Integrated Risk and Business Impact Analysis: A Kind of Support for ISO 22301

Andrea Strelicz,
University of Pannonia, Hungary
Ferenc Bognár,
Budapest University of Technology and Economics, Hungary

Doi:10.19044/esj.2020.v16n4p1 URL:http://dx.doi.org/10.19044/esj.2020.v16n4p1

Abstract

This paper focuses on introducing a kind of framework, technical tool, method, platform to risks, and business impact analysis and evaluation based on ISO 22301 –Societal Security Business Continuity Management Systems – requirements. This technical tool is created for three reasons. Firstly, it is created to handle those weak points that are restricting a deep, honest, and completely true to reality risk analysis. Secondly, to provide supports, identifying the possible business impacts, as factors that are able to affect the business continuity of a company. Thirdly, to create a common platform supplemented with visualizing the results of these two different analysis. This paper is aimed at highlighting the advantages of this technical tool and the eliminated weaknesses, while explaining the methodology and logical way of the platform. This technical tool has been introduced to some companies and is used to evaluate their real status. Arising from the aforementioned, this paper also show some usage results. According to the first test in a real environment, this technical tool proved to be more effective for decision makers than the well-known similar methods. The most useful part seems to be the visualization and the provided flexible framework of the tool. This fact encourages further tests and improvement.

Keywords: Business Continuity, Risk Management, Holistic Risk Approach, ISO 22301, Business Effect Analysis

Introduction

There is a worldwide availability of countless and excellent professionals, literatures, education, practices, and experiences in risk management. Furthermore, the need for a proactive approach, risk-based thinking, and insurance are widely spread. Although numerous models already exist for the nature of risks and the framework of analysis and evaluation, the

same cannot be said of business impacts. Nevertheless, good relations with partners, planned revenues, uninterrupted inflow, and safe, cost-efficient and internal operation needs are present in everyday life. The guidelines for those consciously managing and protecting are unavailable, unlike the historical past of risk. Although, these go hand in hand.

The origin of risk and business impact evaluation, based on the same aim and framework, was first defined in ISO 22301:2012 – Societal security Business continuity management systems – requirements. This standard requires two different analysis and evaluations and it offers two different platforms for them. However, if these two different evaluation platforms could be used in an integrated platform, the analyzing and evaluation process can be done at the same time supported by visualized results.

Since a good management needs to know conceptually what it wants, what it can and what it will, technical tools sometimes have lesser emphasis. However, there may be a need for technical support alongside conceptual awareness. Therefore, the purpose of this article is to present a possible technical solution for analyzing and evaluating risks and business impacts in an integrated way that can support sustainable attitudes and mindsets.

About the Prevailing Mindsets

The most significant attitude-shaping indicator dates back to the 1980s when standardization and integrated solutions became the best and most economical practices. They searched for and applied those special kinds of robust solutions that can deliver multiple functions. These approaches are still prevalent and during designing solutions, specialists continue to look for the widest range of usability that can be associated with a primary function or even capable of performing multiple functions independently of each other (be it a product, product generating device, equipment, method, software, system, even operating environment, etc.). Some very good examples are standards. Some of them are independent of company size, industry, dominant national culture, geographic location or others. Also, they are the industry-specific additional or stand-alone standards for the system, process, or product management.

In recent times, such an approach can also be considered as a dominant approach as manufacturers and service providers offer customized solutions to increase and retain their customers. At war-free areas, needs are continuously increasing for welfare and comfort by general human aging, individual differences, and tolerances. These facts can result to an increasing need for diversity of products and services also.

Consequently, questions such as how to meet these different needs with the same solution arises. The foregoing interrogative statement clearly present a sort of difficulty and complexity. In practice, it is either there is real

customization, which has a significant effect on price, or the supply is so wide that the real need for customization did not arise or there os no much differences based on requirements. This means that a customer can be satisfied with the choice or combination of unified solutions.

The same is true of methods and models. While all methods and models are designed to be uniform and universally true under given boundary conditions, it is the first task of the knowledgeable to revise the method or model and to confirm or disprove the universal truth. This process is entirely appropriate as it indicates continuous improvement.

