Jūlija Saveļjeva

Digital trust impact on third-party risks of an organisation

Summary of the Doctoral Thesis

Discipline: Social Sciences
Sub-Discipline: Economics and Business

Research Supervisor
Dr.oec., prof. Tatjana Volkova

Riga 2026

Saveljeva, J. (2026). Digital trust impact on third-party risks of an organisation. Summary of the Doctoral Dissertation, Riga, 124 pp. Published in accordance with the resolution confirmed by the RISEBA Promotion Council meeting as of 8 May 2026; No. 26/10-3.1/3.

This doctoral thesis was carried out at the RISEBA University of Applied Sciences and the BA School of Business and Finance of the University of Latvia (UL) from February 2023 to May 2026. The doctoral thesis is written in English. It consists of an introduction, three main chapters, conclusions and recommendations, a list of bibliographic references, and seven annexes. It has a total volume of 309 pages. The list of bibliographic references contains 261 literature sources.

SCIENTIFIC SUPERVISOR:

Dr.oec.Tatjana Volkova, Professor, BA School of Business and Finance of the University of Latvia (Latvia)

REVIEWERS:

1. Dr. sc. administr. Iveta Ludviga, Professor, RISEBA University of Applied Sciences (Latvia)
2. Dr. oec. Piotr Grzegorz Pietrzak, Assistant Professor, Warsaw University of Life Sciences (Poland)
3. Dr. sc. ing. Oksana Ņikiforova, Professor, Riga Technical University (Latvia)

The doctoral thesis will be defended at the public session of the Promotion Council of Economics and Business, RISEBA University of Applied Sciences, at 15:00 on 17 September 2026 in Meža Street 3, Riga.

The doctoral thesis and summary are available at the RISEBA University of Applied Sciences Library, Meža Street 3, Riga. The doctoral thesis was accepted for the commencement of the scientific degree Doctor of Science (PhD) in Social Sciences by the Promotion Council of the RISEBA University of Applied Sciences on 8 May 2026.

Chairman of the Promotion Council: Dr. oec. Andrejs Čirjevskis, Professor
Secretary of the Promotion Council: Dr. hab. oec. Vulfs Kozlinskis, Professor Emeritus

CONFIRMATION: I herewith confirm that I am the author of this doctoral thesis, which was submitted to the Promotion Council of RISEBA University of Applied Sciences for review to obtain the Doctor of Science (PhD) degree in Social Sciences. This doctoral thesis has not been submitted to any other university in order to receive a scientific degree.

Jūlija Saveļjeva 15.07.2026

To submit reviews, please contact RISEBA, Meža Street 3, Riga, LV-1048, Latvia. E-mail: riseba@riseba.lv. Phone: +371 26465351; +371 67500265.

© Jūlija Saveļjeva, 2026
© BA School of Business and Finance of the University of Latvia, 2026
© RISEBA University of Applied Sciences, 2026

ISBN 978-9984-705-75-0

Acknowledgements

There is a saying that “it takes a village to raise a child”, and I can very much relate this to the PhD journey. Indeed, it takes a whole faculty, sometimes even more than one, family, the professional community, and work colleagues to raise a new PhD. While gaining this degree and working on this thesis, I felt support from all layers and sides of my surroundings.

I am endlessly grateful to my supervisor, Dr. oec. Professor Tatjana Volkova, for empowering me to start this journey in the middle of 2022 and for making me believe that I could go through this phase and earn my PhD degree. It was a challenging journey that sometimes took me far beyond my comfort zone and perceived capabilities, resulting in exponential academic growth. At each small step and in each period of this journey, my supervisor was by my side, ready to support, help, challenge, and motivate me when needed. I definitely cannot imagine going through this journey without her.

I would like to thank my colleague, Dr. sc. Irmantas Aleliūnas, for supporting me and brainstorming with me on topic selection when I was stuck finding the exact topic for my study that would be both academically valuable and practically relevant to the professional world.

Throughout this journey, I had the pleasure of meeting many brilliant people in academia who, in one way or another, contributed to my development as a researcher, and it would be impossible to name them all.

The whole faculty of the joint doctoral programme of BA School of Business and Finance, the University of Latvia, and RISEBA did a tremendous job in forming my critical academic thinking, raising me as a researcher, and setting high standards, so that I now feel confident in the international scientific environment and in representing my research at international conferences. I am especially grateful to Dr. hab. oec., Professor Emeritus Vulfs Kozlinskis, for making me think more widely and understand the meaning of scientific discussion and the development of theoretical novelty.

I would like to express my gratitude to Dr. oec., Professor Līga Peiseniece and Dr. oec., Assoc. Professor Andris Fomins for guiding me through the programme and supporting me in obtaining the PhD grant No. 5.2.1.1.i.0/2/24/I/CFLA/007, “Internal and External Consolidation of the University of Latvia”. The value of this grant support cannot be underestimated, as it allowed me to share my research with a wider scientific community and significantly improve as a researcher while developing this thesis.

Likewise, participation in the scientific project “CyberSustain” helped me improve my research and presentation skills, broaden my scientific interests and expand my scientific community. I would like to separately thank Dr. sc., Assoc. Professor Inga Uvarova for supporting me at every stage of my PhD research and motivating me to move beyond my capacity.

I would also like to thank my fellow doctoral students and colleagues with whom I shared this PhD journey. I am especially grateful to Dr. sc. Jekaterina Novicka for her belief in me and recognition of my skills, sometimes even more than I believed in myself. I would like to thank Eldar Mardanov for showing a great example of participation in conferences and the creation of publications, motivating me to keep up and do more. I thank Dmitrii Gimmelberg for allowing me to look at the research process from another angle and for encouraging me to broaden my research horizons. I also thank Sandra Starke for sharing this PhD journey with me and supporting me along the way.

Separately, I would like to acknowledge the support of my work colleagues in SEB across all three Baltic states, who cheered me up throughout this journey. They also helped with empirical data collection by personally recruiting respondents from the Baltic banking industry and forwarding my data-gathering request to various financial associations and groups across the Baltics. I would like to separately thank my manager, Dr. Ramūnas Bičuilaitis, for understanding the complexity of this journey and supporting me at each step necessary for obtaining the degree.

I am grateful to the reviewers of this thesis, Dr. sc. administr., Professor Iveta Ludviga, Dr. oec. Piotr Grzegorz Pietrzak, Assistant Professor, and Dr. sc. ing., Professor Oksana Ņikiforova, for providing valuable feedback and their assessment of the conducted research.

Finally, I must thank my family for being by my side, supporting my decision to pursue this degree from day one, and never having any doubt that this day would come. This was a challenging journey for my husband, Vadims Saveļjevs, and our young children, Zlata and Agata, whose mother spent long evenings and weekends working on the research and travelling abroad to share the results with a wider scientific community. I have never heard any words from them other than full commitment and support. Therefore, this degree has become a joint asset of our family.

The support and encouragement of my mother, Diāna Jablonska, helped me move forward. I also know that my father, Vjačeslavs Šuļgins, was endlessly proud of my decision to aim high and start my PhD journey. Unfortunately, he passed away before the first noticeable research results appeared. I know that he was sure it could not have happened otherwise, and this degree, in a sense, is also devoted to his memory.

Table of Contents

LIST OF ABBREVIATIONS USED IN THE SUMMARY 6

INTRODUCTION 7

CHAPTER 1 SUMMARY: THE RELATIONSHIP BETWEEN DIGITAL TRUST AND THIRD-PARTY RISKS 16

1.1. The essence of digital trust and its characteristics 16
1.2. Foundations of Trust in Risk Management 21
1.3.The third-party risk management and its frameworks 24
1.4. Hypotheses and Research Model 27
1.5. Research Design and Methodology 29

CHAPTER 2 SUMMARY: EVALUATION OF THIRD-PARTY RISK MANAGEMENT IN THE FINANCIAL SECTOR 32

2.1. Characteristics of the Baltic banking industry 32
2.2. Third-party risk management challenges in the Banking industry 32
2.3. Digital trust impact on third-party risks of Baltic banks 33

CHAPTER 3 SUMMARY: QUALITATIVE INSIGHTS ON DIGITAL TRUST AND THIRD-PARTY RISKS: FINDINGS AND RECOMMENDATIONS 44

3.1.Third-party risk category findings and tests of the hypotheses 45
3.2.Capability-driven digital trust framework for enhanced third-party risk management 47
3.3 Future state of ICT third-party risk management in the Baltic banking industry . 50

CONCLUSIONS 52

RECOMMENDATIONS 54

FINAL REMARKS 56

BIBLIOGRAPHY USED IN THE SUMMARY 113

List of Abbreviations Used in the Summary

AML – Anti-Money Laundering
B2B – Business-to-business
CSR - Corporate social responsibility
DORA – Digital Operational Resilience Act
DT – Digital trust
EBA - European Banking Authority
ESG - Environmental, Social, and Governance factors
EU – European Union
ICT – Information and Communication Technology
PLS-SEM - Partial Least Squares Structural Equation Modelling
SEM - Structural Equation Modelling
SLR - Systematic literature review
TPRM – Third-party risk management
US - United States

Introduction

Topicality of the research

With the financial sector shifting towards digital transformation, digital trust is becoming increasingly relevant due to its role in ensuring the safety, confidentiality, and reliability of technological systems. This reflects the growing necessity for secure digital interactions and data privacy in a rapidly evolving technological landscape. This trend is also evident in scientific literature. According to information from the Scopus database (Elsevier 2025), the number of articles and conference papers featuring the keyword “digital trust” in their title, abstract, or keywords has significantly risen from one or two per year until 2017 to 121 in 2025.

At the same time, the concept of digital trust appears prominently in professional literature as a new approach to assessing the trustworthiness of digital technologies (World Economic Forum 2024; PwC 2024; ISACA 2024; Deloitte 2024a). It highlights the relevance of “digital trust”, which is still developing in scientific literature and varies according to context and sector (Pietrzak and Takala 2021). This emphasises the need for a validated definition and further research to identify additional characteristics of the digital trust concept. Moreover, trustworthiness has been recognised as a critical factor for collaboration with service providers (Urbano et al. 2013). Yet, the idea of “digital trustworthiness” has to be explored in the scientific literature. Although researchers acknowledge a conceptual distinction between traditional interpersonal trust and digital trust in technology-mediated environments, theoretical consolidation remains limited (Chaudhuri 2021; Zhghenti and Chkareuli 2021). Previous research also highlights the absence of consensus regarding the core characteristics of digital trust (Papic et al. 2022).

Simultaneously, the Digital Operational Resilience Act (DORA), which took effect on 17 January 2025 and applies to the entire European financial sector, requires a comprehensive approach to various third-party risks associated with information and communication technology (ICT) service providers (European Commission 2022b). Consequently, financial institutions must prioritise the management of third-party ICT service risks. While adopting ICT third-party risk management is crucial for ensuring effective oversight and addressing emerging technological risks (Giacchero and Moretti 2021), historically, organisations assessed third-party risks within a limited context (Deloitte 2024b).

The interest in “third-party risk” and “supplier risk” (terms often used interchangeably in scientific and professional literature) has steadily increased since 2007, according to the Scopus database (Elsevier 2025), with a notable spike in interest from 2020, resulting in 62 publications in 2024. Furthermore, the literature provides limited clarity in distinguishing between different categories of third-party risks, while the debate continues between technology-driven approaches and more traditional management tools for third-party risk management. Consequently, the gaps in the third-party risk management framework, regulatory requirements, and the high dependency of financial institutions on ICT service providers make third-party risk management a pertinent issue for the financial sector.

The studies on the interrelationships between trust and risk have a rich history (Jøsang and Presti 2004), and researchers highlighted the significance of trust in effective risk management practices three decades ago (Slovic 1993). It has been shown that trust can act as a means of "complexity reduction” in decision-making within an offline environment, particularly when assessing risks. This approach may serve as an efficient complement to rational risk management strategies (Lewis and Weigert 1985; Mclain and Hackman 1999). However, further analysis revealed that there is a lack of standardised approaches to conceptualising and assessing trust within risk management frameworks.

Furthermore, the connection between trust and third-party risk management has not been extensively explored in the literature. A search for the keywords “digital trust” AND

("third-party" OR "supplier" OR "supply chain") conducted in November 2025 in the *Scopus* database identified 589 publications in scientific journals and conference papers (Elsevier 2025). Furthermore, a bibliometric analysis was conducted using the VOSviewer tool and the keywords mapping method, which involves the co-occurrence of keywords. The analysis identified a significant gap in the scientific literature: a lack of recurring keywords associated with risk and risk management. This suggests that the concept of digital trust has not been sufficiently explored within the context of third-party or supplier risk management, and the mechanisms through which different trust factors influence third-party risks remain insufficiently understood.

Research aim, questions, hypotheses, object, and subject

The research aim is to identify the impact of digital trust on an organisation's third-party risks and to develop a capability-driven framework that enables organisations to assess and manage digital trust more effectively, thereby improving third-party risk management and overall third-party risk management governance maturity.

The main **research questions** are:

RQ1: What is the essence of digital trust, and what are its characteristics?

RQ2: How does digital trust impact third-party risks of ICT services?

RQ3: What digital trust assessment and management capabilities must be facilitated in the organisation to reduce third-party risks of ICT services?

RQ4: What sources of information should be considered by the organisation for digital trust assessment?

The **hypotheses** of the research are:

H1: Digital trust reduces third-party risks.

H2: The effect of digital trust on reducing third-party risks is moderated by the organisation's capabilities for digital trust assessment and management.

H3: A higher level of transparency in digital trust assessments during third-party onboarding has a positive impact on digital trust.

H4: Higher transparency in digital trust assessment during third-party onboarding reduces third-party risks.

H5: Digital trust acts as a mediator between transparency in digital trust assessment during third-party onboarding and the level of third-party risk.

H6: The effect of digital trust on reducing third-party risk is moderated by the level of transparency in digital trust assessment during third-party onboarding.

H7: The level of transparency in digital trust assessment during the onboarding of a third-party has a positive impact on the level of organisational capabilities for digital trust assessment and management.

H8: The extensive use of various sources of information for digital trust assessment has a positive impact on the level of digital trust.

H9: The effect of digital trust on reducing third-party risks is moderated by the extensive use of various sources of information for digital trust assessment.

H10: The extensive use of various sources of information for digital trust assessment has a positive impact on organisational capability for digital trust assessment.

H11: Organisational capabilities for digital trust assessment and management positively impact the maturity of third-party risk management.

The research object is the Baltic banking industry, which is required to implement the DORA regulation in full scope and is expected to have third-party risk management practices at a sufficiently mature level, allowing employees to participate meaningfully in the study. Currently, there are 40 licensed banks and affiliated branches of foreign credit institutions operating in the Baltic. These banks often belong to cross-border banking groups and share historically similar business cultures across the region.

The research subject is digital trust.

Research tasks

1. To explore the concept of digital trust in relation to third-party risk management of ICT services by defining and emphasising key characteristics and their effects on third-party risks.

2. To explore how organisations assess digital trust, with a focus on identifying the organisational capabilities required for effective assessment and management, and to propose recommendations for strengthening those capabilities.

3. To evaluate the role of transparency in digital trust assessments, by analysing how organisations communicate trust criteria to third parties and how transparency impacts digital trust perception and third-party risk reduction.

4. To analyse the use of diverse information sources in digital trust assessments and their contribution to digital trust assessment quality.

5. To develop a framework for organisations to enhance digital trust assessment practices, with the goal of improving third-party risk management effectiveness and advancing the overall maturity of third-party governance.

6. To analyse the future development of third-party risk management in the financial industry by examining emerging shifts in its regulatory environment, governance frameworks, and third-party cooperation models

Research methods

This doctoral thesis employs a mixed-methods approach, enabling methodological triangulation and thereby enhancing the credibility of the findings. The research design integrates both qualitative and quantitative approaches.

The theoretical basis of the research is grounded in six systematic literature reviews employing the PRISMA methodology (Page et al. 2021), which provide a comprehensive understanding of the current state of knowledge on digital trust, third-party risk management, and the relationship between trust and risk management in a digital environment. Bibliometric analysis, which applies full-counting keyword co-occurrence analysis using VOSviewer (VOSviewer 2024), enables the identification of publication patterns, research trends, and gaps within relevant scholarly domains. Content analysis is applied to academic and professional literature to examine the key characteristics of digital trust, third-party risk management, and its frameworks, as well as the trust–risk relationship in a digital context. Additionally, the study employs a construct validity method to verify the reliability and clarity of the proposed digital trust definition and its measurable items.

The theoretical part of the thesis draws on secondary data sourced from scientific publications indexed in Scopus and Web of Science, conference proceedings, academic literature, professional reports, industry associations, and business networks relevant to the research topic. Additional contextual information was obtained from companies' websites, annual and sustainability reports, and publicly available statistics.

The empirical part of the research is based on two methodological approaches:

1. Quantitative research is based on a survey of employees of the Baltic banking industry involved in third-party risk management. The survey employed a 5-point Likert scale and collected 138 valid responses, which provided a 95% confidence level and an 8.34% margin of error (Calculator.net 2026). The sampling approach combines convenience sampling with elements of purposive sampling, ensuring the inclusion of respondents directly engaged in third-party risk management activities. For data processing and analysis, the study employs descriptive statistics using JAMOVI software (jamovi 2026) and Partial Least Squares Structural Equation Modelling (PLS-SEM) with bootstrapping using SmartPLS software (Ringle et al. 2025), enabling the examination of the conceptual research model derived from the theoretical framework and literature review. The model includes constructs such as digital trust, third-party risks, transparency in digital trust assessments, organisational capabilities for digital trust assessment and management, and the maturity of third-party risk management within organisations. PLS-SEM is particularly

suitable for testing the conceptual model due to its ability to assess complex, multidimensional relationships, such as mediation and moderation, and it was selected as the statistical testing method because of its proven effectiveness in examining trust and risk management relationships in a digital context (identified in 73% of the empirical papers analysed in the systematic literature review of this thesis). The model was tested using the full sample of responses and a reduced subsample of employees working in risk, compliance, and security roles to examine whether the trust–risk relationship depends on the respondent's role in the organisation.

2. Qualitative research is based on semi-structured expert interviews (n = 13) with representatives from the financial sector across the three Baltic countries, employing purposive sampling. The number of interviews was determined based on theoretical saturation, ensuring both the validation of quantitatively obtained results from the conceptual model testing and an in-depth understanding of the state of third-party risk management in the Baltic financial sector, current practices in digital trust assessment, and the organisational capabilities required for its effective management.

For proofreading and text-flow improvement, the author used the Grammarly writing-assistance software v. 1.164 (Grammarly 2026) and ChatGPT v. 4 and v. 5 (OpenAI 2026).

Limitations of the research

The research has several limitations that should be acknowledged when interpreting the findings. First, it is limited to the **digital environment** of trust and ICT third-party risks as a category of an organisation's non-financial risks.

Second, the research is **geographically limited** to the Baltic region. The organisations included in the study operate within Estonia, Latvia, and Lithuania. Baltic economies are characterised by historically similar institutional development, regulatory structures, and business cultures. Although this enhances the internal consistency of the sample, it may limit the generalisability of the findings to regions with substantially different regulatory, cultural, or technological environments.

Third, the research is limited to the **banking industry**. This is motivated by the need to analyse organisations that manage third-party risks at least at an average maturity level. This category of risk management is still emerging worldwide, and less than 40% of organisations consider it sufficient (SupplyWisdom 2025). The banking sector provides a context where more advanced and structured approaches can be observed. However, this also restricts the applicability of the results to non-financial industries or sectors with lower third-party risk management maturity.

Fourth, the quantitative component of the study relies on **self-reported** data, which may introduce biases such as subjective perception of organisational capabilities. Although triangulation with qualitative interviews helps mitigate this limitation, it cannot be fully eliminated.

Fifth, the **unit of analysis** is limited to a single third-party relationship as reported by each respondent. While this approach allows for the examination of specific trust–risk dynamics, it does not capture portfolio-level risk exposure, interdependencies between multiple third parties, or aggregated risk across an organisation's third-party portfolio. As a result, the study may not fully reflect the systemic aspects of third-party risk that emerge only at a broader portfolio level.

Finally, the study examines organisational practices and perceptions at a **single point in time**. Given the initial stage of third-party risk management in the industry, a longitudinal approach would be beneficial for capturing changes in organisational capabilities, regulatory pressures, and risk maturity over time.

Theses for defence

Based on the conducted research, the following original scientific contributions are derived:

1. Digital Trust is reducing third-party risks. It has a positive impact on reducing ten out of twelve specific third-party risk categories (excluding vendor and supply chain cybersecurity risks and partner-specific factor risks).
2. The strengthening effect of organisational capabilities on digital trust assessment in the trust–risk relationship depends on the assessor's role. While the hypothesised moderation effect was not supported in the full sample, it became statistically significant within the governance-level group. This indicates that the quality-enhancing influence of dynamic capabilities in digital trust assessment is recognised and effective only among risk, compliance, and security professionals who operate with an awareness of governance-level practices.
3. Transparency in digital trust assessment has a positive impact on digital trust and acts as a full mediator between transparency and third-party risk, suggesting that transparency reduces uncertainty and builds relational trust. This relationship is primarily observed in the broader employee sample, while governance-level professionals rely more strongly on objective evidence than on process transparency when forming trust judgments.
4. When assessment criteria are transparent, transparency acts as a moderating factor that weakens the relationship between digital trust and third-party risk. Third parties can manipulate the signal to build an artificially high perception of digital trust, thereby diluting the negative impact of that perceived trust on actual third-party risks.
5. Transparency has a significant and positive impact on the level of organisational capabilities for digital trust assessment.
6. Utilising a variety of information sources positively impacts the level of digital trust.
7. The use of various information sources has a positive impact on organisational capabilities for digital trust assessments, as confirmed through testing on a full data set. However, the hypothesis was rejected in the governance-level group, suggesting that for experienced governance staff, the quantity of sources may create "noise and reconciliation burdens" rather than strengthening the capabilities.
8. Organisational capabilities for digital trust assessment have a significant and positive impact on the overall maturity level of third-party risk management.

Research period

The analysed scientific literature included in the thesis has the following time limitations: research focused on digital trust spans from 2010 to September 2024, while studies on the relationship between trust and risk management in a digital environment range from 2000 to July 2024, and those addressing third-party risks extend from 2016 to October 2024. The entire body of relevant scientific articles and conference proceedings from Scopus (Elsevier 2025) and Web of Science (Clarivate 2024) databases was included within the analysis scope, and the initial search had no time limitations.

The doctoral dissertation research and development period lasted from early 2023 to the end of 2025. The empirical component, which included surveys and interviews, was developed from January 2025 to July 2025.

Theoretical novelty of the research

The theoretical foundations of this research are the integrative model of trust (Mayer et al. 1995) and signalling theory (Spence 1973), which have been previously employed in research on trust and risk management in digital contexts. As a novel contribution, it introduces information asymmetry theory (Akerlof 1970) and dynamic capabilities theory (Teece et al. 1997) into trust-risk management research in digital settings, which allows to theorise and empirically test, that transparent digital trust assessment criteria and outcomes can mitigate information asymmetry in relationships between organisations and third parties, leading to an increase in digital trust and a reduction in third-party risk and that organizational capabilities for digital trust assessment and management may strengthen the positive impact of digital trust on third-party risk reduction.

