ASPECTS OF THE EVOLUTION FROM RISK MANAGEMENT TO ENTERPRISE GLOBAL RISK MANAGEMENT

Ivan Popchev[1], Irina Radeva[1*] and Irena Nikolova[2]

[1] *Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Acad. Georgy Bonchev St., Bl. 2, 1113 Sofia, e-mails: ipopchev@iit.bas.bg; iradeva@iit.bas.bg*

[2] *New Bulgarian University, Department of Economics, 21, Montevideo St., 1618 Sofia, e-mail: inikolova@nbu.bg*

Abstract. Industry 4.0 transforms the economy through "destructive" technologies and new risks. It is requiring update of the views and the dealing with uncertain environment. The goal of this paper is to summarize the mainly used risk management standards, to analyze the general aspects of evolution of risk management, enterprise risk management, enterprise integrated risk management and to suggest the concept for the next step which is enterprise global risk management, where are implemented Industry 4.0 risk and Artificial Intelligence. The proposed concept considers organizational-hierarchical structure of the enterprise as complex, the risk management policy as global, the respective actions as permanent and the orientation toward risks as adaptive. It is determent the future development in connection with enterprise resource planning.

Keywords: risk standards, Risk Management, Enterprise Risk Management, Enterprise Integrated Risk Management, Enterprise Global Risk Management, Industry 4.0, Artificial Intelligence, Enterprise Resource Planning.

1. INTRODUCTION

Industry 4.0 is transforming the global economy through the "destructive" technologies and new risks during the process of expansion of human activities from the traditional physical ecosystem to the cyber-physical and digital

* Corresponding author.

DOI: 10.7546/EngSci.LVIII.21.01.02

ecosystems. The world is already global. This requires a rapid adaptation of risk management approaches and practices, which is vital for functionality, viability, survival and protection of all economic, social and political levels. The "disruptive" technologies risks are associated with privacy and data security, changes in labor market, social and professional fragmentation, responsibility and accountability, ecology, ethics and est. issues [1].

In [2] K. Schwab has described the challenges and opportunities that the Fourth Industrial Revolution introduces. It was expected that a next generation of information and communication technologies will guarantee that the technologies would be used for the universal improvement of the quality of life [3]. Nevertheless, the pandemic circumstances in 2020 have worsened the macroeconomic indicators and this most probably would lead to a slow economic recovery worldwide [4, 5]. The later views and ideas, shared by Schwab and Malleret in [6] about "the future landscape" emphases on the inevitable globality that depends on macroeconomic, societal, geopolitical, environmental and technological factors, affects micro terms, on specific industries and companies and finally will reach and change the individual level. The additional challenges of Industry 4.0 are the education and the e-learning environment [7, 8].

The advancement of technology requires update of views, focus and attention to various exposures to risks and methods for risk management. Their analysis shows an evolution that starts from the Risk Management (RM), through the Enterprise Risk Management (ERM) and the Enterprise Integrated Risk Management (EIRM). RM considers only the individual risks: credit, business, financial, systemic, etc. as individual, and independent ones, and it is aimed at managing each risk separately. In the ERM, the risks are considered within the individual structural and functional departments, according to circumstances. The integration of all risks into a single enterprise management system determines the EIRM where the risks of the external environment, such as financial crises, natural disasters, risk of epidemics, earthquakes and etc., are already part of it [5]. It is evident now that exists a need for revision and the next EIRM step forward in order to include the risks of Industry 4.0. This step forward in the paper is considered to be a concept of Enterprise Global Risk Management (EGRM).

The goal of this paper is to present the guidelines and the role of the most significant and used risk management standards, to analyze the general aspects of evolution of risk management, enterprise risk management and enterprise integrated risk management and to suggest a possible extension of enterprise integrated risk management to the concept of enterprise global risk

management, where the accent is to Industry 4.0 risk and implementation of the Artificial Intelligence (AI) in cyber-physical systems.