The practical need is that both approaches must be present and realized in a solution at the same time. Today's professionals are working to simultaneously overcome this contradiction, and success is counted as innovation.

General Approach to Risk Management and its Support

When it comes to risk management, there is a wealth of excellent literature available to understand the nature of risks and the importance of controlling them. Their main goal is to be global, understand all possible corporate contexts, consider the importance of the strategy, and formulate guidelines that can help decision-makers to fully manage risk and possible risky situations. From the available risk management approaches and models, it is clear that the main aim is to develop conceptual awareness of decision-makers (Amirshenava & Osanloo, 2018; Giannakis & Papadopoulos, 2016; Pym, 2015; Wu, Chen, & Olson, 2014). However, it is also clear that when moving up on the leadership hierarchy, it is increasingly uncommon for decision-makers to sit down and physically perform analysis and evaluations. At the same time, when moving down the leadership hierarchy, the occupied area becomes smaller by the given position. As a result, the transparency of the entire corporate operation and the need for thinking decreases. However, a well-prepared and presented decision-based results are general expectations. That is why it is not uncommon that an independent consultant comes, review the organizations, and carry out the analysis and evaluations. At the end, they are expected to formulate responsibilities and recommendations (Ali, Warren, & Mathiassen, 2017).

Consequently, since each risk management approach and model is typically similar, they are able to give a hand-free approach in terms of methods and tools. This means that each actor should select or develop the most appropriate methods and tools according to the guidelines. This may be the reason why the most obvious and widespread method is the Failure Mode and Effect Analysis (FMEA) from the automotive industry. This was partly due to the size of the automotive industry, its requirements for integration into its supply chain, and finally its transparency. On the other hand, its logic and

framework are suitable for analyzing and evaluating all types of risk even in other industries. The truth is that no methods have been created since then. Hence, it is logically different from the FMEA, providing any choice to analysts. All analysis methods involve quantifying risks according to a given criteria, adding value to them, using certain mathematical formulas, and sometimes giving limits or tolerances to handle the high-value risks (Barafort, Mesquida & Mas, 2017; Jenei, 2016). All methods aim is minimizing the influence of the "Human[1]" factors, the objectivity, and the reproducibility and, the latter one cannot be achieved due to the "Human" factors. As the importance of risk and risk management cannot be overemphasized in a company life, the continuous customization and testing of effectiveness and influence of them are indispensable as well (Mbuva, Rambo & Oketch, 2018). All in all, scientists are looking for a way to implement possessive and recommending policies in risk management (Bevilacqua & Ciarapica, 2018).

Considering the Business Impacts and Its Support

There are several papers on the possible impact of growing or the sustainability of a company. All of them try to define those factors that are possible to lead to the success and long life cycle of the company (Janeska-Iliev & Debarliev, 2015; Perveen, Ahmed & Begum, 2018). However, these possible business impact factors are defined only on model level such as strategy, information, or competence. The certainty is that these possible factors are general needs. The examination of them is necessary because the importance level, relevancy, and related value of national culture differs everywhere (Ra'ed & Taisir, 2015). On the other hand, these factors cannot be evaluated without a kind of quantity, quality, availability, intention, or direction context.

For this reason, the analysis and evaluation of business impact were required at first by ISO 22301. According to the standard, there is a perfectly legitimate and logical need, since it is a good starting point if a company is aware of the potential risks of business processes. However, nobody can get a full picture of what the risks are until the examination and definition of their potential effects, prevention, intervention if necessary, or recovery activity can work effectively (minimizing extra cost and time, saving partnerships and assuring uninterruptedly the planed revenue) if the effects are clearly seen and understood (ISO, 2012).