Furthermore, this thesis provides the following theoretical novelty:

1. A systematic literature analysis of scientific publications devoted to digital trust identified six thematic groups of digital trust definitions, revealing diverse academic focuses and meanings associated with this concept.
2. The research is providing a validated holistic definition of digital trust "the confidence that an entity or digital environment consistently demonstrates competence and reliability, maintains robust security and a secure system architecture, fosters fair and honest practices, provides a positive user experience, complies with governance and regulatory standards, and ensures auditability and traceability of data and operations" based on 86 analysed papers identified within systematic literature review and 42 various existing digital trust definitions.
3. The research systematically identified 24 digital trust factors from the analysed literature, organising them into a comprehensive framework of four main categories, which serves as a foundation for measuring and managing digital trust.
4. The research identified four categories contributing to and extending "Integrative model of trust" (Mayer et al., 1995) by a newly introduced category specific to the digital context (Openness).
5. The research provides a theoretical justification through four systematic literature reviews for the distinction between third-party risk and risks associated with vendors, suppliers, and service providers. This distinction is based on the assertion and detailed justification of their non-synonymity, despite the common usage of these terms interchangeably in professional and scientific literature.

The practical novelty of the research

1. The study provides a tested measurement foundation for digital trust, including nine empirically validated items and a consolidated factor framework structured around four trust dimensions (Ability, Benevolence, Integrity, and Openness). These tools enable practitioners to measure the digital trustworthiness of ICT third parties.
2. The research provides a comprehensive list of twelve third-party risks, compiled through a systematic literature review, which categorises them into seven distinct categories. This offers a structured overview of the potential range and complexity of issues organisations face when dealing with external parties.
3. The study identifies the most commonly used and effective sources of information for digital trust assessment, which organisations can apply to assess the digital trustworthiness of ICT third parties.
4. The study confirms that higher digital trust contributes to a lower level of 10 out of 12 specific third-party risk types, while supply chain cybersecurity risks and partner-specific factor risks areas require additional controls beyond trust-building.
5. The research empirically demonstrates that organisational dynamic capabilities for digital trust assessment and management positively influence third-party risk management maturity. In turn, organisational transparency in digital trust assessment enhances organisational capabilities, underscoring the importance of clear documentation and well-defined trustworthiness criteria within the organisation.
6. Through the confirmed moderation effect, the research shows that high transparency in digital trust assessment may enable third parties to "manipulate the signal", potentially inflating perceived trust. This highlights the practical need for continuous monitoring and complementary controls beyond initial digital trust assessments.
7. The research develops the "Capability-driven Digital Trust framework for enhanced Third-Party Risk Management" specifically to help organisations improve their digital trust assessment and management maturity. The framework provides a practical roadmap for linking capability development to better governance of third-party risks.
8. Based on expert opinions, the research proposes a tiered evidence hierarchy designed as a practical guide for assessors to ensure comprehensive and reliable assessment of ICT third-

party trustworthiness. This addresses the practical challenge of avoiding duplicative or subjective self-reported information.

9. The research demonstrates that transparency in digital trust assessment enhances organisational capabilities for digital trust assessment and management by promoting standardisation and enabling suppliers to prepare relevant documentation, thereby highlighting the value of clear and well-documented assessment criteria. At the same time, it identifies a practical warning that such transparency can weaken the trust–risk link by encouraging box-ticking and "designed answers". Therefore, transparency must be complemented with substantive content evaluation and independent verification to avoid signalling risks.
10. The research offers practical foresight for financial institutions preparing for forthcoming regulations such as DORA, drawing on expert consensus regarding expected developments in the field over the next 3–5 years.

The methodological novelty of the research

1. The research develops and empirically validates a methodology for assessing and measuring the digital trustworthiness of ICT third-party service providers. The methodology operationalises digital trust through a structured set of trust factors and measurable indicators, enabling its integration into third-party risk management practices.

Approbation of the most relevant results

The results of the research were presented at 13 international conferences:

1. ASBBMC 2024 - 17th Annual Scientific Baltic Business Management Conference, 28–30 May 2024, Riga, Latvia
   Digital Trust in the Financial Sector: A Systematic Literature Review
2. ICABE 2024 – 20th International Conference on Applied Business & Economics,12–14 September 2024, Szczecin, Poland
   Trust and Risk Management in Digital Settings: A Systematic Literature Review
3. SCEE 2024 – 65th Riga Technical University International Scientific Conference "Scientific Conference on Economics and Entrepreneurship", 11 October 2024, Riga, Latvia
   Examining the Role of Trust in Digital Risk Management Practices
4. FEMIB 2025 – 7th International Conference on Finance, Economics, Management and IT Business, 5–6 April 2025, Porto, Portugal
   Trust and Risk Management Interplay: A Review in the Digital Context
5. ASBBMC 2025 - 18th Annual Scientific Baltic Business Management Conference 2025 28 – 29 May 2025, Riga, Latvia
   Digital Trust: Assessment Approaches and Communication Strategies
6. ESREL SRA-E 2025 - European Safety and Reliability & Society for Risk Analysis Europe Conference, 15 – 19 June 2025, Stavanger, Norway
   Third-Party Risk in Research: A Literature Review
7. ITSM 2025 - 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University, 9 – 10 October, 2025, Riga, Latvia
   Communicating and Assessing Digital Trust: Insights from Financial Institutions
8. SCEE'2025 – RTU 66th International Scientific Conference on Economics and Entrepreneurship, 16 October, 2025, Riga, Latvia
   When Digital Trust Reduces Risk: ICT Third-Party Management in the Financial Sector
9. ComManTel 2025 - 4th IEEE International Conference on Computing, Management and Telecommunications, 14 – 17 December, 2025, Madrid, Spain
   Openness as a Catalyst for Organisational Capabilities in Digital Trust Assessment: Insights from the Financial Sector
10. 84th International Scientific Conference of the University of Latvia 2026, 15 April, 2026, Riga, Latvia

Digital Trust Assessment Capabilities as a Driver of Third-Party Risk Management Maturity

11. 16th International Scientific Conference "BUSINESS AND MANAGEMENT 2026" of Vilnius Gediminas Technical University
    14 – 15 May, 2026, Vilnius, Lithuania
    From Compliance to Capability: The Evolving Role of Third-Party Risk Management in Strengthening Organisational Resilience
12. ASBBMC 2026 - 19th Annual Scientific Baltic Business Management Conference
    27 – 28 May 2026, Riga, Latvia
    Beyond Cybersecurity: The Category-specific Value of Digital Trust in Third-party Risk Management
13. 34th Annual Conference of the Society for Risk Analysis – Europe
    26 – 29 May 2026, Alicante, Spain
    a. Digital Trust and Third-Party Risk in the Financial Industry: The Moderating Roles of Transparency and Organisational Capabilities
    b. The Future Development of ICT Third-party Risk Management in the European Financial Industry

Publications

The main results of the research have been published in the following scientific sources:

1. Saveljeva, J. and Volkova, T. (2025), "A survey on digital trust: towards a validated definition", *Digital*, 5(2), 14. DOI: 10.3390/digital5020014.
2. Saveljeva, J. (2025), "Trust and risk management interplay: a review in the digital context", in *Proceedings of the 7th International Conference on Finance, Economics, Management and IT Business (FEMIB 2025)*, Porto, Portugal, 5–6 April. Porto: SciTePress, pp. 189–196. DOI: 10.5220/0013344200003956.
3. Saveljeva, J. (2025), "Third-party risk in research: A literature review", in *Proceedings of the 35th European Safety and Reliability Conference (ESREL2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025)*, Stavanger, Norway, June 15–19, 2025. Research Publishing, Singapore, pp. 267 – 274. DOI: 10.3850/978-981-94-3281-3_esrel-sra-e2025-p8074-cd
4. Saveljeva, J. (2025), "Digital trust in the financial sector: A systematic literature review", in *Proceedings of the 17th Annual Scientific Baltic Business Management Conference (ASBBMC 2024)*, 28–30 May 2024, Riga, Latvia.
5. Saveljeva, J., Volkova T. (2025), "Communicating and assessing digital trust: Insights from financial institutions", in *Proceedings of the 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITSM 2025)*, 9–10 October 2025, Riga, Latvia, pp 1- 6, DOI: 10.1109/ITMS67030.2025.11236559
6. Saveljeva, J., & Volkova, T. (2025), "Openness as a catalyst for organisational capabilities in digital trust assessment: Insights from the financial sector" in *Proceedings of the 4th International Conference on Computing, Management and Telecommunications (ComManTel 2025)*, Madrid, Spain, 14–17 December, pp. 88-92, DOI: 10.1109/ComManTel68363.2025.11368434
7. Saveljeva, J., & Volkova, T. (2026), "Category-specific effects of digital trust on third-party risks in the banking industry"*, The Journal of Risk Finance*, Vol. 27 No. 2 pp. 329–345, DOI: https://doi.org/10.1108/JRF-08-2025-0383
8. Saveljeva, J., & Volkova, T. (in press), "From Compliance to Capability: The Evolving Role of Third-Party Risk Management in Strengthening Organisational Resilience" in *Proceedings of the 16th International Scientific Conference "BUSINESS AND MANAGEMENT 2026" of Vilnius Gediminas Technical University,* 14-15 May 2026, Vilnius, Lithuania.

Other publications:

1. Peiseniece, L., Uvarova, I., Volkova, T., Saveljeva, J., Novicka, J., Polis, G., Kristapsone, S. and Vembris, A. (2025), "Integrating cybersecurity into sustainability management: current practices and future directions", in *Proceedings of the 12th IEEE Conference on Technologies for Sustainability (SusTech 2025)*, Santa Ana, California, USA, 20–23 April. Piscataway, NJ: IEEE, pp. 1-2, DOI: 10.1109/SusTech63138.2025.11025583
2. Saveljeva, J., Uvarova, I., Peiseniece, L., Volkova, T., Novicka, J., Polis, G., Kristapsone, S. and Vembris, A. (2025), "Cybersecurity for sustainability: a path for strategic resilience", in *Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience (CSR 2025)*, Chania, Crete, Greece, 4–6 August. Piscataway, NJ: IEEE, pp. 1–8, DOI: 10.1109/CSR64739.2025.11129980.
3. Saveljeva, J., Peiseniece, L., Volkova, T., Uvarova, I., Novicka, J., Polis, G., Kristapsone, S., & Vembris, A. (2026), "Integrating cybersecurity into sustainability: Emerging trends and the role of artificial intelligence", in *Proceedings of the 5th International Conference on Novel & Intelligent Digital Systems (NIDS 2025)*, 24–26 September 2025, Athens, Greece. Lecture Notes in Networks and Systems, vol 1706. Springer, Cham., pp. 313-324, DOI: 10.1007/978-3-032-10827-2_25

Structure and volume of the Doctoral thesis

This doctoral thesis consists of an Introduction, three main chapters (which include nine sub-chapters), a conclusion, recommendations and seven annexes. The dissertation is written on 309 pages and includes 40 figures and 40 tables. The bibliography includes 261 sources.

Chapter 1 Summary: The relationship between digital trust and third-party risks

Trust has been recognised as an essential element of effective risk management practices for decades (Slovic 1993). Mayer et al. (Mayer et al. 1995) incorporated risk into their trust model. The authors stated that the level of trust and perceived risk in the situation would lead to risk-taking in the relationship. The study suggested that a higher level of trust increases the likelihood that the trustor will engage in the relationship, which they consider risky. Namely, if the level of trust is higher than the level of perceived risk, the trustor will take a risk in the relationship.

It is worth mentioning that Mayer et al. (1995) highlighted the multidimensional nature of trust and proposed splitting these dimensions into three categories: ability, benevolence, and integrity.

Three forms of trust are more often discussed in the scientific literature: social trust, digital trust, and trust in technology (Rychkova and Ghriba 2023). Social trust refers to the willingness of one party to be vulnerable to the actions of another (Mayer et al. 1995). Trust in technology centres on the belief that a specific technology possesses the attributes necessary to perform as expected in situations where negative consequences are possible (Rychkova and Ghriba 2023). Digital trust, situated within digital interactions and environments, reflects the confidence placed in actors, processes, and technologies operating in digitally mediated contexts. These forms of trust are intrinsically linked to organisational decision-making and technology adoption (Rychkova and Ghriba 2023).

Researchers have demonstrated that trust in all three dimensions must be considered when designing technological solutions. Already in 2017, according to the Deloitte Global Survey, over 50% of respondents reported a significant increase in their dependence on third parties, while only 20% considered this factor when enhancing their risk management mechanisms (Deloitte 2017). More recent findings indicate that the primary challenge in resilience is the lack of integration of frameworks and data points associated with third parties (Deloitte 2023). This confirms the applicability of the information asymmetry theory to the third-party risk management environment and encourages the pursuit of solutions to this asymmetry. Mature third-party risk management practices are gradually shifting from questionnaire-based governance towards collaborative, trust-based engagement (Deloitte 2023).

Trust functions as a mechanism for reducing complexity in decision-making (Lewis and Weigert 1985; Mclain and Hackman 1999) and has been associated with more accurate risk perceptions (Mclain and Hackman 1999). However, trust is contextual (Marsh 1994; Mayer et al. 1995) and differs between online and offline environments (Alpacan et al. 2011). Consequently, proper assessment instruments for digital trust in organisational settings are required.

The theoretical foundation of this chapter is based on six systematic literature reviews (SLRs) conducted in accordance with PRISMA 2020 methodology (Page et al. 2021). Searches were performed in Scopus (Elsevier 2025) and Web of Science (Clarivate 2024), and both journal articles and conference proceedings were included, recognising the importance of conference publications in emerging digital topics (Bates and Maack 2009).

1.1. The essence of digital trust and its characteristics

Despite growing academic interest, no unified definition and set of digital trust characteristics of digital trust exists (Pietrzak and Takala 2021; Tunkevichus and Rebiazina 2021; Chen et al. 2023). Therefore, an SLR was conducted to gather comprehensive information on the digital trust concept. The search using the keywords “digital trust” was performed on

September 15, 2024, and was limited to 1) titles, abstracts, and keywords; 2) scientific articles and conference papers; and 3) English language. In total, 156 records were identified in Scopus (Elsevier, 2025) and 84 in Web of Science (Clarivate 2024) databases. After removing duplicates, 170 papers remained. After abstract screening and full-text reading, 86 research papers - 27 conference proceedings and 59 scientific articles - were included for theoretical analysis of the digital trust concept.

Existing definitions of digital trust

The authors of various papers have stated that there is no single definition of digital trust (Pietrzak and Takala 2021; Tunkevichus and Rebiazina 2021; X. Chen et al. 2023). Indeed, the research revealed a wide range of definitions of digital trust in academia: 86 analysed papers identified 42 different definitions of digital trust.

The most frequently cited definition describes digital trust as "the confidence of stakeholders in the competence of actors, technologies and processes for establishing reliable and secure business networks", (M. F. Mubarak and Petraite 2020, p.3) which was included in the analysed papers and additionally quoted three times (Mo et al. 2023; Han et al. 2024; Mubarak et al. 2024), i.e. used four times. Nevertheless, the diversity of definitions demonstrates fragmentation in conceptual understanding.

Content analysis allowed the classification of these definitions into six thematic groups summarised in Table 1.1 below.

Table 1.1. Digital trust definitions distribution by the thematic group

Group no.	**Main group's theme**
Group 1 (n=12)	Confidence in people, processes and technology to create a secure digital environment
Group 2 (n=8)	Trust in data protection, privacy, security, and ethical information handling
Group 3 (n=8)	Trust in the technical capability and reliability of technology
Group 4 (n=7)	Trust as a mental state involving cognitive, emotional, and experiential factors
Group 5 (n=4)	Trust as an enabler in digital relationships, interactions, and business networks
Group 6 (n=3)	Trust based on ethical behaviour and cultural principles

Source: Created by the author

Key characteristics of digital trust

The existence of a common understanding of the digital trust concept and its characteristics is supported by the fact that previous attempts have been made to identify its characteristics using a systematic literature review methodology. Rychkova and Ghriba's (2023) review of blockchain literature identified 21 technology-neutral trustworthiness requirements, emphasising the importance of digital, technological, and social trust in organisational decision-making. Based on the trustworthiness factors mentioned by Mayer et al. (1995), the requirements were divided into three categories: ability, benevolence, and integrity.

Out of 86 papers, 36 included the characteristics of digital trust, yet none were included in the systematic review conducted by Rychkova and Ghriba (2023). From these papers, 24 factors of digital trust were identified and organised into four categories and eight sub-categories.

Since this research aims to identify generally applicable digital trust factors that can subsequently enable the measurement of digital trust, all identified factors were mapped on three layers:

1. Category, based on initial trustworthiness factors introduced by Mayer et al. (1995);

2. Sub-category, representing the foundational elements of the category in the context of digital trust; and

3. Consolidated digital trust factors, since many researchers used different elements to articulate a single digital trust factor.

Although nearly all identified factors can be sorted into three main categories: 1. The system's or organisation's competence/capacity (Ability); 2. The positive intent of organisations/service providers towards users (Benevolence); and 3. The organisation's alignment with acceptable standards and principles (Integrity), a particular subset of digital trust factors, does not entirely align with these three pillars.

In the modern world, particularly within the digital environment, there are numerous ways to verify trustworthiness through external sources or assurances. Consequently, trust is becoming demonstrable and publicly verifiable. This concept may be described as "openness" and was offered as a fourth category of digital trust factors.

Digital trust is a complex and multidimensional concept (Ferraro et al. 2023); thus, it is not easy to identify which factors are more important in establishing it than others. The analysis conducted reveals that the top three sub-categories of digital trust factors are "security and control" (n=25), "openness" (n=23) and "competence and performance" (n=19). Other sub-categories are comparatively secondary, with "relational credibility" and "secure system architecture" being less influential. All identified categories and sub-categories of digital trust are depicted in Figure 1.1 below.

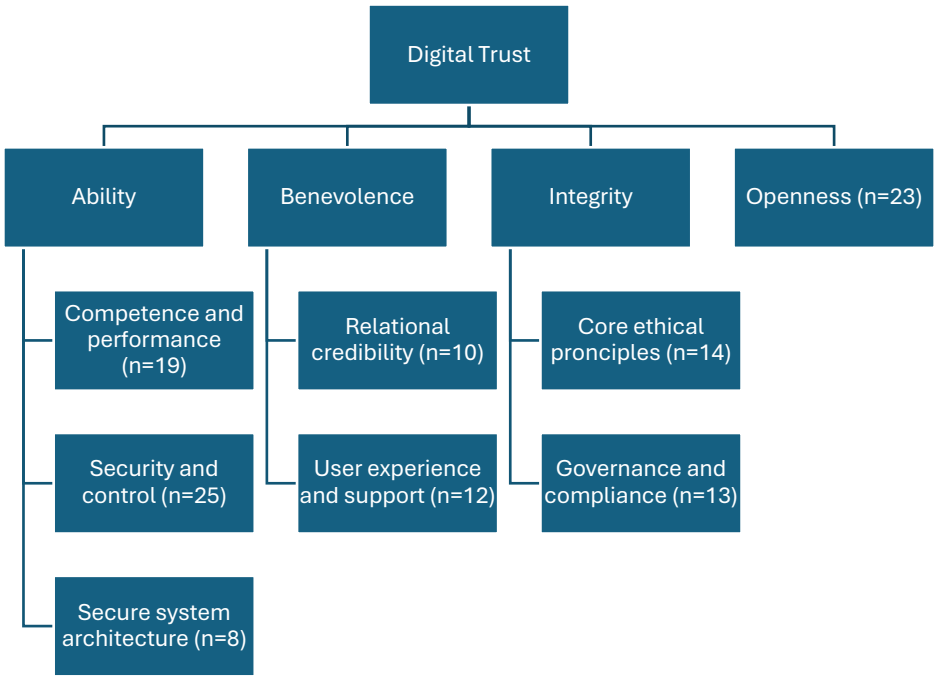


Figure 1.1. Digital trust factors categories and sub-categories

Source: Created by the author

Based on the previously analysed digital trust definitions and key factors that compose the concept, the author proposes the following definition of digital trust: *Digital trust is the confidence that an entity or digital environment consistently demonstrates competence and reliability, maintains robust security and a secure system architecture, fosters fair and honest practices, provides a positive user experience, complies with governance and regulatory standards, and ensures auditability and traceability of data and operations.*

Considering the current existence of 42 different definitions of digital trust and the lack of a singular dominant definition, the concept validation method will be employed to demonstrate the validity of the proposed definition.

Validation of digital trust definition

Clear conceptual definitions are crucial for scientific progress and further theoretical development (Podsakoff et al. 2016). Even more important is to create a formal definition with precise language to prevent ambiguities and repetitive reasoning (Sell 2018). Therefore, the proposed definition was validated using content validity methodology (Colquitt et al. 2019; Hinkin and Tracey 1999).

A questionnaire for content validation of the definition, created using Hinkin and Tracey's approach (1999), was piloted among five respondents to gather feedback and assess its validity. Further, it was distributed among doctoral students and professionals, resulting in 99 valid responses. 5-point Likert scale was used to determine the degree to which the definition corresponded to the key factors that compose it.

The operationalised descriptions of the validation factors were based on the factor descriptions proposed by Rychkova and Ghriba (2023) and are listed in Table 1.2 below. To operationalise the first three categories (F1 – F7), the author summarised the descriptions of the factors included in the sub-category, as provided by Rychkova and Ghriba (2023). The fourth category factors (F8, F9) were created directly from the descriptions provided by Rychkova and Ghriba (2023).

Table 1.2. Description of measurable items

Code	Category	Factor
	Category 1: Ability	
F1	1.1.Competence and performance	The entity demonstrates competence and reliably delivers services or products.
F2	1.2. Security and control	The entity ensures secure access, protects data, and maintains its integrity.
F3	1.3. Secure system architecture	The entity employs a secure architecture and processes to ensure efficiency, control, and integration.
	Category 2: Benevolence	
F4	2.1. Relational credibility	The entity demonstrates fairness, honesty, and reliability, building a strong reputation.
F5	2.2. User experience and support	The entity ensures a positive user experience and provides responsive support.
	Category 3: Integrity	
F6	3.1. Core ethical principles	The entity demonstrates integrity, protects data privacy, and adopts sustainable practices.
F7	3.2. Governance and compliance	The entity ensures governance and compliance in accordance with regulations and standards.
	Category 4: Openness	
F8	4.1. Auditability	The entity ensures compliance through certifications, audits, and supervision.
F9	4.2. Traceability	The entity ensures traceability by providing information about data origins.

Source: created by the author, based on (Rychkova and Ghriba 2023)

Four definitions were provided for the respondents' judgment: the first one, developed by the author to validate it; the second, the most popular existing definition, to check whether the proposed one better represents the concept's essence; and the third and fourth, related to the digital trust concepts of "cyber-trust" and "online trust."

