MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software şi Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.

„___” _____ 2025

ANALIZA ŞI EVALUAREA RISCURILOR ASOCIATE TEHNOLOGIEI INFORMAȚIEI ÎN CADRUL MANAGEMENTULUI CONTINUITĂȚII AFACERII

Proiect de master

Student: _____ **Goliş Boris, TIA-221M**

Coordonator: _____ **Cojocaru Sergiu, lect. univ.**

Consultant: _____ **Cojocaru Svetlana, asist.univ.**

Chişinău, 2026

REZUMAT

Cuvinte-cheie: riscuri IT, continuitatea afacerii, managementul riscurilor, evaluarea riscurilor, matricea riscurilor, FMEA, OCTAVE, DAS Solutions, mitigare, reziliență organizațională.

Lucrarea „Evaluarea riscurilor IT în contextul continuității afacerii” analizează relația dintre riscurile tehnologice și capacitatea organizațiilor de a menține funcționarea proceselor critice în condiții de incident sau întrerupere operațională. Cercetarea este construită pe două direcții complementare: fundamentarea teoretică și metodologică a domeniului și aplicarea acestor repere într-un studiu de caz privind o organizație din domeniul IT.

Capitolul 1 prezintă fundamentele teoretice privind riscurile IT și continuitatea afacerii. Sunt analizate conceptele de risc, amenințare și vulnerabilitate, precum și relația dintre securitatea informațională și procesele de business. Capitolul tratează managementul continuității afacerii, planificarea recuperării în caz de dezastru, standardele și cadrele metodologice relevante și strategiile generale de tratament al riscurilor. De asemenea, este evidențiat impactul riscurilor IT asupra proceselor critice de business și asupra continuității organizaționale.

Capitolul 2 este dedicat metodelor și modelelor de evaluare a riscurilor. Sunt prezentate analiza calitativă și analiza cantitativă a riscurilor, utilizarea matricei probabilitate–impact, precum și metodele FMEA și OCTAVE. Capitolul evidențiază rolul instrumentelor analitice în clasificarea, evaluarea și prioritizarea riscurilor și subliniază utilitatea combinării mai multor metode pentru obținerea unei perspective complete asupra expunerii organizaționale.

Capitolul 3 dezvoltă studiul de caz privind evaluarea riscurilor IT într-o organizație. Lucrarea adoptă o abordare hibridă, utilizând drept ancoră factuală date publice despre compania DAS Solutions și completându-le prin modelarea unui context operațional realist. Sunt prezentate organizația analizată, activele IT critice, procesele de business, corelarea acestora, riscurile potențiale identificate și clasificarea lor în funcție de impactul asupra businessului. Ulterior, riscurile sunt evaluate și prioritizate, fiind evidențiate acele scenarii care pot afecta în mod semnificativ continuitatea activității.

Capitolul 4 formulează strategiile de mitigare și recomandările. Riscurile prioritare identificate sunt corelate cu măsuri tehnice, organizaționale și strategice, precum backupul și recuperarea datelor, redundanța infrastructurală, controlul accesului, monitorizarea continuă, instruirea personalului, auditul periodic și dezvoltarea planurilor de continuitate și recuperare. Capitolul evidențiază faptul că managementul riscurilor IT trebuie integrat în guvernanța organizațională și corelat cu obiectivele de business pentru a susține reziliența pe termen lung.

Lucrarea integrează în total 2 formule, 13 figuri și 20 de tabele.

ABSTRACT

Keywords: IT risks, business continuity, risk management, risk assessment, risk matrix, FMEA, OCTAVE, DAS Solutions, mitigation, organizational resilience.

The thesis “IT Risk Assessment in the Context of Business Continuity” examines the relationship between technological risks and the ability of organizations to maintain critical processes during incidents or operational disruptions. The research is built on two complementary directions: the theoretical and methodological foundation of the field and the practical application of these concepts within a case study involving an IT organization.

Chapter 1 presents the theoretical foundations of IT risks and business continuity. It analyzes the concepts of risk, threat, and vulnerability, as well as the relationship between information security and business processes. The chapter addresses business continuity management, disaster recovery planning, relevant standards and methodological frameworks, and general risk treatment strategies. It also highlights the impact of IT risks on critical business processes and organizational continuity.

Chapter 2 is devoted to risk assessment methods and models. It presents qualitative and quantitative risk analysis, the use of the probability–impact matrix, and the FMEA and OCTAVE methods. The chapter emphasizes the role of analytical instruments in risk classification, evaluation, and prioritization, and underlines the value of combining multiple methods to obtain a comprehensive view of organizational exposure.