[1]"Human", as a set of attributes, is given when considering and evaluating risks and impacts. In a reduced approach, a set of attributes can be understood as a combination of knowledge, experience, skills, and physical and psychological status. This is over a period of time when potential risks and impacts are identified and assessed and when they are actively involved in the operation of the company. (Bognár, Strelicz, Katona & Szentes, 2018)

Since the need for business continuity is a basic requirement and a day-to-day central task for all employees throughout the company, the management approach of the ISO 22301 standard helps to understand the awareness and importance of business continuity. The business impact analysis and examination can help the decision-makers not only to be prepared for internal hazards but understand all kinds of contexts in which they are involved directly or indirectly way. It means to be clear not just on how to operate the company safely, but understand that the company's safe functioning is essential to others and it influences the safe functioning of others. Since ISO 22301 requires an examination of the potential impact on business continuity, the range of methodological and technical recommendations for analysis is much smaller than the risk. There are special pieces of literature about possible business impacts and their evaluation methods as well (Delen & Zolbanin, 2018; Goldberg, 2008; Kingswood, 2015; Oliveira, Marins, Rocha & Salomon, 2017; Torabi, Giahi, & Sahebjamnia, 2016; Torabi, Rezaei, Soufi & Sahebjamnia, 2014). However, there is no literature or recommendations fully covering the potential kind of business impacts. This means there is no common list on what should be considered while analyzing the potential impacts of our business continuity. The standard does not define the aspects in which business impact should be examined.

The standard was first released in 2012, and the number of users of the standard is low. Also, it conveys important guidelines and there is no appropriate practice and experience base for analyzing the business impacts completely.

The Integrated Risk and Business Impact Analysis Method with a Holistic Approach

The world loves integrated, simple, and compact solutions and all-in-one features and methods. While the method described below is certainly incomplete for some missing latent needs, it may still provide the analysts with a kind of tangible solution. This is only if it has a thought-provoking starting point. As it is mentioned in the previous section, FMEA is able to be a generic model to lead the risk analysis and evaluation process. There are numerous hybrid or industry-specific FMEA transformations, which also means that the logic of the method is suitable for serving other industries or fields. Therefore, it was obvious to use it as a starting point for a holistic integrated approach (ISO, 2012; Bognár at colleagues, 2018).

A Holistic Approach from the Aspect of the Presented Method

Risk management efforts have already been mentioned in previous sections of this paper. In this section, without any other expert approaches, this

paper introduces a risk and business impact analysis method by considering the holistic approach.

Level of Definitions

There are many definitions of risk that have been formulated by the industry, profession, or science. A professional definition describes the risk as an impact, an outcome, an event, an entire process, or a set of resources that are used for the operation. Starting from social and cultural anthropological factors, risk can be a community decision, a culture, a result of a communication process, a value system and others. At the "Human" level, risk can be a physical, physiological, or psychic state, a feeling, a level of competence, experience, knowledge, support, background, or relationships, and more. In accordance with this diversity of definitions, this method can be considered as the risk that the decision-maker(s) formulate since only those risks will be considered, interpreted, and dealt with as risks that they agree with. At this point, it becomes clear that the diversity of organizations and their future may be different. Thus, it may not be appropriate to examine these organizations or systems in the same context and perspective.

In terms of business impacts, the industrial or professional difference in definitions is still missing as stated by ISO 22301.

Level of Contextualization

The way certain decision-makers place the role and substance of their organization in their environment in time and space also has a significant impact on the outcome of analysis and evaluation. The accuracy of the contextualization is relevantly dependent on the factors that are involved in the definition that appears in both analysis and evaluation. This method accepts the contextual factors that are recognized by the decision-makers. This means that it does not define the exact and obligatory factors to consider, but there are recommendations from which one can selecte the proper ones. Thus, the context of analysis and evaluation may be influenced by the existing characteristics, language, operating disciplines, complete competence and experience, prevailing national and organizational culture, operational profile, stakeholder, geographical characteristics, time and others.

Aims and Application

The most important aspect when developing the method was to provide an analysis and an evaluation method of the system that can offer information to decision-makers, including strategy development. The primary expectation of the method was that the analysis and evaluation of the risks and business effects identified for a potential function should be limited to a single line and include all information. It could be used to make statements on various aspects

either on risks or business impacts, consider the maturity of the system and level of competence of the system or company, be universal, independent of context, circumstance, size, and corporate culture. In addition, it should be customizable at the same time and provide a mirror image of the system to decision-makers.

