The Need for an Enterprise Risk Management Framework for Big Data Science Projects

Jeffrey Saltz and Sucheta Lahiri
Syracuse University, Syracuse, NY, U.S.A.

Keywords: Risk Management Framework (RMF), Big Data, Data Science, Enterprise Risk Management (ERM).

Abstract: This position paper explores the need for, and benefits of, a Big Data Science Enterprise Risk Management Framework (RMF). The paper highlights the need for an RMF for Big Data Science projects, as well as the gaps and deficiencies of current risk management frameworks in addressing Big Data Science project risks. Furthermore, via a systematic literature review, the paper notes a dearth of research which looks at risk management frameworks for Big Data Science projects. The paper also reviews other emerging technology domains, and notes the creation of enhanced risk management frameworks to address the new risks introduced due to that emerging technology. Finally, this paper charts a possible path forward to define a risk management framework for Big Data Science projects.

1 INTRODUCTION

Despite an increase in the use of Big Data Science by government, industry and educational institutions, there is currently no universally accepted definition that describes the key characteristics of Big Data (Al-Mekhlal & Khwaja, 2019). For example, the three V's (Volume, Variety and Velocity) is a common framework used to describe Big Data analytics (Chen, Chiang & Storey; 2012). However, additional dimensions have been added to that framework, such as Veracity, Variability (Gandomi & Haider, 2015). A yet broader definition of Big Data Science has been used by Saltz and Stanton (2017), who focus on the collection, processing, analysis, visualization, preservation and management of vast amount of information. Furthermore, some use the term Big Data Analytics, rather than Big Data Science. Independent of the specific term used, this field leverages data to develop functional ideas to facilitate performance measurement, create sustained value, and competitive advantage (Fosso, Akter, Edwards, Chopin, & Gnanzou, 2015).

Risk Management is a different field that is also critically important for a wide range of organizations. One view of Enterprise Risk Management is described by Lam (2017, pp.6), who notes that it is "an integrated and continuous process for managing enterprise-wide risks—including strategic, financial, operational, compliance, and reputational risks". Thus, an Enterprise Risk Management Framework (RMF) enables organizations to understand and mitigate potential project risks as well as enabling the alignment of the interests of the stakeholders to a common goal (Lam, 2017).

In short, enterprise risk management enables organizations to manage project risk via the identification and management of risk elements that are contained within the organization's project portfolio (e.g., Lam, 2003, Liebenberg and Hoyt, 2003, Nocco and Stulz, 2006, Beasley et al., 2008, Hoyt and Liebenberg, 2009). Furthermore, to properly address project risks, organizations need to have an enterprise risk management framework, as this will help model, measure, analyze, and respond to the project risks. This is done by treating the potential risks as a portfolio of risks to be managed collectively (Gordon, Loeb, and Tseng, 2009).

To help evaluate the need for a new RMF for Big Data Science projects, this paper explores the following questions:

- Q1: Do Big Data Science projects introduce new risks into an organization?
- Q2: Can current RMFs handle these risks?
- Q3: Is there research that exists, with respect to integrating Big Data Science risks within enterprise risk management?

Saltz, J. and Lahiri, S.
The Need for an Enterprise Risk Management Framework for Big Data Science Projects.
DOI: 10.5220/0009874502680274
In *Proceedings of the 9th International Conference on Data Science, Technology and Applications (DATA 2020)*, pages 268-274
ISBN: 978-989-758-440-4

2 BIG DATA SCIENCE AND ENTERPRISE RISK

2.1 Big Data Science Risks

Independent of what specific Big Data Science definition is used, organizations should be aware of the risks that can occur when using Big Data Science. A classic example of a risk that could arise when using Big Data Science predictive analytics was seen by Target, a large retailer in the United States. Target used predictive analytics to understand future consumer needs, including predicting if one of their consumers was pregnant (Someh et al. 2016; Erevelles, Fukawa & Swayne, 2016). With the capabilities of Big Data to perform predictive analysis, Target predicted a female shopper's pregnancy, and sent marketing material to her family residence, weeks before she told her family about the pregnancy.