Chapter 3 develops the case study on IT risk assessment in an organization. The thesis adopts a hybrid approach, using publicly available data on DAS Solutions as a factual anchor and complementing them with the modeling of a realistic operational context. The analyzed organization, critical IT assets, business processes, their interdependencies, the identified potential risks, and their classification according to business impact are presented. Subsequently, these risks are evaluated and prioritized, highlighting the scenarios that may significantly affect operational continuity.

Chapter 4 formulates mitigation strategies and recommendations. The prioritized risks are correlated with technical, organizational, and strategic measures such as data backup and recovery, infrastructural redundancy, access control, continuous monitoring, staff training, periodic auditing, and the development of business continuity and disaster recovery plans. The chapter shows that IT risk management must be integrated into organizational governance and aligned with business objectives in order to support long-term resilience.

The thesis integrates 2 formulas, 13 figures and 20 tables.

CUPRINS

LISTĂ DE ABREVIERI

- **ALE** – Annual Loss Expectancy;
- **ARO** – Annual Rate of Occurrence;
- **AV** – Asset Value;
- **BCM** – Business Continuity Management;
- **BCP** – Business Continuity Plan;
- **BIA** – Business Impact Analysis;
- **COBIT** – Control Objectives for Information and Related Technologies;
- **CSF** – Cybersecurity Framework;
- **DAS** – DAS Solutions;
- **DRP** – Disaster Recovery Plan / Disaster Recovery Planning;
- **EDR** – Endpoint Detection and Response;
- **EF** – Exposure Factor;
- **FMEA** – Failure Mode and Effects Analysis;
- **FMECA** – Failure Mode, Effects and Criticality Analysis;
- **GRC** – Governance, Risk and Compliance;
- **IDS** – Intrusion Detection System;
- **IEC** – International Electrotechnical Commission;
- **ISO** – International Organization for Standardization;
- **IT** – Information Technology;
- **MFA** – Multi-Factor Authentication;
- **NIST** – National Institute of Standards and Technology;
- **OCTAVE** – Operationally Critical Threat, Asset and Vulnerability Evaluation;
- **RMF** – Risk Management Framework;
- **RPN** – Risk Priority Number;
- **SIEM** – Security Information and Event Management;
- **SLA** – Service Level Agreement;
- **SLE** – Single Loss Expectancy.

INTRODUCERE

În contextul transformării digitale accelerate, organizațiile contemporane își desfășoară activitatea într-un mediu operațional din ce în ce mai dependent de infrastructura IT, de date și de procese informatizate. Sistemele informaționale nu mai reprezintă doar un suport tehnologic auxiliar, ci constituie o componentă esențială a funcționării organizaționale, influențând direct eficiența operațională, relația cu clienții, gestionarea resurselor și capacitatea de adaptare la schimbările mediului economic. Pe măsură ce organizațiile devin tot mai digitalizate, crește și expunerea la riscuri IT, iar efectele incidentelor tehnologice pot depăși sfera strict tehnică, afectând procesele critice de business și continuitatea activității.

Relevanța temei este determinată de faptul că riscurile IT trebuie abordate astăzi nu doar ca probleme de securitate informatică, ci ca factori strategici care pot influența stabilitatea, performanța și reziliența organizațională. Atacurile cibernetice, defecțiunile infrastructurii, pierderea datelor, erorile umane sau dependența excesivă de servicii externe pot genera întreruperi semnificative ale activității și pot afecta imaginea, încrederea și sustenabilitatea organizațiilor. În acest context, evaluarea riscurilor IT în raport cu continuitatea afacerii devine o direcție importantă de cercetare, orientată spre identificarea vulnerabilităților, analiza impactului și formularea unor strategii de mitigare capabile să reducă expunerea la incidente.

Lucrarea de față pornește de la premisa că managementul riscurilor IT trebuie integrat în mecanismele de guvernanță și continuitate ale organizației. În acest sens, cercetarea urmărește să evidențieze relația dintre riscurile tehnologice și procesele critice de business, precum și modul în care organizațiile pot utiliza metode, modele și standarde consacrate pentru a evalua și trata aceste riscuri într-o manieră sistematică. Demersul este relevant atât din perspectivă teoretică, prin clarificarea conceptelor și a cadrelor metodologice, cât și din perspectivă aplicativă, prin dezvoltarea unui studiu de caz hibrid și a unui set de recomandări concrete pentru management.

Scopul cercetării constă în evaluarea sistematică a riscurilor IT care pot influența continuitatea afacerii și în elaborarea unui cadru coerent de strategii de mitigare și recomandări adaptate contextului organizațional. Pentru atingerea acestui scop au fost formulate obiective care vizează: definirea și analiza conceptelor fundamentale privind riscurile IT și continuitatea afacerii; examinarea standardelor și cadrelor metodologice relevante; analiza metodelor calitative, cantitative și hibride de evaluare; identificarea riscurilor potențiale într-un context organizațional realist; evaluarea și prioritizarea acestora; formularea unor strategii de tratament și a unor recomandări strategice pentru management.