However, the method and approach are not intended to apply a common set of criteria and factors to all organizations and systems. Furthermore, this method is not intended to protect the system by itself as there is no particular solution that protects each system and organization equally against its own limitations or capabilities. Its purpose is to provide a mirror that allows for continuous improvement step by step based on the growth rate and boundary conditions set by decision-makers because the method is developed for systems. Also, it can be used for the entire company, group of companies, and supply chain, but it also works for a project, LEAN systems or other systems.

The Main Features of the Method

These features are described as shown below:

- The framework for analysis and evaluation is bound, but the criteria setting and method of evaluation can be individually customized according to the values and properties of the system.
- Examining a given function so that the risks and the business impact factors can be seen in a row, and the entire evaluation data can be visible together.
- It does not focus on checking points but prefers control and standardization base. This is because the concept is not in implementation but in regulation at the decision-making level, and the appropriate regulation ensures the proper controls and checking points.
- Visual stats can be created from it:
    - Prioritize risks, including systemic risk factors,
    - Prioritize the business impact, including business impact factors,
    - The departments can be ranked in terms of risk, that is, the ranking of the operating units that pose a risk to the system,
    - Organizational units can be ranked in terms of business impact, that is, the rank of the functional units most influencing system security and business continuity,
    - Any other frequency that may be needed to make a decision.
- Functions that carry the same or similar risks become visible. Therefore, the intervention can be accomplished in a "multiple birds at one stroke" and the result can be cost and time-saving at the same time.

- Those surfaces become visible which are reduction target and efficiency-oriented.
- Applying any correction can affect other functions making them more functional while saving time and cost.
- The analyzes, evaluations, and results of individual organizations and systems will be different.
- Weaknesses become visible for continuous improvements or to support strategic decisions.
- Based on the experience so far, the method is easy to learn and does not require a full-day training.

Operational Concept

The structure of the method can be divided into five main parts:

1. Contextualization – Definition of the framework and the elements to be evaluated, a summary description of the operational requirement, and malfunction. The level of analysis can be set individually (even by standard). The requirements and its opposites have to be explored, not only a short sentence.

Figure 1. An example of the Contextualization part

Serial numb.	System Description	Process Description/ Department ID	Function Description	Specified Operation description	Lack of Operation Descrition

2. Identify the potential impact of the elements to be evaluated on the aspect of business continuity where the amount and nature of potential factors can be individually adjusted.

Figure 2. An example of the Business Impact Analysis part – In practice in one line

Business Impact Analyses (selected factors)									
Environmental (Biological, Chemical, Physical)	KS	Human (Physical, Psichological, Competence, Availability)	ES	Time	IS	Material/Financial (Extra Cost, Lost Revenue)	AS	Inner Prestige/Morals	
Business Impact Analyses (selected factors)									
PS	Product/Service	TS	Social/Collaborative/Political/Stakeholders	XS	Default/Miscond uct	JS	Partners (Customers/Supilers, Market tendencies)	PS	CS	CSS

3. Identify the potential risks of the elements to be evaluated at the level of factors where the quantity and nature of the factors can be individually adjusted. The analysis can be realized with numerical or text data as well.

Figure 3. An example of Risk Factor Analysis part

Risk Factor Analyses (selected factors)								
Human	**Material**	**Methode**	**Infrastructure (Equipments, Devices)**	**Environment**	**Information**	**Measurement, monitoring and controlling system**	**CO**	**SCO**

4. Review and evaluate the regularity of the items to be evaluated such as the checkpoint to observe if the existing standards and tools are appropriate on this analysis aspect.

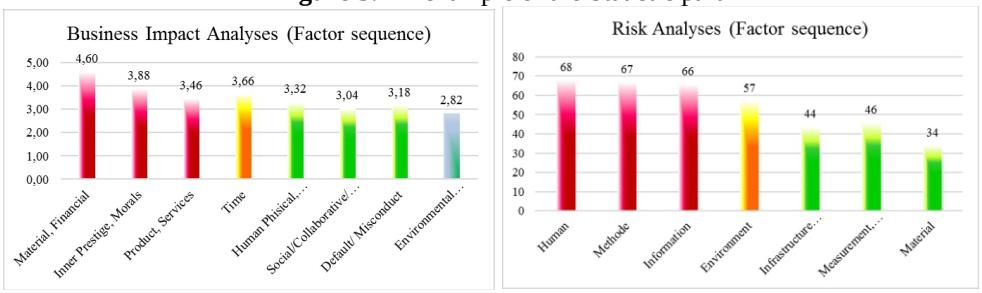
Figure 4. An example of Regularity and Standardization part

Regularity, Standardization		
Regularity, Standardization Level Description	**CD**	**Evidence**

- It provides several possible computational solutions for evaluation, and it can be configured.

