention the risk pooling technique used in investments or insurance. There is already a rich literature in decentralized risk management approaches in disaster management (Hermansson 2019), (UNDP 2015) cybersecurity (Jarjoui and Murimi 2021; Hu et al. 2021), supply chain management (Andersen 2010) or critical infrastructure management (Crowther 2008), as well.

Advisory giants, like KPMG, McKinsey or Deloitte, made several surveys and issued proposals for more agile risk management. According to a KPMG technology risk management survey "traditional technology risk methods have evaporated and enterprises need to create an agile and dynamic technology risk organization to keep up with the pace of change". (KPMG 2018) "A time for boards to act" is the conclusion of a global survey carried out on 1100 directors by McKinsey, and they posit that "potential disruptions can arise at any time, it is important that boards maintain flexible agendas rather than become prisoners of their annual schedules" (McKinsey 2018). Deloitte, addressing the challenges of decentralization propose, as a result of a survey on 170 executives, proposes "Allocating activity ownership for TPGRM (Third Party Governance & Risk Management) activities to capable and appropriately trained individuals at the group and local levels with decision

making authority" (Deloitte 2016). In all these cited documents of expert organization the idea of the new era of decentralization is presented.

Here, decentralized enterprise risk management means a structure that allows entities (departments and/or individual employees) within the organization to manage risk. Under normal circumstances, a risk management (method, tool, process) is considered decentralized if much of the risk assessment process (and sometimes the strategic decision-making related to it) is transferred to the risk owners and operators. Due to the fact that during our survey in the studied organizations, such entrustment was not present, the level of decentralization was measured by the existence and size of the cross-functional risk assessment teams. It was studied if the multidisciplinary knowledge is among the selection criteria. If created teams are empowered to prepare risk management decisions and could create policies, it was interpreted as an embryonic form of decentralization.

Here, linear thinking means a way of acting based only on data, facts and written rules, a conscious and rational way to create knowledge, and avoiding thinking differently, unconventionally, or from a new perspective. It is linear thinking, when during risk evaluation the effects of a risk are measured only by the size of material damage or the cost associated with it. For example, the effect of losing 10 customers due to a quality issue is definitively not double that of losing five of them. In the same manner, a 10$ hamburger, in a world-wide known franchise, may have as a consequence a million-dollar loss due to the emerging bad reputation (only a single picture is necessary and the unsatisfied celebrity customer may share it with their few millions of followers). Recently, one of the best sportsmen of the world just made a gesture during a press conference. He moved away a bottle of soft drink put in front of him while mentioning that is better to drink water. This very likely spur-of-the-moment action had negative impact on the stock market for the famous brand. Risk management should not rely only on linear thinking; the risk assessment and mitigation techniques should go beyond the rigid "cause-and-effect"- or "if-and-then"-based approach.

2.3. Literature Review of Common Risk Management Tools

2.3.1. Risk Management Standards

Risk standards are linear and centralized because usually there is a need for a cyclical routine and a person in charge has to lead the activities. Anything is supervised by the top-management, and there are strict procedures on how things should be done. The reference standard in risk management is unquestionably the ISO31000:2018 Risk management standard family. Beside these specific risk management standards, there are several other general purpose standards closely related to risk management. Let us mention the ISO45000 occupational health standard family or the ISO 23932-1:2018 Fire safety engineering standard. According to the International Standardization Organization the most commonly used quality management standard for companies and organizations of any size in manufacturing is definitively the ISO 9000 Quality Management family. (Source: www.iso.org, accessed on 31 August 2021). There is a major on-going paradigm shift in quality management, and as result of this that the ISO9001:2015 revision moved away from the traditional preventive action perspective toward a risk-based thinking. According to the same source, beside ISO9000, the two most frequently used standards are: the ISO/IEC 27,000 family for Information Security Management and the ISO45000 for occupational health and safety. Both standards are closely related to risk management. These laws and standards provide a scientific fundament for risk assessment, however they have at least two important weaknesses. First, they rely on a linear cause-and-effect risk evaluation, and second, due to their generic characteristic, they are not able to provide hints for the *speed*, how risk assessment processes should be performed. As is presented in Figure 1, risk assessment is a cyclical activity, a step-by-step linear approach. The dotted line suggests a continuous linear cyclical activity, but there are no general valid recommendations on how often should be the cycle repeated.

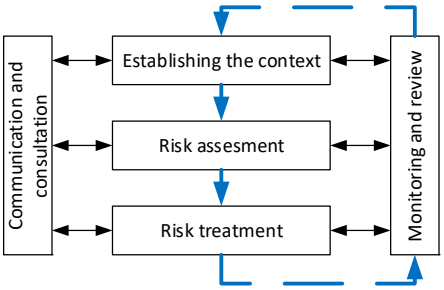

Figure 1. Risk assessment cycle based on ISO31000.

The above presented periodicity may depend on many variables resulting both from outside or inside the organization. The risk assessment methods, as most of the above presented standards suggest, represent a relatively slow, strategic and comprehensive process. In practice, there are cases when circumstances changes in such a quick manner when there is no room for complete and broad analysis.

During the comprehensive cycle of the risk evaluation it is possible to use cross-functional teams and brainstorming-like methods. Due to the involvement of professionals from multiple domains, certainly there is a synergic effect, characteristic to non-linear thinking. Still, risk evaluation based on standards as ISO31000/ISO9000 mostly consists of iterative actions of relative homogeneous professional groups, the exhaustive identification of risk groups. To conclude: risk evaluation based on standards can be considered centralized (due to the supervised and coordinated risk assessment), linear (due to high formalization and the If-Then construct) and time consuming (it takes time to complete the cycle).

2.3.2. The PDCA Cycle

The second risk evaluation tool discussed is closely related to the risk management standards; the PDCA method is included in the working procedures of standards (Gupta 2006). For example, ISO/IEC 27002 Standards uses the Plan-Do-Check-Act model for the assessments and treatment of information security risks. The PDCA cycle (the meaning of letters: P-plan, D-do, C-check, A-act) is extremely common in the risk assessment practice, in spite of the fact that is acknowledged as a quality assurance method. The PDCA methodology, known as the Deming Cycle (Deming 1986), is based the philosophy of continuous improvement. The PDCA methodology itself is an example of continuous improvement. With its origins dating back centuries, the method was made popular by W. Edwards Deming in 1950 during his lectures in Japan. Being based on Walter A. Shewhart's old cycle "Specification-Production-Inspection" (Shewhart [1939] 1986), the PDCA cycle sometimes is called Shewhart cycle, as well. In the scientific literature the PDCA concept is mostly related to Deming, who promoted it and improved it several times. In the latest of his versions, he replaced the "C"-check, with "S"-studying, this way he intended to emphasize the importance of inspection over analysis (Moen and Clifford 2009).