Definition No. 1: "Digital trust is the confidence that an entity or digital environment consistently demonstrates competence and reliability, maintains robust security and a secure

system architecture, fosters fair and honest practices, provides a positive user experience, complies with governance and regulatory standards, and ensures auditability and traceability of data and operations" (proposed by the author).

Definition No. 2: "Digital trust is the confidence of stakeholders in the competence of actors, technologies and processes for establishing reliable and secure business networks" (M. F. Mubarak and Petraite 2020, p.3), the most popular definition within the analysed sample.

Definition No.3: "The user's confidence in the predictability of the "behaviour" of software and hardware systems (digital technologies), their reliability, which is manifested in the willingness to delegate several tasks to various software and hardware systems" (Vidiasova et al. 2020, cited in Tunkevichus and Rebiazina 2021, p. 433). The definition of the related concept – "cyber-trust".

Definition No. 4: "Consumers' perception of a web site's usefulness, security, privacy, reputation, quality, and e-vendors' willingness to customise" (Wu et al. 2010, cited in (Tunkevichus and Rebiazina 2021, p. 433). The definition of the related concept, "online trust".

Since Colquitt et al. (2019) stated that a minimum sample size of 100 respondents would provide sufficiently precise results, we conclude that the current sample is adequate for the purpose of this study.

Exploration statistical calculations in this study were conducted using Jamovi v. 2.6.26 (jamovi 2026) software. The author's proposed definition - definition number 1 - was analysed based on the index of definitional correspondence, referred to as *htc* (for Hinkin Tracey correspondence), calculated using the following formula:

$$\text{htc} = \text{average definitional correspondence rating} / a$$

Following Hinkin and Tracey (1999), a minimum value of 4.2 for htc provides a confirmation of content adequacy. As per Colquitt et al., (2019) the htc value from 0.87 to 0.90 confirms strong content adequacy, whereas 0.84 to 0.86 suggests that the correlation is moderate while still sufficient. Overall, statistical analysis conducted in Jamovi confirmed moderate to strong content adequacy (overall htc = 0.86).

Afterwards, the results of the similar (D2) and alternative (D3, D4) definitions were analysed using the *htd* or Hinkin Tracey distinctiveness index, which was calculated using the formula below:

$$\text{htd} = \text{Average of all (Intended Correspondence Rating} - \text{Orbiting Correspondence Rating)} / (a - 1), \text{ where } a \text{ is the number of anchors}$$

According to Colquitt et al., (2019) htd value from 0,18 to 0,26 is moderate, whereas from 0,27 to 0,34 it is strong. Following the calculations of the factors/measurable items ratings, No. 2 – the most popular definition of digital trust – exhibits moderate distinctiveness from the newly proposed definition (htd = 0.23). Thus, we may conclude that the proposed definition (D1) better represents the conceptual essence of digital trust than the existing definition.

In turn, definition No. 3 (D3) – the definition of cyber-trust – exhibits strong distinctiveness (htd=0.27), while definition No. 4 (D4) – the definition of online trust – shows moderate distinctiveness (htd=0.24) compared to the proposed D1. Based on this, we may conclude that the proposed D1 represents the digital trust concept, not the orbiting ones.

Measurement of digital trust

The literature review reveals no unified approach to measuring digital trust and identifies four main measurement methods. The most common approach (n = 11) relies on multi-dimensional Likert-scale surveys (using ranges of 1-4 (Svenson et al. 2024), 1-5 (Balci 2021), or 1-7 (Mubarak et al. 2024)). A second method uses secondary data, such as reputation scores, certifications, compliance records, security incidents, and third-party evaluations (Das

et al. 2023; Kluiters et al. 2023). A third approach applies direct trust perception measures through a simple Likert-scale item with a question about the extent to which the service or service provider is trustworthy or can be trusted (J. K. C. Chen et al. 2022). Finally, technically oriented studies propose measuring digital trust through Industry 4.0 constructs or trust architecture design (Akram and Ko 2014; Mubarak and Petraite 2020; Rane and Huang 2022).

Despite these approaches, none of the studies addresses the organisational capabilities required to assess digital trust. Given the dynamic nature of trust (Oudina et al. 2024) and its relationship with risk perception (Mclain and Hackman 1999), the concept of dynamic capabilities (Teece et al. 1997) provides a relevant theoretical foundation. Building on Teece's framework, dynamic capabilities may be categorised into sensing, seizing, and reconfiguring functions (Jantunen et al. 2012), which may support the development of organisational capacity for effective digital trust assessment.

Prior studies on digital trust as a key service provider attribute

The reviewed studies indicate limited research on digital trust in intra-organisational settings. Corsaro and D'Amico (2022) identified digital trust as a key dimension influencing B2B relational changes accelerated by digital transformation. Empirical evidence shows that digital trust positively affects open innovation performance, mediated by technological absorptive capacities (Mubarak and Petraite 2020), and supports sustainable blockchain-based supply chains through transparency, cybersecurity, accountability, and regulatory compliance (Sharma et al. 2024).

In B2B contexts, digital trust enhances perceived usefulness, satisfaction, and customer loyalty (Balci 2021; Loh et al. 2024). It also correlates with Corporate Digital Responsibility (Jelovac et al. 2022) and contributes to increased firm value from a governance perspective (Kluiters et al. 2023).

Communication of digital trust

Digital trust can be communicated through technological, reputational, and signalling mechanisms. Blockchain is frequently proposed as a tool to enhance transparency, immutability, and verifiability across sectors (Piccininni et al. 2020; Kayhan 2022; Kobzan et al. 2018). However, technology alone is insufficient, and overreliance on certain technologies without building trust in institutions and processes may lead to distrust. Therefore, digital trust also depends on institutional trust, governance, and human factors (Ferraro et al. 2023; Katete 2021).

Reputation, certifications (e.g., ISO 27001), prior track records, and governmental assurances serve as additional trust signals (Das et al. 2023; Deprez et al. 2016). Digital trust may further be demonstrated through ratings and feedback from partners or customers, qualitative public representation, and communication of cybersecurity investments (Oukarfi and Sattar 2020; Mohlmann 2021; Kluiters et al. 2023). Educating customers about product architecture and technology and building communities around the organisation also support digital trust communication (Levine 2019; Zolfaghari et al. 2023; Pivavarava and Koop 2024).

Information asymmetry theory (Spence 1973) explains how unequal access to information affects trust and was studied both in both offline and digital environments (Oukarfi and Sattar 2020; Sattar et al. 2022; Cerić 2021; Baumgaertner and Soluk 2023). Relatedly, signalling theory (Spence 1973) examines how one party strategically communicates information to reduce uncertainty. While prior studies have examined trust communication through ratings or blockchain usage, the transparency of digital trust assessment criteria and the complementarity of multiple independent signals in organisational third-party contexts remain insufficiently explored.

1.2. Foundations of Trust in Risk Management

The relationship between trust and risk has long been a subject of research, highlighting their inherent connection (Jøsang and Presti 2004). This was also confirmed by a search using

the keywords “risk management” AND “trust” limited to article titles, abstracts, keywords and articles and conference papers in the Scopus (Elsevier 2025) database in February 2025, which yielded 2190 papers meeting these criteria. According to the analysed documents, interest in the topic began to emerge in the early 1990s, followed by a wave of growth in 2004 and a surge of interest since 2020.

In recent years, the European Union (EU) has increasingly emphasised regulatory measures to enhance risk management in the digital environment (European Commission 2022b, 2022a). However, the effectiveness of the risk management system within the European context remains a pertinent question (Ghazieh and Chebana 2021), particularly as traditional mitigation approaches are increasingly challenged by growing cybersecurity threats (Aslan et al. 2023), highlighting the need for an effective risk management framework (Luther et al. 2023). Earlier research had already emphasised the importance of trust in effective risk management (Slovic 1993; Rousseau et al. 1998), demonstrating that trust may function as a mechanism of “complexity reduction” in decision-making and complement rational risk assessment approaches (Lewis and Weigert 1985; Mclain and Hackman 1999).

To examine how trust enhances risk management in digital environments, a systematic literature review was conducted using the keywords trust AND “risk management” AND (“digital” OR “online” OR “cyber”) on June 30, 2024, in Scopus (n = 272) and on July 7, 2024, in Web of Science (n = 55). The search identified 281 unique papers, of which 45 (22 conference papers and 23 journal articles) met the inclusion criteria, focusing on the correlation between trust and risk management in digital settings.

Keyword and co-occurrence analyses using VOSviewer software (VOSviewer 2024) indicated that existing research predominantly concentrates on perceived risk, behavioural intention models, cybersecurity, and e-commerce contexts. However, the multidimensional role of trust in organisational, B2B digital risk management remains underexplored. This gap justifies further investigation of digital trust as a determinant of third-party risk within the present study.

Core theoretical perspectives on trust and risk

The analysis of the selected papers revealed that there is no single standout theory or model exploring the interrelationship of trust and risk within a digital context. Instead, the researchers employed multiple theories in various combinations to construct conceptual models and investigate these relationships.

The Technology Acceptance Model (TAM) (Davis 1989) was the most frequently applied (n = 7), followed by the Theory of Planned Behaviour (TPB) (n = 5) (Ajzen 1991). The Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003) (n=3) and its extension UTAUT2 (Venkatesh et al. 2012) (n=2) were also employed to explain behavioural intention towards technology adoption. The Theory of Reasoned Action (TRA) (Hansen et al. 2018) (n=4) was used in four studies, typically in combination with TAM and TPB.

Additionally, the integrative model of organisational trust (Mayer et al. 1995) was applied (n = 4) to conceptualise trust as a multidimensional construct and as a mediating or moderating variable reducing perceived risk. Signalling theory (Spence 1973) was likewise incorporated in several studies (n=4) to explain information asymmetry mechanisms.

Prior research methodologies in trust and risk management for digital environments

The analysis revealed that most papers (n = 31, 68.9%) were empirical, while ten (22.2%) were conceptual and four (8.8%) purely theoretical. The dominant empirical method was the survey (n = 19, 42.2%), applied in quantitative (n = 15) and qualitative (n = 4) forms, often using 5-, 6-, or 7-point Likert scales. Modelling (n = 9, 20%) and non-systematic literature review (n = 9, 20%) were equally prevalent. Interviews contributed to four papers (8.9%), constructive research methods were used in four, and case study and experimental methods

were applied twice each. Six studies used multi-method approaches, resulting in 51 methods across 45 papers.

One-third of the studies (n = 15, 33%) tested conceptual models via survey-based quantitative analysis. Most research was conducted in business-to-consumer contexts (n = 10, 66.7%), followed by P2P (n = 2, 13.3%), while only one study (6.67%) examined the organisational B2B context. In the conceptual models, risk was mainly positioned as an independent (n = 7, 46.7%) or moderating/mediating variable (n = 6, 40%), whereas trust was predominantly treated as a moderating/mediating variable (n = 9, 60%). Only one study examined the influence of trust on risk (Zhang and Cozma 2022), treating trust as monodimensional concept. The distribution of risk and trust variables by type in the conceptual models is depicted in Figure 1.2 below.

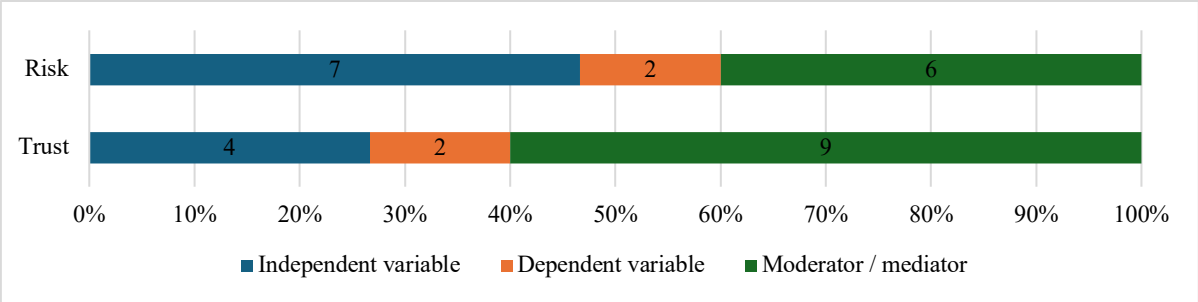


Figure 1.2. Distribution of risk and trust by variable types in the conceptual models

Source: Created by the author

Most studies (n = 11, 73%) applied SEM or PLS-SEM for model validation. Overall, the findings indicate that the interrelationship between trust and risk remains underexplored in organisational digital contexts, particularly regarding trust as a multidimensional independent variable influencing risk (Marsh 1994; Dimitrakos 2001).

The role of trust in risk management

The reviewed studies confirm that trust and perceived risk are interdependent and mutually influential: increased trust reduces perceived risk and enhances adoption, while high perceived risk diminishes trust (Aldás-Manzano et al. 2009; Ksibi et al. 2023; San Martín and Camarero 2009; Putri et al. 2022). Trust also facilitates risk-taking behaviours across financial, digital, and sharing economy contexts (Hansen et al. 2018; Mollazehi et al. 2024; Sun et al. 2016). However, excessive trust may result in complacency, reduced vigilance, and greater vulnerability (Bishop et al. 2020; Larsen et al. 2022; Terry Morris et al. 2020).

Assurance frameworks and emerging technologies such as blockchain were shown to reduce uncertainty and transaction risks and strengthen trust (Ghaffarian et al. 2023; Hampton et al. 2021; Shaytura et al. 2021). Transparent communication and explainable information further enhance trust, whereas low trust leads to risk-averse behaviour (Ghaffarian et al. 2023; Windelberg 2016; McInnis et al. 2016; Setty 2018). Incorporating trust assessments into decision-making improves risk management effectiveness (Oudina et al. 2024; Yuan et al. 2010). Finally, trust and risk perceptions are context-dependent and influenced by social and cultural factors (Bhattacharya and Saha 2004; Windelberg 2016). It confirms that trust–risk relationships are complex and dynamic rather than purely causal.

Assessing approaches for integrating trust into risk management

The reviewed studies indicate multiple ways to integrate trust into digital risk management. From the service provider perspective, trust can be strengthened through robust security measures (San Martín and Camarero 2009), transparent communication about risk practices (Ghaffarian et al. 2023; Tehrani et al. 2020), cultural alignment (Bhattacharya and

Saha 2004), enhanced transparency and explainability of technologies (Ghaffarian et al. 2023) and user involvement in service development (McInnis et al. 2016; Zhang et al. 2016).

Internally witin the organisations, trust may be incorporated through trust metrics and scoring systems in risk assessments (Abdul-Rahman and Hailes 2000; Yuan et al. 2010), supported by independent audits and certifications (Hafver et al. 2021) and the adoption of trusted-by-design technologies such as blockchain (Shaytura et al. 2021). However, as trust is dynamic (Oudina et al. 2024), it requires continuous reassessment and monitoring to avoid overreliance (Larsen et al. 2022).

The literature shows that integrating trust into risk management requires both technical and human-centred measures. Nevertheless, no standardised framework for trust assessment or its systematic integration into risk management has been developed. Moreover, the specific influence of different trust characteristics on various third-party risks remains insufficiently explored, motivating further investigation in this thesis.

1.3.The third-party risk management and its frameworks

Financial institutions face multiple risk categories, most significant being credit, market, operational, and liquidity risks (Vashisht et al. 2022; Korneev et al. 2023). Operational risk includes cybersecurity, human, technical, and third-party risks and is closely linked to banking system stability. While traditional risk management frameworks are well established, recent research increasingly focuses on emerging risks driven by digital transformation, fintech expansion, and IT disruptions (Gai et al. 2018), emphasising the need for continuous adaptation of risk management practices (Minh Sang 2024). Since 2017, ICT-related third-party risk has become a major concern for European banks, and practitioners believe that third-party risks remain a key risk driver in 2025 (Were 2025).

To analyse third-party risk management frameworks, a systematic literature review was conducted (October 12, 2024) using a word combination “third party risk” in Scopus (Elsevier 2025) (n = 108) and Web of Science (Clarivate 2024) (n = 26), resulting in 107 unique papers. After applying inclusion and exclusion criteria, 16 papers (5 conference proceedings and 11 journal articles) were included. Publications on third-party risk began appearing in 2016 and peaked in 2024. The studies reflect diverse industry contexts and geographical contributions.

A full-count co-occurrence keyword analysis was conducted using VOSviewer (VOSviewer 2024), examining 63 keywords, of which 13 were interconnected. The analysis identified three thematic clusters: (1) a technological cluster focusing on blockchain, encryption, IoT, privacy, and security; (2) a process-oriented cluster centred on information, risk, and self-assessment; and (3) an industry-specific cluster emphasising construction, engineering, integrity, and risk-based due diligence. Although the sample size was limited, the results demonstrate that third-party risk research is multidimensional, extending across technological, procedural, and industry-specific perspectives rather than being confined to a single domain.

The qualitative review revealed a multidimensional research landscape. Conceptual papers (n = 6) focus either on innovative tools and methods (Ramasubramaniam and Singh 2020; Fortner 2021; Mohta et al. 2024; Agrawal et al. 2024) or on identifying regulatory and strategic gaps (Jadwani et al. 2024; Neumannová et al. 2023). Empirical studies (n = 10) propose new frameworks, tools, and procedural approaches or evaluate existing third-party risk management practices.

Preliminary analysis showed that in professional and scientific literature, authors often refer to “third-party risk” as a synonym for “vendor risk” or “supplier risk”. Therefore, to understand the essence of the third-party risk concept and its relationship with other similar risk types, four separate analyses were conducted within this thesis and are described further.

Third-party risk

Only six analysed papers provided explicit definitions of third-party risk, and only one specifically addressed the IT domain (Ramasubramaniam and Singh 2020). The remaining

definitions describe third-party risk broadly as risks arising from relationships with external entities, including vendors, suppliers, subcontractors, consultants, and joint venture partners (Keskin et al. 2021; Roy et al. 2022; Mohta et al. 2024; Jadwani et al. 2024; Jallan and Ashuri 2020).

The diversity of definitions reveals the absence of a unified understanding of what constitutes a third party and the associated risks. This creates challenges for establishing consistent third-party risk management frameworks and necessitates tailoring the scope of third-party risk to the organisation's industry and operational context. Although some authors treat third-party risk as synonymous with vendor or supplier risk (Schelegia and Fleşer 2021; Keskin et al. 2021), the analysed definitions suggest conceptual distinctions. Therefore, this thesis does not consider third-party, vendor, and supplier risks interchangeable and further clarifies their differences.

Vendor risk

Preliminary research revealed no unified definition of vendor risk; therefore, a systematic literature review was conducted on 23 October 2024 using the keyword "vendor risk" in Scopus (Elsevier 2025) (n = 36) and Web of Science (Clarivate 2024) (n = 6), resulting in 36 unique sources after duplicates were removed. Following abstract screening and full-text review, 19 papers were analysed, allowing the identification of seven various definitions.

The review revealed two main perspectives: an organisational view (Natovich 2003; Keskin et al. 2021; John et al. 2024) and a consumer-oriented view (Tainyi et al. 2009; Mascha et al. 2011; Herrero and San Martín 2012; Pappas 2017). Most definitions define vendors in a digital environment, making the term applicable to ICT-related relationships.

Organisational definitions often incorporate risk management processes such as selection, contracting, and monitoring. Across definitions, vendor risk relates to legitimacy and ethical behaviour, potential losses, privacy and data protection, and operational continuity.

Supplier risk

Supplier risk, often perceived as synonymous with vendor risk, was analysed through a systematic literature review conducted on October 12, 2024. The search of the word combination "supplier risk" in Scopus (Elsevier 2025) (n = 238) and Web of Science (Clarivate 2024) (n = 69) resulted in 243 unique papers after duplicates were removed. Research activity increased significantly after the early 2000s, peaking in 2021 and 2022 (25 publications each year). Following screening and full-text review, 47 papers were analysed, of which only 11 provided explicit definitions of supplier risk.

The definitions predominantly reflect an organisational perspective and are mostly connected with the offline sectors. Supplier risk is mainly associated with environmental, operational (e.g., delivery delays, quality failures, supply chain disruptions), and ethical risks (Lockamy 2011; Globočnik Žunac et al. 2019; Collier et al. 2022; Zhou et al. 2022; Leite et al. 2024; Puncreobutr and Puncreobutr 2024; Lau et al. 2024). Unlike vendor risk, supplier risk is closely linked to supply chain performance and upstream disruptions, making "supply" and "supply chain" central to its conceptualisation.

Service provider risk

Since third-party risk definitions include service providers among the external parties that may produce a risk, research was also conducted on this type of risk. To examine service provider risk, a search using a words combination "service provider risk" was conducted on October 26 identified 17 unique papers (Scopus n = 17; Web of Science n = 1) (Elsevier 2025; Clarivate 2024). The term first appeared in 2007 and showed no clear upward trend, peaking in 2024 with four publications. After applying inclusion criteria and full-text review, only two papers were found relevant.

Neither paper provides a direct definition of supplier risk. One paper (Mathew and Aundhe 2011) used the term "supplier risk" interchangeably with "vendor risk" in the context

of outsourced ICT services, while the other (Ray et al. 2013) referred to "service provider risk" in strategic outsourcing contracts without defining it.

Analysing these papers, it may be concluded that service provider risk is a rarely used term that can be considered a synonym for vendor risk.

Risk management cycle and third-party risk management frameworks

Previous research has shown that existing frameworks do not fully meet the industry's requirements for party risk management. Neumannová et al. (2023) identified gaps in ISO 27001:2013, noting that existing controls do not fully address DORA requirements, particularly regarding external partners and cloud vendors. The analysed studies do not provide a unified framework and vary in granularity, ranging from high-level models (Roy et al. 2022; Mohta et al. 2024) to detailed multi-stage approaches (Monev 2021).

By integrating these approaches, seven main stages of third-party risk management were identified: (1) establishing governance and roles; (2) defining and tiering the scope of third parties; 3) conducting risk assessment through information gathering and model development; (4) contracting with risk-mitigating clauses; (5) continuous monitoring and reassessment; (6) reporting and governance oversight; and (7) continuous improvement and integration into the broader operational risk framework (Ramasubramaniam and Singh 2020; Monev 2021; Aliane and Zakariya 2023; Roy et al. 2022; Mohta et al. 2024)

The literature also highlights differing preferences between technology-driven solutions (e.g., real-time detection, automated scoring) and traditional tools such as questionnaires and on-site audits. Effective third-party risk management requires combining both approaches (Aliane and Zakariya 2023; Monev 2021; Keskin et al. 2021).

Types of third-party risks

Nine papers examined the types of third-party risks, varying in scope and level of detail. Based on their findings, seven categories of third-party risks were identified and are outlined in Table 1.3 below.