5. Statistics and statements summarize the results of the analysis and evaluation by various aspects.

Figure 5. An example of the Statistic part



The method handles teamwork and individual assessment with complementary calculations but is not opposed to it. In this way, it gives room for the internal characteristics, culture, and size of the system. Although the method seems to render the results of analysis and evaluation unstable due to its customization. At this point, it is necessary to remember that systems and organizations differ in terms of culture, competence, maturity, preferences, values and more.

In terms of risk factors, the factors that influence the level of risk can only be those that appear as resources to operate. According to this, all available resources at any given time, in terms of quality and quantity and possibly surplus or shortage, can be a possible risk factor. According to this inverse approach, the Kauro Ishikawa herringbone model which is originally

designed for root cause analysis is virtually perfect for identifying resources since only resources can cause errors or risk.

With regard to business impact factors, the Ishikawa model can only be interpreted as the availability of sufficient quality and quantity of resources for secure internal operation in time and space so that those nonconformities do not interfere with business processes. However, since the system also has an operating environment, it is necessary to consider factors independent of the system, direct/indirect, intentional/accidental, calculated/unexpected, which may affect business continuity as well. Thus, for example, the PESTEL model can be applied well as a set of business influencing factors.

In practice, there is no system-level phenomenon whereby a function or process can be interpreted as a single malfunctioning resource or a single area that affects business continuity. At the system level, causes and domino effects are delayed over time. Therefore, interventions need to be performed in a more complex manner. This means that the root cause of a possible occurrence can be different in time and space to the error. On the other hand, it can also be preceded by a number of causal events so that the cause does not directly result in damage only in a multi-step and indirect way.

Practical Experience

The method has been tested several times in a real-world environment, which has led to new demands for statistics as well as unique factors. Since this method is still young, further improvements will likely evolve.

In practical application, the classic FMEA was continuously running in parallel. Comparing the results of the two methods, it has been discovered that this one provides more information to decision-makers. They also looked at the potential for underestimation and overestimation possibility. Therefore, it was discovered that most of the reality employees perceive in their daily work was shown by the method. In all cases, the process of analysis was conducted with a moderator, which in some cases may give room for emotions. In one case, one year later, it could have managed to repeat the analysis with the same team, in the same environment, and on the same surface. Here, due to passion in the earlier analysis, certain values were seemingly overestimated. However, because the team was tired at the second analysis due to overload, the same factors were evaluated less rigorously. From this point, one of the main conclusions is that the another year's assessment is needed and that the "Human" factor could not be eliminated as long as a human is doing the analysis. An assessment with emotions also reflects the feeling of a group, which should not only appeal to decision-makers but also to the moderator. Thus, they should be able to manage their feelings throughout the process of analysis.

Limitations

While business impact analysis is still not widespread, there are few literatures that can help the analyst identify and evaluate potential factors. In other words, along with a general set of values and certain trends, newer factors that may affect business continuity are slowly being formulated. Accordingly, research is currently underway to capture, on a theoretical and practical basis, all the factors that could potentially affect business. As its practical application is not yet significant, the method has received little criticism and its viability and acceptability are not yet clearly visible.

