ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse234952020.pdf
https://doi.org/10.30534/ijatcse/2020/234952020

Applying Preliminary Risk Assessment Method on Research Websites

Tarek Heggi[1], Nevien Moawad[2]
[1]Climate Change Information Center & Renewable Energy (CCICRE), Agricultural Research Center (ARC), Egypt, tarek.heggi@arc.sci.eg
[2]Climate Change Information Center & Renewable Energy (CCICRE), Agricultural Research Center (ARC), Egypt, nevienmoawad@arc.sci.eg

ABSTRACT
Research websites represents the objectives of the research entities such as preparing a community among researchers to improve the developing process for new researches activities, the engagement of different target users according to their interests, getting sources of funds for new projects, and other activities. From this perspective, applying assessment the websites to identify the risks that have bad impact on achieving its objectives are playing a vital role in maintaining and improving the performance of the website. Nowadays, the risk management usage has been increasing globally, and increasingly requires organizations to develop a policy to deal with high risk level in their plans, projects, and processes. The development of efficient processes for managing and analyzing risks that allow identifying a solution or plan to prevent risks is essential, thus, risk analysis aims at protecting the organization's human, material, and financial resources. A Prelimianary Risk Assessment Technique is used to evaluate the capabilities of the currently used Agricultural Research Center (ARC) website as an example for the research websites to identify, and analyze the risks and set the required suggesting recommendations on how to solve or minimize these risks. Results have shown, the main risks found through the ARC website were: power outage (PO), network subsystem failure (NSF), Attacking System Security (ASS) and Saftey System Failure (SSF), Failure in Usability of the ARC web site (FUWS), Failure in Supportive Entities, Failure in Supportive Processes, and Failure in Work Processes. The main recommendations suggesting having a maintenance contract and standrad operation procedure for power subsystem including UPS and gernerator, high availability solution for network equipment and internet connectivity, build procedures to handle emergency cases inside the ARC website such as ensure the good performance for accessing the ARC website as a daily action. Employees training and awareness considers as another solution to alleviate the failure in work process.

Key words: Risk Assessment Methodology, Website Accessibility, Website Usability, Website Relevance, Website Engagement.

1. INTRODUCTION

The ARC website represents a repository for the achievement for all research entities that are belonged to the ARC and research engine for the ARC researchers and their research activities in addition to other elements that show the ARC latest news and activities.

The purpose of this research paper is to assess the capabilities of the currently used ARC website based on applying a risk management approach. Risk management is a quick development field of study and there are several and varied aspects and descriptions of what risk management includes, how it should be conducted and what it is for. The use of efficient process for risk assessment that allow for the treatment and prevention of risks is essential, thus, it aims at protecting the organization's resources.

2. LITERATURE REVIEW

2.1 The Concept of Risk

A risk is the probability of something happening that will have an impact on objectives [1]. Woodruff [2] delimit the risk as the chance that someone or something that is valuated will be harmfully affected by the hazard while "hazard" is any vulnerable condition or potential source of an undesirable event with potential for harm or damage [3]. Moreover, a risk has been defined as a measure of the probability and severity of adverse effects [4].

2.2 Basic Concepts of Risk Assessment and Management

Risk assessment is an essential and systematic process for assessing the impact, occurrence and the consequences of human activities on systems with hazardous characteristics and constitutes a needful tool for the safety policy of a company. The process of risk assessment acts as a modification to improve risk understanding and so to encourage a process of proactive risk management [5].

A risk management process contains the core activities risk identification, risk analysis, risk evaluation, risk treatment, and risk monitoring [1]. The activities risk identification, risk analysis, and risk evaluation are usually referred to as risk assessment, while the activities risk treatment and risk

monitoring are referred to as risk control. In the risk identification phase risk items are identified. In the risk analysis phase the probability and impact of risk items and their risk exposure values are estimated. In the risk evaluation phase, the significance of risk is assessed based on the estimated risk disclosure values. In the risk treatment phase actions for obtaining a satisfactory situation are decided and executed. In the risk monitoring phase risks are tracked over time and their status is reported [6].