2. RISK AND RISK MANAGEMENT STANDARDS

The regulations are the cornerstone for the risk management and a number of standards are adopted and are applicable in different fields worldwide. Moreover, they assist the enterprises in introducing their own internal rules and guidelines.

The risk standards are the ground for managers and for practitioners, and they are implemented and integrated in the internal documents and strategies in enterprises in both the financial and non-financial sector. In most cases the standards are recommendable for certain business areas and they play a significant part in the functioning of organizations, their certification, and activities. Table 1 presents the most used standards for risk and risk management.

Table 1

Terms	Standards
Definition for risk: general	ISO 31000:2018 Risk management – Guidelines ISO/ Guide 73:2009 Risk management – Vocabulary
Definition and description for risk management: general	ISO 31000:2018 Risk management – Guidelines ISO/ Guide 73:2009 Risk management – Vocabulary ISO/TR 31004:2013 on Risk management – Guidance for the implementation of ISO 31000 ISO 31010:2009 on Risk management – Risk assessment techniques FERMA Risk Management Standard Australia and New Zealand: AS/NZS 4360:2004 Risk Management and the new standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
Specific definitions and description of risk and risk management	USA: NIST SP 800-37 Risk Management Framework for Information Systems and Organizations USA: NIST SP 800-100 Information Security Handbook: A Guide for Managers USA: NIST SP 800-30 Guide for Conducting Risk Assessments

The most applicable and recognizable standards are those of the International Organization for Standardization (ISO). In ISO 31000:2018 Risk management – Guidelines [10] and ISO/Guide 73:2009 Risk management – Vocabulary, Risk is formulated as:

a. effect of uncertainty on objectives, and
b. additional clarifications: as an effect of deviation from the expected – positive and/or negative; as different objectives and goals (financial, health and safety, and environmental) and applied to different levels (strategic, organization-wide, project, product and process); as reference to potential events, consequences, or a combination; as combination of the consequences of an event (including changes in circumstances) or likelihood of occurrence; as uncertainty, deficiency of information in understanding or knowledge about events, consequences, or likelihood [1, 4].

The definitions formulated by ISO are commonly applied in theory and practice. They are explaining the nature of risk and in comparison to the ones presented in the dictionaries, there is not any accent on the negativity or threat, but instead the focus is on the opportunity and the potential events. The ISO standards review and formulate the general definition of risk which is applicable in all fields of science and practice. Identifying risk is one of the key elements but the higher priority is attributed to the management of potential events and consequences in order to ensure the secure future functioning of the enterprises.

Risk management implies a special culture of "communication" with the risk which is included in the definition of ISO/IEC Guide 73: "The culture of the organization is reflected in its risk management system". It is based on the factors which preserve the generation, protection and increase of the worth and the values of the organization in the transition from real to digital management environment.

The management of the risk is regarded as a process. The standard ISO 31000:2018 Risk management – Guidelines [10] consists of general steps for constant communication, consultation, monitoring, reporting, and recording. The risk management guidelines and "communication" with risk are presented in Fig. 1.

Of course, that is the general understanding for the management process and in specific areas it is adapted in regard to the internal and external environment of the organization. In cyber systems [3] and in e-learning in emerging technologies [1] the risk management process is described as: risk identification; quantitative and qualitative assessment of risk; selection of a tool and/or instruments for risk impact (standards, norms, rules, models, methods, algorithms); risk management, impact on the environment or the object; monitoring, control, and evaluation.

