**MINISTRY OF EDUCATION AND RESEARCH**

**Technical University of Moldova**
**Faculty of Computers, Informatics and Microelectronics**
**Department of Software Engineering and Automatics**

**Admitted to defence**
**Department Head:**
**Ion Fiodorov, PhD, associate professor**

**_____**

**«____» _____ 20__**

# FACTOR ANALYSIS OF INFORMATION RISK (FAIR™) WHEN ASSESSING THE INFORMATION SECURITY

## Master Thesis

**Master Student:** **Inga Ignat, SI-201M**

**Supervisor:** **Rodica Bulai, university assistant**

**Chisinau, 2022**

# EXECUTIVE SUMMARY

The master thesis „Factor Analysis of Information Risk (FAIR™) when assessing the Information Security", developed at the Technical University of Moldova, Chisinau, presented by me, Inga Ignat, is written in English and contains 78 pages, 44 figures and 41 tables. The structure of the thesis includes: introduction, 4 chapters and conclusions.

The aim of the thesis is to assist top management in making correct and balanced decisions regarding information security risks and investments in information security measures by ensuring the consistency and quality of risk analysis results.

In order to achieve the purpose proposed, key features of a reliable information risk analysis methodology were analyzed and established, the structure and theoretical concept of the Factor Analysis of Information Risk approach (FAIR) was reviewed, the possibility of using this approach within ISO/IEC 27005 (Information Technology. Security Techniques. Information Security Risk Management) and NIST (Cyber Security Framework) was examined, as well as differences in the terminology used, and finally, several risk scenarios were analyzed with the application of this information risk analysis methodology to identify eventual problems and difficulties or, conversely, possible factors, which may simplify the risk analysis process. The concept was also elaborated and presented, which can be used for the development of the information risk analysis tool within enterprises, which have a serious attitude towards risks and financial decision-making.

During the application of this concept by analyzing the real risks in practice, it has been demonstrated, that the risk analysis becomes simpler and faster once certain input values were entered in the database. These values are part of some factors such as primary and secondary loss, and can easily be reused in different scenarios without consulting a subject matter expert opinion.

# REZUMAT

Teza de master „Analiza factorilor de risc informațional (FAIR™) la evaluarea securității informaționale” elaborată la Universitatea Tehnică a Moldovei, Chișinău, prezentată de către mine, Inga Ignat, este scrisă în limba engleză și conține 78 de pagini, 44 figuri și 41 tabele. Structura tezei include: introducerea, 4 capitole și concluzii.

Scopul lucrării este de a ajuta managementul de top în luarea deciziilor corecte și echilibrate legate de riscurile de securitate informațională și de investițiile în măsurile de securitate informațională prin asigurarea consistenței și calității rezultatelor analizei riscurilor.

Pentru a atinge scopul propus, s-au analizat și s-au stabilit caracteristici cheie ale unei metodologii fiabile de analiză a riscurilor informaționale, a fost revizuită structura și conceptul teoretic al abordării de analiză a factorilor riscului informațional (FAIR™), s-a analizat posibilitatea utilizării acestei abordări în cadrul ISO/IEC 27005 (Tehnologia informației. Tehnici de securitate. Managementul riscului securității informației) și NIST (Cadrul de Securitate Cibernetică), la fel și diferențele în terminologia utilizată, și, într-un final, s-au analizat câteva scenarii de risc cu aplicarea acestei metodologii de analiză a riscului informațional pentru identificarea eventualelor probleme și dificultăți sau, invers, eventualelor factori, care pot simplifica procesul de analiză a riscurilor. La fel s-a elaborat și s-a prezentat conceptul, ce poate fi utilizat pentru dezvoltarea instrumentului de analiză a riscului informațional în cadrul întreprinderilor, care manifestă o atitudine serioasă față de riscuri și luarea deciziilor financiare.

Pe parcursul aplicării acestui concept prin analiza riscurilor reale din practică, s-a demonstrat, că analiza riscurilor devine mai simplă și mai rapidă odată cu înregistrarea anumitor valori de intrare în bază de date. Aceste valori sunt părți componente ale anumitor factori (de exemplu a pierderilor primare și pierderilor secundare) și ușor pot fi reutilizate în diferite scenarii fără a se adresa către un expert în materie.

## CONTENTS

# INTRODUCTION

*Risk itself is simple. It's the complex world*
*that makes risk analysis so challenging.*
**Jack Freund**

In the overall context of risk management, it's important to understand that the business objective in performing risk assessments is to identify and estimate levels of exposure to the likelihood of loss, so that business managers and business owners can make informed business decisions about how to manage those risks of loss – either by accepting each risk, or by mitigating them by investing in appropriate measures, that are sufficient to lower the potential loss to an acceptable level, or by investing in external indemnity. Using risk assessment methodologies that provide the most objective, relevant, and consistent outcomes is therefore critical to enabling weighed decision-making.

