The European Proceedings of
Social & Behavioural Sciences
EpSBS

Future Academy ISSN: 2357-1330

http://dx.doi.org/10.15405/epsbs.2017.07.5

LF-TEEC 2017
Living the Future: International Conference on Technology, Engineering, Education & Computer

METHODS USED IN THE RISK MANAGEMENT PROCESS – A COMPARATIVE APPROACH

Bogdan Tiganoaia (a)*, Clementin Cercel (b)
*Corresponding author

(a) Politehnica University of Bucharest, Romania, bogdantiganoaia@gmail.com
(b) Politehnica University of Bucharest, Romania, clementin.cercell@gmail.com

Abstract

According to the Business Dictionary (Web Finance Inc., 2017), risk management is the process of identification, analysis, assessment, control and avoidance, minimization or elimination of unacceptable risks. In order to avoid risks, an organization should choose a suitable method for its risk management (it should include all types of risks). A risk is presented as the possibility of an event occurring at a certain period of time. The existence of risks can have a negative impact on the organizational achievement of its objectives. There are many types of risks that an organization can face such as human resources risks, operational risks, network security risks, IT risks and financial risks. To handle the risks, organizations can use a risk management approach that identifies, assesses, manages and controls potential negative events. Among other things, the goal of effective risk management is to ensure that each risk is identified, documented, prioritized, and mitigated whenever possible (The Institute of Internal Auditors, 2017). Since all organizations face risks, whether positive (i.e., opportunities) or negative (i.e., events that hinder company processes), the challenge for auditors is to know when risks will occur and the impact these will have on the organization (The Institute of Internal Auditors, 2017). This article presents an exploratory research based on a comparative study regarding the risk management methods in an organization. The risk management methods were identified and analysed in detail through a template. This comparative study is based on representative common criterions and data obtained from different specialized sources. The article concludes with some issues open for consideration among the practitioners in the field

Keywords: Organizational risks, risk management methods.

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

As per the International Standards Organization (ISO), risk relates to the uncertainty arising from any known or unknown sources. In order to manage the risk, it is useful to understand how the organization/ the system works. A system is said to be a set of tangible and intangible components working together to achieve a common goal (Bright Hub Inc, 2017). According to (E.N.I.S.A Technical Department, 2006), the management of risks consists of:

- Definition of the scope and framework for the management of risks;
- Assessment of the security risks;
- Treatment of security risks;
- Communication of risks ;
- Monitoring and reviewing;
- Acceptance of risks (the decision of accepting a risk by the top management).

There are a lot of methods / methodologies to manage the risk (all type of risks) in an organization, an analysis of these can be found in the chapters listed below.

Typically, risk management plans have the following objectives:

1. To eliminate negative situations/events.
2. To reduce risks to an acceptable level, if these risks cannot be removed. This implies that there will be a risk level the company can accept, making sure that optimal controls are in place to keep risks within an acceptable range - based on (The Institute of Internal Auditors, 2017).
3. To transfer the risks from a company to another one – for example using a third-party provider/vendor to install network equipment so that the provider/vendor is made responsible for the installation's failure or success; or to transfer risks by means of insurance – for example the insuring company assets for destruction or theft, for example fire damage or hurricane - based on (The Institute of Internal Auditors, 2017).

2. Problem Statement

There are a lot of general tools and methodologies used for risk management such as - based on (Clarizen Inc., 2017):

- Brainstorming;
- Delphi technique;
- Interviewing;
- Checklist analysis;
- Risk probability and impact assessment;
- Probability and impact matrix / Risk categorization;
- Quantitative risk analysis & modelling techniques;
- Expected Monetary Value analysis (EMV) ;
- Cost risk analysis;

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

But, in addition to these general methodologies, there are methods used for risk management with special characteristics which refer to:

- compatibility with the software tools (tools which support the method)
- consultancy support,
- target organization,
- geographical spread,
- certification possibility.