Table 1.3. Types of third-party risks

Code	Category	Risks included	Source
R1	1. Regulatory and Compliance	Compliance and regulatory risks, such as conformity to tax laws, sanctions, and legal aspects	(Ramasubramaniam and Singh 2020; Roy et al. 2022; Mohta et al. 2024)
	2. Operational		
R2.1	2.1. General Operational Risks	Risks related to the management of a third party. governance framework	(Ramasubramaniam and Singh 2020; Mohta et al. 2024).
R2.2	2.2. Supply Chain and Partner Process Issues	Supply chain disruptions, isolated processes, limited visibility, onboarding challenges, and ineffective collaboration	(Fortner 2021; Kähkönen et al. 2016).
R2.3	2.3 Concentration Risk and Contingency Planning	Over-reliance on specific third parties or a lack of contingency measures	(Jadwani et al. 2024; Abbasi et al. 2023).
R3	3. Financial	Financial risks such as high intermediary fees and cost exposures	(Abbasi et al. 2023; Kähkönen et al. 2016; Mohta et al. 2024).
	4. Security and Privacy		

R4.1	4.1. Vendor and Supply Chain Cybersecurity Risks	Cybersecurity vulnerabilities of vendors and supply chains	(Keskin et al. 2021; Mohta et al. 2024; Jadwani et al. 2024).
R4.2	4.2. Data Privacy Risks	Data security breaches, leakage, and sovereignty issues	16/07/2026 10:13:00.
R5	5. Strategic	Risks related to alignment with business objectives and frameworks, such as outsourcing strategies	(Neumannová et al. 2023; Ramasubramaniam and Singh 2020).
	6. Ethical and Social		
R6.1	6.1. Reputational risks and conflict of interest	Risks of corruption, bribery, and collusion	(Roy et al. 2022).
R6.2	6.2. Corporate social responsibility (CSR)	Risks involving human rights and other social responsibility aspects	(Roy et al. 2022; Kähkönen et al. 2016).
	7. Partner and Supply Chain		
R7.2	7.1. Risks Related to Partner-Specific Factors	Geographical location, industry type, partner profile, proximity to officials, reasons for partnership, and contract complexity	(Roy et al. 2022; Kähkönen et al. 2016).
	7.2. Fourth-Party and Nth-Party Risks	Risks associated with suppliers and sub-contractors in the extended supply chain	(Ramasubramaniam and Singh 2020; Fortner 2021)

Source: Created by the author

The diversity of identified risks highlights the multidimensional nature of third-party risk management. Notably, the frequent inclusion of cybersecurity and data-related risks underscores the growing importance of digital threats, while the recognition of fourth- and nth-party risks reflects the need to manage exposures across the extended supply chain.

1.4. Hypotheses and Research Model

The theoretical research conducted in the thesis allowed for the formulation of research hypotheses for further testing. Hypothesis 1 is derived from the integrative model of organisational trust (Mayer et al. 1995). Its sub-hypotheses are as follows, based on the analysis of the types of third-party risks. In essence:

H1: Digital trust reduces third-party risks.

H1a: Digital trust reduces regulatory and compliance risks.
H1b: Digital trust reduces general operational risks.
H1c: Digital trust reduces supply chain and partner process issues risks.
H1d: Digital trust reduces concentration and contingency planning risks.
H1e: Digital trust reduces financial risks.
H1f: Digital trust reduces vendor and supply chain cybersecurity risks.
H1g: Digital trust reduces data privacy risks.
H1h: Digital trust reduces strategic risks.
H1i: Digital trust reduces reputational and conflict of interest risks.
H1j: Digital trust reduces corporate social responsibility risks.
H1k: Digital trust reduces risks related to partner-specific factors.
H1l: Digital trust reduces fourth-party and N-th-party risks.

The assumption that organisational capabilities for digital trust assessment and management may strengthen the negative impact of digital trust on third-party risk is grounded in dynamic capabilities theory (Teece et al. 1997) and led to the formulation of the following hypothesis:

H2: The effect of digital trust on reducing third-party risks is moderated by the organisation's capabilities for digital trust assessment and management.

Another assumption of this study is grounded in information asymmetry theory (Akerlof 1970). It posits that the transparency of digital trust assessment criteria and outcomes can help mitigate information asymmetry in relationships between organisations and third parties. This, in turn, is expected to increase the level of digital trust and reduce the level of third-party risk. This assumption is reflected in the following hypotheses:

H3: A higher level of transparency in digital trust assessments during third-party onboarding has a positive impact on digital trust.

H4: Higher transparency in digital trust assessment during third-party onboarding reduces third-party risks.

H5: Digital trust acts as a mediator between transparency in digital trust assessment during third-party onboarding and the level of third-party risk.

H6: The effect of digital trust on reducing third-party risk is moderated by the level of transparency in digital trust assessment during third-party onboarding.

Furthermore, the described theories may allow for theorising that open assessment criteria sharing during onboarding might be a routine that helps the organisation sense weak spots in its criteria, seize new vendor insights and quickly transform controls. Such repeated, transparent exchanges gradually scale up into a higher-order capability for evaluating digital trust. Thus, there is a hypothesis:

H7: The level of transparency in digital trust assessment during the onboarding of a third-party has a positive impact on the level of organisational capabilities for digital trust assessment and management.

The following hypotheses are motivated by signalling theory (Spence 1973) and are based on the idea that various informational signals used to communicate digital trust, such as external certifications or audit results, may have a positive effect on the perceived level of digital trust and may also strengthen the negative impact of digital trust on third-party risk. The related hypotheses are:

H8: The extensive use of various sources of information for digital trust assessment has a positive impact on the level of digital trust.

H9: The effect of digital trust on reducing third-party risks is moderated by the extensive use of various sources of information for digital trust assessment.

Similarly, as with transparency, we may theorise that consistent use of multiple sources of information strengthens the organisation's ability to sense risks, seize opportunities, and reconfigure assessment strategies. Exposure to a wider range of digital trust indicators helps refine and update digital trust assessment processes in response to emerging threats and new practices. Thus, the related hypothesis is:

H10: The extensive use of various sources of information for digital trust assessment has a positive impact on organisational capability for digital trust assessment.

Finally, this study posits that an organisation's capability to assess digital trust can positively influence its overall third-party risk management maturity. In line with dynamic-capabilities theory, a refined trust-assessment routine enhances the organisation's ability to sense weak signals in vendor behaviour, seize corrective options early, and adjust contracts or controls before risks materialise. Consequently, the more adept an organisation is at evaluating digital trust, the more structured, proactive, and data-driven its third-party risk management becomes, which is reflected in a higher maturity level. Therefore, the following hypothesis is formulated:

H11: Organisational capabilities for digital trust assessment and management positively impact the maturity of third-party risk management.

Based on the described hypotheses, the research model was designed and is presented in Figure 1.3.

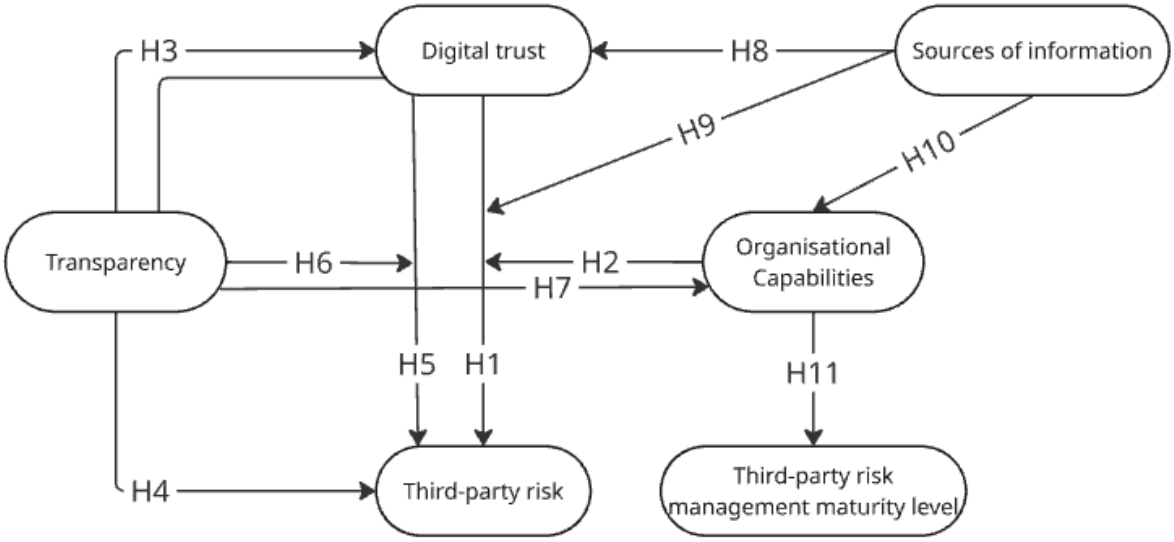


Figure 1.3. Research model

Source: Created by the author

Summarising the theoretical foundation of this research, the study builds on the integrative theory of trust and signalling theory, and, as a novel contribution, introduces information asymmetry theory and dynamic capabilities theory into trust-risk management research in digital settings. The analysis is conducted at the B2B level and is situated within a third-party risk management context. Finally, the level of third-party risk is treated as the dependent variable, an angle that has been explored in only a limited number of previous studies.

1.5. Research Design and Methodology

The research design of this doctoral thesis follows a mixed-methods approach that integrates theoretical analysis, quantitative empirical testing, and qualitative interpretation. This approach enables methodological triangulation and strengthens the reliability and credibility of the research findings. The overall research design is presented in Figure 1.4

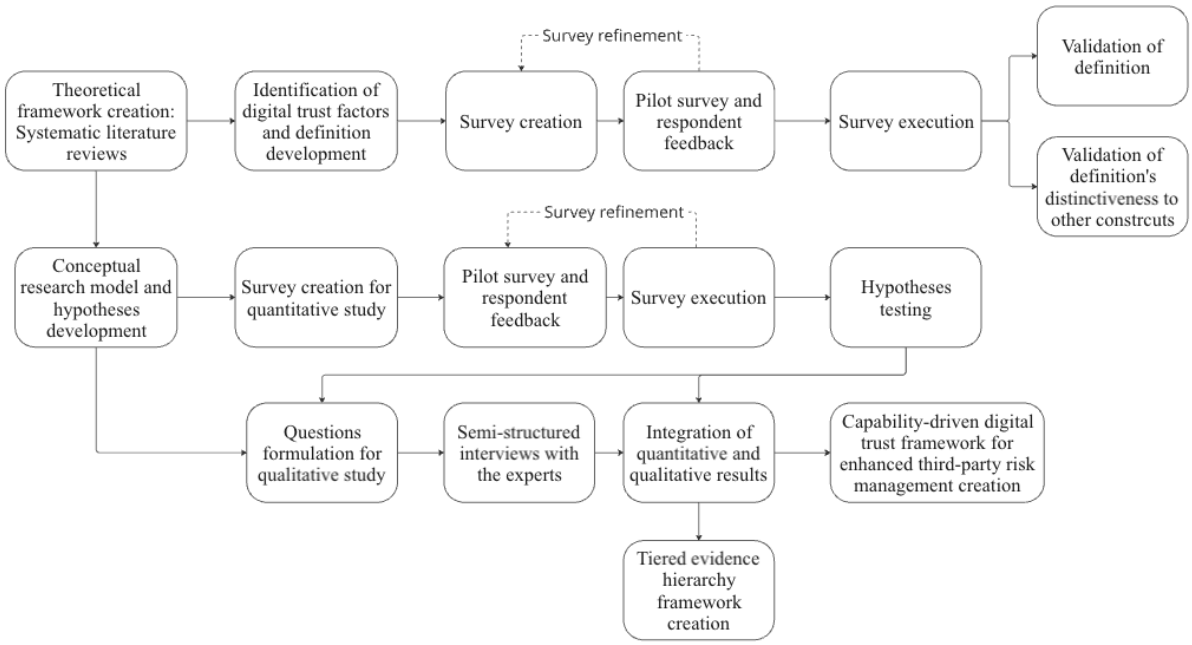


Figure 1.4. Research design

Source: Created by the author

The research begins with the creation of the theoretical framework based on SLRs employing the PRISMA methodology (Page et al. 2021). Six SLRs were conducted to analyse the existing body of knowledge on digital trust, third-party risk management, and the relationship between trust and risk management in digital environments, covering a total of 217 scientific publications.

The analysed literature included scientific publications indexed in the Scopus (Elsevier 2025) and Web of Science (Clarivate 2024) databases. Bibliometric analysis using the VOSviewer software tool (VOSviewer 2024) was applied to identify research patterns, publication trends, and thematic clusters within the analysed literature. In addition, content analysis was employed throughout the theoretical part of the thesis to examine the key characteristics of digital trust, third-party risk management and its frameworks, the distinction between third-party, vendor, supplier, and service provider risks, as well as the relationship between trust and risk management in a digital context.

Based on the results of the SLRs, a conceptual research model was developed and the research hypotheses were formulated. The literature review also enabled the identification of digital trust factors and the development of a holistic digital trust definition. To verify the reliability and clarity of the proposed definition, a construct validity procedure was conducted using survey data and content validity analysis methods (Colquitt et al. 2019; Kinkin and Tracey 1999). The process included a pilot survey (n = 5) to refine the wording of the questionnaire items, followed by the main content validation study with 99 respondents. During this stage, the htc index was calculated to assess the adequacy of the proposed digital trust definition, while the htd index was calculated to evaluate the distinctiveness of the definition in relation to other related constructs. The structure of the methodological framework and the main analytical stages of the research are presented in Figure 1.5.

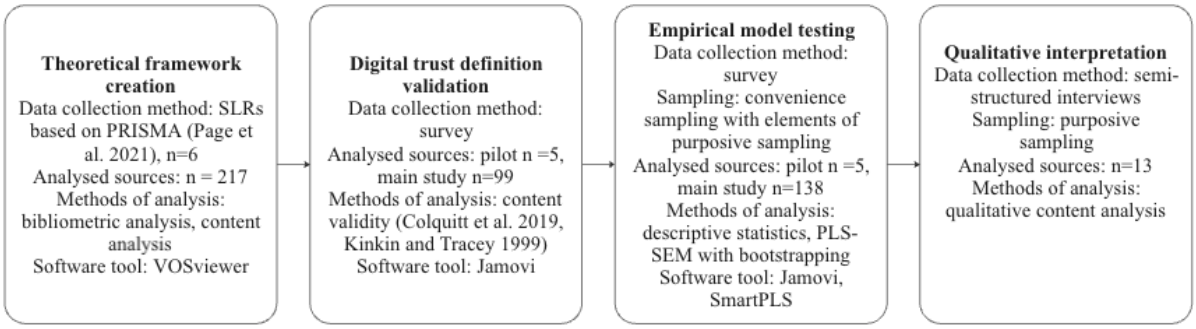


Figure 1.5. Mixed-methods methodological model

Source: Created by the author

The quantitative part of the research is based on a survey of employees working in the Baltic banking industry who are directly involved in third-party risk management activities. The survey was developed based on the theoretical framework and identified digital trust factors. A pilot survey (n = 5) was conducted to test the clarity and reliability of the questionnaire items, and the feedback obtained from respondents was used to refine the survey before the main data collection. The final survey employed a five-point Likert scale and collected 138 valid responses. The obtained sample provides a confidence level of 95% with a margin of error of 8.34%.

The sampling approach combines convenience sampling with elements of purposive sampling to ensure that respondents possess relevant experience in third-party risk management processes. The collected data were analysed using descriptive statistics in the Jamovi software (jamovi 2024) and PLS-SEM with bootstrapping in the SmartPLS software (Ringle et al. 2025). The PLS-SEM method was selected due to its suitability for analysing complex conceptual models with multiple constructs and relationships, including moderation and mediation effects. In addition, it was selected as the statistical testing method because of its proven effectiveness in examining trust and risk management relationships in a digital context, as this method was identified in 73% of the empirical papers analysed within the systematic literature review conducted in this thesis.

To obtain deeper insights into the empirical findings and the current practices of third-party risk management in the Baltic financial sector, the research also incorporates a qualitative methodological component. It is based on semi-structured expert interviews conducted with representatives of financial institutions across Estonia, Latvia, and Lithuania. The interviews were conducted using purposive sampling and included 13 experts with experience in risk management, compliance, cybersecurity, and vendor management functions.

The qualitative analysis aims to complement and interpret the quantitative results obtained from the survey and model testing. Qualitative content analysis was applied to examine expert perspectives on digital trust assessment practices, organisational capabilities for managing digital trust, and the future development of third-party risk management in the financial sector. The number of interviews was determined based on the principle of theoretical saturation, ensuring that sufficient depth of insight was obtained regarding the research topic.

Finally, the integration of quantitative and qualitative results enabled the development of a capability-driven digital trust framework for enhanced third-party risk management. In addition, based on the findings of the expert interviews, a tiered evidence hierarchy framework was proposed to support organisations in improving the reliability and quality of digital trust assessments when evaluating ICT third-party service providers.

Chapter 2 Summary: Evaluation of third-party risk management in the financial sector

2.1. Characteristics of the Baltic banking industry

The financial sector comprises wholesale, retail, formal, and informal institutions providing financial services to consumers, businesses, and other financial institutions (Department for International Development 2004). It includes credit institutions, payment institutions, insurance companies, pension and investment funds, and FinTech companies (Spitzer and Sabol 2025; Arner et al. 2015). Globally, the financial services market was valued at approximately 33.5 trillion United States (US) dollars in 2024, with projected growth to 35.85 US dollars in 2025 (Benchmark International 2024; Research and Markets, n.d.). In 2023, the EU financial sector (NACE Rev. 2 code "K") recorded 2.45 trillion euros in net turnover, while the Baltic financial sector accounted for 14,070 million euros, distributed across Estonia (4,127 million), Latvia (3,155 million), and Lithuania (6,788 million) (Eurostat 2025).

In total, 6,359 enterprises operated in the Baltic region under NACE code "K," although only 7.38% had at least 10 employees and 3.98% at least 20 employees, indicating a predominance of small entities (Eurostat 2025). The Baltic banking sector comprises 24 licensed credit institutions and 16 affiliated branches ("Latvijas Banka," n.d.; "Lietuvos Bankas," n.d.; "Eesti Pank," n.d.), with eight banks operating pan-Baltic and five largest institutions holding approximately 90% of the market share (Buch 2024).

The Baltic financial systems are highly integrated with the Nordic region and characterised by strong digitalisation. Digital transformation supports fintech innovation, reshapes value chains and delivery models, enhances operational efficiency, and promotes financial inclusion (Mavlutova et al. 2022; Ellex 2025).

2.2. Third-party risk management challenges in the Banking industry

Digitalisation expands financial institutions' market opportunities but simultaneously introduces new threats, including cyberattacks and money laundering, increasing the relevance of third-party risk management (Buch 2024). The Baltic banking industry operates within a highly regulated EU framework aimed at ensuring stability and resilience (Korneev et al. 2023).

The central regulation governing third-party ICT risks is the Digital Operational Resilience Act (DORA), applicable from January 2025 (European Commission 2022b). DORA establishes stringent requirements for ICT risk management, including third-party risk assessments, contractual safeguards, concentration risk analysis, sub-outsourcing controls, ICT registers, exit strategies, and data protection measures. It builds on the European Banking Authority (EBA) Guidelines on Outsourcing Arrangements (European Banking Authority 2019), which provided a foundation for managing outsourcing lifecycles and are currently being revised to align with DORA and extend coverage to non-ICT third-party risks (European Banking Authority 2025).

Industry data confirm the significance of the issue: 74.6% of financial institutions rank third-party risk among the top operational risks, while 46% question the effectiveness of their current practices (Operational Riskdata eXchange Association 2025). Taking into consideration the strict regulatory expectations placed on banks (Enria 2023) and the central role of the banking sector in the Baltic economies (Mavlutova et al. 2022), this research focuses on the Baltic banking industry. Moreover, given the emerging nature of third-party risk management practices and the newly introduced requirements for managing ICT third-party risks, the banking industry is expected to lead in implementing these practices, and banking professionals are expected to possess the relevant knowledge and skills to manage such risks effectively.

2.3. Digital trust impact on third-party risks of Baltic banks

Initially, the unit of analysis was defined at the organisational level, focusing on overall third-party risk and digital trust in suppliers. However, validation with three Baltic non-financial risk professionals revealed that even organisations with defined or integrated third-party risk management maturity levels lacked a portfolio-level view of third-party risks and could not assess overall digital trust in ICT vendors. Consequently, the unit of analysis was shifted to the third-party level.

The survey was redesigned accordingly, piloted with five banking risk management professionals, and launched on 30 April 2025. It was distributed across the Baltic financial sector using random and snowball sampling, including direct outreach to approximately 250 professionals, LinkedIn dissemination, distribution via Baltic financial and risk management associations, and targeted contact with employees of licensed credit institutions and branches. More than 200 connection requests and 80 direct messages were sent.

The outreach targeted professionals in risk, compliance, IT, audit, and security roles, reflecting the fragmented governance of third-party risk management (Ncontracts 2025). Feedback confirmed limited ownership and awareness across organisations, consistent with ORX findings that centralisation of third-party risk management remains incomplete (Operational Riskdata eXchange Association 2025). he survey remained open until 15 June 2025 and resulted in 157 responses from banking industry employees. The modest response rate aligns with industry data showing that 73% of institutions have two or fewer full-time employees dedicated to vendor risk management (Ncontracts 2025).

Participation was limited to financial sector representatives from the Baltic countries. After excluding one geographically invalid response (Sweden), 156 responses were retained. Additional data quality checks identified identical responses across digital trust factors (n = 10) and across third-party risk categories (n = 8). These responses were excluded, resulting in a final sample of 138 responses. Further, Harman's single-factor test was conducted to assess potential common method bias, as all variables were collected using a self-reported questionnaire (Podsakoff et al. 2003). The first factor explained 26.6% of the total variance, which is below the recommended 50% threshold, indicating that common method bias is unlikely to significantly affect the results.

The study, therefore, operates at a 95% confidence level with an 8.34% margin of error (Calculator.net 2026).

Most respondents were from Latvia (n = 59, 42.8%), followed by Lithuania (n = 45, 32.6%) and Estonia (n = 32, 23.2%), with two pan-Baltic respondents (1.4%). In total, 28 roles were reported and consolidated into five groups: IT (n = 46, 33.3%), Business and Commercial (n = 40, 29.7%), Risk Management (n = 23, 16.7%), Compliance and Security (n=17, 12%) and Operations and Support (n=12, 9%). This split indicates representation from multiple stakeholders involved in ICT third-party management.

Regarding third-party risk management maturity (Capability Maturity Model Integration Institute's described levels of maturity scale 1 - 5), 84.1% (n = 116) assessed their organisation at least at Level 3 ("Defined"), with an average maturity of 3.57 and a median of 4, demonstrating a general tendency towards quantitatively managed practices (CMMI Institute, n.d.). These results confirm the adequacy of the sample for further analysis of ICT third-party risks.

Respondents were asked to select one ICT third-party service provider with which they were directly involved and to assess its level of digital trust before evaluating third-party risks, to reduce common method bias. A 5-point Likert scale (1 = strong disagreement; 5 = strong agreement) was applied, with an "N/A" option available when information was lacking. Digital trust was operationalised through nine sub-categories grouped into four categories: Ability, Benevolence, Integrity, and Openness, each represented by two statements derived from the theoretical framework.