However, the risks of using Big Data Science extend beyond possible misuses of predictive analytics. Data inconsistency is another risk that must be considered when using Big Data Science, especially since data inconsistencies are often exacerbated due to the velocity of the data, as old data may become obsolete or not be consistent in meaning with newly generated data (Kim & Cho, 2018; Tse, Chow, Ly, Tong, & Tam, 2018).

There are also regulatory risks associated with the protection of data. This is particularly important where regulatory requisites, such as General Data Protection Regulation (GDPR) and US Privacy Act, have introduced specific regulatory risks associated with data privacy. Hence, a different concern that organizations need to address is how to do Big Data Science without impeding on the data privacy of consumers. For example, using Big Data analytics, one can analyze a person's political preference, spending habits, and other private information via the content or posts published on the internet (Zhang, 2018).

2.2 The Need for a Big Data Science Informed RMF

It is therefore important for organizations to address these risks (e.g., Ethical, Reputational, Operational) pre-emptively. In other words, as Big Data Science is increasingly used, it is creating new risks for the organizations to understand and manage.

To manage these risks, there needs to be a framework that encompasses and manages all Big Data Science risks encountered by an organization. Using a conceptual framework for data governance combined with an existing risk management standard is one approach for Big Data Science risk management. However, as discussed in the next section, existing frameworks are generic in nature and unequipped in managing the risk of Big Data Science on an enterprise level.

3 EXISTING RMF PITFALLS FOR BIG DATA SCIENCE

Standards such as *NIST,* the *Committee of Sponsoring Organizations (COSO)* Enterprise Risk Management Framework, and *ISO 31000:2009. Risk management: Principles and guidelines* are all focussed on risk management activities, assessment process and deployment. Each of these standards are explored to determine if they could properly handle Big Data Science specific risks.

3.1 COSO RMF

In 2004, the first comprehensive guidance on enterprise risk management was published by *Committee of Sponsoring Organizations* – COSO (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2004). Revisions were done in 2013 and then again in 2017 (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2016). The COSO-ERM Integrated Framework has been popular for incorporating enterprise risk (Fox, 2018).

There are five components of COSO ERM – Governance & Culture, Strategy & Objective-Setting, Performance, Review & Revision, Information, Communication & Reporting. As shown in Figure 1, the COSO enterprise risk management framework also has 20 principles, ranging from exercising board risk oversight to reporting on risk performance (Prewett & Terry, 2018).

Figure 1: 2017 Enterprise Risk Management Framework Principles and Components (Prewett & Terry, 2018).

While, these principles encourage organizations to identify and manage risks, they are all at a high

level, and do not offer a framework on how to actually identify the risks. In other words, COSO-ERM is a general set of guidelines which are focussed on the processes deployed in a firm. It is an integrated approach that describes how to implement risk management guidelines via the setting and meeting program goals and reviews. However, Big Data Science may introduce new risks that the organization would not identify, and hence, would not manage via the COSO-ERM framework. In short, COSO ERM by itself is not sufficient to manage Big Data Science risks.

3.2 ISO 31000

The ISO 31000 standard was developed in 2009 by the ISO Technical Management Based Working Group on risk management (International Organization for Standardization, 2009; Choo & Goh; 2015). In conjunction with the earlier standards of AS/NZS 4360:2004, ISO 31000 incudes new definitions of risk management, including eleven risk management principles (Olechowski, Oehmen, Seering, & Ben-Daya, 2016), which are:

1. Risk management creates value
2. Risk management is an integral part of organizational processes
3. Risk management is part of decision making
4. Risk management explicitly addresses uncertainty
5. Risk management is systematic, structured and timely
6. Risk management is based on the best available information
7. Risk management is tailored
8. Risk management takes human and cultural factors into account
9. Risk management is transparent and inclusive
10. Risk management is dynamic, iterative and responsive to change
11. Risk management facilitates continual improvement

As can be seen via these principles, the framework focuses on risk assessment via risk identification, analysis and evaluation. It provides a conceptual approach that creates exhaustive ERM practices in an organization (Gjerdrum & Salen, 2010). The backbone of the risk management process is the ability to create and deploy risk assessments that eventually lead to risk treatments.