2.3 Classifications of Risks

Risk is classified into financial, operational, technological, economic, environmental, political, market, and social [7]. Financial risk is the exposure to contrary events that consume profit and in extreme circumstances situation bring about business collapse. The operational risk is the potential for loss due to failures of humans, processes, technology, and external dependencies [8]. Technological risk may be defined as events that would lead to insufficient, inappropriate, or mismanagement of investment in technology, in terms of manufacturing processes, product design and/or information management [7]. Economic risk is the influence of national macroeconomics on the performance of an individual business [7]. The environmental risk can be defined as, "the deterioration of bottom-line performance from: increased regulation on energy usage, eroded reputation, brand name and market share from an environmental incident, increased operating costs from the effects of global warming, higher fuel costs as natural resources are depleted and loss of market share to more environmentally 'savvy' competitors" [7]. Political risk is the uncertainty that stems, in whole or in part, from the exercise of power by governmental actors and the actions of non-governmental groups [9]. Market risk described as, "the exposure to a potential loss arising from diminishing sales or margins resulting from changes in market conditions" [7]. The social risk comes from changes in society that create changes in demand. This leads to new opportunities and may change businesses' responsiveness to demand and the characteristics of the workplace.

2.4 Classification of Risk Assessment Approaches

There are three approaches of risk assessment, namely qualitative, quantitative, and semi-quantitative risk assessment. Quantitative risk analysis uses hard metrics, such as dollar amounts, while qualitative risk analysis uses simple approximate values. Quantitative is more objective; qualitative is more subjective. Semi-quantitative risk assessment provides an intermediary level between the textual evaluation of qualitative risk assessment and quantitative risk assessment methods [10]

Quantitative risk analysis assigns the probability of the occurrence of identified hazards and determines their impact or consequence, usually resulting in a value such as an Annual Loss Expectancy or Annual Cost. Qualitative Risk Analysis, more akin to assessment or vulnerability analysis, concentrates less (or not at all) on probability and looks at threats, vulnerability, and consequences or controls [11].
Table 1 indicates the differences between qualitative, and quantitative approaches.

Table 1: Comparison between Quantitative and Qualitative Risk Approaches

qualitative	quantitative
A faster process	Very time intensive
Emphasizes descriptions	numerical results in nature
simple in relative terms	Used for cost benefit analysis
perceived values, not actual values	Can justify the procurement safeguards
Requires less training	Requires tracking the asset value

Most of the systems use qualitative risk assessment methods simply because it's usually faster to perform than quantitative methods. Semi-quantitative approach is suitable for specific cases that both qualitative and quantitative approaches are not suitable for them. In semi-quantitative approach in addition to numerical description is used in addition to textual description. An example of semi-quantitative approach is applying it on health exposure to risky chemical agents in a petrochemical plant [12].

2.5 Risk Assessment Controls

There are multiple control measures that can be used as indicated in [13]:

1- Elimination of hazards by changing products or technique or equivalent, if it cannot be eliminated the hazard, then go to second level of control,
2- Second level, to substitute or isolate or take engineering actions on the hazard, if it cannot be achieved, then go to third level of control,
3- Third level, to put administrative procedures and increase the awareness.

3. THE RISK MANAGEMENT METHODS

Risk Management methods may include three main phases [14]:

- Identification phase, in this first phase of the methodology, the possible specific causes of business risks are identified in a systematic manner, together with the range and possible effects. Those data are necessary to develop the processes of the methodologies. This requires an intimate knowledge of the organization, the market in which it operates, the legal, social, political and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives [15].
- Evaluation phase, risk evaluation therefore, is used to make decisions about the significance of risks to the organization and whether each specific risk should be accepted or treated [15].

- Hierarchization phase, which aims at ranking some results obtained in the two previous phases in order to put preponderant risks forward. The goal of this phase is to implement modifications or corrective actions on the most severe risk systems.