Theoretically, in the PDCA methodology the cycle can be iterated infinitively until the desired (perfect) state is achieved. The basic idea of the method is that if the cycle is iterated enough times, the improvements will take place sooner or later (Figure 2).

The pace at which the improvements become visible depends on many variables, but usually the concept can be effective in timescale of weeks, months or years. In manufacturing environments to identify and address risks (plan) to take actions to improve performance (act) there are several time consuming activities. It is very difficult to estimate the time needed for the implementation of what was planned (do) and to monitor and measure processes (check). If the conditions are met, the cycle will improve the risk management course over time, and will lead to better results.

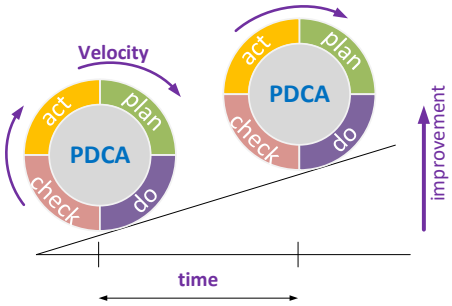

Figure 2. The PDCA cycle (based on the Deming cycle).

In practice, the PDCA cycle is used both in time limited processes (for example risk mitigation in a project) and in the case of a continuous activity (for example quality assurance/process management in the mass production). The PDCA methodology in the recent decades has become an important analysis tool, and it is still an appealing research topic. The research literature published in 2015–2020 is presented in (Isniah et al. 2020) and shows primarily the strengths of the method. At the same time, some weaknesses of the method should be mentioned as well. The cycle allows careful planning, but sometimes the progress is very slow. The risk assessment might be locked for a long time in the early stages. Over analysis is not well-suited for emergencies, the method being very methodical; it may obstruct any swift reaction during rapidly changing environments. A second weakness of the method: its rigidity. In the studied organizations the cycle is iterated several times, but the person(s) involved just follow some procedures automatically. In this form of carrying on, the innovative and creative processes will not merge. Sometimes the most important feature of PDCA, the continuous improvement, is skipped when people act mechanically not really knowing why they do what they do.

Further weakness of the PDCA technique is that it is mostly used to study technical risk. Activities such as education, benchmarking, stakeholder management (other than customers and suppliers) that might influence the successful improvement are disregarded. To conclude, the PDCA cycle is linear, centralized and time consuming.

2.3.3. Failure Mode and Effects Analysis (FMEA)

The third assessing risk method analysed is the FMEA safety and reliability analysis. Failure Mode and Effects Analysis (FMEA) is a widely used powerful method, developed by the U.S. military back in the mid 1960s. It is a step-by-step approach that has as a goal the identification of all possible failures from the early design phase of a product until the after-sales period, sometimes until the end of the product lifecycle (when it becomes a waste). In the beginning it was generally used by the aviation industry (McDermott et al. 2008); later, it became a basic tool to reduce the risk associated with a system or manufacturing/assembly processes in automotive industry, being enforced by the QS-9000 standard (Stamatis 1996). Today it is intensively used in a wide range of other domains (such as aerospace and nuclear industry, medicine) and many types of organizations (manufacturing/services, profit/non-profit, private/public, non-governmental/government organizations). It became a conventional tool for assessing risk even in the case of specific risks such as those related to information technology (Najwa and Subriadi 2018). The FMEA technique became a common tool for managers to identify potential failure modes, potential causes, and mitigation (Sharma and Sharma 2010).

One of the strengths of FMEA consists of documenting the current knowledge about the risks of failures and also the actions to remediate them. For example, in (Murphy et al. 2011) a methodology for extracting innovation constraints from building projects is presented. Through FMEA, a database of innovation constraints is generated which can be used as a benchmarking framework for further researches. In the manufacturing practice FMEA it is an excellent tool for continuous improvement from the earliest stages of design until the end of the life of the product. After more decades of FMEA it is still developing in

the context of intelligent manufacturing (Wu et al. 2021). Among the weaknesses must be counted its linearity (depicted in Figure 3). As we can see the FMEA is a time consuming multi step process.

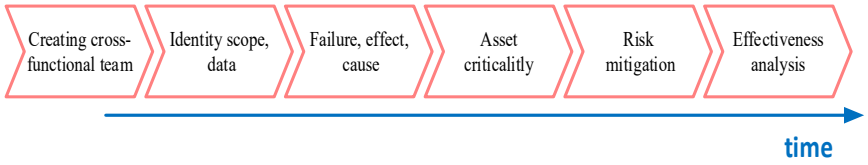

Figure 3. FMEA process analysis tool.

The linear thinking consists not only of the step by step approach of the method but also the basic concept: FMEA focuses on the highest-priority failures, and takes actions to eliminate these failures first. During the effects analysis, the experts study the consequences of the identified failures. The ranking of each failure is determined by its occurrence and a Risk Priority Number (RPN) is assigned to it. This will prioritize also the action, failures are prioritized according to how serious their consequences are.

Despite numerous successful applications, the FMEA, its traditional form, faces much criticism and is widely debated in literature. Several studies recommend some improvements or adjustments to the traditional FMEA. (Bouti and Kadi 1994; McDermott et al. 2008; Hippel 2006)

One of the identified weaknesses of the FMEA is related to a consistency issue. (Subriadi and Najwa 2020). Very often results show inconsistency; among the causes are the difficulties in identifying the root causes, inaccurate evaluation of risk factors, subjectivity, ill-defined scale criteria in determining of RPN (Barends et al. 2012). While Estorilio and Posso highlighted seven factors that contribute to inconsistencies in the automotive industry (Estorilio and Posso 2010), Subriadi et al. identified four main causes for inconsistencies: the prioritization methods, the procedures for assessing risks, the skills and knowledge of the teams involved, and the ability of facilitators to conduct FMEA-based risk assessments. (Subriadi et al. 2018). Oldenhof et al. suggest that in order to overcome this weakness FMEA must be carried out under the supervision of an experienced FMEA-facilitator and that the FMEA team has at least two members with competence in the analytical method (Oldenhof et al. 2011).