Furthermore, all the ISO standards are concentrated on the risk management process. For example, in ISO/TR 31004:2013 on Risk management –

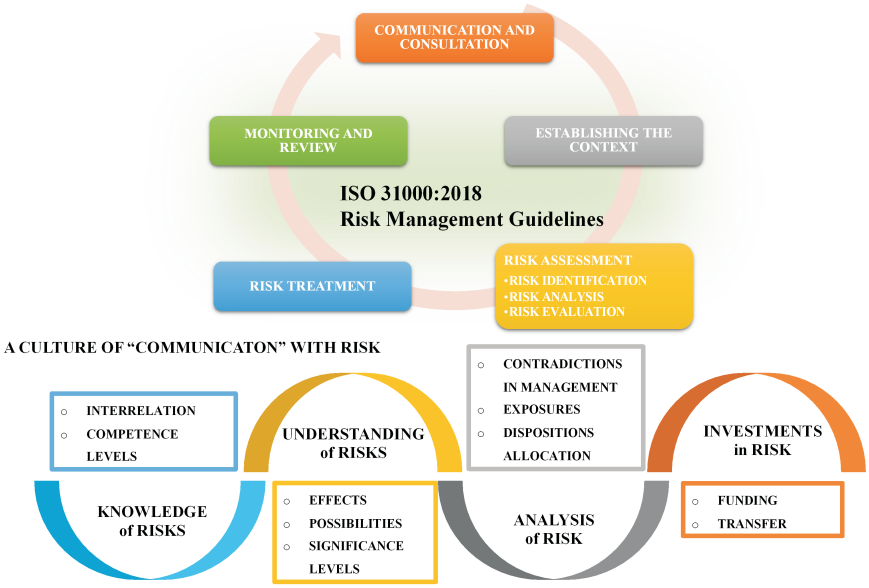

Fig. 1. Culture of Communication with Risk

Guidance for the implementation of ISO 31000 and in ISO 31010:2009 on Risk management – Risk assessment techniques [10], there are explained the management process details and are given recommendations.

Another standard that presents the general understanding of the risk management as a process is the Risk Management Standard of the Federation of the European Risk Management Associations (FERMA) [11]. In general, it is based on the ISO/ Guide 73:2009 Risk management – Vocabulary.

In various countries the standards are adopted either in the way the International Organization for Standardization has formulated them, or they are modified in accordance with the national legislation, rules, and practice. For instance, in the USA the National Institute of Standards and Technology to the U.S. Department of Commerce (NIST) prepares the standards in the field of the risk management for specific purposes. The NIST SP 800-37 Risk Management Framework for Information Systems and Organizations presents the risk framework in several a certain sequence as well as NIST SP 800-100 Information Security Handbook: A Guide for Managers and NIST SP 800-30 [12]. The general and different steps recommended in the listed standards can be traced in Fig. 2.

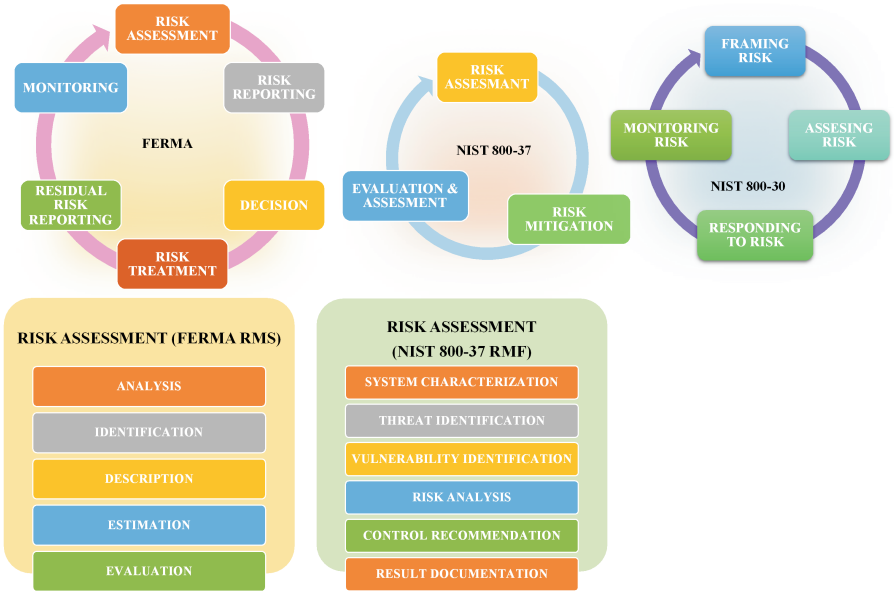

Fig. 2. Risk Management procedures comparison

All risk management processes in information and communication technologies of the enterprises are formulated in steps and recommendations. Nevertheless, each organization may transform them in accordance with their particular needs and goals.