The phase of risk identification is essential, because the data of risk identification will be the input of the evaluation and/or hierarchization phases. To obtain the best results, it is necessary to make an identification phase in an exhaustive way.

A risk analysis methodology does not necessary contain these three phases. It can be constituted of only the following combinations:

- an identification phase,
- an identification and evaluation phases,
- Or an identification, evaluation and hierarchization phases.

There are various methods that have been developed to analyze the risk factors within any given project. For the purposes of this paper five methods are analyzed in detail, they are as follows:

- Preliminary Risk Analysis (PRA)
- BOEHM
- RISKIT
- Software Engineering Institute, Software Risk Evaluation (SEI-SRE)
- Software Engineering Risk Index Management (SERIM)

3.1 PRA

PRA is a technique for identifying hazards and a risk analysis that consists of identifying hazardous events, causes and consequences, and establishing control measures. In order to develop the PRA, the following steps should be done [16]:

- First, to describe the hazards and characterize them,
- Second, the causes and effects identified,
- Third, allow for the research and preparation of preventive or corrective actions and measurements for eventual failures detected,
- And at last, prioritizing actions depending on the characterization of the hazards, considering they must be mitigated as fast as they are hazardous.
- The main advantages of the PRA are: early identification and awareness on the potential hazards by the project team, and identification and/or the deployment of guidelines and criteria for the process development team to follow. As a result, the main hazards can be eliminated, minimized, or controlled right from the start [17].

3.2 BOEHM

The Boehm's method developed by Boehm a risk management method [18] that can be applied to almost any software related project. According to the Boehm's method, the practice of risk management involves two primary steps, each with three subsidiary steps.

The first step is the risk assessment involves risk identification, risk analysis, and risk prioritization:

- Risk identification: is the first step to successful risk management is to write down the risks and make them visible to all.
- Risk analysis: assesses the loss probability and loss magnitude for each identified risk item.
- Risk prioritization: produces a ranked ordering of the risk items identified and analyzed.

The second primary step, risk control, involves risk-management planning, risk resolution, and risk monitoring:

- Risk-management planning helps prepare you to address each risk item, including the coordination of the individual risk-item plans with each other and with the overall project plan.
- Risk resolution: produces a situation in which the risk items are eliminated or otherwise resolved.
- Risk monitoring: involves tracking the project ' s progress toward resolving risk items and taking corrective action where appropriate.

3.3 RISKIT

RISKIT was originally developed for software development projects, but it can be applied in many other areas, such as business planning, marketing and in technology related fields [19]. RISKIT follows seven different steps of implementation as follows:

1- Providing precise and unambiguous definitions for risks. In this step risk is defined as a possibility of loss, the loss itself, or any characteristic, object or action that is associated with that possibility.

2- Finding explicit definition of objectives, constraints and other drivers that influence the project.

3- Modelling and documenting risks qualitatively.

4- Using both ratio and ordinal scale risk ranking information to prioritize risks reliably.

5- Using the concept of utility loss to rank the loss associated with risk.

6- Different stakeholder perspectives are explicitly modelled in the RISKIT method.

7- Finally, The RISKIT method has an operational definition so that it can be applied easily and consistently.

3.4 SEI-SRE

The area of application is mainly in the US Department of defense IT projects; however, it can also be applied to large organizations IT projects [20]. The techniques used in the SEI-SRE method are identified as continuous activities through the life cycle of a project. These activities are identification, analysis, planning, tracking and control:

- In the identification activity, a taxonomy-based questionnaire (TBQ) is used to elicit as many risks as possible from the project team.
- The analysis activity is defined as the conversion of risk data into decision-making information.
- Planning is defined as the conversion of decision-making information into plans and actions; this includes planning both mitigating actions and

also the acquisition of further information concerning a risk, where more information is needed to inform subsequent decisions.

- During tracking, suitable metrics of overall project risk are identified and monitored. Trigger events are identified and mitigating actions are monitored.
- Control consists of correcting for deviations from planned actions; this may involve all the key elements from one through to seven.