Din punct de vedere metodologic, lucrarea combină analiza teoretică a literaturii de specialitate cu abordarea aplicativă specifică studiilor de caz.

Prima parte a lucrării oferă fundamentul conceptual necesar înțelegerii riscurilor IT și a legăturii acestora cu continuitatea afacerii, prin raportare la standarde și cadre metodologice precum ISO 31000, ISO/IEC 27005, ISO 22301, NIST RMF, COBIT, FMEA și OCTAVE. A doua parte valorifică aceste repere metodologice într-un studiu de caz privind o organizație din domeniul IT, construit în manieră hibridă pornind de la date publice disponibile despre compania DAS Solutions și completat cu modelarea unui context operațional realist, pentru a permite analiza activelor, a proceselor critice, a riscurilor potențiale și a strategiilor de mitigare.

Structura lucrării reflectă această logică graduală. Capitolul 1 este dedicat fundamentelor teoretice privind riscurile IT și continuitatea afacerii. Sunt analizate conceptele de risc, amenințare și vulnerabilitate, relația dintre securitatea informațională și procesele de business, precum și rolul continuității afacerii și al managementului situațiilor de criză. De asemenea, sunt prezentate standardele și cadrele metodologice relevante pentru managementul riscurilor IT și sunt discutate strategiile generale de tratament și impactul riscurilor asupra proceselor critice de business.

Valoarea lucrării este dată de combinarea dimensiunii teoretice cu cea aplicativă și de orientarea clară spre continuitatea afacerii. Cercetarea propune o perspectivă în care evaluarea riscurilor IT nu este tratată exclusiv ca exercițiu de securitate informatică, ci ca instrument de analiză managerială și de sprijin pentru deciziile strategice. Prin structurarea riscurilor în raport cu procesele critice, prin utilizarea unui studiu de caz hibrid și prin formularea unor recomandări corelate cu specificul unei organizații IT, lucrarea contribuie la dezvoltarea unui model coerent de analiză și tratament al riscurilor în contextul continuității afacerii.

BIBLIOGRAFIE

[1] STALLINGS, W.; BROWN, L. *Computer Security: Principles and Practice*. Pearson, 2018. ISBN 978-0134794105.

[2] WHITMAN, M.; MATTORD, H. *Principles of Information Security*. Cengage Learning, 2017. ISBN 978-1305508200.

[3] PELTIER, T. *Information Security Risk Analysis*. CRC Press, 2016. ISBN 978-1498745533.

[4] ANDERSON, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. ISBN 978-1119642787.

[5] HERBAN, I.; O'BRIEN, J. *Business Continuity Management*. Rothstein Publishing, 2017. ISBN 978-1944480105.

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 22301: Security and Resilience – Business Continuity Management Systems*. ISO, 2019. ISBN 978-0580959721.

[7] SNEDAKER, S. *Business Continuity and Disaster Recovery Planning for IT Professionals*. Syngress, 2013. ISBN 978-0124114517.

[8] WALLACE, M.; WEBBER, L. *The Disaster Recovery Handbook*. AMACOM, 2017. ISBN 978-0814438763.

[9] HOPKIN, P. *Fundamentals of Risk Management*. Kogan Page, 2018. ISBN 978-0749483074.

[10] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 31000: Risk Management – Guidelines*. ISO, 2018. ISBN 978-9264277153.

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27005: Information Security Risk Management*. ISO, 2018. ISBN 978-0738154732.

[12] BSI GROUP. *ISO 22301 Business Continuity Management Systems – Guidance and Implementation*. BSI, 2019. ISBN 978-1785759840.

[13] NIST. *Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2)*. National Institute of Standards and Technology, 2018.

[14] ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2019. ISBN 978-1604207644.

[15] JESTON, J.; NELIS, J. *Business Process Management: Practical Guidelines to Successful Implementations*. Routledge, 2014. ISBN 978-0415834058.

[16] STONEBURNER, G.; GOOGINS, A.; FERINGA, A. *Risk Management Guide for Information Technology Systems*. NIST Special Publication 800-30, 2012.

[17] SHMUELI, G.; BRUCE, P.; PATEL, N. *Data Mining for Business Analytics*. Wiley, 2017. ISBN 978-1118879368.