For analysis, mean values were calculated at sub-category, category, and overall digital trust levels. The Shapiro-Wilk test was performed to assess normality, and descriptive statistics were calculated using JAMOVI (jamovi 2026). The results indicate that respondents assessed a generally trustworthy ICT third party (overall mean = 4.11), with similar means across Ability (4.09), Benevolence (4.07), Integrity (4.19), and Openness (4.11). The average standard deviation was 0.82, confirming internal consistency, while Shapiro-Wilk results ($W = 0.750–0.945$; $p < .001$) indicated non-normal distribution. Some missing values occurred, primarily within the Openness category (Auditability and Traceability), but this did not significantly affect further analysis.

The next survey block measured the level of ICT third-party risks faced by the respondent's organisation. Risks were assessed on a 5-point scale (1 = very low; 5 = very high), without an "N/A" option, as non-relevance was interpreted as very low risk. Based on the theoretical framework, seven thematic categories of third-party risks and five sub-categories were operationalised and assessed separately (twelve third-party risks in total), as they represent distinct risk types and cannot be consolidated.

Overall, the assessed third-party risk level was medium-low (mean = 2.19), which aligns with the assumption that financial institutions typically cooperate with relatively low-risk ICT providers. The highest mean risk was concentration and contingency risk (R2.3; mean = 2.68), while the lowest was corporate social responsibility risk (R6.2; mean = 1.73).

Shapiro-Wilk test results ($W = 0.756–0.945$; $p < .001$) indicated non-normal distribution. Standard deviations ranged from 0.948 to 1.227, reflecting variability across different ICT third parties. As respondents evaluated existing providers, the reported risks largely represent inherent risk levels after preventive controls. The most current third-party risk priorities in the financial industry were further explored through expert interviews.

The next survey block examined the clarity and accessibility of DT assessment criteria applied to ICT third parties and the transparency of the information sources used for evaluating their DT level. Respondents assessed three author-developed statements (TRAN1, TRAN2 and TRAN3) on a 5-point Likert scale (1 = completely disagree; 5 = fully agree), aimed at capturing whether third parties are aware of how their digital trustworthiness is evaluated and whether this transparency supports alignment with organisational trust expectations, thereby reflecting the role of agency theory in the relationship between digital trust and third-party risks.

Overall, respondents tended to agree that the DT evaluation process was transparent (mean = 3.71; median = 4.00). Individual statement means ranged from 3.57 to 3.93, with standard deviations between 0.928 and 0.949, indicating consistent responses. The Shapiro–Wilk test confirmed non-normal data distribution ($W = 0.838–0.938$; $p < .001$). These findings suggest a generally transparent DT assessment process across the surveyed organisations.

The second set of questions aimed to identify which sources of information are most frequently used and perceived as effective for assessing the DT of ICT third parties - how ICT third parties communicate their digital trustworthiness. Four statements (SOU1 - SOU4), developed based on the DT communication methods identified in the theoretical analysis, were assessed on a 5-point Likert scale (1 = completely disagree; 5 = fully agree). Additionally, respondents could provide alternative sources of information in an open-ended question.

The results indicate that the most commonly used source of information for DT assessment is the documentation of the provider's solution, including technical and architectural descriptions (mean = 4.06), followed by proof of reputation (mean = 3.93). Ratings and feedback from partners and customers were used less frequently (mean = 3.14), while reliance on blockchain technology as a trust indicator was rare (mean = 2.49). Standard deviations ranging from 0.983 to 1.426 suggest variation in assessment practices across organisations. The Shapiro–Wilk test confirmed non-normal data distribution ($W = 0.807–0.903$; $p < .001$).

Open-ended responses (n = 23) revealed 39 sources used in practice, which were incorporated into a word cloud by the author in Figure 2.1. It included ISO 27001 certifications,

audited financial statements, governmental registry data, credit bureau and court case information, internal stakeholder feedback, previous cooperation experience, internal policies (e.g., security and data protection), business continuity plans, service level agreements, data protection agreements, internally developed questionnaires, security scanning and penetration test results, public information, case studies, demo sessions, and evaluation of third-party staff competence. These findings demonstrate that organisations apply a broad and multifaceted set of information sources when assessing digital trustworthiness.

Figure 2.1. Word cloud with the sources of information used for DT assessments

Source: created by the author

The final survey block was conducted at the organisational level and aimed to assess how extensively organisations implement DT assessment and management practices for ICT third parties. The statements were developed based on the dynamic capabilities framework (sensing (SEN1 and SEN2), seizing (SEI1 and SEI2), and reconfiguring (REc1 and REC2)) and adapted to the context of DT assessment, using a 5-point scale (1 = not implemented at all; 5 = fully implemented).

The results indicate that organisations represented by the respondents demonstrate stronger seizing and reconfiguring capabilities (both mean = 3.72), while sensing capability is slightly less developed (mean = 3.58). In particular, collecting and analysing trust-related information (SEN1 mean = 3.86), integrating DT data into risk management and vendor selection (SEI1 mean = 3.92), and continuously improving assessment methods (REC1 mean = 3.91) are more implemented than continuous monitoring of trust level changes (SEN2 mean = 3.30), formal response protocols (SEI2 mean = 3.52), and investments in technology and expertise (REC2 mean = 3.53).

Standard deviations (0.785- 1.05) suggest moderate consistency across organisations. The Shapiro–Wilk test confirmed non-normal data distribution ($W = 0.838–0.945$; $p < .001$).

Afterwards, statistical calculations were performed using SmartPLS v.4.1.1.4 (Ringle et al. 2025). For all models, the PLS-SEM algorithm with the factor weighting scheme was applied first, followed by bootstrapping with the path weighting scheme, 5,000 subsamples and a one-tailed test, since the direction of the hypotheses was known.

Design and testing of Model 1

The Model 1 (depicted in Figure 2.2) was designed to test the impact of DT on each type of third-party risk.

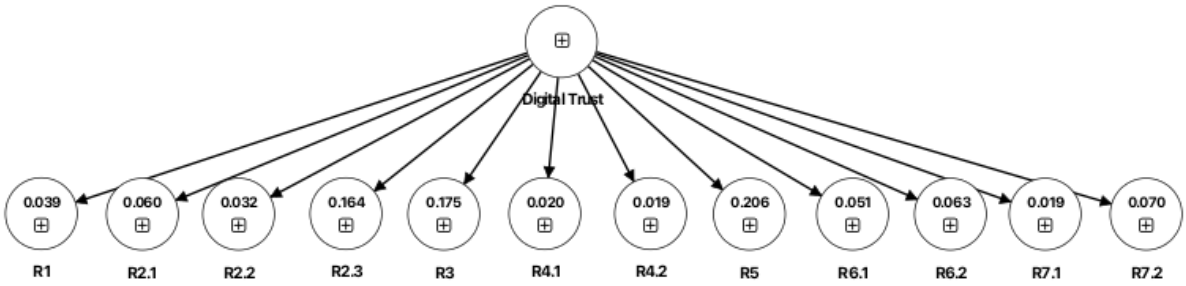


Figure 2.2. Model 1 design with R^2 values calculated
Source: created by the author

Digital Trust was modelled as one reflective construct comprising 18 measurable items representing nine factors. Heterotrait-monotrait ratio (HTMT) analysis showed insufficient discriminant validity for modelling DT as four separate categories or distinct factors, as several HTMT values exceeded the recommended threshold of 0.85 (Franke and Sarstedt 2019). Therefore, DT was retained as one higher-order construct. In contrast, third-party risks were included as separate observable risk categories in order to assess DT's impact on each specific risk type. All variables were subsequently tested for model fit.

Regarding **outer loadings**, seven of the eighteen DT items exceeded the recommended threshold of 0.708 (Joe F. Hair et al. 2020), while the remaining items were below this level. This result is explained by the multidimensional nature of DT, which consists of nine sub-categories. As the removal of these items was not required to improve internal consistency, reliability, or convergent validity, all items were kept in the measurement model (Joseph F. Hair et al. 2021a).

Construct reliability indicators demonstrated strong internal consistency: Cronbach's alpha reached 0.929 and composite reliability 0.937, both well above the 0.7 threshold. **Convergent validity**, measured by the average variance extracted (AVE), was slightly below the recommended level (0.455) but close to 0.5, indicating an acceptable level of shared variance among the items.

Discriminant validity between DT and third-party risk categories was confirmed using the HTMT ratio, with all values below 0.85, demonstrating clear differentiation among the latent variables. **Collinearity statistics** also showed no multicollinearity concerns, as all values were well below the threshold of 10 (maximum 3.011). Overall, the measurement model demonstrated acceptable reliability and validity for further structural analysis.

Afterwards, the inner model analysis results were interpreted to predict capacity power and the effect of DT on third-party risks. Given the smallest statistically significant path coefficient ($\beta = -0.138$), the sample size ensured sufficient power (0.80) to detect effects at the 10% level (Joseph F. Hair et al. 2021b).

According to Hair et al. (2011), the interpretation of R^2 significantly depends on the context. While the rule of thumb is to interpret R^2 values of 0.75, 0.50, or 0.25 as substantial, moderate, or weak, respectively, in some social science disciplines, a 0.20 value is considered high. According to Falk and Miller (1992), an adequate R^2 value for a model fit is at least 0.10 and above.

When interpreting R^2 values, it should be considered that third-party risk management is a developing area without established R^2 thresholds. Therefore, based on the analysis results, it can be concluded that DT has adequate predictive power for concentration risk and contingency planning (R2.3; 0.164), financial risks (R3; 0.175), and strategic risks (R5; 0.206), with sufficient statistical power to detect effects.

DT has a statistically significant negative impact on 10 of 12 third-party risks. The strongest negative relationships are with concentration risk (R2.3), financial risks (R3), and

strategic risks (R5). Small-to-medium negative effects are observed for fourth-party risks (R7.2), general operational risks (R2.1), reputational risks (R6.1), and CSR risks (R6.2). Smaller effects are found for regulatory (R1), supply chain (R2.2), and data privacy risks (R4.2). DT has no standard statistically significant (≥ 95%) effect on vendor and supply chain cybersecurity risks (R4.1) and partner-specific factors risks (R7.2), and this correlation has exploratory significance. The latter may be explained by strict Anti-Money Laundering (AML), sanctions, and data protection requirements limiting cooperation with high-risk jurisdictions, while the absence of significance for cybersecurity risks required further expert discussion. Therefore, the author assumes that these findings **confirm all sub-hypotheses**, with the direct impact of DT on third-party risk types, except for **rejected hypotheses H1f** and **H1j**. The results are summarised in Table 2.1 below.

Table 2.1. Inner Results of Model 1

	R^2	Path Coefficient	P Value		R^2	Path Coefficient	P Value
R1	0.039	-0.199	0.017	R4.2	0.019	-0.138	0.050
R2.1	0.060	-0.246	0.002	R5	0.206	-0.454	0.000
R2.2	0.032	-0.179	0.013	R6.1	0.051	-0.227	0.006
R2.3	0.164	-0.405	0.000	R6.2	0.063	-0.250	0.002
R3	0.175	-0.419	0.000	R7.1	0.019	-0.137	0.068
R4.1	0.020	-0.140	0.057	R7.2	0.070	-0.265	0.002

Source: created by the author

Design and testing of Model 2: full data sample

Further, Model 2 was created to test other hypotheses. **Digital Trust** was modelled as in Model 1, as one reflective construct. **Third-party risk** was modelled as a reflective variable including all 12 third-party risks. **Transparency** in DT evaluation was specified as a reflective construct assessing the clarity and accessibility of DT assessment criteria. **Capability** was modelled as a single reflective construct of six items and not split into sensing, seizing, and reconfiguring dimensions due to insufficient discriminant validity. The **source of information** was modelled as a reflective latent variable comprising four types of informational sources, while **third-party risk management maturity** was included as a separate observable item. Model 2 design is presented in Figure 2.3 below.

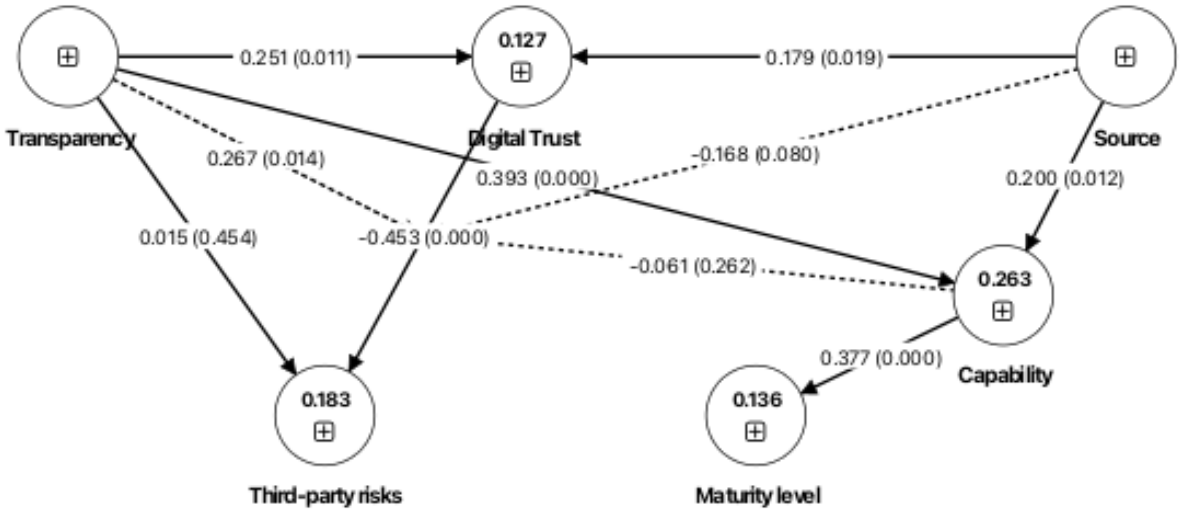


Figure 2.3. Model 2 design with R2 adjusted values, path coefficients and p-values calculated

Source: created by the author

Outer loadings were largely consistent with Model 1. Most Capability and Transparency items exceeded the 0.708 threshold; third-party risk items were partly above and partly slightly below the threshold (lowest R3 = 0.597), which was accepted due to their multidimensional nature. Three Source items exceeded the threshold, with SOU4 slightly below (0.614), which was considered acceptable.

Reliability and validity indicators confirmed adequate measurement quality. Cronbach's alpha exceeded 0.7 for four constructs, with Source slightly below (0.663), but acceptable when rounded. **Composite reliability** values were above 0.7, and AVE values were close to or slightly below 0.5 for some constructs, still indicating sufficient convergent validity. HTMT ratios confirmed **discriminant validity**, with all values below 0.85. **Collinearity statistics** were well below the threshold of 10, confirming the robustness of the model.

Afterwards, the model was checked for a fit. The analysis demonstrated adequate predictive power for all latent variables, with the model exhibiting the greatest predictive power for the capability level (R^2 adj. = 0.263) and the third-party risks level (R^2 adj. = 0.182). Further, bootstrapping was calculated, and the results are presented in Table 2.2 below.

Table 2.2. Inner Results of Model 2

	Digital Trust		**Third-party risks**		**Capability**		**Maturity level**	
R^2 adj.	0.127		0.183		0.263		0.136	
	Path coef.	p-value	Path coef.	p-value	Path coef.	p-value	Path coef.	p-value
Digital trust			-0.453	0.000				
Capability							0.377	0.000
Transparency	0.251	0.011	0.015	0.454	0.393	0.000		
Source	0.179	0.019			0.200	0.012		

Source: Created by the author

According to the performed tests, digital trust has a statistically significant negative impact on third-party risks (β = -0.452, p = 0.000), **confirming H1** that digital trust reduces third-party risks.

Transparency in DT assessment has a small but significant positive effect on digital trust (β = 0.251, p = 0.011), **confirming H3**. However, transparency does not have a direct significant impact on third-party risks (β = 0.014, p = 0.458); instead, its effect is fully mediated by digital trust (β = -0.114, p = 0.023). Thus, **H4 is rejected**, while **H5**, stating that digital trust mediates the relationship between transparency and third-party risks, is **confirmed**. At the same time, transparency significantly moderates the impact of digital trust on third-party risks (β = 0.267, p = 0.014), **confirming H6**, although higher transparency may reduce the strength of digital trust's negative effect on risks. The moderation and mediation results of Model 2 are presented in Table 2.3 below.

Table 2.3. Moderation and mediation test results of Model 2

Test	**Path coef.**	**p-value**
Capability x Digital Trust -> Third-party risks	-0.061	0.262
Source x Digital Trust -> Third-party risks	-0.168	0.080
Transparency x Digital Trust -> Third-party risks	0.267	0.014
Transparency -> Digital Trust -> Third-party risks	-0.114	0.023
Source -> Capability -> Maturity level	0.075	0.043
Transparency -> Capability -> Maturity level	0.148	0.001

Source: Created by the author

The extensive use of various information sources has a small but significant positive impact on digital trust (β = 0.179, p = 0.019), **confirming H8**, but does not significantly moderate the DT–risk relationship (β = -0.168, p = 0.080), leading to the **rejection of H9**. Transparency (β = 0.393, p = 0.000) and use of information sources (β = 0.200, p = 0.012) both positively impact organisational capabilities for digital trust assessment, **confirming H7** and **H10**. Organisational capability, in turn, has a moderate positive impact on third-party risk management maturity (β = 0.377, p = 0.000), **confirming H11**. The effects of transparency and information usage on maturity are small but significant and mediated by capability.

However, organisational capability does not significantly moderate the effect of digital trust on third-party risks (β = -0.063, p = 0.258), leading to the **rejection of H2**. A possible explanation lies in the difference in measurement levels: digital trust and risks were assessed at the third-party level, while capability was measured at the organisational level, and respondents may not have had full visibility of organisation-wide digital trust governance practices.

Design and testing of Model 2: governance-level group sample

An additional explanatory analysis was conducted using Model 2 with a selected subset of respondents involved in organisational-level digital trust assessment and monitoring (risk managers and compliance/security roles; n = 40), referred to as the "governance-level group" to test the previously described assumption.

Outer loadings were comparable to the full data set and remained within acceptable ranges, even where below 0.7, due to the multidimensional nature of organisational capability, sources of information, digital trust, and third-party risk.

Reliability and validity results were broadly consistent with the full sample. The only construct below recommended reliability thresholds was "sources of information" (Cronbach's alpha = 0.642; composite reliability = 0.637). **AVE values** for "sources" (0.491) and "third-party risks" (0.470) were slightly below 0.5 but acceptable when rounded.

Discriminant validity (HTMT) confirmed conceptual distinctness of all constructs (values below 0.85). **Collinearity** was not a concern, as all VIF values were below 10, despite relatively higher values for RC1 (8.012), TR1 (7.014), and AU (6.963).

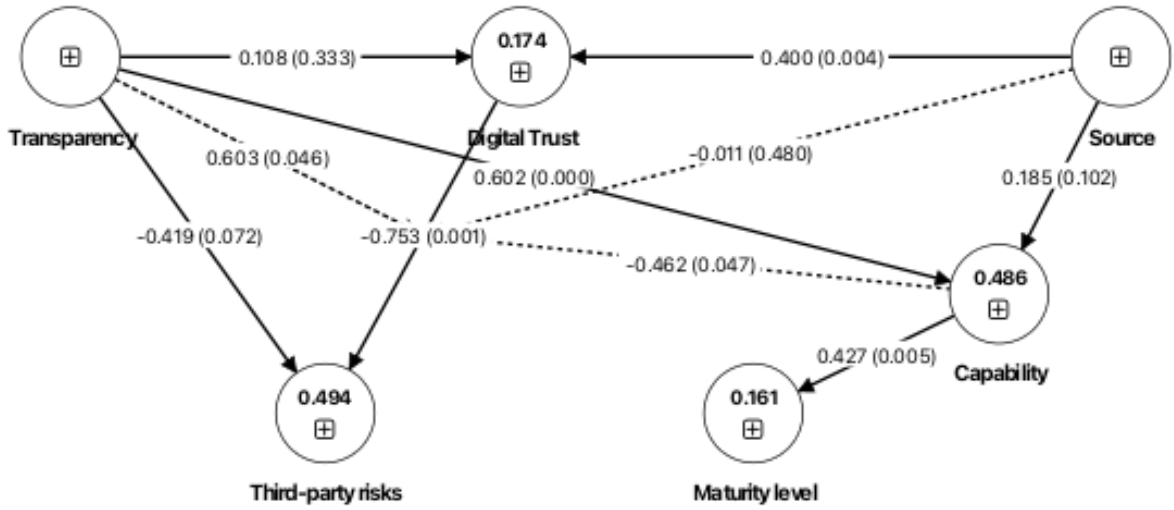


Figure 2.4. Model 2 design (governance-level group) with R^2 adjusted values, path coefficients and p-values calculated

Source: created by the author

The Model 2 with governance-level data set (Figure 2.4) has significantly better, strong predictive power for the digital trust negative impact on third-party risk level (R^2 adj. 0.494 compared with R^2 adj. 0.183 for complete data set) and source of information and transparency

of digital trust assessment to the organisational capabilities (R^2 adj. 0.486 vs R^2 adj. 0.263 for complete data set). Inner results for Model 2, using governance-level group data, are presented in Table 2.4.

Table 2.4. Inner Results of Model 2 (governance-level group)

	Digital Trust		**Third-party risks**		**Capability**		**Maturity level**	
R^2 adj.	0.174		0.494		0.486		0.161	
	Path coef.	p-value	Path coef.	p-value	Path coef.	p-value	Path coef.	p-value
Digital trust			-0.753	0.001				
Capability							0.427	0.005
Transparency	0.108	0.333	-0.419	0.072	0.602	0.000		
Source	0.400	0.004			0.185	0.102		

Source: Created by the author

The performed test for governance-level group data set confirmed the following results obtained while testing with the complete data set:

- **H1** was strongly supported, with digital trust reducing third-party risks with even higher predictive power ($\beta = -0.753$, $p = 0.001$), reinforcing that the negative relationship between trust and perceived risk, as described by Mayer et al. (1995), also works in digital B2B contexts involving ICT service providers.
- **H4** was again rejected ($\beta = -0.419$, $p = 0.072$), confirming that transparency in digital trust assessment during onboarding does not directly reduce third-party risks, which appear to remain independent of transparency levels.
- **H6** was confirmed with a stronger moderation effect ($\beta = 0.603$, $p = 0.046$), indicating that transparency weakens the negative impact of digital trust on third-party risks. This finding contradicts information asymmetry theory but supports signalling theory, suggesting that when ICT third parties understand assessment criteria, they may strategically manage signals to create a perception of trustworthiness — a view also supported by expert interviews.
- **H7** was confirmed with strong positive power ($\beta = 0.602$, $p = 0.000$), demonstrating that transparency enhances organisational capabilities for digital trust assessment and management.
- **H8** was confirmed ($\beta = 0.400$, $p = 0.004$), showing that extensive use of diverse information sources positively influences digital trust, consistent with signalling theory.
- **H9** was rejected ($\beta = -0.011$, $p = 0.480$), as information sources did not moderate the relationship between digital trust and third-party risks.
- **H11** was confirmed ($\beta = 0.427$, $p = 0.005$), indicating that organisational capabilities for digital trust assessment and management positively impact the maturity of third-party risk management, supporting dynamic capabilities theory in this context. Moderation and mediation test results for Model 2 are presented in Table 2.5 below.