The list of risk management standards is long and constantly growing. One example might be the standards presenting the general framework for risk management is Australia and New Zealand. Both countries have united in that field and have a joint risk management framework. The standard describes the process based on the ISO standard on risk assessment 31000. It is AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines [13] and it relies on the steps in the ISO standard. The previous standard was AS/NZS 4360:2004 Risk Management and was particularly developed for Australia and New Zealand.

The ISO standards completely present the risk not only as a threat or a weakness in the organization, but as its opportunity and strength. In that way the risk management is prescribed as a process of acting on opportunities of possible future events.

The risk management process in general and in a specific field is similar and follows certain logic and steps. There are specifics in terminology concern-

ing information technologies and understanding of definitions, but the overall dynamic of the risk process is similarly structured and synchronized.

3. ENTERPRISE RISK MANAGEMENT POLICY

As it was shown in the introduction, risk management goes through several stages of evolution. The ERM Framework was introduced by the Committee on Sponsoring Organizations of the Treadway Commission (COSO) in 1992. It aimed to evaluate the internal control in the organizations. It was accepted as an informal standard in the field of control and monitoring of the strategy and objectives of the organizations. The framework included the risk assessment and the management of change.

The ERM Framework from 2017 is a risk management, where the ongoing process is considered as an integrated approach. That extends the understanding of the risk management by integration of external environment, updates the concept of risk management and suggests five components, Fig. 3:

- governance and culture (leadership, operating structures, attracting and developing the right individuals);
- strategy and objective setting (strategic planning, internal and external factors for risk for the organization, defining risk appetite);
- performance (identification and assessment of risk and how to prioritize and respond to risks);
- review and revision (assessment of all the implemented changes) and information communication and reporting (sharing information within the company and reporting on risk, culture and performance in the enterprise).

The EIRM is set as ongoing process that affects all activities within the en-

Fig. 3. ERM Framework 2017 by COSO [14]

terprises, considers various external and internal environment risks, emphasis on the organizational and individual culture and focuses on the strategic development as well. The regulations for risk and risk management are regarded as a framework which is affected by the changes, including technological. EIRM is a system, operating in the enterprise and it is part of the managerial process as well.

4. ENTERPRISE GLOBAL RISK MANAGEMENT

The Industry 4.0 has defined the structure of economic relations at the global level. It unambiguously defines the need of revision of the risk management paradigm. The extension of the EIRM can be found in the inclusion of Industry 4.0 risk. Here, based on an analysis of the main differences between ERM and EIRM it is proposed that extension of the framework to be an EGRM.

The concept that translates EIRM to the conceptual framework of EGRM assumes that: EGRM = EIRM + Industry 4.0 Risks.

The frameworks are presented in Fig. 4. The evolution can be seen through four generally defined criteria: level of implementation in enterprise hierarchy, risk management policy, actions and orientation toward risks. The criteria shown are not exhaustive, but the aim is to show where the logical and fundamental difference in these approaches is.

Concerning the enterprise level of hierarchy, the evolution follows from departmental level (decentralized within the enterprise), through centralized at the top management level and it is possible to develop to a complex decentralized external level of the enterprise. This would allow the use of unemployed risk diversification.

Risk management policy has evolved through fragmented, integrated to global policy. This shows that the development should exceed the enterprise environment from physical–digital–physical to digital–physical–digital dimensions.

The development of "actions" is from ad hoc, through continuous to permanent. Industry 4.0 means the technologies that grant access to practically unlimited in volume and speed computing and analytical resources, decision-making instruments and exchanging information networks. This allows a quick, pointed, coordinated and shared response to risks. The main problem is that the risk exposure increases accordingly.