Several challenges exist as a result of the current risk assessment methodology landscape. This includes:

a) Risk assessment results cannot reliably be compared, either between different organizations and scenarios or even amongst assessments that were performed in a single organization. So, risk posture comparisons and analyses of trends within and between industries are difficult, or sometimes even impossible. Also, tracking risk posture improvement within an organization becomes more challenging.
b) Management may not be able to differentiate more effective risk methodologies from less effective ones. As a result, the chosen risk assessment methodology may not provide management with the information they need.
c) Those developing risk assessment methodologies will continue to introduce variability into the landscape, aggravating the current situation.

Many risk assessment methodologies tend to focus on providing a step-by-step process for risk assessment without discussing how things should be measured, or at times even what the IT risk practitioner should be using to create measurement. But, if some critical aspects of the measurement and calculation process are not considered, even a good risk assessment methodology will provide poor results. Deep understanding of how the risk assessment should go about measuring, calculating, and expressing risk is critical to creating a logical and defensible assessment.

Current risk assessment approaches use either qualitative or quantitative measurement, estimation and risk expression. Ideally, a risk assessment methodology will be useful regardless of what kind of scale is chosen by the company. If quality information is available to the IT risk practitioner, the same risk assessment will produce similar results when both qualitative and quantitative assessments are performed by the IT risk practitioner. The decision to use one means of expression over another is going to be primarily

dependent on two factors: suitability within the organization and quality of available information.

All mentioned above emphasizes the importance and relevance of the topic under consideration. Thus, the main goal of the present master thesis is to help executives in taking good and weighed decisions related to information security risks and information security investments by ensuring consistency and quality of risk assessment results. The goal is achieved by reaching several objectives: Factor Analysis of Information Risk approach revision, the analysis of its practical use within ISO/IEC 27005 and NIST Frameworks and exploration of challenges that can be met using the above-mentioned approach based on examples.

The present thesis has the following structure:

First chapter – The key characteristics of a reliable risk assessment methodology – describes main traits of a good risk assessment methodology, that should be taken into consideration during methodology establishment within a company.

Second chapter – The structure and theoretical concepts of FAIR approach – contains the taxonomy description of the approach with brief explanation of each factor.

Third chapter – FAIR practical reconciliation with risk management frameworks – describes how this risk analysis method can be used within the companies with already established and approved frameworks like ISO/IEC 27005 and NIST. The chapter explains differences in terminology used and the place of FAIR in these frameworks.

The last chapter – Practical implementation of FAIR method – is the case study research using most common risk scenarios that aims to identify difficulties and challenges of the approach and to demonstrate that the approach can be easily used by the companies satisfying the main goal of risk assessment: to help executives in taking good and weighed decisions related to information security risks and information security investments.

The research methodologies used during thesis elaboration are theoretical analysis and case study.

# BIBLIOGRAPHY


1. THE OPEN GROUP. Risk Management – The Open Group Guide. Zaltbommel, Netherlands: Van Haren Publishing, 2011. 120 p. ISBN 978-90-8753-663-3.
2. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guide for Conducting Risk Assessments. Version 1. Approved on: 2012-09-17.
3. NICCS: NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, ©2018 [cited on 14.09.2021]. Available on: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#T.
4. INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Certified in Risk and Information Systems Control review manual 6th edition. ISACA, 2015. 207 p. ISBN 978-1-60420-504-6.
5. THE OPEN GROUP. The Open Group Standard. Risk Analysis (O-RA), Version 2.0. The Open Group, 2020. 46 p. ISBN 1-947754-65-2.
6. THE OPEN GROUP. Requirements for Risk Assessment Methodologies. Technical Guide. The Open Group, 2009. 18 p. ISBN 1-931624-78-X.
7. THE OPEN GROUP. The Open Group Standard. Risk Taxonomy (O-RT), Version 3.0. The Open Group, 2020. 32 p. ISBN 1-947754-66-9.
8. HUBBARD Douglas W., SEIERSEN Richard. Measuring and Managing Information Risk. A FAIR Approach. Hoboken, New Jersey, USA: John Wiley & Sons, Inc., 2016. 280 p. ISBN: 978-1-119-08529-4.
9. FREUND, Jack, JONES, Jack. Measuring and Managing Information Risk. A FAIR Approach. Oxford, UK: Butterworth-Heinemann, 2015. 408 p. ISBN: 978-0-12-420231-3
10. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. Approved on: 2013-09-05.
11. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. Approved on: 2018-06-10.
12. THE OPEN GROUP. Open FAIR - ISO/IEC 27005 Cookbook. Technical Guide. The Open Group, 2010. 44 p. ISBN 1-931624-87-9.
13. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Approved on: 2018-04-16.
14. THE OPEN GROUP. The Open FAIR – NIST Cybersecurity Framework Cookbook. The Open Group, 2016. 20 p. ISBN 1-937218-80-5.