References:

1. Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management*, *37*(6), 639–649. https://doi.org/10.1016/j.ijinfomgt.2017.05.008
2. Amirshenava, S., & Osanloo, M. (2018). Mine closure risk management: An integration of 3D risk model and MCDM techniques. *Journal of Cleaner Production*, *184*, 389–401. https://doi.org/10.1016/j.jclepro.2018.01.186
3. Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010
4. Bevilacqua, M., & Ciarapica, F. E. (2018). Human factor risk management in the process industry: A case study. *Reliability Engineering & System Safety*, *169*, 149–159. https://doi.org/10.1016/j.ress.2017.08.013
5. Bognár, F., Strelicz, A., Katona, A., & Szentes, B. (2018). A flexible Risk and (Business) Impact Analysis under Holistic Approach. *Magyar Minőség*, *XXVII*(11), 61–75.
6. de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production*, *151*, 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054
7. Delen, D., & Zolbanin, H. M. (2018). The analytics paradigm in business research. *Journal of Business Research*, *90*, 186–195. https://doi.org/10.1016/j.jbusres.2018.05.013
8. Giannakis, M., & Papadopoulos, T. (2016). Supply chain sustainability: A risk management approach. *International Journal of Production Economics*, *171*, 455–470. https://doi.org/10.1016/j.ijpe.2015.06.032

9. Goldberg, E. M. (2008). Sustainable Utility Business Continuity Planning: A Primer, an Overview and a Proven Culture-Based Approach. *The Electricity Journal*, *21*(10), 67–74. https://doi.org/10.1016/j.tej.2008.10.016
10. International Organization for Standardization (2012). *ISO 22301:2012 Societal security Business continuity management systems - Requirements*
11. Janeska-Iliev, A., Debarliev, S. (2015). Factors Affecting Growth of Small Business: The Case of a Developing Country Having Experienced Transition. *European Scientific Journal, ESJ, October 2015 edition vol.11, No.28, 28.* http://eujournal.org/index.php/esj/article/view/6371/6156
12. Janeska-Iliev, A., Debarliev, S. (2015). Factors Affecting Growth of Small Business: The Case of a Developing Country Having Experienced Transition. *European Scientific Journal, ESJ, October 2015 edition vol.11, No.28, 28.* http://eujournal.org/index.php/esj/article/view/6371/6156
13. Jenei, T. (2016) Compare the most frequently used models of risk management. *International Journal of Engineering and Management Sciences Vol. 1. No. 1.*
14. Kingswood, M. (2015). Climate change will require more agile business continuity planning. *Network Security*, *2015*(7), 5–10. https://doi.org/10.1016/S1353-4858(15)30057-X
15. Mbuva, P. M., Rambo, C., M., & Oketch, T. (2018). Influence of Risk Assessment on Performance of SME Projects in Machakos County, Kenya. *European Scientific Journal, ESJ*, *14*(19), 181. https://doi.org/10.19044/esj.2018.v14n19p181
16. Perveen, S., Ahmed, M., & Begum, R. (2018). A Review on the Economic Instability and Derivative Market of Pakistan. *European Scientific Journal, ESJ*, *14*(22), 13. https://doi.org/10.19044/esj.2018.v14n22p13
17. Pym, A. (2015). Translating as risk management. *Journal of Pragmatics*, *85*, 67–80. https://doi.org/10.1016/j.pragma.2015.06.010
18. Ra'ed, D., & Taisir, M. (2015). Knowledge Management Strategies as Intermediary Variables Between IT- Business Strategic Alignment and Firm Performance. *European Scientific Journal, ESJ, March 2015 edition vol.11, No.7,* 25. http://eujournal.org/index.php/esj/article/view/5326/5152
19. Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, *89*, 201–218. https://doi.org/10.1016/j.ssci.2016.06.015

20. Torabi, S. A., Rezaei Soufi, H., & Sahebjamnia, N. (2014). A new framework for business impact analysis in business continuity management (with a case study). *Safety Science*, *68*, 309–323. https://doi.org/10.1016/j.ssci.2014.04.017
21. Tsiga, Z., Emes, M., & Smith, A. (2017). Implementation of a risk management simulation tool. *Procedia Computer Science*, *121*, 218–223. https://doi.org/10.1016/j.procs.2017.11.030
22. Wu, D. D., Chen, S.-H., & Olson, D. L. (2014). Business intelligence in risk management: Some recent progresses. *Information Sciences*, *256*, 1–7. https://doi.org/10.1016/j.ins.2013.10.008