The orientation toward risks evolves from narrow, broad to adaptive. Currently all participants in the economy worldwide are dealing with "traditional"

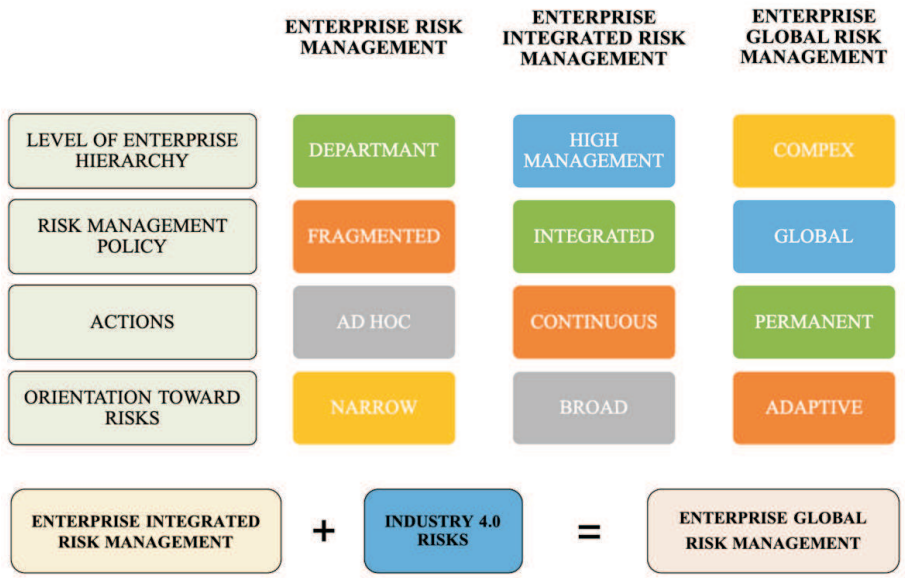

Fig. 4. Aspects of the evolution from Risk Management

risk and now with an expanding number of digital risks. It is recommended the application of decision-making model and procedures for selection of the "disruptive" technologies regarding technologies risk exposures. An approach to such task is proposed in [15]. It could also assume the risk ranking and prioritization, because the list of risks concerning Industry 4.0 increases significantly. Here are presented identified risk exposure groups and dialed decryption of what threats they include [9]:

- Privacy and data security: privacy/potential surveillance, online bullying/stalking, decreased data security, hacking, security threat, cyberattacks, crime, vulnerability to cyberattacks, cyber risk, opportunity for short-term abuse of trust, identity theft.
- Change in labor market: job losses, resilience after a job loss, contract/task-based labor (versus typically more stable long-term employment), global and regional supply and logistics chain: lower demand resulting in job losses, job automation, 24-hour services.
- Mental distraction: accidents, trauma from negative immersive experiences, increased addiction and escapism, increased distractions, escapism and/or addiction.
- Manipulation and echo camera: risk to be triggered by disseminating inaccurate information, lack of transparency where individuals are not privy

to information algorithms (for news/information), complexity and loss of control, trust, "falling foul of the algorithm", becoming incomprehensible, increased manipulation and echo chambers.
- Fragmentation: political fragmentation, groupthink within interest groups and increased polarization, increased inequality, lobbying against automation (people not allowed to drive on freeways), legal structures for driving, battles over algorithms, walled gardens (i.e. limited environments, for authenticated users only), forbidden full access in some regions/countries.
- Responsibility and accountability: formulas for specifying accountability (who owns the algorithm?), liability and accountability, governance, accountability (who is responsible, fiduciary rights), change to legal, financial disclosure, risk, decreased ability to measure this potentially grey economy.
- Ecology, ecosystems and ethics: comprehensive impact and provoke risks associated with growth in waste for disposal, and further burden on the environment, impact on agriculture from printing food, perverted disincentives for health: "If everything can be replaced, why live in a healthy way?", existential threat to humanity, gun control: opening opportunities for printing objects with high levels of abuse, brand and product quality, major disruption of production controls, consumer regulations, trade barriers, patents, taxes and other government restrictions and, the struggle to adapt, ethical debates stemming from the printing of body parts and bodies: Who will control the ability to produce them? Who will ensure the quality of the resulting organs? Uncontrolled or unregulated production of body parts, medical equipment or food, production of parts in the layer process that are anisotropic, i.e. Their strength is not the same in all directions, which could limit the functionality of parts, risk of collapse (total black out) if the (energy) system fails.
- Change in income/cost structure and ownership of assets: effects on the whole economic and social system and redistribution mechanisms associated with the risk of primacy of intellectual property as a source of value in productivity, less investment capital available in the system, decreased revenue from traffic infringements, permanent insurance and roadside assistance ("pay more to drive yourself"), elimination of car ownership.