It is useful to have a descriptive view of these methods used in the risk management process in an organization. In the next sections, a comparative analysis of the risk management methods is presented, with the mention that this analysis is based on some certain criterions.

3. Research Questions

1. Which are the most commonly used methods for risk management in an organization?
2. Which are the main characteristics of each method used for risk management?
3. Which is the most suitable method of risk management taking into consideration the following criterions: compatibility with tools, consultancy support, skills needed to introduce/use/ maintain, target organization, geographical spread, certification possibility?

4. Purpose of the Study

The research is an exploratory study, having as the main scope, a comparative presentation of various methods used for risk management in an organization.

The main objectives of the research are listed down below:

- To present in a descriptive manner some methods used for risk management: Ebios, It-Grundschutz, Marion, Mehari, ISO 27001
- To undertake a comparative study regarding some risk management methods based on some criterions, such as: compatibility with tools, consultancy support, skills needed to introduce/use/maintain, target organization, geographical spread, certification possibility etc. This comparative presentation represents the main objective of the paper.
- To develop some conclusions (useful for organization's management) based on the research findings on a topic that is both timely and important, that is risk management in an organization.

5. Research Methods

The research methods and tools used in this paper consist of:

- Bibliographical research;
- Comparative analysis;
- Exploratory study;
- Descriptive approach;

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Every method has been analysed using a set of criterions: compatibility with tools, consultancy support, skills needed to introduce/use/maintain, target organization, geographical spread, certification possibility etc.

The descriptive approach represents the presentation of the main characteristics of each method.

6. Findings

6.1 The methods – a descriptive approach

It is useful to have a descriptive view of the above mentioned methods used in risk management process. This non-exhaustive study presents, based on some bibliographic sources (E.N.I.S.A, 2006) and the authors' experience, five methods.

6.1.1. Ebios - Expression des Besoins et Identification des Objectifs de Sécurité is a wide-spread method (a set of guides supports the software tool) for risk management. It originates from France, but now the method is managed by a club of experts from different countries. The method helps managers to reach a global and coherent vision, plus it is useful when it comes to supporting the process of decision making in an organization regarding its security policies, business continuity planning etc. EBIOS consists of 5 stages (Ţigănoaia, 2012):

- **Stage 1:** Context analysis, global business process dependency on the information system: perimeter definition, decomposition into information flows, etc;
- **Stage 2 and 3:** Threats and security necessities analysis;
- **Stage 4 and 5**: Risk analysis (it also includes the residual risks) and the proposals for increased security measures.

More information about the method in Tables 1-6.

6.1.2. It-Grundschutz – In order to implement an ISMS – Information Security Management System in an organization, IT- GRUNDSCHUTZ provides a method. The method consists of:

- generic recommendations regarding IT security;
- technical recommendations to obtain the optimal IT level for a specific field.

The IT security process suggested by IT-Grundschutz consists of the following steps (ENISA IT-Grundschutz, 2017):

- Initialization of the process:
- Definition of IT security goals and business environment;
- Establishment of an organizational structure for IT security;
- Provision of the necessary resources;
- Creation of the IT Security Concept:
- IT-Structure Analysis;
- Assessment of protection requirements;

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

- Modelling;
- IT Security Checks;
- Supplementary Security Analysis;
- Implementation planning and fulfilment;
- Maintenance, monitoring and improvement of the process;
- IT-Grundschutz Certification (optional).

IT-Grundschutz:

- provides a framework for IT security management;
- lists the relevant threats and required countermeasures - these elements can be adapted according to the needs of the organization.

More information about this method can be found in Tables from 1 to 6.

6.1.3. Marion – Methodology of Analysis of Computer Risks Directed by Levels

- Methodology of audit for estimating the level of IT security risks of an organization (for which have been used questionnaires);
- For the estimation of the security level there are used 27 indicators (each of them assigns a grade between 0 and 4) and it's categorized in 6 main domains;
- Level 3 is the level which is considered as "correct" for an organization;
- The objectives of MARION are:

- to estimate the security level of a company in comparison with level 3 – level considered as "correct";
- to compare the security level of the organization with other companies which have answered to the same questionnaire;

Finally, a more detailed risk analysis is needed in order to identify threats and vulnerabilities of a company.