Similar to COSO, the standard is not without limitations in that the scope of ISO 31000 is high level and does not help to identify new risks to an organization. Furthermore, the framework's definition of risk is the "uncertainty effect on defined goals" (Kamarulzaman, Bakar & Abas, 2019). In other words, goals and objectives must be defined pre-emptively before risk can be known. However, this objective is challenging, as the goals and objectives within a Big Data Science project keep on changing, due to new data and insights generated during the project.

3.3 NIST RMF

The U.S. National Institute of Standards and Technology (NIST) developed a framework to address cyber risk. There are three parts of NIST framework - Core, Profile and Implementation Tiers (Hiller & Russell, 2017). For example, the Core detects and responds to attacks/vulnerabilities and protects assets.

In short, the NIST Risk Management Framework was created to manage and mitigate the risks that get generated in information systems within an organization (Kohnke, Sigler, & Shoemaker, 2016), such as cyber-attacks, and no other risk elements are addressed.

3.4 Analytics Governance Framework

The Analytics Governance Framework (AGF) focuses on improving big data project management and minimizing project management risk (Yamada & Peran; 2017). While some might view AGF as a Big Data Science specific approach to manage Big Data Science risk, its focus is only on project execution risk.

For example, it proposes a list of guiding principles that streamline the responsibilities of project managers, analytics specialists, and data management specialists. As such, the goal of AGF is to produce successful projects by prioritizing projects in the pipeline, with clear guidelines for data management practitioners on a top-down enterprise level. This will minimize misunderstandings between stakeholders and practitioners, keep timelines in place, and manage expectations.

This framework could possibly be leveraged to help create a foundation for a Big Data Science ERM (since it aligns the objectives and interests of both the clients and the practitioners along with the managers). However, by itself, AGF is not a risk management framework but rather, a project management framework. Hence, there is a need of adding another framework (or layer) to help manage Big Data Science that will help create context, as well as analyze, evaluate, and manage risk.

4 RMFS FOR OTHER EMERGING TECHNOLOGIES

The need of having a new risk management framework for an emerging technology is not unique to Big Data Science. Below we discuss three other examples: cloud computing, industry 4.0 and supply chain management that also required a new risk management framework.

4.1 Cloud Computing

Cloud computing is a model for allowing ubiquitous, convenient, and on-demand network access to a number of configured computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). Internet and different data avenues are used to host software and hardware as a Service via cloud computing (Armbrust, 2010).

Big data and cloud computing are associated with each other. Big data facilitates the use of computing applications to perform queries and retrieve desired outcomes in a timely and seamless manner. Furthermore, cloud computing can use Hadoop, a big data storage service, to facilitate the foundational engine for data processing (Hashem et al., 2015).

Cloud-based technologies have clearly defined benefits – such as providing a centralized location for storing high volume data on remote servers (Hao & Yang, 2019). As cloud services are shared, dynamic and scalable, these services have faced concerns around data security and cyber-attacks (Durowoju, Chan & Wang, 2011; Grobauer, Walloschek & Stocker; 2011). Some of the cloud computing challenges that require a top down approach on an enterprise level include data vulnerabilities, the threat to employee privacy, sharing cloud links, cloud file synchronization, and the security issues related to enterprise directory integration.

However, in exploring how to understand and minimize these risks, it has been shown that it is difficult to manage these cloud computing risks with an existing RMF; and there is a need for having an adaptive risk management framework specifically for cloud computing (Medhioub and Kim, 2017). Hence, it has been suggested that an integrated risk management framework is required to address cloud computing issues and align the interest of the management and stakeholders (Medhioub and Kim, 2017).

4.2 Industry 4.0

The concept of Industry 4.0 was coined in 2011 at the Hanover Fair. It is an umbrella term that encompasses concepts of the Internet of People (IoP), Internet of things (IoT), Internet of Services, Internet of Energy and Cyber Physical System (Hermann, Pentek, & Otto, 2015; Lom, Pribyl, & Svitek, 2016). Apart from operational risks generated with machines, methods, materials, and human resources, Industry 4.0 introduces new and unknown risks with machine, robots and data vulnerability (Tupa, Simota & Steiner, 2017).

Initially the ISO 31000 standard was proposed to address these risks (Niesen, Houy, Fettke, and P. Loos, 2016). However, later research noted that to manage these risks, a new risk management model was needed that integrated BPM (Business Process Management) and PPM (Process Performance Management) with other, more traditional, risk management elements (Tupa, Simota and Steiner; 2017).