The EGRM framework suggests several assumptions and recommendations:
- risk management procedures based on a complex vision of organizational-hierarchical structure of the enterprise and product chain participants. This structure is considered to be flexible and adaptive to variable external participants;
- essential enterprise predisposition to partial or almost complete globaliza-

tion of its information and communication technologies, understanding of risk exposures;
– the permanently updatable risk management policy;
– adaptive decision-making based orientation toward risks.

The EGRM framework is addressed to risks that affect physical and digital dimensions and ecosystems and is orientated towards the new risks and crises. Risks often are interdependent. They can form, destroy, even enter in global networks of risks. Thus, the unknown systemic risks are possible to arise, which could manifest in cascade, hierarchical or with complex multi-connected behavior in cyberspace.

5. A VISION ON IMPLEMENTATION OF RISK MANAGEMENT AND ARTIFICIAL INTELLIGENCE

The Artificial Intelligence is the heart of the emerging technologies. The development of the notions about natural intelligence and the sciences connected to it appear as a new direction and application of the systems with AI. It is expected that AI will provide positive and negative impacts on all the human processes [1]. Furthermore, FERMA explains that the AI is a term that describes the performing of human tasks by computers or in other words "human intelligence performed by a machine" [11].

The European Commission has adopted a White Paper on Artificial Intelligence [16] that is focused on its integration in all economic and social areas. According to the European Commission, the AI is regarded as a collection of technologies that combine data, algorithms and computing power. Thus, three major groups that may benefit from the AI ecosystem are: citizens with benefits in improved healthcare, transport systems, better public services; business that may further develop a new generation of products and services in machinery, transport, cybersecurity, farming, green and circular economy, etc., and society with more service of public interest, e.g. by reducing costs of providing services, by improving the sustainability of products, etc.

The benefits of integrating AI in business and society can be regarded as one side of the coin, while the risks are the other. The detailed list of risks is given in previous section. The risk groups specially concerning AI will be emphasized again: privacy and data security, change in labour market, mental distraction, manipulation and echo camera, fragmentation, responsibility and accountability, ecology, ecosystems and ethics, changes in income/cost structure and ownership of assets.

The digitalization of economics and AI are the core elements of Industry 4.0. However, before their fully implementation, there is an intermediary stage of interaction and machines via Cyber-Physical Systems (CPS).

CPS integration can be considered in vertical and horizontal perspectives [17]. The vertical integration is directed towards the different levels of hierarchy in the organization and requires exchange of increasing volume of information. The horizontal integration is collaboration between enterprises within the same value creation network, Fig. 5. AI has to be integrated into the enterprises activities through CPS and other intelligent manufacturing components.