Note: The CLUSIF does not sponsor this method anymore, as MARION has been replaced by MEHARI. However, MARION is still used by various companies (E.N.I.S.A. Marion, 2017). More information about this method can be found in Tables from 1 to 6.

6.1.4. Mehari 2010 – is a method that (ENISA Mehari, 2017):

- provides a complete risk management model compliant to ISO 27005 requirements;
- includes the classification of assets, the likelihood of the threats and it also measures the vulnerabilities through audit;
- analyzes a generic list of risk situations and provides seriousness levels for each scenario;
- bases its analysis on formulas and parameters;
- allows an optimal selection of corrective actions;
- can be considered also as an RA/RM tool by the automatic use of formulas.

More information about this method can be found in Tables from 1 to 6.

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

6.1.5. I.S.O. 27001 – This standard is dedicated to the process of certification. It enables the comparison of an Information Security Management System through a series of controls. This standard does not cover risk analysis or certification of the risk management (E.N.I.S.A. Inventory of Risk Management, 2017). ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). Like any other ISO management system standards, certification to ISO/IEC 27001 is possible but not mandatory. Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed (*Sennewald & Baillie, 2016*).

More information about the method can be found in Tables from 1 to 6.

6.2. The methods - A Comparative Approach

It is useful to have a comparative view of these methods based on some common criterions. Using a template, each method is analysed, the data is from (E.N.I.S.A Technical Department, 2006) and (E.N.I.S.A. Inventory of Risk Management, 2017). The comparison can be found below, tables from 1 to 6.

Table 01. Preliminary data

Method Name	Country Of Origin	Website / Links
EBIOS	France	http://www.ssi.gouv.fr http://ebios.cases-cc.org
IT-GRUNDSCHUTZ	Germany	http://www.bsi.de/gshb/index.htm http://www.bsi.de/english/gshb/index.htm
MARION	France	https://www.clusif.asso.fr/en/clusif/present/
MEHARI	France	https://clusif.fr/home-page-english/
I.S.O. 27001	International – I.S.O.	http://www.iso.org/iso/home.html

Table 02. Available in European languages, Price, Possibility of certification

Method name	Available in The Following European languages	Costs/Availability	Certification possibility
EBIOS	French, English, the German language, Spanish	No costs/Free	No
IT-GRUNDSCHUTZ	English, the German language	No costs/Free	Yes
MARION	French, English	Not free	No
MEHARI	French, English	No costs/Free	No
I.S.O. 27001	French, English	Not free	Yes

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Table 03. Target organizations

Method name	Gov. agencies	Large Org.	Commercial Org.	Non-commercial Org.
EBIOS	X	X	X	X
IT-GRUNDSCHUTZ	X	X	X	X
MARION		X		
MEHARI	X	X	X	X
I.S.O. 27001	X	X	X	

Table 04. M/T/O: Management - M, Operational - O, Technical - T; Geographical spread

Method name	Level of detail	Used in E.U. / Non E.U. / U.S.A.
EBIOS	M, O	Large – E.U. and non E.U.
IT-GRUNDSCHUTZ	M, O, T	Large - E.U. and non E.U
MARION	M, O	Used in France, Belgium, Luxemburg; Used in non E.U countries Switzerland, Canada (Quebec)
MEHARI	M, O, T	Used in EU member states, Used in non-EU countries, including SUA
I.S.O. 27001	M, O	Large – E.U. and non E.U.