3.5 SERIM

The SERIM method is a simple and flexible way to perform software risk management. It is particularly well suited for small manufacturers that may not be able to use more expensive and complex processes. SERIM process is as follows [21]:

- Identifies different risks for technical implementation, cost, and schedule.
- Predicts risks by software development phases.
- Provides a means for corrective action to reduce risks.
- Identifies the effectiveness of your software risk management activities.
- Measures the risk associated with your software product and process.
- Handles multiple projects for analyzing software risks

These five methods may be classified into two main groups according to the classifications presented before in section III, table 2 lists these classifications.

Table 2: Risk Management Methods

	Qualitative	***Quantitative***
Methods	PRA	SERIM
	BOEHM	
	RISKIT	
	SEI-SRE	

3. RISK MANAGEMENT METHODOLOGY

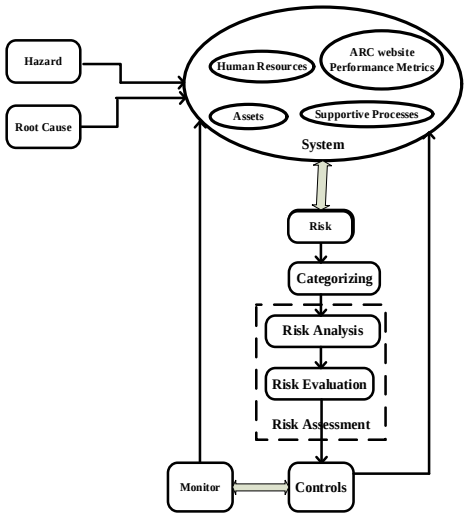

Figure 1: Risk Management Methodology

Figure 1 shows the components of the risk management methodology and it includes the system that is represents by the human resources who are responsible for operating the website, the network and other related activities. The ARC website developers, the performance metrics which include usability, engagement. and accessibility. The assets that include network, and server equipment. The hazards are represented in table 3:

Table 3: Hazards

General Hazard	**Abrev.**
Network subsystem Failure	NSF
Failure in Web Server	FWS
Power Outage	PO
Air Conditioner Failure	ACF
Attacking System Security	ASS
Safety System Failure	SSF
Documentation	Doc
Failure in Usability of the ARC web site	FUWS
Failure in Tracking Engagement parameters	FTEP
Failure in Accessibility parameters	FAP
Failure in work processes	FWP
Staff (Human Resources)	STF
Supportive entities	SUPP

The risk [22] may be defined more broadly as the probability of occurrence of an adverse outcome and the severity of the consequences if the outcome does occur.

Relying on [17][23][24] and other related references, we have developed our methodology to handle the risk management on the ARC website. The system that should be existed to operate the ARC website includes but not limited to:

- The assets that are used to host the ARC website including servers, network devices, and Internet connectivity.
- The ARC website metrics, which include usability, engagement, and accessibility.
- The human resources include the all department developer, network, and other.
- Supportive Processes, which represents all other entities that achieve part of the system components and operations such as purchases department.

4. RESULTS AND DISCUSSION

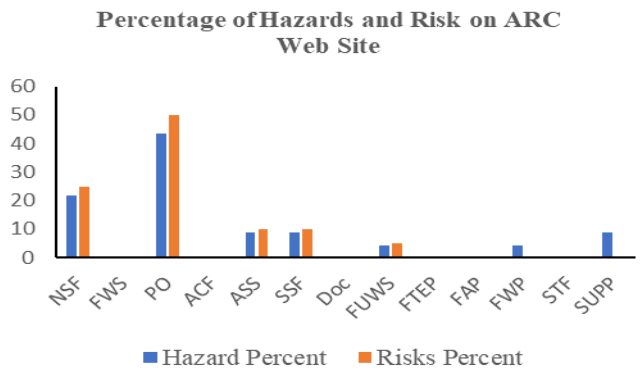

Figure 2: Risk Percentage on ARC Web Site

Figure 2 indicates the impact of hazards and risks by percents. First risk is the power outage (PO) represents 43.47 % of hazards and it represents 50 % of risks. PO hazards can be mitigated using two solutions:

1- Having a maintenace contract and Standard Operation Procedure (SOP) to ensure the correctness of the maintenance steps

2- Applying a high availiability solution will minimize the down time to very low duration.