The impact of inconsistent risk assessment results is critical. If FMEA is improperly applied, an incorrect risk mitigation process will follow. In this case, beside the consequence of being unprepared for some critical risks, there are important resources used to mitigate unimportant risks. In FMEA, high-risk priority means high cost. This weakness is due to the linear thinking. FMEA uses a breakdown structure to identify single failure causes and has less consideration for interconnected failures. That is the reason for which FMEA does not give good results in the case of new systems. It usually takes time to perform the FMEA well. In order to overcome the fact that FMEA is limited to normal expectations of occurring failures, some of the researches propose to combine FMEA with AFD (anticipatory failure determination) and/or AHP (analytical hierarchy processes) (Thurnes et al. 2015; Mzougui and Felsoufi 2019; Kulcsár et al. 2020). Additionally, some studies propose hybrid models, for example with fuzzy methods (Fuzzy Preference Programming, Fuzzy Cognitive Maps and others) as was proposed by (Baykasoğlu and Gölcük 2017).

A further major weakness of the traditional FMEA is related to the time required by it: in FMEA, risk assessment requires time and job division. That is the reason why FMEA performs well in existing systems, where there is time to build consistent teams, time to analyse the possible issues and to build multiple points of view. While regarding the cross-functional teams there is rich literature, there are only few experiments found in the literature about time issues. Mostly there are some experiments regarding the duration of the risk assessment sessions, and the whole FMEA process. According to the studies made by Estorilio and Posso, the risk assessment process should be less than 90 min.

The longer evaluation time made the FMEA team follow emotions and feelings, and the shorter evaluation times had an impact on minimizing subjective and bias issues (Estorilio and Posso 2010). The FMEA process can be a tool used by all parties in a collaborative environment, but at the same time that inconsistency in the ranking of severity, occurrence, and detection may delay FMEA implementation in a supply chain. (Teng et al. 2006). The FMEA sequences are repeated from time to time for certain identified risks. In the shortened ready to market period requirements the FMEA seems to be too static. The traditional FMEA is not a really an efficient tool to work with during really dynamic conditions.

As presented above, the risk management practices are designed as iterative processes, where often it is supposed that there is plenty of time for a deep analysis. Under dynamic conditions, these techniques may underperform. At least three weaknesses of some risk assessment tools were presented. In the following sections, arguments for these weaknesses will be provided based on a survey in a real manufacturing context.

3. Research

The goal of our research is to study risk management techniques under rapidly changing environments in highly standardized industries. This qualitative phase of the research investigates the risk management techniques being focused on the role of human resources and to what extent a decentralized risk management is present in the studied organizations under rapidly changing environments.

By decentralized risk management, a risk management done through multidisciplinary teams (MDT) from inside the company is considered. The team members are experts, in our assumption, mostly from engineering, ICT (Information and Communications Technology), HR (Human Resources), PR (Public Relations) and legal. It was assumed that each member has competences to make decisions in their own expertise field, and is able to make compromises during the work in the multidisciplinary team.

The studied organizations were from two highly regulated and standardized industries: the automotive and pharmaceutical industry. Due to confidentiality agreements the names of the organizations cannot be provided. Additionally, it is prohibited to present here even some open information about them, for example turnover or profit, because through these data they might become distinguishable. Still, some descriptive statistical data are presented in Table 1 to give information about the type of companies and their risk management opportunities. The size of the company is important in analyzing risk management tools.

Table 1. Descriptive statistics of the studied companies.

		Average Values in 2020		
Industry	**Number of Firms**	**Turnover**	**Total Assets**	**Number of Employees**
Automotive	3	$38,450,000	$27,541,666	1748
Pharmaceutical	2	$7,737,500	$10,550,000	543

Source: National Agency of Fiscal Administration, Romania.

Our investigation was not focused on data about specific risks; the high level of confidentiality in both industries was already known from the previous experiences. Thus, the investigation was focused on the existing risk management methods, tools and processes, and not on particular risks. As a whole, the technical risks assessment was the main target, however in some interviews the answers included statements regarding other business-related risks, such as investments, cybersecurity, workplace safety, and stakeholder issues. A major concern was how risk assessment processes are conceived from a human resources point of view. Secondly, the scope of the investigations was focused on how the methods, tools and teams work under rapidly changing conditions.

All the studied organizations showed several documents regarding their risk assessment analysis methods. Each of them has ISO9001, ISO14000 and HACCP (Hazard

Analysis Critical Control Point) certification, and they developed some sort of company-specific risk management routine. Each of them has a PDCA cycle-based risk evaluation technique, some of them use FMEA to evaluate certain risks. These might help covering specific scenarios, especially for fire cases, accidents, product failures, natural disasters, and technological breakdowns.

During the research, semi-structured interviews were used as the mean of data collection. The interviewees were top level managers of five Romanian manufacturing companies. The companies are branches of large multinational organizations. In fact, this research is part of a larger, in-depth investigation started in 2017 and finished in 2019 (Bakos and Dumitrașcu 2017; Bakos et al. 2019), and at the same time is a pilot for a quantitative research which will to take place in September–December 2021. While the focus in our previous research was on how the companies are prepared for unexpected events, now there is a slight extension to include the study of the organization's risk assessment methodologies. Having the previous results, it was an obvious challenge to see if the lack of preparedness against unpredictable events is due to an inefficient risk evaluation technique. Twelve questions (presented in Appendix A) were prepared for the ten managers selected for our interview-based investigation. In the beginning of the interviews, a common vocabulary was framed on multidisciplinary decentralized teams, risk management, crisis communication and crisis management. Once the common language was set, the 60–70 min face-to-face survey started. Questions and the discussions associated to some hypothetical situations were discussed in the first part, followed by inquiries related to real contexts in the second part.