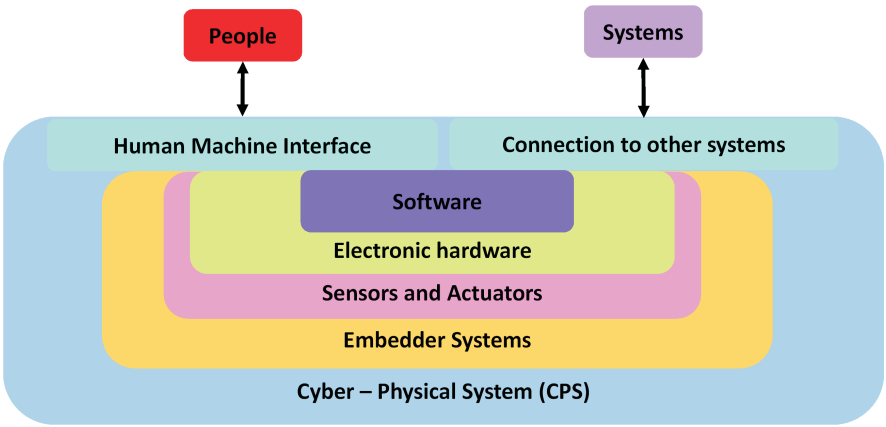

Fig. 5. Cyber-Physical System – interaction and machines via CPS [17]

Referring to the EIRM Framework 2017 by COSO, the integration of AI and CPS is possible due to five components:

1. Governance and culture for AI- and CPS-related risks. That is the stage where the possibilities for integrating AI- and CPS-related risks are regarded.
2. Strategy and objective setting for AI- and CPS-related risks. Here, all the actions are related to the strategy of the organization, its objectives and their implementation in regard to the AI- and CPS-related risks.
3. Performance. Three major stages are described in this element and they include the identification of AI- and CPS- related risks, their assessment and prioritization, and the implementation of risk responses.
4. Preview and revision. The implemented model of the AI- and CPS-related risks is reviewed and discussed in order to include the possible changes in the environment that happened in the meantime.

5. Information, communication, and reporting. The results from the stages so far are presented to the stakeholders and the focus is on the information for the AI- and CPS-related risks.

Based on the FERMA, NIST, ISO and COSO the implementation of AI and CPS into the EGRM could benefit by several characteristics:

- It is appropriate for implementation as it additionally considers Industry 4.0 risks.
- The new FERMA approach to Framework of COSO clearly defines the stages of integrating the AI into the business activities.
- EGRM as the ongoing processes and environmental monitoring is the key activity to adaptation to the volatile changes.
- The regulatory framework of the risk management could be updated regularly regarding to all changes for the AI- and CPS-related risks.

If enterprises do not manage the Industry 4.0 challenges and the integration of AI or CPS, they would lose competitiveness. The understanding of the AI, CPS and all digitalization processes is of utmost importance for the ERM.

6. CONCLUSION

In this paper were presented the main approaches of risk management and the most used risk management standards. There were analysed the general aspects of evolution of RM, ERM, EIRM and were suggested an extension of EIRM to the concept of EGRM, where the accent is to Industry 4.0 risk and the implementation of the Artificial Intelligence in cyber-physical systems. There were described how the risk and risk management standards contribute to the improvement of the flexibility towards the changes in the environment in order to respond to challenges of Industry 4.0 technologies and risks.

From a system point of view, EIRM and EGRM are structures – modules in the well-known Enterprise Resource Planning (ERP). ERP is the integrated management of business processes, usually in real time, mediated by software and technology. It is used by enterprises for integration and coordination of the information in enterprise-wide business processes, by using common database and shared management reporting tools [18]. According to the functions, characteristics and criteria of the specific enterprise, the design of the EIRM and EGRM modules as structures in Enterprise Resource Planning necessarily requires new research areas.

By managing risks and integrating risks into the EGRM, the enterprises will be competitive no matter of the dynamics in the environment. However, in future new challenges are expected for the enterprises and their development

and therefore new decisions should be sought. That is related to the risks and challenges in the global economy.

ACKNOWLEDGEMENTS

This work is supported by grand KP-06-H36/2 BG PlantNET "Establishment of National Information Network GENEbank – Plant Genetic Resources".

REFERENCES

[1] I. Popchev and D. Orozova, Towards a multistep method for assessment in e-learning for emerging technologies, *Cybernetics and Information technologies* (2020) **20** (3) 116–129, ISSN: 1311-9702 (Print), ISSN: 1314-4081 (Online), DOI: 10.2478/cait-2020-0032, http://www.cit.iit.bas.bg/CIT-2020/v-20-3/10341-Volume20_Issue_3-09_paper.pdf.