Table 2.5. Moderation and mediation test results of Model 2 (governance-level group)

Test	Path coefficient	p-value
Capability x Digital Trust -> Third-party risks	-0.462	0.047
Source x Digital Trust -> Third-party risks	-0.011	0.480
Transparency x Digital Trust -> Third-party risks	0.603	0.046
Transparency -> Digital Trust -> Third-party risks	-0.081	0.341
Source -> Capability -> Maturity level	0.079	0.148
Transparency -> Capability -> Maturity level	0.257	0.010

Source: Created by the author

In the governance-level subgroup, several results differed from the full data set. Hypothesis **H2** was **confirmed**, showing a statistically significant and close-to-strong negative moderation effect ($\beta = –0.462$, $p = 0.047$). This indicates that, among respondents aware of governance-level practices, stronger organisational capabilities for digital trust assessment enhance the reducing impact of digital trust on perceived third-party risks.

In contrast, hypotheses related to transparency during onboarding were not supported. **H3** ($\beta = 0.108$, $p = 0.333$) and **H5** ($\beta = –0.081$, $p = 0.341$) **were not statistically significant**, suggesting that the transparency effects observed in the full sample were not replicated among governance-level respondents. A possible explanation is that governance-level professionals are typically involved in designing and overseeing digital trust assessment processes rather than managing specific third-party relationships. For them, transparency during onboarding may be less directly linked to perceived trust and risk.

Finally, **H10** was also **rejected** ($\beta = 0.185$, $p = 0.102$). The use of multiple information sources did not significantly impact organisational capability within this subgroup. From a dynamic capabilities perspective, this may reflect the distinction between possessing information resources and having the institutionalised ability to integrate and reconfigure them. These differences between the two samples were further explored during expert interviews. A full summary of the hypothesis testing results is presented in Table 2.6 below.

Table 2.6. Results of the hypotheses testing

Code	Hypothesis	Model	Sample	Effect	Result
H1	Digital trust reduces third-party risks.	Model 2	Full	Direct	Confirmed
			Governance-level group	Direct	Confirmed
H1a	Digital trust reduces regulatory and compliance risks.	Model 1	Full	Direct	Confirmed
H1b	Digital trust reduces general operational risks.	Model 1	Full	Direct	Confirmed
H1c	Digital trust reduces supply chain and partner process issues risks.	Model 1	Full	Direct	Confirmed
H1d	Digital trust reduces concentration and contingency planning risks.	Model 1	Full	Direct	Confirmed
H1e	Digital trust reduces financial risks.	Model 1	Full	Direct	Confirmed
H1f	Digital trust reduces vendor and supply chain cybersecurity risks.	Model 1	Full	Direct	Rejected

H1g	Digital trust reduces data privacy risks.	Model 1	Full	Direct	Confirmed
H1h	Digital trust reduces strategic risks.	Model 1	Full	Direct	Confirmed
H1i	Digital trust reduces reputational and conflict of interest risks.	Model 1	Full	Direct	Confirmed
H1j	Digital trust reduces corporate social responsibility risks.	Model 1	Full	Direct	Confirmed
H1k	Digital trust reduces partner-specific factors.	Model 1	Full	Direct	Rejected
H1l	Digital trust reduces fourth-party and N-th-party risks.	Model 1	Full	Direct	Confirmed
H2	The effect of digital trust on reducing third-party risks is moderated by the organisation's capabilities for digital trust assessment and management.	Model 2	Full	Moderation	Rejected
			Governance-level group	Moderation	Confirmed
H3	A higher level of transparency in digital trust assessment during third-party onboarding positively impacts digital trust.	Model 2	Full	Direct	Confirmed
			Governance-level group	Direct	Rejected
H4	Higher transparency in digital trust assessment during third-party onboarding reduces third-party risks.	Model 2	Full	Direct	Rejected
			Governance-level group	Direct	Rejected
H5	Digital trust acts as a mediator between transparency in digital trust assessment during third-party onboarding and the level of third-party risk.	Model 2	Full	Mediation	Confirmed
			Governance-level group	Mediation	Rejected
H6	The effect of digital trust on reducing third-party risk is moderated by the level of transparency in digital trust assessment during third-party onboarding.	Model 2	Full	Moderation	Confirmed
			Governance-level group	Moderation	Confirmed
H7	The level of transparency in digital trust assessment during the onboarding of a third-party has a positive impact on the level of organisational capabilities for digital trust assessment.	Model 2	Full	Direct effect	Confirmed
			Governance-level group	Direct effect	Confirmed
H8	The extensive use of various sources of information for digital trust assessment has a	Model 2	Full	Direct	Confirmed
			Governance-level group	Direct	Confirmed

	positive impact on the level of digital trust.				
H9	The effect of digital trust on reducing third-party risks is moderated by the extensive use of various sources of information for digital trust assessment.	Model 2	Full	Moderation	Rejected
			Governance-level group	Moderation	Rejected
H10	The extensive use of various sources of information for digital trust assessment has a positive impact on organisational capability for digital trust assessment.	Model 2	Full	Direct effect	Confirmed
			Governance-level group	Direct effect	Rejected
H11	Organisational capabilities for digital trust assessment and management positively impact the maturity of third-party risk management.	Model 2	Full	Direct effect	Confirmed
			Governance-level group	Direct effect	Confirmed

Source: created by the author

In summary, the hypothesis-testing results confirm that digital trust reduces third-party risk, although the magnitude of this effect varies by risk type and respondent group. The findings also show that organisational capabilities for assessing and managing digital trust play an important role in higher third-party risk management maturity. At the same time, mixed results for transparency and information sources indicate that digital trust depends not only on the availability of information but also on the organisation's ability to interpret and integrate it into governance and risk management practices. Therefore, the observed differences between the full sample and the governance-level group were further explored through expert interviews.

Chapter 3 Summary: Qualitative insights on digital trust and third-party risks: findings and recommendations

Following the quantitative analysis and hypothesis testing, the study proceeded to a qualitative phase involving semi-structured interviews with industry experts. The aim was to discuss the initial findings, gather insights for developing a capability-driven DT framework for enhanced TPRM and explore the future development of Third-party Risk Management (TPRM) in the Baltic banking industry.

The interviews involved experts directly engaged in ICT third-party relationships and risk management across Latvia, Lithuania, and Estonia. Various stakeholder perspectives were represented, including IT risk, non-financial risk, information security, compliance, third-party relationship management, procurement, and legal functions. Although some Baltic banks belong to Nordic groups, none of the experts indicated that ICT third-party risk management was outsourced to parent banks. Theoretical saturation was achieved within the Baltic expert group.

The sample was deliberately limited to practitioners responsible for the day-to-day assessment and management of ICT third-party risks. Representatives of supervisory authorities and consultancy firms were excluded, as they observe such risks externally rather than manage them operationally.

Interviews were conducted remotely via Microsoft Teams between 18 July and 1 August 2025. The final sample consisted of 13 experts representing different Baltic countries and roles within banking institutions. The list of experts, their countries, and their roles is presented in Table 3.1. below.

Table 3.1. The list of experts who participated in the interviews.

	Code	**Country**	**Role**
Expert 1	E1	Latvia	Third-party relationship manager
Expert 2	E2	Lithuania	IT risk manager
Expert 3	E3	Lithuania	Non-financial risk manager
Expert 4	E4	Latvia	IT risk manager
Expert 5	E5	Latvia	Information security manager
Expert 6	E6	Estonia	Third-party risk manager
Expert 7	E7	Lithuania	Third-party relationship manager
Expert 8	E8	Latvia	Compliance manager
Expert 9	E9	Estonia	Information security manager
Expert 10	E10	Lithuania	Information security manager
Espert 11	E11	Estonia	IT risk manager
Expert 12	E12	Latvia	Lawyer
Expert 13	E13	Estonia	Purchasing manager

Source: created by the author

Participation was voluntary and anonymous; informed verbal consent was obtained to avoid storing personal data. Transcripts were recorded, manually edited, anonymised, and proofread. Before each interview, a short introductory presentation explained the study design, model, and research questions.

3.1.Third-party risk category findings and tests of the hypotheses

Experts most frequently identified vendor and supply chain cybersecurity risks (R4.1) and regulatory and compliance risks (R1) as the most relevant ICT third-party risks, particularly in light of DORA. These were followed by data privacy risks (R4.2) and fourth- and Nth-party risks (R7.2).

While there was alignment between survey and expert views on security and privacy risks, regulatory and fourth/Nth-party risks were not among the highest in the survey results. This divergence may be explained by the survey methodology, as respondents assessed existing ICT providers where mitigation measures were already applied, reflecting inherent rather than gross risk levels.

Experts agreed that concentration and contingency risks (R2.3) may represent the highest inherent risks. Key drivers include the monopolised Baltic ICT market (e.g., telecommunications), preference for large established vendors, and regulatory pressures such as DORA that encourage supplier consolidation. The low rating of corporate social responsibility (CSR) risk (R6.2) was explained by its perceived irrelevance for EU-based ICT providers, limited sanctions, and possible underestimation or lack of verification of CSR claims.

Based on expert opinions, organisations should prioritise the following third-party risks in their programmes:

1. Security and privacy (both R4.1 and R4.2)
2. Supply-chain exposure through fourth- and N-party dependencies (R7.2),
3. Regulatory and compliance obligations, particularly under DORA (R1)

Survey results, however, indicate higher inherent levels for below risks that should therefore be continuously monitored throughout the third-party management lifecycle:

1. Concentration and contingency planning (R2.3; mean 2.68),
2. Supply-chain and process risks (R2.2; mean 2.51),
3. Strategic dependence (R5; mean 2.33),
4. Vendor and supply-chain cybersecurity (R4.1; mean 2.32) and data privacy (R4.2; mean 2.31).

The above indicates that both perspectives are necessary for a balanced view of third-party risk management priorities.

Discussion of hypothesis testing results with experts

Experts generally accepted the absence of correlation between digital trust and third-party cybersecurity risk (**H1f).** The main explanation was that cyberattacks are externally driven and stochastic ("not if but when"), and even mature or trusted vendors remain vulnerable. Digital trust is often assessed pre-contractually (service quality, governance, continuity), while cybersecurity exposure depends on evolving external threats. Experts also noted possible perception bias in questionnaire-based trust assessments, where high trust scores may not reflect actual cyber exposure.

Regarding **H2** (DT and third-party risk moderation by organisational capabilities)**,** experts agreed that digital trust capabilities should strengthen the reducing effect of digital trust on third-party risks. The difference between the full sample and governance-level group was explained by role visibility: second-line functions (risk, compliance, legal) have an end-to-end view of the lifecycle and governance mechanisms, while first-line roles see only parts of the process. Some experts highlighted a "theory versus practice" gap, where governance roles assume frameworks work as designed, while operational roles respond based on practical execution.

For **H3** (transparency increasing digital trust)**,** experts found both dataset testing results plausible. Transparency may increase perceived trust among operational stakeholders, but governance-level roles rely on verification rather than process openness. Some warned that transparency may allow vendors to "reverse-engineer" assessment criteria and inflate perceived trust.

The rejection of **H5** (DT mediation of transparency and third-party risk) was largely supported. Experts argued that transparency can increase perceived trust without reducing actual exposure, as vendors may optimise documentation to "pass the test." Risk scoring remains evidence-based and may even increase when more information surfaces.

For **H10** (sources of information increasing capability)**,** governance-level experts emphasised that capability depends not on the quantity but on the quality and effective use of information sources. Once a baseline is met, additional sources add limited value. Some prefer a single reliable "golden source" over multiple fragmented inputs.

Finally, **H9** (sources of information moderating DT – third-party risk relationship) was rejected by experts. They agreed that additional sources may refine trust assessments, but do not alter underlying structural risks. Risk reduction requires improved controls or mitigation measures, not merely more information.

Theoretical implications

The results of the hypotheses testing, together with the expert interviews, provide evidence on the applicability and limitations of the theoretical frameworks adopted in this thesis.

Most findings for H1 and its sub-hypotheses confirm the Integrative Model of Organisational Trust (Mayer et al. 1995): higher digital trust is associated with lower third-party risk, particularly in categories where the provider's behaviour, controls, and governance directly influence risk outcomes (e.g., regulatory, operational, supply-chain risks). However, predictive power is limited for risks driven by external or structural factors (e.g., cybersecurity exposure, geopolitical risks), confirming that trust as willingness to be vulnerable does not always translate into measurable risk reduction.

H2 received partial confirmation of the moderating role of organisational capabilities (Teece et al., 1997). Organisational capabilities moderate the DT–risk relationship only within the governance-level group. Expert feedback highlighted role-based visibility as the explanation, with second-line functions better positioned to evaluate capability effects. H7 was confirmed in both samples, indicating that transparency embedded in structured assessment processes strengthens organisational capability.

H10 was confirmed in the full sample but rejected in the governance group, suggesting that capability depends not on the quantity of information sources but on the ability to evaluate and reconcile them. H11 was supported, confirming that strong digital trust assessment routines enhance third-party risk management maturity.

The results for H3, H4, H5, and H6 provide insight into the organisation's openness with potential ICT service providers during its onboarding process, as a mechanism for reducing information asymmetry (Akerlof 1970) during digital trust assessment. Transparency does not directly reduce third-party risk (H4 rejected), and its mediation effect (H5) is not the same across the two samples. The confirmed moderation effect (H6) suggests that openness may even weaken DT's risk-reducing impact, as vendors adapt their presentation to stated criteria without necessarily improving underlying capabilities. This challenges information asymmetry assumptions and aligns with signalling theory (Spence 1973).

Finally, H8 confirms that multiple information sources increase perceived digital trust, yet H9 was rejected in both datasets: additional sources do not reduce third-party risk. Experts explained that while more information may increase trust, it may also surface additional issues, leaving actual risk exposure unchanged.

3.2.Capability-driven digital trust framework for enhanced third-party risk management

Experts assessed the current level of organisational capabilities for digital trust (DT) assessment and management as early-stage**,** with most interviewees placing it at level 1 or 2 out of 5. Higher maturity assessments (levels 3–4) were mainly given by information security representatives, who tend to have more structured third-party trustworthiness practices.

The statistical analysis confirmed that stronger organisational capabilities for DT assessment significantly enhance the risk-mitigating effect of DT and increase the credibility of DT assessments within the broader TPRM framework. Moreover, higher DT capability is directly linked to higher TPRM maturity**,** contributing to improved governance of non-financial risks.

To help organisations improve their DT assessment and management maturity, as well as to enhance the effectiveness of digital trust in mitigating third-party risk, this research develops the "Capability-driven DT framework for enhanced TPRM" depicted in Figure 3.1. below.

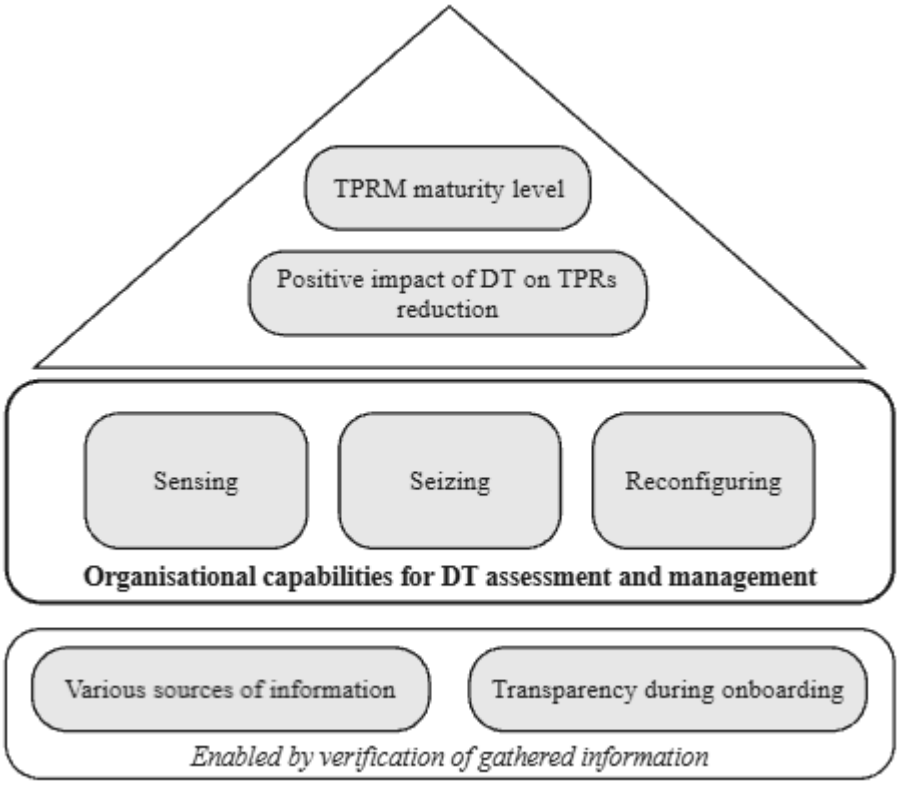


Figure 3.1. Capability-driven DT framework for enhanced TPRM

Source: created by the author

The structure of the framework is based on three main components:

1. **Enablers for capabilities development constitute the necessary information sources** for the assessment and transparency in the DT assessment during third-party onboarding.
2. **Capabilities for DT assessment and management** represent three pillars of dynamic capabilities required for processing this information.
3. **Outcomes of enhanced DT practices** are the results produced by the framework, i.e., a higher level of TPRM maturity and enhancement of the positive DT effect on TPRs reduction.

The following sections will, therefore, begin by detailing the foundational inputs required for the framework's operation.

The importance of diverse information sources

Experts emphasised that while using diverse information sources can enhance DT assessment, the quality, independence, and effective integration of these sources are critical. Organisations should establish a reliable baseline of probative sources, avoid duplicative or noisy inputs, and ensure assessors have the skills to evaluate and reconcile information properly.

The most useful sources for DT assessment were grouped into several perspectives:

1. Independent view - audit reports, certifications, penetration tests, and incident history (highest assurance).
2. Official view - public registries, sanctions lists, regulatory status, EU oversight.
3. Market view - peer and client feedback (requiring bias assessment).
4. Inside view - vendor-provided documentation, questionnaires, architecture descriptions, contractual texts.
5. Risk view - external screening tools (adverse media, AML/KYC, ESG (environmental, social and governance factors)).

The diverse sources identified by experts for assessing digital trust can be synthesised into a holistic profile of an ICT third-party service provider depicted in Figure 3.2. below.

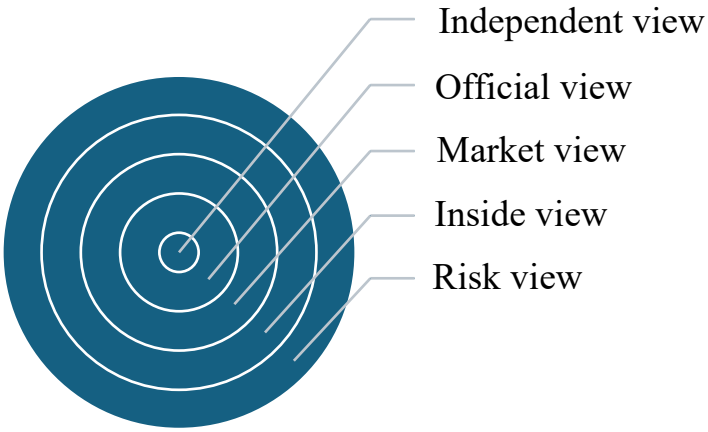


Figure 3.2. A holistic profile of an ICT third-party service provider

Source: created by the author

Survey findings confirm that institutions already use diverse sources, but experts recommend prioritising independent and outcome-based evidence over self-reported information. Blockchain was not identified as a meaningful DT signal, likely due to limited applicability and the multidimensional nature of trust.

Based on expert insights, a tiered evidence hierarchy is proposed:

- Tier A (Outcome-based verification): independent audits, penetration tests, and incident disclosures.
- Tier B (Fact-based validation): official registries, financial statements, recognised certifications.
- Tier C (Supporting evidence): screening platforms, peer references, vendor materials (requires cross-checking).

The role of transparency in enhancing capabilities

The statistical test for H7 confirms that transparency in DT assessment during third-party onboarding positively enhances organisational capabilities for DT assessment and management. Transparency can be implemented through clear, well-documented assessment

criteria (e.g., structured due diligence questionnaires), accessible evaluation processes, and alignment of trust expectations with ICT third parties.

Experts noted that transparency strengthens capabilities through:

- Standardisation and repeatability, enabling comparable evidence collection;
- Supplier enablement, improving documentation quality and efficiency;
- Improved relationships, increasing fairness, responsiveness, and completeness of submissions.

However, transparency enhances capability only when:

- It is paired with substantive evaluation and independent verification;
- A documented methodology (scoring, sampling, follow-ups) governs evidence weighting;
- Teams possess sufficient skills and time to analyse expanded evidence sets.

Experts also warned that excessive transparency may lead to box-ticking, reverse-engineering of criteria, inflated perceived trust, or artificial compliance, and may even discourage some suppliers.

The core process: the three elements of the capabilities

Based on expert interviews and dynamic capabilities theory, the study develops three core capabilities for DT assessment and management to enhance TPRM maturity and reduce ICT third-party risks:

1. **Sensing: identifying, understanding and monitoring digital trust signals**

This capability focuses on how the organisation systematically collects, interprets, and detects changes in signals and evidence related to third-party trustworthiness through:

- Multi-source information gathering across independent, official, market, and vendor inputs
- Continuous and event-driven monitoring (performance, incidents, regulatory changes)
- Systematic evidence verification and provenance
- Emerging risk and trend analysis

2. **Seizing: integrating digital trust insights into TPRM decision-making**

This capability operationalises the insights gathered through Sensing. It embeds these findings into core decision-making frameworks and risk management workflows. This enables the organisation to make timely, intelligent, and well-informed decisions regarding its third-party service providers through:

- Risk-based calibration of oversight
- Trust-based sourcing and TPRM governance
- Structured incident and remediation response

3. **Reconfiguring: adapting and enhancing assessment practices over time**

This capability drives continuous improvement, aiming to constantly adapt and enhance the organisation's overall approach to digital trust management. It involves systematically learning from past assessments to upgrade the methods, tools, and governance, ensuring the entire framework adapts and matures over time through:

- Standardisation of the DT assessment framework
- Systematic knowledge and data management

Finally, experts emphasised the need for orchestration – the managerial capability to synchronise Sensing, Seizing, and Reconfiguring (Eurico Soares De Noronha et al. 2024).