The first theme discussed during the interviews was the risk assessment methods they use. The managers had to explain briefly how the risk management in their organization is done: what kind of risk identification tools/methods are in use, who sets the procedures, who is in charge to make decisions. Additionally, there was a focus on the time issues: how often do they repeat their risk assessment? Do they change anything if there are rapidly changing conditions in their environments?

In order to see if there is a gap between theory and practice, a short list with advanced risk identification tools and techniques from the scientific literature was presented to the managers in order to see if they are familiar with them: Delphi groups, Force-Field Analysis, Variance/Earned Value Analysis, Risk Breakdown Structure, Affinity Diagrams, Monte Carlo Simulations, Route-Cause Analysis, Nominal Group Technic, Fuzzy Maps. Among others, (Ching and Colombo 2014) and (Thaheem and De Marco 2013) made such kinds of investigations searching for the convergence between theoretical practices and those adopted by the companies. Preparation activities for risk evaluation demands trust and special skills. Thus, investigation was made if the managers can choose their risk assessment team, or this matter is established by internal regulations. It was assumed that the team is predetermined and consists of leaders from certain departments, and the risk evaluation activity is done by a team designed by the branch manager. Still, further analysis was made on this latter version, when there is a room for choosing the crew.

Risk identification, by definition, is a more or less collective activity in which cross-functional, multidisciplinary experts share knowledge and work together. The first issue was if the risk assessment team is based on confidence or does only the professional expertise matter? What kind of experts are usually involved? Do they prefer a more multidisciplinary risk assessment team or, rather, do they use a homogenous staff with similar professional background? Additionally, it was presumed that confidence is a matter of decision in this selection. It was investigated if, beside the professional background, other characteristics such as communication skills, ICT competences or open-mindedness are considered during the selection. The number of team members was also the subject of our study. The study assumed that managers choose members with multiple skills and knowledge, in order to decrease the number of persons involved. It was investigated which professionals are engaged, how the knowledge transfer is done, is there a conciliation divergent professional goals, and to what extent these experts are involved to prepare the

system for unknown risks. Further details were asked about what kind of decision the team can make; do they proceed with any risk management activity without the approval of the executives?

Finally, the managers were asked to present some weaknesses they met during previous emergencies. The subject of inquiry was how the knowledge gain during risk management is maintained, how they learn from their previous mistakes, and how the industry, their consortium/holding or professional groups or other networks provide useful information and knowledge for a better risk management.

The conducted survey was interesting, challenging and provided useful and interesting data. Certainly, the number of interviews definitively will not lead to general valid conclusions. In fact, from the beginning this was not the scope of the research. Based on the findings, some proposals were made that hopefully may give some ideas for professionals and researchers for further improvements in their work related to risk assessment.

4. Results

As presented above, during the survey the focus was on the study of risk management actions in rapidly changing environments. During the discussions, the first remark was that there are several internal and legal rules, but there are no specific risk assessment techniques for the case when the environmental conditions are changing fast. The risk assessment techniques in all the studied organizations, according to the 10 interviewed managers, are based on some general purpose standards (ISO 9001, ISO14000) and some industry-specific standards, as well. The procedures are not set by the branch management, but there is a narrow margin in which they can change the rules. This might be due to new legal requirements or customer demands. The risk assessment teams are settled by the top management after previous discussions with quality management, HR and technical experts; the only competencies they have is to evaluate the possible risks and to propose risk mitigations for the identified risks. Risk identification is more or less collective activity in which cross-functional, multidisciplinary experts work together. At the branch level, the studied organizations do not use advanced risk identification tools (Delphi technique, force-field analysis, statistics, variance/earned value analysis), and usually do not build risk models by converting information into risk data. The risk assessment is mostly based on ISO31000 and ISO9001 recommendations, but it seems, contrary to ISO31000 recommendations, that the organizations just partially integrated the process for managing risk into the overall governance, values and culture. The risk evaluation is more a document-based activity (indicating a kind of "surface" compliance to the standards), and less a brainstorming-like creativity-based activity. This finding has some similarities with the deep and surface compliance issue in safety management presented in (Hu et al. 2020).

The PDCA cycle is a very common process analysis tool, most of the organizations use lean principles (especially the studied organizations from the automotive industry) and FMEA analysis.

The interviewed managers did not provide detailed data about the risk assessment teams, but it seems that each team is predetermined, according to internal rules. Neither the number of members, nor the professional background of them were exactly revealed by the interviewed top-managers. Thus, they were asked to select from a list of professions those that are involved in risk assessment activities in their firm. From Table 2, we can see that all managers admitted that there are multidisciplinary teams involved in this activity. All managers checked from the list the financial and technical experts and added at least one profession to our list. That is the reason why in column "other" the number is higher than the number of interviewed persons. The domains not listed in our original list, but mentioned by the managers, are related to technical fields. In spite of the fact that there is a "Tech" column, they intended to emphasize the importance of handling technical risks by inserting professionals from process control, process management, quality control, operations management, logistics, supply chain management, and information technology.

Table 2. The structure of the risk assessment teams.

Risk Assessment Crew Structure						
Fin	**Tech**	**PR**	**Sales**	**HR**	**Legal**	**Other**
10	10	5	7	7	8	18

Most of the managers itemized worries related to contradictory goals of certain team members during the risk assessment process. In their approach, a cross-functional, multi-disciplinary team means by definition conflicting interests, competition and difficulties in goal setting meetings, and fight. We selected some of their statements.

- "Engineers are only interested in showing me, that there are no design errors, the machine failure was due to a human error".
- "The staff members with technical background always see in risk management and risk evaluation a paperwork that must be accomplished due to requirements of the ISO9001—and many other similar—standards and regulations. At the same time, they protect their interest by requesting a huge amount of spare-parts, and they try to automatize everything".
- "I think, for them is more important *formally* to comply with safety rules, and less important if these will *really* work in difficult times"; "(...) they are mostly afraid about the occurrence of accidents, but they are not really interested on other issues".
- "My chief accountant is only interested about how to cut the costs. I never invite him to participate on risk and quality management meetings, it is counterproductive".
- "IT people and system engineers are one of the challenges I have to deal with during these meetings. They see the world though algorithms, and they have a "black or white" logic. They are not really creative in designing for example a crisis management plan; without well-defined inputs they are not able to foresee issues. If there is no way to compute or room to automatize a problem, they become quickly passive and bored. "The rest of us, usually have difficulties to understand their way of thinking".
- "I have only few people for PR activities, they are at the Sales Dept. They are interested to have strong relationship with the mass media, to have our website up-to-date and to post everything on our Facebook account. During crises, I think, they are definitively needed, but the relationship with the media is not our competence, experts from our parent company do this stuff".