[2] K. Schwab, *The Fourth Industrial Revolution*, World Economic Forum (2016) 192 pages, ISBN-13: 978-1-944835-01-9 and ISBN-10:194483501.

[3] D. Orozova and I. Popchev, Cyber-Physical-Social Systems for Big Data, XXI-st International Symposium on Electrical Apparatus and Technologies SIELA 2020, Bourgas, Bulgaria, 3–6 June 2020, IEEE, ISBN: 978-1-7281-4346-0,

[4] International Monetary Fund, *World Economic Outlook Update*, June (2020), https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020

[5] I. Nikolova, External Debt and Debt Crises in European Economies, in: International Scientific Conference Proceedings "Bulgaria and Romania: Country Members of the EU, Part of the Global Economy", Economic Research Institute, Bulgarian Academy of Sciences, 10 December 2018, pp. 153–158, ISBN: 978-954-9313-14-7 (Print) and ISBN: 978-954-9313-15-4 (Online), https://www.researchgate.net/publication/348556278_EXTERNAL_DEBT_AND_DEBT_CRISES_IN_EUROPEAN_ECONOMIES.

[6] K. Schwab and T. Malleret, *Covid-19: The Great Reset*, World Economic Forum (2020) 212 pages, ISBN: 978-2-940631-11-7.

[7] I. Popchev, D. Orozova, and S. Stoyanov, IoT and Big Data Analysis in E-Learning, in: Big Data, Knowledge and Control Systems Engineering BDKCSE'2019, Bulgarian Academy of Sciences, Sofia, November (2019), ISSN: 2367-6450.

[8] D. Orozova and I. Popchev, Towards Big Data Analytics in the E-learning Space, *Cybernetics and Information Technologies* (2019) **19** (3) 16–25, ISSN: 1311-9702, http://www.cit.iit.bas.bg/index.html.

[9] I. Popchev and I. Radeva, Risk Analysis – an Instrument for Technology Selection, *Engineering Sciences* (2019) **LVI** (4) 5–20, ISSN: 1312-5702 (Print), ISSN: 2603-3542 (Online), http://es.ims.bas.bg/indexx.htm.

[10] International Organization for Standardization, https://www.iso.org/standards.html, viewed September (2020).

[11] Federation of European Risk Management Associations (FERMA), https://www.ferma.eu/publication/, viewed September (2020).

[12] National Institute of Standards and Technology to the U.S. Department of Commerce (NIST), https://www.nist.gov/

[13] Standards Australia and New Zealand, AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, https://www.standards.govt.nz/.

[14] Committee on Sponsoring Organizations of the Treadway Commission (COSO), *Guidance on Enterprise Risk Management* (2017), https://www.coso.org/Pages/default.aspx.

[15] I. Popchev and I. Radeva, Decision Making Model for Disruptive Technologies in Agriculture, in: Proc. of 10-th International Conference of Intelligent Systems, IEEE 2020, 258–264, ISSN: 978-1-7281-5456-5/20/$31.00, © 2020 IEEE, https://ieeexplore.ieee.org/document/9199962.

[16] European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, *February* (2020), https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

[17] J. Tupa, J. Simota, and F. Steiner, Aspects of risk management implementation for Industry 4.0, 27^{th} International Conference on Flexible Automation and Intelligent Manufacturing, FAIM'2017, 27–30 June 2017, Modena, Italy, *Procedia Manufacturing* (2017) 11 1223–1230, https://www.sciencedirect.com/science/article/pii/S2351978917304560.

[18] E. Monk and B. Wagner, *Concepts in Enterprise Resource Planning*, Forth edition, *Cengage Learning* (2012) 272 pages, Student Edition ISBN-13: 978-1-111-82039-8, Instructor ISBN-13: 978-1-111-82040-4.

Received January 19, 2021