Second risk is the network subsystem failure (NSF), which represents 21.7 % of hazards and it repesents 25 % of risks. The risk of NSF can be minimized through the using of

1- High availability solution for network equipment.

2- High aviailabiliy solution in Internet connectivity.

Also, lower cost solution can be applied to alleviate the effect of failure in NSF by using a maintenance contract for network equipment and Service Level Agreement (SLA) for Internet connectivity.

The third and fourth risks are equal in percent and they are Attacking System Security (ASS) and Saftey System Failure (SSF) have 8.7% of Hazards and 10 % of Risks. The Fifth risks are generated from Failure in Usability of the ARC web site (FUWS), which represents 4.3 % of hazards and it repesents 5 % of risks. The Failure in the incompletence of the task that user need to do. The possible causes of this hazard are:

1-the lack of well designed task structure

2-the lack of testing for network performance during accessing Web Site through Internet. This hazard can be alleivated by having sufficient time to determine the required information from users and apply the communication testing methods to ensure the good performance for accessing the ARC website.

The seventh hazards is the Failure in Supportive Processes, which represents 8.7 % of hazards. Failure in Supportive Processes can be alleviated by changing the procedures of purchasing o have a well determined timelines and how to handle emergency cases.

The eighth hazard is the Failure in Work Processes (FWP), represents 4.3% of hazards and it represents 0 % of risks. FWP hazards can be mitigated by setting procedures for reviewing project scope and goals.

5. CONCLUSION

One can conclude that amongst the capabilities of the currently used ARC website based on applying a risk management method, the main risks found were: power outage (PO), network subsystem failure (NSF), Attacking System Security (ASS) and Saftey System Failure (SSF), Failure in Usability of the ARC web site (FUWS), to add the sixth, Failure in Supportive Processes, and Failure in Work Processes. Its worth suggesting each risk solutions to enhance the work processes and the website capabilities.

The main sloutions suggestions concern having a maintenance contract and standrad operation procedure, high availability solution for network equipment and internet connectivity. Other recommendations to be applied is build procedures to handle emergency cases inside the ARC website such as ensure the good performance for accessing the ARC website as a daily action. Employees training and awareness considers as another solution to alleviate the failure in work process.

An important observation to be made is that the experience of the employees bring benefits for the development, operate, and maintenance of the ARC website, because the professional can evaluate, and perform solutions processes for the risks surveyed with more safety and punctual. Thus, risk management method aims at protecting the organization human, material, and financial resources.

ACKNOWLEDGEMENT

Thanks for ARC administrations who avail the needed resources to acompplish this paper.

REFERENCES

[1] Zou, Patrick XW, Ying Chen, and Tsz-Ying Chan. "Understanding and improving your risk management capability: Assessment model for construction organizations." Journal of Construction Engineering and Management 136.8 (2010): 854-863.

[2] Woodruff, J. M. (2005). Consequence and likelihood in risk estimation: a matter of balance in UK health and safety risk assessment practice. Safety Science, 43(5e6), 345-353.

[3] Reniers, G. L. L., Dullaert, W., Ale, B. J. M., & Soudan, K. (2005). Developing an external domino prevention framework: Hazwim. Journal of Loss Prevention in the Process Industries, 18, 127-138.

[4] Haimes, Y. Y. (2009). Risk modelling, assessment, and management (3rd ed.). A John Wiley & Sons Inc. Publication, ISBN 978-0-470-28237-3.

[5] van Duijne, F. H., Aken, D., & Schouten, E. G. (2008). Considerations in developing complete and quantified methods for risk assessment. Safety Science, 46(2), 245-254.