4.3 Supply Chain

Supply chain risk is defined by potential incidents associated with inbound supply (i.e., from supplier failures) or the supply market, in which its outcomes result in the inability of a purchasing organization to meet customer demand (Zsidisin, Melnyk, and Ragatz, 2005).

It has been noted that it is imperative to have a supply chain risk management framework that can collect, analyze and monitor supply chain real time data (Fan, Heilig & Voβ; 2015). The need for a supply chain risk management framework has arisen in order to manage or mitigate risks related to utilized resources, network systems and performance criteria (Lassar, Haar, Montalvo, and Hulser; 2010). This need was initially identified due to significant financial losses at companies such as General Motors (1996) and Boeing (1997). More recently, COVID-19 and the related supply shock has also demonstrated this supply chain risk (Baldwin & Tomiura, 2020).

To help address these risks, a Supply Chain Management Framework, which is integrated into a Knowledge Management Framework that hosts all the known risk elements on the knowledge base, has been proposed (Solomon, Ketikidis & Choudhary, 2012).

5 BIG DATA SCIENCE RMF RESEARCH – A SYSTEMATIC LITERATURE REVIEW

To explore the existing research on Big Data Science and risk management frameworks, a Systematic Literature Review (SLR) was performed. An SLR was used since it provides an understanding of the relevant literature and more generally, provides a good idea of what is known about a particular topic or discipline (Boell & Cecez-Kecmanovic; 2014).

5.1 Methodology

As shown in Table 1, six repositories were searched for literature on Risk Management Frameworks relating to Big Data Science – ACM Digital Library, Science Direct, IEEE Explore, Scopus, Web of Science, and Google Scholar. As the domain of Big Data Science is an emerging domain, we restricted the search to articles published in last five years i.e., from 2015 (through February 2020). In addition, only articles published in English were considered.

Table 1: Search Summary.

Repository searched	ACM digital library, Google Scholar, science direct, scopus, web of science, IEEE xplore
Publication period	2015 to 2020
Language	English
Search applied	Full text

As shown in Table 2, the search consisted of two separate terms, the first was related to risk management framework, and the second term related to big data science.

Table 2: Keyword combinations used for literature search.

"risk management process"	+ "big data"
"risk management framework"	+ "data science"
"risk management process"	+ "big data"
"risk management framework"	+ "data analytics"
"risk management framework"	+"data mining"
"risk management framework"	+ "business analysis"
"risk management framework"	+ "artificial intelligence"
"risk management framework"	+" text mining"

After the documents were retrieved, a content analysis was performed that focused on ensuring that the article focused on risk management frameworks for Big Data Science project risks, and was performed as follows using the following two step process. First, the title, abstract and conclusion were reviewed to determine if the paper had the appropriate focus. For papers where it was not clear if they should be included or excluded, they were then briefly reviewed in full. Finally, the articles that past this analysis were reviewed in depth and categorized into key themes.

5.2 Findings

There was a total of 334 articles identified by the previously defined search criteria. After the content analysis, 46 articles remained relevant.

As shown in Table 3, the literature search did not identify any article that provided a risk management framework for Big Data Science projects. In fact, the articles were broadly classified into several other categories (risk management standards, RMFs in different sectors, Big Data execution challenges).

We note that one article within the big data execution challenges category did highlight legal risk, and the potential risks related to the quality of the analysis (Waterman & Bruening; 2014).

Table 3: Resultant documents with assigned categories.

Categories	# of articles
Risk management standards (ISO, NIST, COSO)	13
RMF in different sectors (e.g., Banking, Supply Chain Management, Cloud Computing, Industry 4.0)	19
Big Data Execution Challenges	7
Big Data Ethics	2
Big Data as a solution	2
What is Big Data/Data Analytics/AI?	3
RMF for specifically for Big Data Science Projects	0

Hence, this SLR supports the notion that there is minimal currently research on exploring a Big Data Science appropriate RMF.

6 CONCLUSIONS

While organizations are continuing to increase their use Big Data Science, there has been less attention focused on the risks associated with the use of Big Data Science.