Table 05. Skills needed to introduce / use / maintain; Consultancy support

Method name	Skills	Consultancy support
EBIOS	Standard/Standard/Standard	Yes
IT-GRUNDSCHUTZ	Standard/Standard/Standard	Yes
MARION	Basic / Standard / Basic	Yes
MEHARI	Standard/Standard/Standard	Yes
I.S.O. 27001	Specialist/Standard/Standard	Yes

Table 06. International standards, Compatibility with tools

Method Name	Conformity To International Standards	Tools Which Support The Method
EBIOS	I.S.O. 27001, 15408, 17799, 13335, 21827	Non-commercials, free
IT-GRUNDSCHUTZ	ISO/IEC 17799, ISO/IEC 27001	1. GSTOOL-free for public authorities, 2. BSI- GSTOOL 3. HiSolutions AG HiScout SME 4. Swiss Infosec AG -

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

		Baseline-Tool 5. WCK - PC-Checkheft
MARION	NO	MS. Excel
MEHARI	ISO/IEC IS 13335-1, ISO/IEC 27001, ISO/IEC 27005:2008	RISICARE
I.S.O. 27001	I.S.O./I.E.C. I.S. 17799	Commercials: wide range

7. Conclusion

It is useful to have a look at the methods used for identification, evaluation and treatment of risks. The paper presents, in a comparative manner, various methods used for risk management in an organization. The results can be used by both the academic and industrial sector. Industry demands more than just “talking about risks”, especially hazardous ones, where very large private investments are at stake and critical consequences are lurking (Oboni, 2013).

Instead of a conclusion, as a result of studying the international literature, the risk assessment process encompasses the following steps (Oboni, 2013):

- Defining the context and boundaries of the system;
- Describing the system in terms of elements and links;
- Identifying the hazards and fundamental failure modes;
- Evaluation of the probability of hazards and fundamental and compound failure modes occurring;
- Evaluation of potential targets and costs of failure;
- Determination of tolerable versus intolerable risks;
- Present Risk and Decision Making based on risk prioritization.

A risk can be acceptable for an organization, while the same risk can be unacceptable for another one. As future opened issues, the concepts of risk tolerance and interoperability of methods can be analysed.

Acknowledgments

This work has been funded by University Politehnica of Bucharest, through the “Excellence Research Grants” Program, UPB – GEX. Identifier: UPB–EXCELENȚĂ–2016, Contract number 11/30.09.2016.

http://dx.doi.org/10.15405/epsbs.2017.07.5
Corresponding Author: Bogdan Tiganoaia
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

References

Bright Hub Inc. (2017). *The Basics of Risk Management*, Retrieved from http://www.brighthubpm.com/risk-management/71742-the-basics-of-risk-management/

Clarizen Inc. (2017*). Risk Management - Useful Tools and Techniques*,. Retrieved from

https://success.clarizen.com/hc/en-us/community/posts/203996208-Risk-Management-Useful-Tools-and-Techniques

E.N.I.S.A (Technical Department). (2006). *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*, Retrieved from http://www.enisa.europa.eu

E.N.I.S.A. (2017). *Inventory of Risk Management / Risk Assessment Methods*, Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

E.N.I.S.A. (2017). *IT-Grundschutz*, Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html

E.N.I.S.A. (2017). *Marion*, Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_marion.html

E.N.I.S.A. (2017). *Mehari,* Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_mehari.html

E.N.I.S.A. (2017).*Inventory of Risk Management / Risk Assessment Methods and Tools*, Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

Oboni, F., Oboni, C., (2013). *What You Need to Know About Risk Management Methods*, Riskope International.

Sennewald, C. A., Baillie, C., (2016). Chapter 21 – International Security Standards, *Effective Security Management Sixth Edition,* (pp. 205–212).

The Institute of Internal Auditors. (2017. *)Understanding the Risk Management Process,*Retrieved from https://iaonline.theiia.org/understanding-the-risk-management-process

Ţigănoaia, B. (2012). *"*Comparative study regarding the methods used for security risk management*", Nic. Bal. La. For. Acad. Sci. Bull*., *XVII, No. 2* (34)*,* 149.

Web Finance Inc. (2017). *Business Dictionary,* Retrieved from http://www.businessdictionary.com/definition/risk-management.html