[6] Michael Felderer, Christian Haisjackl, Viktor Pekar, Ruth Breu. A Risk Assessment Framework for SoftwareTesting. Leveraging Applications of Formal Methods, Verification and Validation. Specialized Techniques and Applications: 6th International Symposium, ISoLA 2014, Imperial, Corfu, Greece, October 8-11, 2014, Proceedings, Part II.

[7] Khumpaisal, Sukulpat. (2011). A Classification of Risks in Real Estate Development Business. Journal of architectural and planning research. 8. 1-8.

[8] Peccia, T. (2001). Designing an Operational Risk Framework from a Bottom-Up Perspective. Mastering Risk Volume 2: Applications, Pearson Education Ltd, UK.

.[9] Zonis, M., & Wilkin, S. (2001). Driving Defensively Through a Minefield of Political Risk. Financial Times Mastering Risk Volume 1: Concepts, Pearson Education Ltd, UK.

[10] Fao.org. 2020. [online] Available at: <http://www.fao.org/3/i1134e/i1134e04.pdf> [Accessed 29 May 2020].
[11] James F. Broder, Eugene Tucker. Risk Analysis and the Security Survey (Fourth Edition), 2012.
[12] Beheshti, M. H., et al. "Semi-quantitative risk assessment of health exposure to hazardous chemical agents in a petrochemical plant." Journal of Occupational Health and Epidemiology 4.1 (2015): 1-8.
[13] Westernsydney.edu.au. 2020. [online] Available at: <https://www.westernsydney.edu.au/__data/assets/pdf_file/0020/12917/12917_Hazard_Identification,_Risk_Assessment_and_control_Procedure.pdf> [Accessed 30 May 2020].
[14] Jerome Tixier, Gilles Dusserre, Olivier Salvi, Didier Gaston. Review of 62 risk analysis methodologies of industrial plants. Journal of Loss Prevention in the Process Industries, Elsevier, 2002, 15 (4), pp.291-303.
[15] The institute of Risk Management. A Risk Management Standard Report, 2002.
[16] de Andrades, Silvana Alves, André Nagalli, and Ronaldo Luis dos Santos Izzo (2014). "Preliminary risk analysis in the operation of a sanitary landfill." *Electron. J. Geotech. Eng* 19 (2014): 3167-3177.
[17] Dumbravă, Vasile, and Vlăduț-Severian Iacob (2013).. "Using Probability–Impact Matrix in Analysis and Risk Assessment Projects." Descrierea CIP/Description of CIP–Biblioteca Națională a României Conferința Internațională Educație și Creativitate pentru o Societate Bazată pe Cunoaștere–ŞTIINȚE ECONOMICE (2013): 42.
[18] Boehm B. W, (1991) "Software Risk Management: Principles and Practices." IEEE Software, January 1991, pp. 32-42.
[19] Freimut, Bernd & Hartkopf, Susanne & Kaiser, Peter & Kontio, Jyrki & Kobitzsch, Werner. (2001). An industrial case study of implementing software risk management. Proceedings of the 8th European software engineering conference held jointly with 9th ACM SIGSOFT international symposium on Foundations of software engineering, Volume 26 (5) : 277-287.
[20] Stern R., Arias J.C. - Review of Risk Management Methods. (2011). Business Intelligence Journal - January, 2011 Vol.4 No.1 : 59-78.
[21] Karolak, D.W (1998) Software Engineering Risk Management: Finding Your Path through the Jungle. Prentice-Hall.
[22] North, D. Warner. "Limitations, definitions, principles and methods of risk analysis." Revue scientifique et technique-office international des epizooties 14.4 (1995): 913-924.
[23] Sami Hagi, Qing Tan, Rebeca Soler Costa. A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering, 2019, 8 (1.1), pp. 100-106.
[24] Mohamad Yusof Darus, Mohd Afham Omar, Mohd Farihan Mohamad, Zulhairi Seman, Norkhusahini Awang. Web Vulnerability Assessment Tool for Content Management System, 2020, 9(1.3), pp. 440-444