Specifically, this paper notes that there are new risks that a Big Data Science project introduces into an organization (which addresses RQ1), that the current RMFs do not handle these risks (which addresses RQ2) and that there is currently minimal research with respect to evaluating Big Data Science risks within enterprise risk management (addressing RQ3). Hence, this paper demonstrates the need for a Big Data Science RMF that can address the unique Big Data Science project risks.

In short, using an existing enterprise framework for Big Data Science projects is not sufficient, in that these frameworks will not capture all the risks of Big Data project. These risks include model risk (e.g., model bias), reputation risk (e.g., in appropriate use of data insights) and data risk (e.g., inconsistencies in the data). These new risks need to be incorporated within an enterprise level risk management framework. Hence, the lack of a well-defined RMF for this domain suggests that organizations have unknown and/or unmanaged risks, and that a new RMF for Big Data Science projects is required to accurately capture and manage these new project risks.

One potential next step, towards the creation of an effective Big Data Science RMF, is to survey organizations to identify best practices, identify organizations that have extended standards such as COSO, ISO-31000 or NIST. The survey could also help to gain an understanding of internally deployed RMFs for Big Data Science efforts. With this information, one could consolidate the existing organization specific models and frameworks used, to see if there were components that could be leveraged to create an enterprise level risk management framework for Big Data Science projects.

REFERENCES

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424-438.

Al-Mekhlal, M., & Khwaja, A. A. (2019, August). A Synthesis of Big Data Definition and Characteristics. In *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)* (pp. 314-322). IEEE.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A.,. & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

Ardagna, C. A., Ceravolo, P., & Damiani, E. (2016, December). Big data analytics as-a-service: Issues and challenges. In *2016 IEEE international conference on big data (big data)* (pp. 3638-3644).

Asadi Someh, I., Breidbach, C. F., Davern, M., & Shanks, G. (2016). Ethical implications of big data analytics. *Research-in-Progress Papers*, *24*.

Baldwin, R., & Tomiura, E. (2020). 5 Thinking ahead about the trade impact of COVID-19. *Economics in the Time of COVID-19*, 59.

Boell, S. K., & Cecez-Kecmanovic, D. (2014). A hermeneutic approach for conducting literature reviews and literature searches. *Communications of the Association for Information Systems*, *34*(1), 12.

Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS quarterly*, 1165-1188.

Choi, T. M., Chan, H. K., & Yue, X. (2016). Recent development in big data analytics for business operations and risk management. *IEEE transactions on cybernetics*, *47*(1), 81-92.

Choo, B. S. Y., & Goh, J. C. L. (2015). Pragmatic adaptation of the ISO 31000: 2009 enterprise risk management framework in a high-tech organization using Six Sigma. *International Journal of Accounting & Information Management*.

Duhigg, C. (2012). How companies learn your secrets. *The New York Times*, *16*(2), 1-16.

Durowoju, O. A., Chan, H. K., & Wang, X. (2011). The impact of security and scalability of cloud service on supply chain performance. *Journal of Electronic Commerce Research*, *12*(4), 243-256.

Erevelles, S., Fukawa, N., & Swayne, L. (2016). Big Data consumer analytics and the transformation of marketing. *Journal of Business Research*, *69*(2), 897-904.

Fan, Y., Heilig, L., & Voß, S. (2015, August). Supply chain risk management in the era of big data. In *International conference of design, user experience, and usability* (pp. 283-294). Springer, Cham.

Fox, C. (2018). Understanding the new ISO and COSO updates. *Risk Management, 65*(6), 4-7. Retrieved: https://search.proquest.com/docview/2065314658

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, *35*(2), 137-144.

Gjerdrum, D. & Salen, W.L. (2010), "The new ERM gold standard:ISO31000:2009", Professional Safety, Vol.55 No.8, pp.43-44.

Gordon, L. A., Loeb, M. P., & Tseng, C. Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of accounting and public policy*, *28*(4), 301-327.

Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, *47*, 98-115.

Hermann, M., Pentek, T., & Otto, B. (2016, January). Design principles for industrie 4.0 scenarios. In *2016 49th Hawaii international conference on system sciences (HICSS)* (pp. 3928-3937). IEEE.

Hill, K. (2012). How Target figured out a teen girl was pregnant before her father did. *Forbes, Inc*.