Finally, we share the thoughts of a general manager for the local branch of a multi-national company. It presents in one sentence our conclusion regarding the possible self-centredness of some professionals: "When it comes to work together on future plans, engineers ask for new technologies/machines, HR experts for new people, and ICT experts . . . , well I don't really understand what they want. But for sure, the Board Members and the economists will definitively say: there is no money for that. It is incredibly difficult to satisfy all demands; it seems most of them speak only for themselves."

After the discussions, we are confident that each person involved in risk assessment at the studied organizations tries to do their best to contribute to identify all risks and to provide arguments for the best possible outcome at the occurrence of the risk. Still, this "best possible outcome" might look differently for the different team members. In order to share the same goals, the risk assessment team members should search for the *overall* best solution and not that solution which is optimal only from their professional side.

During the interviews, 10 out 10 managers, as a source of the weakness during a previous emergency, in the first place mentioned causes related to human resources such as the lack of experts or the unavailable staff:

- "at that moment he [head of the sales department] was not available",
- "the system engineer was afraid to call me at the week-end, when he finally did it, but it was a little bit too late",

- "we don't have, as a branch, a 7/24 full time lawyer available, we didn't know what to do".

Surprisingly to us, some important personal features, other than the professional skills of the co-workers (self-confidence, skill using ICT, communication skills in foreign languages, loyalty, trust), were not taken in account when selected for the risk management team. Almost solely, the position occupied in the organization represents the criteria to be part of the risk analysis team. While discussing the additional skills and special training of the persons involved in risk analysis, it seems there is confidence only in few persons (usually one to two persons) within each company that might have competences to make decisions regarding risk management issues. Even those persons have no competencies to override the previously developed protocols in order to mitigate a risk. All of them confirmed that risk assessment processes bring new tacit knowledge and the professional skills of each individual increase through practice. Each year brings more complex and better-suited assessment techniques, the managers admitted, while the risk management activity systematically improves their skills. When asked about the use of some advanced risk identification tools (for example Delphi groups, root-cause analysis, trend analysis, affinity diagram, force-field analysis, variance/earned value analysis), 7 out the 10 managers admitted that they have not even have heard about such tools. The results are presented in briefly in Table 3. The numbers in the table indicate the number of managers without the knowledge of a certain tool.

Table 3. Lack of knowledge of advanced techniques and tools in risk assessment.

Tools						
Delphi	**Force Field**	**Variance**	**Earned Value**	**Risk Breakdown**	**Affinity**	**Fuzzy**
4	2	7	7	7	5	2

These results present some similarities with the research made by Thaheem and De Marco. Their results show that most of their sample uses only simple methods for risk identification. According to them, 72% of respondents identify risks through "Documentation review", 64% through "Brainstorming", 64% of respondents use "Expert Judgment" and 48% through "Checklist Analysis" (Thaheem and De Marco 2013). On the other hand, the more complex techniques such as the Influence Diagrams, Delphi Technique and Ishikawa Diagram scored as the least (6%) used risk identification techniques. Techniques such as Expected Monetary Value, Modeling and Simulations, Sensitivity Analysis, and Probability Distributions on average are used by 30% of respondents. (Thaheem and De Marco 2013).

In most of the cases in our study, risk management only consists of a systematic application of enterprise policies. Expert judgment represents the most important source for risk data. The risk management plans are built on these data, additionally stakeholder information is converted into risk data. The piece of resistance of the risk management plans consists of the designated risk owners (units/persons with accountability and authority to manage the risk). Sometimes, as a proactive attitude, it is set when the risk exposure is re-evaluated. The answers provided during the interviews indicate that in these highly standardized industries, the risk assessment techniques are mostly centralized (coordinated by a single person/unit), linear (based on If-Then construct) and rigid, definitively not suitable when quick changes are in the organization environment. The used methods it seems are unfocused on time as a constraint.

During the interviews, each of the managers showed confidence in their organization and how their enterprise handles the risk. Many times during the interviews the idea of security provided by their organizational background can be sensed (most of them being part of a larger organization). The managers were positive that if they follow the rules nothing bad can happen, and they are protected. If still something goes wrong, the international PR and legal experts are strong enough to protect them. This overconfidence can be correlated with their risk taking abilities. Hilton et al. in their survey related to societal risks found

that the better-than-average effect, the positive illusion measures are correlated negatively with optimism concerning societal risks. (Hilton et al. 2011). More recently, Park et al. demonstrated that CEOs who have a high level of overconfidence have fewer CSR activities (Park et al. 2020). Less CSR activity (Corporate Social Responibility) mostly means less concern about public image, less perceived stakeholder pressure, and finally less concern about external risks. On the other hand, in the case of large organizations as (Razali and Tahir 2011; Kerraous 2020) demonstrated, the larger firms are more likely to engage in ERM than smaller firms due to the pressure from institutional owners (institutional ownership). Our survey identified this seeming contradiction/duality as well. In one side there was an overconfidence ("we are big and protected") and on the other side there was a lack of confidence ("I have to be cautious, everybody is against us"). These two very opposite, but often coinciding behaviors can be explained by the corporate mentality. If a manager follows the regulations there is nothing to be afraid of; the manager can feel safe and can be confident. Whenever there are chances that a situation may get out of control/rules and also the personal responsibility is at stake, then the highest mindfulness is present. A previous, very detailed, research at the same organizations showed that there is a lack of preparedness to unpredictable events at these organizations. At that time, a sample of 156 valid questionnaires, beside the interviews made, led us to the conclusion that these enterprises when faced with unforeseen situation are not able to "think out of the box"; they are extremely rigid (Bakos et al. 2019). Based on the conducted interviews during the present research, it seems that the lack of preparedness for unpredictable events is also to due to inefficient risk evaluation techniques when there are rapidly changing environments. This statement should be proved in our next survey; it will be one of the hypotheses of the quantitative research that is about to start in few months at the same organizations.