The dynamic capabilities of an organisation for DT assessment and management are depicted in Figure 3.3. below.

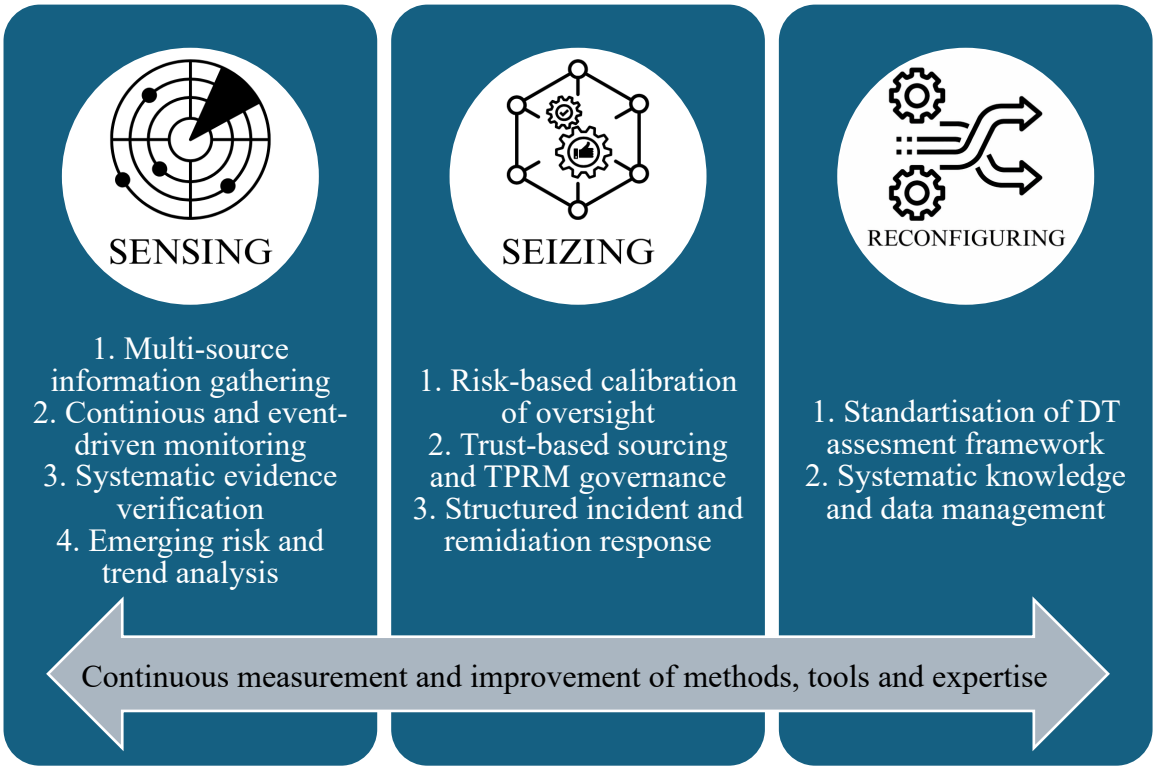


Figure 3.3. Organisational capabilities for DT assessment and management

Source: created by the author

Orchestrating DT assessment capabilities requires continuous measurement and improvement of methods, tools, and expertise used in trustworthiness evaluations. This includes investing in technology or external expertise, monitoring improvements in evidence quality and assessment efficiency, and validating that the evaluation model reliably links higher trust to lower residual risk. It also requires alignment across key functions (e.g., TPRM, Information Security, IT Risk) to ensure a unified approach to digital trust.

3.3 Future state of ICT third-party risk management in the Baltic banking industry

The experts were asked to provide their opinion towards the future of third-party risk management in the Baltic banking industry. TPRM is an emerging area in the EU financial sector, and over the next 3–5 years further regulatory development is expected. While the core ICT third-party requirements are unlikely to change significantly, experts anticipate greater standardisation across EU countries, clearer interpretation, shared templates, and possibly a centralised database of critical vendors supervised by authorities. Regulation is expected to emphasise execution quality, maturity of existing practices, extension to certain non-ICT providers, stronger focus on ESG risks, and deeper oversight of 4th and Nth parties.

To prepare, organisations should:

- Formalise detailed TPRM processes, procedures, and playbooks.
- Extend registries to 4th and Nth parties to map subcontracting chains.
- Integrate ESG-related clauses into questionnaires and contracts.

Governance is expected to become more visible at board level, with higher maturity and dedicated TPRM roles and teams. Resource constraints are currently evident, but increased automation and AI-based tools are anticipated. Stronger cross-functional involvement (procurement, compliance, legal, business) and a unified understanding of third-party risks will be required.

Market impacts are also expected: third parties will professionalise DORA compliance, potentially using it as a competitive advantage, while financial institutions will demand higher-

quality documentation. However, compliance costs may rise. DORA may favour large vendors, potentially increasing concentration risk, while smaller providers and resellers may struggle.

Finally, experts foresee the gradual extension of TPRM-type regulation beyond finance, particularly to critical infrastructure sectors (energy, water, transport, telecom) and possibly large corporations, driven by interconnected supply chains, cyber risk exposure, and alignment between DORA and NIS2 frameworks.

Conclusions

This doctoral thesis examines the impact of digital trust on third-party risks within the banking sector of the Baltic region. The main research conclusions are:

1. The theoretical contribution of this research provides a necessary conceptual clarification of digital trust by developing and validating a new definition, which is grounded in a comprehensive analysis of 42 existing definitions classified into six thematic groups. The study consolidated 24 key factors of digital trust into a conceptual framework structured around four distinct categories: Ability, Benevolence, Integrity, and the newly introduced category of Openness. The subsequent content validation of the new definition confirmed its moderate or strong alignment with these key factors, achieving an overall htc value of 0.86, thereby confirming that it accurately reflects the multi-dimensional essence of digital trust better than the most popular existing definition.
2. The study provides a clear theoretical distinction between third-party risk and related concepts, such as vendor, supplier, and service provider risks, despite the common tendency in the literature to treat them as synonyms. This study establishes third-party risk as the overarching risk type and provides a comprehensive structure for organisational risk management by identifying and classifying it into seven main categories: (1) regulatory and compliance risks, (2) operational risks, (3) financial risks, (4) security and privacy risks, (5) strategic risks, (6) ethical and social risks, and (7) partner and supply chain risks.
3. The core hypothesis (H1) of this research, that Digital trust reduces third-party risks was strongly confirmed in both the full employee sample ($\beta=-0.452, p=0.000$) and the governance-level group ($\beta=-0.753, p=0.001$), demonstrating that high levels of digital trust significantly contribute to the lower level of overall third-party risk within the B2B context of ICT service providers. Detailed analysis further confirmed this negative impact across ten out of twelve specific risk types, including concentration, financial, strategic, and data privacy risks. However, this effect was statistically rejected for vendor and supply chain cybersecurity risks (H1f) and risks related to partner-specific factors (H1k), suggesting that specific technical and geopolitical risks require additional risk management measures.
4. The effect of digital trust on reducing third-party risks is strengthened by organisational capabilities (H2), but this finding was confirmed with a strong negative moderation effect ($\beta = -0.462$, $p = 0.047$) only among employees aware of governance-level practices (i.e., risk, compliance, and security professionals) and was rejected in the full sample.
5. Organisational transparency in digital trust assessment has a context-dependent role, challenging a simplistic application of Information Asymmetry Theory. While transparency positively impacts digital trust (H3) in the full employee sample ($\beta = 0.251$, $p = 0.011$), suggesting that operational stakeholders use it to compensate for uncertainty, this link was rejected in the governance-level group. Furthermore, the confirmation of the moderation effect (H6) in both samples, with positive (weakening) path coefficients ($\beta = 0.267$ and $\beta = 0.603$), suggests that third parties may use high transparency to "manipulate the signal" and build an artificial perception of trust that does not fully translate into risk reduction.
6. The thesis confirmed that dynamic organisational capabilities (H11) for digital trust assessment significantly and positively impact the maturity level of Third-Party Risk Management (TPRM) ($\beta = 0.377$, $p = 0.000$), demonstrating a practical link between the development of these capabilities and the advancement of the third-party risk management level of the organisation. These capabilities, in turn, are positively influenced by transparency (H7) (confirmed in both samples) and the extensive use of various information sources (H10) (confirmed in the full test sample).

7. The most popular sources of information used by practitioners were the documentation of the provider's solution (mean = 4.06) and proof of reputation (mean = 3.93), such as ISO 27001 certifications and audit reports
8. The research validated the mediating role of digital trust in the relationship between transparency and risk, confirming H5 in the full sample. This finding highlights that transparency does not directly reduce risk (H4 was rejected), but rather indirectly achieves risk reduction by fostering a higher perception of digital trust that, in turn, mitigates risks.
9. The methodological decision to analyse data using two distinct samples (a full employee sample and a governance-level group) revealed significant differences in the results for H2, H3, H5, and H10. This differential testing provided evidence that the perception and function of capabilities, transparency, and information usage within TPRM are role dependent.
10. Based on expert opinion, the current level of organisational capability for digital trust assessment and management across the Baltic banking sector is generally defined as "early-stage," typically falling around level 1 or 2.
11. Future changes in the regulated sector will emphasise the maturity, execution quality, and competence of TPRM practices, requiring organisations to start detailed descriptions of processes and playbooks to prepare for supervisor checks.
12. DORA-driven requirements are expected to change the ICT third-party market structure, potentially favouring large global vendors and requiring increased resource allocation, including dedicated TPRM roles and enhanced automation within financial institutions.

Recommendations

Practical recommendations

1. Since higher levels of digital trust were shown to reduce third-party risks, it's recommended that organisations formalise digital trust assessment and management as a risk mitigation control. Simultaneously, the reliance on trust as a substitute for cybersecurity assurance or partner-specific factors should be limited, as it requires separate verification.
2. It is recommended that organisations strengthen their TPRM maturity by developing dynamic capabilities for digital trustworthiness assessment and management. This includes systematically collecting and verifying evidence from diverse sources, embedding trust indicators into decision-making processes, and continuously refining assessment tools to ensure consistency and repeatability across the organisation.
3. Organisations should openly share their digital trustworthiness assessment criteria to support capability development, but must also monitor the risks of "designed answers" through independent verification to ensure that the disclosed information accurately reflects real practices.
4. When assessing the digital trustworthiness of ICT third parties, organisations should avoid relying on a single data channel. Instead, they should integrate certifications, solution documentation, market signals, and third-party evaluations, while ensuring that employees are trained to synthesise diverse and sometimes conflicting data into a coherent trust assessment.
5. To improve the quality of trust evaluations, organisations should prioritise evidence based on reliability rather than volume. Independent, outcome-based verification (Tier A) should serve as the primary basis for assessment, supported by fact-based validation from official records (Tier B). Self-reported or contextual information (Tier C) should be used cautiously and only to complement higher-quality evidence.
6. Organisations should formalise trust assessment processes and develop sensing, seizing, and reconfiguring capabilities, while aligning perspectives across governance and operational roles through a unified assessment framework.
7. Since transparency reduces risk only through the trust it helps generate (H5), organisations should focus on fostering genuine relationship quality rather than treating transparency as a procedural requirement. When transparency strengthens perceptions of benevolence and integrity, risk decreases; however, when it is treated as a compliance exercise, no meaningful risk reduction occurs.
8. Since governance roles emphasise evidence while operational teams often rely on relational trust, organisations should align these perspectives through unified frameworks and shared information repositories. Centralised trust artefacts, such as scoring records and verified evidence, help synchronise decision-making and reduce fragmented assessments across teams.
9. To meet evolving regulatory expectations, organisations should expand their TPRM practices by mapping subcontractors and Nth-party dependencies, formalising detailed operational playbooks, and integrating ESG considerations into due diligence. Investments in automation and artificial-intelligence-driven analysis will become increasingly necessary to manage the rising complexity and regulatory scrutiny.

Recommendations for future research

1. Considering the early stage of third-party risk management in the Baltic banking industry, it is recommended to conduct a longitudinal study to research the dynamics of digital trust's impact on third-party risks of these organisations, along with their maturity growth.

2. A cross-industry study within the financial sector may demonstrate how the size of the organisation, its maturity, or the intensity of regulation impacts the study's relationship between digital trust and third-party risks.
3. To enhance generalisability, future research could examine the identified relationships within other regulatory regimes, cultural norms, and levels of digitalisation by conducting comparative studies across various EU countries or by comparing the results with those from the US, Asian, or emerging markets.
4. To mitigate self-reporting bias, future research may incorporate objective data, such as audit results, incident reports, performance metrics, behavioural logs, or externally validated trust indicators.
5. Future studies could analyse digital trust and risk dynamics across an organisation's full third-party ecosystem, rather than focusing on a single relationship, and use the organisation's third-party risk portfolio as a unit of analysis.
6. Building on the interview findings, future studies could use case studies, ethnographies, or action research to examine how digital trust capabilities are developed, operationalised, and embedded into organisational routines over time.
7. Future research could further develop the practical applicability of the proposed recommendations by proposing prioritisation frameworks tailored to smaller financial institutions with limited financial and organisational resources.
8. Given that CSR-related risks were identified by experts as among the least mature and least clearly understood, future studies could focus on the development of auditable digital ESG metrics relevant to ICT service providers.

Final Remarks

This doctoral thesis has addressed all research questions and completed all research tasks defined at the beginning of the study. By integrating theoretical analysis, quantitative modelling, and qualitative expert insights, the research provides a comprehensive understanding of the role of digital trust in third-party risk management.

Although the empirical component of the study focuses on the Baltic banking industry, where regulatory requirements and technological maturity provide a particularly relevant research context, the conceptual insights developed in this thesis extend beyond this geographical and sectoral scope. The identified relationships between digital trust and third-party risks reflect broader patterns characteristic of digital environments and organisational reliance on ICT service providers. Therefore, the proposed conceptual framework and methodological approach to digital trust assessment may also be applicable in other industries, regulatory environments, and organisational contexts that cooperate with external ICT service providers.

In addition, the identified categories of third-party risks represent a comprehensive structure that may be relevant across different industries and organisational contexts. These categories may therefore be considered generally applicable to organisations worldwide that rely on third-party service providers.

Thus, this thesis provides a foundation for further academic research and practical development in the field of digital trust and third-party risk management, offering insights that may support organisations in strengthening digital trust assessment practices and improving third-party risk management.

Jūlija Saveļjeva

Digitālās uzticības ietekme uz trešās puses riskiem organizācijā

Promocijas darba kopsavilkums

Zinātnes nozare: Sociālās zinātnes
Zinātnes apakšnozare: Ekonomika un uzņēmējdarbība

Zinātniskais vadītājs
Dr.oec., prof. Tatjana Volkova

Riga 2026

Saveljeva, J. (2026). Digitālās uzticības ietekme uz trešās puses riskiem organizācijā. Promocijas darba kopsavilkums, Rīga, 124 lappuses. Publicēts saskaņā ar RISEBA Promocijas padomes sēdes lēmumu. Protokola datums 2026. gada 8. maijā; Nr. 26/10-3.1/3.

Šis promocijas darbs tika izstrādāts Biznesa, mākslas un tehnoloģiju augstskolā RISEBA un Latvijas Universitātes Banku augstskolā laikā no 2023. gada februāra līdz 2026. gada maijam. Promocijas darbs ir izstrādāts angļu valodā. Tas sastāv no ievada, trim nodaļām, secinājumiem un ieteikumiem, literatūras saraksta un septiņiem pielikumiem. Tā kopīgais apjoms ir 309 lappuses. Bibliogrāfijā iekļauti 261 informācijas avoti.

ZINĀTNISKAIS VADĪTĀJS:

Dr.oec.Tatjana Volkova, profesore, Latvijas Universitātes Banku augstskola (Latvija)

RECENZENTI:

1. Dr. sc. administr. Iveta Ludviga, profesore, Biznesa, mākslas un tehnoloģiju augstskola RISEBA (Latvija)
2. Dr. oec. Piotr Grzegorz Pietrzak, asistējošais profesors, Warsaw University of Life Sciences (Polija)
3. Dr. sc. ing. Oksana Ņikiforova, profesore, Rīgas Tehniska Universitāte (Latvija)

Promocijas darbs tiks aizstāvēts Biznesa, mākslas un tehnoloģiju augstskolas RISEBA Promocijas padomes atklātā sēdē 2026. gada 17. septembrī, 15:00, Meža ielā 3, Rīgā.

Ar promocijas darbu un kopsavilkumu var iepazīties Biznesa, mākslas un tehnoloģiju augstskolas RISEBA bibliotēkā, Meža ielā 3, Rīgā. Biznesa, mākslas un tehnoloģiju augstskolas RISEBA Promocijas padome pieņēma promocijas darbu sociālo zinātņu doktora zinātniskā grāda (Ph.D.) iegūšanai 2026. gada 8. maijā.

Promocijas padomes priekšsēdētājs: Andrejs Čirjevskis, Dr.oec., profesors.
Promocijas padomes sekretārs: Vulfs Kozlinskis, Dr.habil.oec., emeritētais profesors.

APLIECINĀJUMS: Ar šo apliecinu, ka esmu izstrādājusi šo promocijas darbu, kas iesniegts izskatīšanai Biznesa, mākslas un tehnoloģiju augstskolas RISEBA Promocijas padomei zinātņu doktora zinātniskā grāda (Ph.D.) iegūšanai sociālajās zinātnēs. Promocijas darbs nav iesniegts nevienā citā universitātē zinātniskā grāda iegūšanai.

Jūlija Saveļjeva 15.07.2026

Lai iesniegtu recenzijas, lūdzam sazināties ar RISEBA, Meža iela 3, Rīga, LV-1048, Latvija.
Epasts: riseba@riseba.lv, tālrunis: +371 26465351, +371 67500265.

© Jūlija Saveļjeva, 2026
© Latvijas Universitātes Banku augstskola, 2026
© Biznesa, mākslas un tehnoloģiju augstskola RISEBA, 2026

ISBN 978-9984-705-75-0

Pateicības

Ir teiciens, ka “ir vajadzīgs vesels ciems, lai izaudzinātu bērnu”, un es šo domu ļoti labi varu attiecināt arī uz promocijas darba izstrādes ceļu. Patiesi, ir vajadzīga vesela fakultāte, dažkārt pat vairāk nekā viena, ģimene, profesionālā kopiena un darba kolēģi, lai izaudzinātu jaunu doktora grāda ieguvēju. Iegūstot šo grādu un strādājot pie promocijas darba, es izjutu plašu atbalstu gan akadēmiskajā un profesionālajā vidē, gan savā ģimenē.

Esmu bezgalīgi pateicīga savai promocijas darba vadītājai, Dr. oec. profesorei Tatjanai Volkovai, par to, ka viņa iedrošināja mani uzsākt šo ceļu 2022. gada vidū un lika man noticēt, ka es spēšu iziet šo posmu un iegūt doktora grādu. Tas bija izaicinošs ceļš, kas dažkārt mani aizveda tālu ārpus manas komforta zonas un ārpus manu uztverto spēju robežām, rezultējoties eksponenciālā akadēmiskajā izaugsmē. Katrā mazajā solī un katrā šī ceļa posmā mana darba vadītāja bija man līdzās, gatava atbalstīt, palīdzēt, izaicināt un motivēt mani, kad tas bija nepieciešams. Es noteikti nevaru iedomāties šo ceļu bez viņas.

Es vēlos pateikties savam kolēģim, Dr. sc. Irmantam Aleliūnam, par atbalstu un kopīgām prāta vētrām par tēmas izvēli brīdī, kad biju iestrēgusi, meklējot precīzu pētījuma tēmu, kas būtu gan akadēmiski vērtīga, gan praktiski nozīmīga profesionālajai videi.

Šī ceļa laikā man bija patiess prieks satikt daudzus izcilus cilvēkus akadēmiskajā vidē, kuri vienā vai otrā veidā ir devuši ieguldījumu manā pētnieces attīstībā, un visus viņus nosaukt vārdā nebūtu iespējams.

Visa Latvijas Universitātes Banku augstskolas un RISEBA kopīgās doktora studiju programmas akadēmiskā saime ir paveikusi milzīgu darbu, veidojot manu kritisko akadēmisko domāšanu, pilnveidojot mani kā pētnieci un nosakot augstus standartus, lai šobrīd es justos pārliecināta starptautiskajā zinātniskajā vidē un pārstāvot savu pētījumu starptautiskās konferencēs. Esmu īpaši pateicīga Dr. hab. oec. profesoram emeritus Vulfam Kozlinskim par to, ka viņš lika man domāt plašāk un izprast zinātniskās diskusijas nozīmi un teorētiskās novitātes veidošanu.

Vēlos izteikt pateicību Dr. oec. profesorei Līgai Peiseniecei un Dr. oec. asociētajam profesoram Andrim Fominam par virzīšanu studiju programmas gaitā un atbalstu, iegūstot doktorantūras grantu Nr. 5.2.1.1.i.0/2/24/I/CFLA/007 “Latvijas Universitātes iekšējā un ārējā konsolidācija”. Šī granta atbalsta nozīmi nevar nenovērtēt, jo tas ļāva man dalīties ar savu pētījumu plašākā zinātniskajā kopienā un būtiski pilnveidoties kā pētniecei promocijas darba izstrādes laikā.

Tāpat dalība zinātniskajā projektā “CyberSustain” palīdzēja man pilnveidot pētniecības un prezentēšanas prasmes, paplašināt zinātniskās intereses un zinātnisko sadarbības tīklu. Atsevišķi vēlos pateikties Dr. sc. asociētajai profesorei Ingai Uvarovai par atbalstu katrā mana promocijas pētījuma posmā un motivēšanu virzīties pāri savām spēju robežām.

Es vēlos pateikties arī saviem doktorantūras kolēģiem, ar kuriem kopā piedzīvoju šī ceļa izaicinājumus, šaubas un sasniegumus. Īpaši pateicīga esmu Dr. sc. Jekaterinai Novickai par viņas ticību man un manu prasmju novērtējumu, dažkārt pat lielāku, nekā es pati ticēju sev. Es vēlos pateikties Eldaram Mardanovam par lielisko piemēru dalībā konferencēs un publikāciju veidošanā, motivējot mani turēt līdzi un darīt vairāk. Es pateicos Dmitrijam Gimmelbergam par iespēju paskatīties uz pētniecības procesu no cita skatpunkta un par iedrošinājumu paplašināt manus pētniecības horizontus. Es pateicos arī Sandrai Stārķei par šī doktorantūras ceļa kopīgu iziešanu un atbalstu tā laikā.

Atsevišķi vēlos pateikties saviem SEB kolēģiem visās trīs Baltijas valstīs par atbalstu un uzmundrinājumu visa šī ceļa laikā. Īpaši nozīmīga bija viņu palīdzība empīrisko datu vākšanā - kolēģi personīgi uzrunāja potenciālos respondentus Baltijas banku nozarē, kā arī pārsūtīja manu lūgumu piedalīties pētījumā dažādām finanšu nozares asociācijām un profesionālajām grupām Baltijā. Īpaši vēlos pateikties savam vadītājam, Dr. Ramūnam Bičuilaitim, par šī ceļa sarežģītības izpratni un atbalstu katrā solī, kas bija nepieciešams grāda iegūšanai.