Hiller, J. S., & Russell, R. S. (2017). Privacy in crises: The NIST privacy framework. *Journal of Contingencies and Crisis Management*, *25*(1), 31-38.

Kamarulzaman, M. S., Bakar, N. A. A., & Abas, H. (2019). Risk Processing Framework for Big Data Security in the Enterprise. *Open International Journal of Informatics (OIJI)*, *7*(2), 170-178.

Kim, H. Y., & Cho, J. S. (2018). Data governance framework for big data implementation with NPS Case Analysis in Korea. *Journal of Business and Retail Management Research*, *12*(3).

Kohnke, A., Sigler, K., & Shoemaker, D. (2016). Strategic Risk Management Using the NIST Risk Management Framework. *EDPACS*, *53*(5), 1-6.

Krasnow Waterman, K., & Bruening, P. J. (2014). Big Data analytics: risks and responsibilities. *International Data Privacy Law*, *4*(2), 89-95.

Lam, J. (2017). *Implementing enterprise risk management: From methods to applications*. John Wiley & Sons.

Lassar, W. M., Jerry, H., Montalvo, R., & Hulser, L. (2010). Determinants of strategic risk management in emerging markets supply chains: The case of Mexico. *Journal of Economics, Finance & Administrative Science*, *15*(28).

Lom, M., Pribyl, O., & Svitek, M. (2016, May). Industry 4.0 as a part of smart cities. In *2016 Smart Cities Symposium Prague (SCSP)* (pp. 1-6). IEEE.

Malik, V., & Singh, S. (2019). Cloud, Big Data & IoT: Risk Management. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (pp. 258-262). IEEE.

Medhioub, M., Hamdi, M., & Kim, T. H. (2017, March). Adaptive risk management framework for cloud computing. In *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)* (pp. 1154-1161). IEEE.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Niesen, T., Houy, C., Fettke, P., & Loos, P. (2016, January). Towards an integrative big data analysis framework for data-driven risk management in industry 4.0. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5065-5074). IEEE.

Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management: What role can the ISO 31000 risk management principles play?. *International Journal of Project Management*, *34*(8), 1568-1578.

Prewett, K., & Terry, A. (2018). COSO's Updated Enterprise Risk Management Framework—A Quest For Depth And Clarity. *Journal of Corporate Accounting & Finance*, *29*(3), 16-23.

Raschke, R. L., & Mann, A. (2017). Enterprise content risk management: a conceptual framework for digital asset risk management. *Journal of Emerging Technologies in Accounting*, *14*(1), 57-62.

Saltz, J. S., & Dewar, N. (2019). Data science ethical considerations: a systematic literature review and proposed project framework. *Ethics and Information Technology*, *21*(3), 197-208.

Saltz, J., & Stanton, J. (2017). *An introduction to data science*. Thousand Oaks: SAGE Publications.

Solomon, A., Ketikidis, P., & Choudhary, A. (2012). A knowledge based approach for handling supply chain risk management. In *Proceedings of the Fifth Balkan Conference in Informatics* (pp. 70-75). ACM.

Tse, D., Chow, C. K., Ly, T. P., Tong, C. Y., & Tam, K. W. (2018, August). The challenges of big data governance in healthcare. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 1632-1636). IEEE.

Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. *Procedia Manufacturing*, *11*, 1223-1230.

Yamada, A., & Peran, M. (2017, December). Governance framework for enterprise analytics and data. In *2017 IEEE International Conference on Big Data (Big Data)* (pp. 3623-3631). IEEE.

Walloschek, M., Grobauer, B., & Stöcker, E. (2011). Understanding of Cloud Computing Vulnerabilities. *IEEE Computer and Reliability Society*.

Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2015). How 'big data'can make big impact: Findings from a systematic review and a longitudinal case study. *International Journal of Production Economics*, *165*, 234-246.

Zhang, D. (2018, October). Big data security and privacy protection. In *8th International Conference on Management and Computer Science (ICMCS 2018)*. Atlantis Press.

Zsidisin, G. A. (2003). Managerial perceptions of supply risk. *Journal of supply chain management*, *39*(4), 14-26.

Zsidisin*, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International journal of production research*, *43*(16), 3401-3420.