5. Conclusions

The article presented the results of an interview-based survey with top executives from highly standardized industries. The quality of the interviewees might compensate for the relatively low number of interviews, the added value for the scientific community and practitioners might come from the fact that the interviews provided insights of the studied industries (automotive and pharmaceutical). Being highly regulated organizations, the presented procedures are similar at a global level and can be seen as good practices from top industries.

The research targeted a topic situated on the borderline of multiple scientific fields. Both the presentation of the scientific literature and the survey might show novelties and/or raise questions for different researchers and practitioners from many fields, due to this multidisciplinary approach. The article calls for a less hierarchical, decentralized and holistic approach of risk management at company level. We call attention to some weaknesses of certain risk assessment techniques under rapidly changing environments: centralized approach, linear thinking, unfocused on time as a constraint. In the new era of decentralization, innovation, adaptability and resilience are the new metrics for success. Each person involved in risk assessment should contribute to the identification of risks, and provide arguments for the best outcome in the case of occurrence. At the same time, each team member must be aware that the global optimum might look different from a certain professional point of view.

According to our findings, the risk evaluation is more a document-based activity (indicating a kind of "surface" compliance to the standards), and less a brainstorming-like creativity-based activity. There is mostly a systematic application of enterprise policies, in many cases expert judgment is the single source for risk data. Risk assessment and mitigation techniques should go beyond the rigid "cause-and-effect"- or "if-and-then"-based approach. Risk management should not be characterized just by linear thinking, a conscious and rational way to create knowledge, but also a way of thinking differently, unconventionally. People involved in risk treatment may be aware that they can create new risks or modify existing risks.

The preparedness for the future challenges depends on the efficiency of the organization's risk assessment techniques. The speed at which things in our environments change is fuelled by digital technology, power of networks (of any type) and increasing information processing power. Time became a key parameter in most of the processes. Enterprise risk management theory and practice should keep pace with these changes through new, more adaptive approaches. The answers provided during the interviews indicate that risk assessment techniques are mostly centralized (coordinated by a single person/unit), linear (based on If-Then construct or cemented by previously defined steps) and rigid, definitively not suitable when quick changes are in the organization environment. The used methods it seems do not consider time as a constraint; the risk management practices are designed as iterative processes, where it is supposed that there is plenty of time for a deep analysis.

The number of interviews definitively do not let us to draw general valid conclusions for how risk assessment is done in the studied highly regulated industries. Still, the findings and proposals made during the article hopefully may give some ideas for professionals and researchers for further improvements of their work related to risk assessment.

Author Contributions: Conceptualization, L.B. and D.D.D.; methodology, D.D.D.; formal analysis, D.D.D.; investigation, L.B.; resources, L.B.; data curation, L.B.; writing—original draft preparation, L.B.; writing—review and editing, L.B.; funding acquisition, D.D.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Appendix A

Prepared questions during the semi-conducted interview.
Section A. Questions to explore the intentions/beliefs.

1. Please indicate, from the proposed list, what kind of professionals you may consider to identify threats to your organization (risk evaluation and assessment)?
2. Please indicate, from the proposed list, what kind of professionals you consider it would be advisable to take part in a crisis management team in the case of a hypothetical crisis?
3. What kind of risk assessment methods/tools do your organization use? Do you update these procedures/have special procedures for sudden changes in the internal/external environment?
4. Do you consider skills other than the strictly professional ones, when selecting the team members for risk assessment activities?
5. Can you identify from the following list any risk assessment tool you hear about? (Delphi group technique, Force Field Analysis, Variance Analysis, Earned Value Analysis, Risk Breakdown Structure, Affinity Diagrams, Fuzzy Cognitive Maps/Preference Program). If yes, is any from the list part of the usual risk assessment activities in your organization?
6. During a hypothetical crisis what kind of decisions the team take without the CEO's approval? Section B. Questions to investigate real contexts.
7. Do you remember crisis situations you had to face and with whom you handled it?
8. What kind of risk assessment tools is regularly used within the organization (please indicate also other methods than those required by quality management standards)?
9. Have you experienced any difficulties working with multidisciplinary crews?
10. Do you have a comprehensive risk register with all kind of risks?
11. How the knowledge transfer within the risk assessment team is done (meetings, reports, shared-files . . .)?

12. Can you recall some success stories in the history of your organization, when difficult cases were solved? What were the key factors?

References

Andersen, Torben. 2010. Combining central planning and decentralization to enhance effective risk management outcomes. *Risk Management* 12: 101–15. [CrossRef]

Anton, Sorin Gabriel, and Anca Elena Afloarei Nucu. 2020. Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management* 13: 281. [CrossRef]

Bakos, Levente, and Dan Dumitrașcu. 2017. Holonic Crisis Handling Model for Corporate Sustainability. *Sustainability* 9: 2266. [CrossRef]

Bakos, Levente, Dănuț Dumitru Dumitrașcu, and Katalin Harangus. 2019. Human Factor Preparedness for Decentralized Crisis Management and Communication in Cyber-Physical Systems. *Sustainability* 11: 6676. [CrossRef]

Barends, Dirk M., Margryt Teatske Oldenhof, Marjo J. Vredenbregt, and Maarten J. Nauta. 2012. Risk analysis of analytical validations by probabilistic modification of FMEA. *Journal of Pharmaceutical and Biomedical Analysis* 64–65: 82–86. [CrossRef] [PubMed]

Baxter, Ryan, Jean C. Bedard, Rani Hoitash, and Ari Yezegel. 2013. Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. *Contemporary Accounting Research* 30: 1264–95. [CrossRef]

Baykasoğlu, Adil, and İlker Gölcük. 2017. Development of a two-phase structural model for evaluating ERP critical success factors along with a case study. *Computers & Industrial Engineering* 106: 256–74. [CrossRef]

Beasley, Mark S., Richard Clune, and Dana R. Hermanson. 2005. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy* 24: 521–31. [CrossRef]

Blanco-Mesa, Fabio, Julieth Rivera-Rubiano, Xiomara Patino-Hernandez, and Maribel Martinez-Montana. 2019. The importance of enterprise risk management in large companies in Colombia. *Technological and Economic Development of Economy* 25: 600–33. [CrossRef]

Bouti, Abdelkader, and Daoud Ait Kadi. 1994. A state-of-the-art review of FMEA/FMECA. *International Journal of Reliability, Quality and Safety Engineering* 1: 515–43.