[18] HALL, J. *Information Technology Auditing and Assurance*. Cengage Learning, 2015. ISBN 978-

1285051529.
[19] HILLSON, D. *Practical Project Risk Management*. Management Concepts Press, 2016. ISBN 978-1604270921.
[20] HAIMES, Y. *Risk Modeling, Assessment, and Management*. Wiley, 2015. ISBN 978-1119017981.
[21] BOTHAMLEY, M. *Business Continuity Planning*. IT Governance Publishing, 2018. ISBN 978-1849283274.
[22] SHEFFI, Y. *The Resilient Enterprise*. MIT Press, 2007. ISBN 978-0262195850.
[23] PARSONS, G.; OJA, D. *New Perspectives on Computer Concepts*. Cengage, 2016. ISBN 978-1305657458.
[24] LINKOV, I.; PALMER, J. *Resilience and Risk: Methods and Application*. Springer, 2019. ISBN 978-9402411286.
[25] ZAMBON, E.; AIME, M.; ETALLE, S. Model-based qualitative risk assessment for availability of IT infrastructures. *Software and Systems Modeling*, 2011. https://link.springer.com/article/10.1007/s10270-010-0166-8
[26] CHANDRA, N. A.; et al. Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools. *Risks*, 2022, 10(8), 165. https://www.mdpi.com/2227-9091/10/8/165
[27] ARDI, S.; et al. A Case Study of Introducing Security Risk Assessment in Requirements Engineering in a Large Organization. *SN Computer Science*, 2023. https://link.springer.com/article/10.1007/s42979-023-01968-x
[28] HOPKIN, P. *Fundamentals of Risk Management*. Kogan Page, 2018.
[29] STONEBURNER, G.; GOOGINS, A.; FERINGA, A. *Risk Management Guide for Information Technology Systems (NIST SP 800-30)*. NIST, 2012.
[30] PELTIER, T. *Information Security Risk Analysis*. CRC Press, 2016.
[31] SHMUELI, G.; BRUCE, P.; PATEL, N. *Data Mining for Business Analytics*. Wiley, 2017.
[32] HAIMES, Y. *Risk Modeling, Assessment, and Management*. Wiley, 2015.
[33] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 31000: Risk Management –Guidelines*. https://www.iso.org/standard/65694.html
[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27005: Information Security Risk Management*. https://www.iso.org/standard/75281.html
[35] HOPKIN, P. *Fundamentals of Risk Management*. https://www.koganpage.com/product/fundamentals-of-risk-management-9780749483074
[36] IEC 60812:2018 – *Failure modes and effects analysis (FMEA and FMECA)*. Link în citare.
[37] AIAG & VDA – *FMEA Handbook*.
[38] BOUZIDI, M.; AMRO, A.; DALVEREN, Y.; CHEIKH, F. A.; DERAWI, M. *LPWAN Cyber Security Risk Analysis: Building a Secure IQRF Solution*. *Sensors*, 2023.

[39] BOGNÁR, F. – *Case Study on a Potential Application of Failure Mode and Effects Analysis in Assessing Compliance Risks*. *Risks*, 2021.

[40] MIN, S.; JANG, H. – *Case Study of Expected Loss Failure Mode and Effect Analysis Model Based on Maintenance Data*. *Applied Sciences*, 2021.

[41] ALBERTS, C.; DOROFEE, A. *OCTAVE Method Implementation Guide* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

[42] CARALLI, R.; STEVENS, J.; YOUNG, L.; WILSON, W. *Introducing OCTAVE Allegro* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8417

[43] ISO 31000: Risk Management – Guidelines https://www.iso.org/standard/65694.html

[44] NIST SP 800-30 – Risk Management Guide for Information Technology Systems https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[45] Infodebit, „DAS Solutions SRL – date companie", disponibil online: https://www.infodebit.md/ro/company/1007600035160

[46] Yin, R.K., Case Study Research and Applications: Design and Methods, SAGE Publications, 2018

[47] NIST, Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev.1), disponibil online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906210

[48] NIST, Computer Security Incident Handling Guide (SP 800-61 Rev.2), disponibil online: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[49] Medvedev, B., „Risk Management Cycle", disponibil online: https://www.researchgate.net/figure/Risk-management-cycle_fig1_319998926

[50] Goztepe, K., „Defense in Depth Architecture", disponibil online: https://www.researchgate.net/figure/Layers-of-defense-in-depth-architecture_fig1_274733863

[51] NIST, The NIST Cybersecurity Framework (CSF) 2.0, 2024, disponibil online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[52] Vicente, P., Mira da Silva, M., A Conceptual Model for Integrated Governance, Risk and Compliance, 2011, disponibil online: https://www.researchgate.net/figure/Integrated-GRC-Conceptual-Model_fig5_220921351

.