Bromiley, Philip, Michael McShane, Anil Nair, and Elzotbek Rustambekov. 2015. Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning* 48: 265–76. [CrossRef]

Ching, Hong Yuh, and Thalita Maricone Colombo. 2014. Enterprise Risk Management Good Practices and Proposal of Conceptual Framework. *Journal of Management Research* 6: 69. [CrossRef]

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. Enterprise Risk Management: Integrated Framework. Available online: www.coso.org (accessed on 31 August 2021).

Committee of Sponsoring Organizations of the Treadway Commission, (COSO). 2017. Enterprise Risk Management: Integrating with Strategy and Performance. Available online: www.coso.org (accessed on 31 August 2021).

Crowther, Kenneth G. 2008. Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input–output model. *International Journal of Critical Infrastructure Protection* 1: 53–67. [CrossRef]

Daud, Wan Norhayate Wan Daud, Ahmad Shukri Yazid, and Mohd Rasid Hussin. 2010. The effect of chief risk officer (CRO) on enterprise risk management (ERM) practices: Evidence from Malaysia. *The International Business & Economics Research Journal* 9: 55–64. [CrossRef]

Deloitte. 2016. Available online: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-tpr-decentralisation.pdf (accessed on 31 August 2021).

Deming, Walter Edwards. 1986. *Out of the Crisis*. Cambridge: Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Estorilio, Carla, and Richard K. Posso. 2010. The reduction of irregularities in the use of "process FMEA". *International Journal of Quality & Reliability Management* 27: 721–33. [CrossRef]

Fraser, John RS, Betty Simkins, and Kristina Narvaez. 2015. *Implementing Enterprise Risk Management. Case Studies and Best Practices*. Hoboken: Wiley.

Gates, Stephen. 2006. Incorporating Strategic Risk into Enterprise Risk Management: A Survey of Current Corporate Practice. *Journal of Applied Corporate Finance* 18: 81–90. [CrossRef]

Gordon, Lawrence A., Martin P. Loeb, and Chih-Yang Tseng. 2009. Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy* 28: 301–27. [CrossRef]

Gupta, Praveen. 2006. Beyond PDCA—A new process management model. *Quality Progress* 39: 45–52.

Hamel, Gary. 2011. First, let's fire all the managers. *Harvard Business Review* 89: 48–60.

Hermansson, Helena. 2019. Challenges to Decentralization of Disaster Management in Turkey: The Role of Political-Administrative Context. *International Journal of Public Administration* 42: 417–31. [CrossRef]

Hilton, Denis, Isabelle Régner, Laure Cabantous, Laetitia Charalambides, and Stéphane Vautier. 2011. Do positive illusions predict overconfidence in judgment? A test using interval production and probability evaluation measures of miscalibration. *Journal of Behavioral Decision Making* 24: 117–39. [CrossRef]

Hippel, Jack. 2006. Predictive Failure Analysis: How to use the TRIZ in Reverse. Available online: www.triz-journal.com/archives/2006/09/06.pdf (accessed on 31 August 2021).

Hu, Bowen, Chunjie Zhou, Yu-Chu Tian, Xiaoya Hu, and Xinjue Junping. 2021. Decentralized Consensus Decision-Making for Cybersecurity Protection in Multimicrogrid Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 51: 2187–98. [CrossRef]

Hu, Xiaowen, Gillian Yeo, and Mark Griffin. 2020. More to safety compliance than meets the eye: Differentiating deep compliance from surface compliance. *Safety Science* 130: 104852. [CrossRef]

Isniah, Sarah, Humiras Hardi Purba, and Fransisca Debora. 2020. Plan do check action (PDCA) method: Literature review and research issues. *Jurnal Sistem dan Manajemen Industri* 4: 72–81. [CrossRef]

Jarjoui, Samir, and Renita Murimi. 2021. A Framework for Enterprise Cybersecurity Risk Management. In *Advances in Cybersecurity Management*. Edited by Kevin Daimi and Cathryn Peoples. Cham: Springer. [CrossRef]

Kerraous, El Mehdi. 2020. Literature review of the factors that influence the adoption of an Enterprise Risk Management's process. *Revue Internationale des Sciences de Gestion* 3: 774–98.

KPMG. 2018. Available online: https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2018/disruption-is-the-new-norm-emerging-teck-risk.pdf (accessed on 31 August 2021).

Kulcsár, Edina, Tamás Csiszér, and János Abonyi. 2020. Pairwise comparison based failure mode and effects analysis (FMEA). *MethodsX* 7: 101007. [CrossRef]

Kumar, Sonjai. 2021. Risk Management and Enterprise Risk Management. *Academia Letters*, 2234. [CrossRef]

Lackovic, Ivana Dvorski. 2017. Enterprise Risk Management: A Literature Survey. Paper presented at 26th International Scientific Conference on Economic and Social Development, Building Resilient Society, Zagreb, Croatia, December 8–9; p. 364.

Laloux, Fréderick. 2014. *Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage in Human Consciousness*. Brussels: Nelson Parker.

Lee, Michael Y., and Amy C. Edmondson. 2017. Self-managing organizations: Exploring the limits of less-hierarchical organizing. *Research in Organizational Behavior* 37: 35–58. [CrossRef]

McDermott, Robin E., Raymond J. Mikulak, and Michael R. Beauregard. 2008. *The Basics of FMEA*, 2nd ed. Boca Raton: Productivity Press, 91p, ISBN 9781563273773.

McKinsey. 2018. Available online: www.mckinsey.com/~{}/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/a%20time%20for%20boards%20to%20act/a-time-for-boards-to-act.pdf?shouldIndex=false (accessed on 31 August 2021).

Mensah, Godson K., and Werner D. Gottwald. 2016. Enterprise Risk Management: Factors Associated with Effective Implementation. *Risk Governance & Control: Financial Markets & Institutions* 6: 3745481.

Moen, Ronald, and Norman Clifford. 2009. *Evolution of the PDCA Cycle*. Available online: https://rauterberg.employee.id.tue.nl/lecturenotes/DG000%20DRP-R/references/Moen-Norman-2009.pdf (accessed on 31 August 2021).

Müller-Schloer, Christian, and Sven Tomforde. 2017. *Organic Computing— Technical Systems for Survival in the Real World*. Birkhauser: Springer International Publishing AG.

Murphy, Martina, George Heaney, and Srinath Perera. 2011. A methodology for evaluating construction innovation constraints through project stakeholder competencies and FMEA. *Construction Innovation: Information, Process, Management* 11: 416–40. [CrossRef]

Mzougui, Ilyas, and Zoubir El Felsoufi. 2019. Proposition of a modified FMEA to improve reliability of product. *Procedia CIRP* 84: 1003–9. [CrossRef]

Najwa, Nina Fadilah, and Apol Pribadi Subriadi. 2018. A need to modify the method of failure mode and effect analysis (FMEA) and risk management. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3: 143–58.

Oldenhof, Margryt Teatske, Janneke van Leeuwen, Maaryten J. Nauta, Dries de Kaste, Yvonne Odekerken-Rombouts, Marjo J. Vredenbregt, Marjolein Weda, and Dirk Barends. 2011. Consistency of FMEA used in the validation of analytical procedures. *Journal of Pharmaceutical and Biomedical Analysis* 54: 592–95. [CrossRef] [PubMed]

Osterman, Mark, Thomas G. Reio Jr., and Mandayam Thirunarayanan. 2013. Digital literacy: A demand for nonlinear thinking styles. In *Proceedings of the 12th Annual South Florida Education Research Conference*. Edited by Maria S. Plakhotnik and Sidsel Marie Nielsen. Miami: Florida International University, pp. 149–54.

Paape, Leen, and Roland F. Speklé. 2012. The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review* 23: 1–32. [CrossRef]

Park, Kyung-Hee, Jinho Byun, and Paul M. S. Choi. 2020. Managerial Overconfidence, Corporate Social Responsibility Activities, and Financial Constraints. *Sustainability* 12: 61. [CrossRef]

Qin, Jian, Ying Liu, and Roger Grosvenor. 2016. Categorical Framework of Manufacturing for Industry 4.0 and Beyond. *Procedia CIRP* 52: 173–78. [CrossRef]

Razali, Ahmad Rizal, Ahmad Shukri Yazid, and Izah Mohd Tahir. 2011. The determinants of enterprise risk management (ERM) practices in Malaysian public listed companies. *Journal of Social and Development Sciences* 1: 202–7. [CrossRef]

Razali, Ahmad Rizal, and Izah Mohd Tahir. 2011. Review of the Literature on Enterprise Risk Management. *Business Management Dynamics* 1: 8–16.

Rihani, Samir. 2002. *Complex Systems Theory and Development Practice: Understanding Non-Linear Realities*. London and New York: Zed Books.

Robertson, Bryan. 2015. *Holacracy: The New Management System for a Rapidly Changing World*. New York: Henry Holt LLC, p. 15.

Sharma, Rajiv Kumar, and Pooja Sharma. 2010. System failure behavior and maintenance decision making using, RCA, FMEA and FM. *Journal of Quality in Maintenance Engineering* 16: 64–88. [CrossRef]

Shewhart, Walter Andrew. 1986. *Statistical Method from the Viewpoint of Quality Control*. Dover: Department of Agriculture, p. 45. First published 1939.

Sobel, Paul J., and Kurt F. Reding. 2012. *Enterprise Risk Management: Achieving and Sustaining Success*. Lake Mary: Institute of Internal Auditors Research Foundation (IIARF).

Stamatis, D. 1996. FMEA and the QS-9000 Requirement. *SAE Transactions* 105: 61–73. Available online: http://www.jstor.org/stable/44725488 (accessed on 28 July 2021).

Subriadi, Apol Pribadi, and Nina Fadilah Najwa. 2020. The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon* 6: e03161. [CrossRef] [PubMed]

Subriadi, Apol Pribadi, Nina Fadilah Najwa, Brigitta Devianti Cahyabuana, and Valeriana Lukitosari. 2018. The Consistency of Using Failure Mode Effect Analysis (FMEA) on Risk Assessment of Information Technology. Paper presented at 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, November 21–22; pp. 61–66. [CrossRef]

Teng, S. Gary, S. Michael Ho, Debra Shumar, and Paul C. Liu. 2006. Implementing FMEA in a collaborative supply chain environment. *International Journal of Quality & Reliability Management* 23: 179–96. [CrossRef]

Thaheem, Muhammad Jamaluddin, and Alberto De Marco. 2013. Survey on Usage and Diffusion of Project Risk Management Techniques and Software Tools in the Construction Industry. *World Academy of Science, Engineering and Technology, Stampa* 78: 1383–90.

Thurnes, Christian M., Frank Zeihsel, Svetlana Visnepolschi, and Frank Hallfell. 2015. Using TRIZ to invent failures–concept and application to go beyond traditional FMEA. *Procedia Engineering* 131: 426–50. [CrossRef]

United Nations Development Program (UNDP). 2015. Strengthening Disaster Risk Governance. Available online: http://www.undp.org/content/dam/undp/library/crisis%20prevention/disaster/Strengthening%20Disaster%20Risk%20Governance-Full-Report.pdf (accessed on 31 August 2021).

Vance, Charles M., Kevin S. Groves, Yongsun Paik, and Herb Kindler. 2007. Linear-nonlinear thinking style balance for improved management education and development. *Journal of Management Education* 31: 1–25. [CrossRef]

Wang Shiyong, Jiafu Wan, Daqiang Zhang, Di Li, and Chunhua Zhang. 2016. Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination. *Computer Networks* 101: 158–68. [CrossRef]

Waweru, Nelson, and Eric Simiyu Kisaka. 2013. The effect of enterprise risk management implementation on the value of companies listed in the Nairobi Stock Exchange. *Journal of Applied Finance & Banking* 3: 81–105.

Wu, Desheng, David L. Olson, and Alexandre Dolgui. 2015. Decision making in enterprise risk management: A review and introduction to special issue. *Omega* 57, Pt A: 1–4. [CrossRef]

Wu, Zhongyi, Weidong Liu, and Wenbin Nie. 2021. Literature review and prospect of the development and application of FMEA in manufacturing industry. *International Journal Advanced Manufacturing Technologies* 112: 1409–36. [CrossRef]