Esmu pateicīga šī promocijas darba recenzentiem Dr. sc. administr. profesorei Ivetai Ludvigai, Dr. oec. Piotram Gžegožam Pietrzakam, asistējošajam profesoram, un Dr. sc. ing. profesorei Oksanai Ņikiforovai par vērtīgu atgriezenisko saiti un veikto pētījumu izvērtējumu.

Visbeidzot, man jāpateicas savai ģimenei par to, ka viņi bija man līdzās, atbalstīja manu lēmumu iegūt šo grādu jau no pirmās dienas un nekad nešaubījās, ka šī diena pienāks. Šis bija izaicinošs ceļš manam vīram Vadimam Saveļjevam un mūsu mazajiem bērniem Zlatai un Agatai, kuru mamma garus vakarus un nedēļas nogales pavadīja, strādājot pie pētījuma un dodoties uz ārzemēm, lai dalītos ar tā rezultātiem plašākā zinātniskajā kopienā. No viņiem es nekad neesmu dzirdējusi neko citu kā vien pilnīgu atbalstu un apņēmību. Tāpēc šis grāds ir kļuvis par mūsu ģimenes kopīgu vērtību.

Manas mammas Diānas Jablonskas atbalsts un iedrošinājums palīdzēja man virzīties uz priekšu. Es arī zinu, ka mans tēvs Vjačeslavs Šuļgins bija bezgalīgi lepns par manu lēmumu tiekties augstu un uzsākt doktorantūras ceļu. Diemžēl viņš aizgāja mūžībā, pirms parādījās pirmie pamanāmie pētījuma rezultāti. Es zinu, ka viņš bija pārliecināts, ka citādi nemaz nevarēja būt, un šis grāds savā ziņā ir veltīts arī viņa piemiņai.

Satura rādītājs

IEVADS **63**

1. NODAĻAS KOPSAVILKUMS: DIGITĀLĀS UZTICĪBAS UN TREŠĀS PUSES RISKU SAVSTARPĒJĀ SAISTĪBA **72**

1.1. Digitālās uzticības būtība un tās raksturlielumi 72
1.2. Uzticības pamati risku pārvaldībā 77
1.3. Trešās puses risku pārvaldība un tās ietvari 80
1.4. Hipotēzes un pētījuma modelis 84
1.5. Pētījuma dizains un metodoloģija 86

2. NODAĻAS KOPSAVILKUMS: TREŠĀS PUSES RISKU PĀRVALDĪBAS NOVĒRTĒJUMS FINANŠU SEKTORĀ **88**

2.1. Baltijas banku nozares raksturojums 88
2.2. Trešās puses risku pārvaldības izaicinājumi banku nozarē 88
2.3. Digitālās uzticības ietekme uz trešās puses riskiem Baltijas bankās 89

3. NODAĻAS KOPSAVILKUMS: KVALITATĪVIE IESKATI PAR DIGITĀLO UZTICĪBU UN TREŠĀS PUSES RISKIEM: SECINĀJUMI UN REKOMENDĀCIJAS **100**

3.1. Trešās puses risku kategoriju kvalitatīvās analīzes atziņas un hipotēžu pārbaude 100
3.2. Spējās pamatots digitālās uzticības ietvars pilnveidotai trešās puses risku pārvaldībai 103
3.3 IKT trešo pušu risku pārvaldības turpmākā attīstība Baltijas banku nozarē 106

SECINĀJUMI **108**

REKOMENDĀCIJAS **110**

NOSLĒGUMA ATZIŅAS **112**

KOPSAVILKUMĀ IZMANTOTAIS LITERATŪRAS SARAKSTS……**106**

Kopsavilkumā izmantotais saīsinājumu saraksts

ASV - Amerikas Savienotās Valstis
B2B - Bizness–biznesam
DORA - Digitālās darbības noturības akts (angliski - *Digital Operational Resilience Act*)
DU - Digitālā uzticība
ES - Eiropas Savienība
IKT - Informācijas un komunikācijas tehnoloģijas
NILLN - Noziedzīgi iegūtu līdzekļu legalizācijas novēršana
PLS-SEM - Daļējo mazāko kvadrātu strukturālo vienādojumu modelēšana (angliski - *Partial Least Squares Structural Equation Modelling)*
SEM - Strukturālo vienādojumu modelēšana (angliski - *Structural Equation Modelling)*
SLR - Sistemātisks literatūras pārskats (angliski - Systematic Literature Review)
TPR – Trešas puses risks
TPPR - Trešās puses risku pārvaldība

Ievads

Pētījuma aktualitāte

Finanšu sektoram īstenojot digitālo transformāciju, digitālā uzticība (DU) kļūst arvien nozīmīgāka, ņemot vērā tās lomu tehnoloģisko sistēmu drošības, konfidencialitātes un uzticamības nodrošināšanā. Tas atspoguļo pieaugošo nepieciešamību pēc drošām digitālajām mijiedarbībām un datu privātuma strauji mainīgā tehnoloģiskajā vidē. Šī tendence ir novērojama arī zinātniskajā literatūrā. Saskaņā ar *Scopus* datubāzēs (Elsevier, 2025) pieejamo informāciju, zinātnisko rakstu un konferenuč publikāciju skaits, kuru nosaukumā, kopsavilkumā vai atslēgvārdos ir ietverts atslēgvārds "digital trust", ir būtiski pieaudzis no viena vai diviem darbiem gadā līdz 2017. gadam līdz 121 publikācijai 2025. gadā.

Vienlaikus DU koncepts ir izteikti pārstāvēts arī profesionālajā literatūrā kā jauna pieeja digitālo tehnoloģiju uzticamības novērtēšanai (World Economic Forum 2024; PwC, 2024; ISACA, 2024.; Deloitte, 2024a). Tas izceļ digitālās uzticības koncepta aktualitāti, kas zinātniskajā literatūrā joprojām ir attīstības stadijā un atšķiras atkarībā no konteksta un nozares (Pietrzak and Takala 2021). Tas uzsver nepieciešamību pēc validētas DU definīcijas un turpmākiem pētījumiem, lai noteiktu DU koncepta papildus raksturlielumus. Turklāt uzticamība tiek uzskatīta par nozīmīgu faktoru sadarbībā ar pakalpojumu sniedzējiem (Urbano et al. 2013). Vienlaikus DU koncepts zinātniskajā literatūrā vēl nav pietiekami izpētīts. Lai gan pētnieki atzīst konceptuālu atšķirību starp tradicionālo starppersonu uzticību un digitālo uzticību digitālajā vidē, šo jēdzienu teorētiskā konsolidācija joprojām ir ierobežota (Chaudhuri 2021; Zhghenti and Chkareuli 2021). Turklāt iepriekšējie pētījumi uzsver vienprātības trūkumu attiecībā uz digitālās uzticības pamatīpašībām (Papic et al. 2022).

Savukārt, Digitālās darbības noturības akts (angliski – *Digital Operational Resilience Act*, DORA), kas stājās spēkā 2025. gada 17. janvārī un attiecas uz visu Eiropas finanšu sektoru, nosaka visaptverošu pieeju trešo pušu risku pārvaldībai (TPRP) ar informācijas un komunikācijas tehnoloģiju (IKT) pakalpojumu sniedzējiem. (European Commission 2022b). Tādējādi finanšu iestādēm ir jāpiešķir prioritāte ar IKT pakalpojumu sniedzējiem saistīto TPRP . Lai gan IKT TPRP ieviešana ir būtiska efektīvas uzraudzības nodrošināšanai un jaunu tehnoloģisko risku savlaicīgai noteikšanai (Giacchero and Moretti 2021), vēsturiski organizācijas trešās puses riskus (TPR) ir vērtējušas ierobežotā kontekstā (Deloitte, 2024b).

Interese par "TPR"(*third-party risk*) un piegādātāja risku (*supplier risk*) terminiem kas ir zinātniskajā un profesionālajā literatūrā bieži tiek savstarpēji aizvietojami, kopš 2007. gada ir pastāvīgi pieaugusi kā par to liecina *Scopus* datubāzes dati (Elsevier, 2025),. Interese par šiem terminiem ir ar īpaši izteiktu pieaugumu no 2020. gada, sasniedzot 62 publikācijas 2024. gadā. Turklāt literatūrā joprojām nav pietiekami skaidri nošķirtas dažādas trešo pušu risku kategorijas, un vienlaikus turpinās diskusijas par tehnoloģijās balstītu pieeju un tradicionālo pārvaldības instrumentu izmantošanu trešo pušu risku pārvaldībā. Ņemot vērā nepilnības TPRP ietvarā, pieaugošās regulatīvās prasības un finanšu iestāžu augsto atkarību no IKT pakalpojumu sniedzējiem, TPRP kļūst par īpaši nozīmīgu jautājumu finanšu sektorā.

Pētījumiem par uzticības un riska savstarpējo saistību ir sena pētniecības tradīcija (Jøsang and Presti 2004), un jau pirms trīsdesmit gadiem tika uzsvērta uzticības nozīme efektīvā risku pārvaldībā (Slovic 1993). Pētījumi apliecina, ka uzticība lēmumu pieņemšanas procesā bezsaistes vidē var kalpot kā mehānisms, kas samazina sarežģītību, īpaši risku izvērtēšanas situācijās. Šāda pieeja var efektīvi papildināt racionālās risku pārvaldības stratēģijas (Lewis and Weigert 1985; Mclain and Hackman 1999). Tomēr turpmākā analīze liecina, ka risku pārvaldības ietvaros joprojām trūkst vienotu pieeju uzticības izpratnei un novērtēšanai.

Savukārt uzticības un TPRP savstarpējā saistība zinātniskajā literatūrā līdz šim nav plaši analizēta. Atslēgvārdu "digital trust" AND ("third-party" OR "supplier" OR "supply chain") meklējums, kas 2025. gada novembrī veikts Scopus datubāzē, noteica 589 publikācijas zinātniskajos žurnālos un konferences rakstos (Elsevier, 2025). Papildus tam tika veikta bibliometriskā analīze, izmantojot VOSviewer rīku un atslēgvārdu līdzparādīšanās kartēšanas

metodi (*a full-count co-occurrence keyword analysis*). Analīzes rezultāti atklāja būtisku nepilnību zinātniskajā literatūrā — tajā trūkst atkārtoti lietotu atslēgvārdu, kas būtu saistīti ar risku un risku pārvaldību. Tas liecina, ka DU koncepts trešās puses vai piegādātāju risku pārvaldības kontekstā vēl nav pietiekami sistemātiski izpētīts un mehānismi, kā dažādi uzticības faktori ietekmē trešo pušu riskus, joprojām ir nepietiekami izprasti.

Pētījuma mērķis, jautājumi, hipotēzes, objekts un priekšmets

Pētījuma mērķis ir noteikt DU ietekmi uz organizācijas TPR un izstrādāt uz spējām balstītu ietvaru, kas ļautu organizācijām efektīvāk novērtēt un pārvaldīt DU, tādējādi pilnveidojot trešās puses risku pārvaldību un paaugstinot tās pārvaldības brieduma līmeni.

Galvenie **pētījuma jautājumi** ir:

1. Kā definēt DU un kādi ir tās raksturlielumi?
2. Kā DU ietekmē ar IKT pakalpojumiem saistītos TPR?
3. Kādas DU novērtēšanas un pārvaldības spējas organizācijā ir jāattīsta, lai mazinātu ar IKT pakalpojumiem saistītos TPR?
4. Kādi informācijas avoti organizācijai jāņem vērā DU novērtēšanā?

Pētījuma hipotēzes ir:

H1: DU samazina TPR.

H2: DU ietekmi uz TPR mazināšanu moderē organizācijas spējas DU novērtēšanā un pārvaldībā.

H3: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē DU līmeni.

H4: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā samazina trešās puses riskus.

H5: DU darbojas kā mediators starp caurskatāmību DU novērtēšanā trešās puses piesaistes procesā un TPR līmeni.

H6: DU ietekmi uz TPR mazināšanu moderē caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā.

H7: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē organizācijas spējas DU novērtēšanā un pārvaldībā.

H8: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē DU līmeni.

H9: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā moderē DU ietekmi uz TPR mazināšanu.

H10: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē organizācijas spējas DU novērtēšanā.

H11: Organizācijas spējas DU novērtēšanā un pārvaldībā pozitīvi ietekmē TPRP brieduma līmeni.

Pētījuma objekts ir Baltijas banku nozare, kurai ir pienākums nodrošināt atbilstību DORA regulējumam un kurā sagaidāms pietiekami augsts TPRP prakses brieduma līmenis, lai darbinieki varētu jēgpilni iesaistīties pētījumā. Pašlaik Baltijā darbojas 40 licencētas bankas un ārvalstu kredītiestāžu filiāles. Lielākā daļa no tām ietilpst pārrobežu banku grupās, un reģionā vēsturiski ir izveidojusies līdzīga uzņēmējdarbības kultūra.

Pētījuma priekšmets ir digitālā uzticība.

Pētījuma uzdevumi:

1. Izpētīt DU konceptu IKT pakalpojumu TPRP kontekstā, nosakot tās galvenos raksturlielumus un izvērtējot to ietekmi uz TPR.
2. Izpētīt, kā organizācijas novērtē DU, noteikt efektīvai DU novērtēšanai un pārvaldībai nepieciešamās organizācijas spējas un izstrādāt ieteikumus šo spēju pilnveidei.
3. Izvērtēt caurskatāmības nozīmi DU novērtēšanā, analizējot, kā organizācijas komunicē uzticības kritērijus trešajām pusēm un kā caurskatāmība ietekmē DU uztveri un TPR mazināšanu.

4. Izpētīt daudzveidīgu informācijas avotu izmantošanu DU novērtēšanā un to ietekmi uz novērtēšanas kvalitāti.
5. Izstrādāt ietvaru DU novērtēšanas prakses pilnveidei organizācijās ar mērķi paaugstināt TPRP efektivitāti un veicināt trešo pušu pārvaldības kopējo briedumu.
6. Izanalizēt TPRP turpmākās attīstības tendences finanšu nozarē, izvērtējot pārmaiņas regulatīvajā vidē, pārvaldības pieejās un sadarbības modeļos ar trešajām pusēm.

Pētījuma metodes

Promocijas darbā izmantota jaukto metožu pieeja, kas, apvienojot kvalitatīvās un kvantitatīvās metodes, nodrošina metodoloģisko triangulāciju un paaugstina pētījuma rezultātu ticamību.

Pētījuma teorētiskais pamatu veido seši sistemātiski literatūras pārskati, kas veikti saskaņā ar PRISMA metodoloģiju (Page et al. 2021). Tie sniedz visaptverošu priekšstatu par esošo zināšanu līmeni DU, TPRP, kā arī uzticības un risku pārvaldības mijiedarbības jomā digitālajā vidē. Bibliometriskā analīze, izmantojot pilnā skaitījuma atslēgvārdu līdzparādīšanās analīzi (angliski - *a full-count co-occurrence keyword analysis*) ar *VOSviewer* rīku (VOSviewer, 2024), ļauj noteikt publikāciju struktūru, pētniecības attīstības tendences un nepilnības attiecīgajās zinātniskajās jomās. Satura analīze veikta akadēmiskajā un profesionālajā literatūrā, lai noteiktu DU un TPRP galvenos raksturlielumus un ietvarus, kā arī analizētu uzticības un riska savstarpējo saistību digitālajā kontekstā. Papildus tam pētījumā izmantota konstrukta validitātes metode, lai izvērtētu piedāvātās DU definīcijas un tās mērījuma indikatoru uzticamību un skaidrību.

Promocijas darba teorētiskā daļa veidota pamatojoties uz sekundārajiem datiem, kas iegūti no *Scopus* un *Web of Science* datubāzēs indeksētām zinātniskajām publikācijām, konferences materiāliem, akadēmiskās literatūras, profesionālajiem ziņojumiem, nozares asociācijām un uzņēmējdarbības tīkliem, kas ir saistīti ar pētījuma tematiku. Papildu kontekstuālā informācija iegūta no uzņēmumu tīmekļvietnēm, gada un ilgtspējas pārskatiem, kā arī publiski pieejamiem statistikas datiem.

Pētījuma empīriskās daļas pamatā ir divas metodoloģiskas pieejas:

1. Kvantitatīvā izpēte veikta, pamatojoties uz Baltijas banku nozares darbinieku aptauju, kuri ir iesaistīti TPRP. Aptaujā tika izmantota piecu punktu Likerta skala, un iegūtas 138 derīgas atbildes, kas nodrošina 95 % ticamības līmeni un 8,34 % kļūdas robežu (Calculator.net, 2025). Izlases veidošanā apvienota ērtuma izlase ar mērķtiecīgas izlases elementiem, tādējādi nodrošinot to respondentu iekļaušanu, kuri tieši iesaistīti TPRP procesos. Datu apstrādei un analīzei izmantota aprakstošā statistika ar *Jamovi* programmatūru (jamovi 2024), kā arī daļējo mazāko kvadrātu strukturālo vienādojumu modelēšana (angliski - *PLS-SEM*), izmantojot *bootstrapping* procedūru *SmartPLS* programmatūrā (Ringle et al. 2025). Šī pieeja ļauj empīriski pārbaudīt konceptuālo pētījuma modeli, kas izstrādāts, ņemot vērā teorētisko ietvaru un literatūras pārskatu. Modelī iekļauti šādi konstrukti: DU, TPR, caurskatāmība DU novērtēšanā, organizācijas spējas DU novērtēšanā un pārvaldībā, kā arī TPRP brieduma līmenis organizācijās. *PLS-SEM* metode ir īpaši piemērota konceptuālā modeļa pārbaudei, jo tā ļauj analizēt sarežģītas un daudzdimensionālas sakarības, tostarp mediācijas un moderācijas efektus. Tā tika izvēlēta kā statistiskās analīzes metode, ņemot vērā tās plašo pielietojumu un efektivitāti uzticības un risku pārvaldības savstarpējo attiecību izpētē digitālajā kontekstā (tas konstatēts 73 % empīrisko pētījumu, kas analizēti šīs disertācijas sistemātiskajā literatūras pārskatā). Modelis tika pārbaudīts, izmantojot gan pilnu respondentu izlasi, gan atsevišķu apakšizlasi, kurā iekļauti darbinieki, kas strādā riska, atbilstības un drošības jomā, lai noskaidrotu, vai uzticības un riska savstarpējā saistība ir atkarīga no respondenta profesionālās lomas organizācijā.
2. Kvalitatīvā izpēte balstīta uz daļēji strukturētām ekspertu intervijām (n = 13), kas veiktas ar finanšu sektora pārstāvjiem visās trijās Baltijas valstīs, izmantojot mērķtiecīgu izlasi. Interviju skaits noteikts, pamatojoties uz teorētiskās piesātinātības principu, nodrošinot gan kvantitatīvajā daļā iegūto un konceptuālā modeļa testēšanā pārbaudīto rezultātu validāciju,

gan padziļinātu izpratni par TPRP situāciju Baltijas finanšu sektorā, DU novērtēšanas pašreizējo praksi un organizācijās nepieciešamajām spējām tās efektīvai pārvaldībai.

Teksta pārbaudei un plūduma uzlabošanai autore izmantoja rakstīšanas palīgrīku *Grammarly* v. 1.164 (Grammarly 2026) un *ChatGPT* v. 4 un v. 5 (OpenAI 2025).

Pētījuma ierobežojumi

Interpretējot pētījuma rezultātus, jāņem vērā vairāki ierobežojumi. Pirmkārt, pētījums ir fokusēts uz **digitālās vides** kontekstu, analizējot DU un ar IKT saistītos TPR kā organizācijas nefinanšu risku kategoriju.

Otrkārt, pētījumam ir **ģeogrāfisks** ierobežojums, jo tas aptver tikai Baltijas valstis. Pētījumā iekļautās organizācijas darbojas Igaunijā, Latvijā un Lietuvā. Baltijas valstīm raksturīga vēsturiski līdzīga institucionālā attīstība, regulatīvā vide un uzņēmējdarbības kultūra. Lai gan tas veicina izlases iekšējo viendabību, tas var ierobežot rezultātu vispārināmību uz reģioniem ar būtiski atšķirīgu regulatīvo, kultūras vai tehnoloģisko vidi.

Treškārt, pētījums aprobežojas ar **banku nozari**. Šāda izvēle pamatota ar nepieciešamību analizēt organizācijas, kurās TPRP ir sasniegusi vismaz vidēju brieduma līmeni. Šī risku pārvaldības joma globālā mērogā joprojām ir attīstības stadijā, un mazāk nekā 40 % organizāciju to uzskata par pietiekami attīstītu (SupplyWisdom, 2025). Banku nozare nodrošina vidi, kur iespējams novērot strukturētākas un attīstītākas pieejas. Vienlaikus tas ierobežo rezultātu piemērojamību nefinanšu nozarēm vai sektoros ar zemāku TPRP briedumu.

Ceturtkārt, pētījuma kvantitatīvā daļa balstās uz **paziņojuma datiem**, kas var radīt noteiktus aizspriedumus, piemēram, subjektīvu organizācijas spēju novērtējumu. Lai gan triangulācija ar kvalitatīvajām intervijām palīdz mazināt šo ierobežojumu, to pilnībā novērst nav iespējams.

Piektkārt, **analīzes vienība** ir attiecības ar vienu trešo pusi, par kuru ziņojis katrs respondents. Šāda pieeja ļauj padziļināti analizēt konkrēto uzticības un riska mijiedarbību, tomēr tā neaptver portfeļa līmeņa risku ekspozīciju, savstarpējās atkarības starp vairākām trešajām pusēm vai kopējo risku organizācijas trešo pušu portfelī. Līdz ar to pētījums var pilnībā neatspoguļot sistēmiskos TPR aspektus, kas izpaužas plašākā portfeļa līmenī.

Visbeidzot, pētījumā analizētas organizāciju prakses un uztvere **noteiktā laika posmā**. Ņemot vērā, ka TPRP nozarē vēl ir attīstības stadijā, garengriezuma pētījuma pieeja nākotnē būtu lietderīga, lai analizētu izmaiņas organizācijas spējās, regulatīvajā spiedienā un risku pārvaldības briedumā laika gaitā.

Tēzes aizstāvēšanai

Pamatojoties uz veiktā pētījuma rezultātiem, izvirzīti šādi oriģināli zinātniskie secinājumi:

1. DU samazina TPR. Tā būtiski un pozitīvi ietekmē desmit no divpadsmit analizētajām TPR kategorijām (izņemot piegādātāju un piegādes ķēdes kiberdrošības riskus un ar partneriem saistīto faktoru riskus).
2. Organizācijas spēju loma DU un TPR savstarpējās attiecībās ir atkarīga no vērtētāja profesionālās lomas organizācijā. Lai gan moderācijas efekts netika apstiprināts pilnajā izlasē, tas kļuva statistiski nozīmīgs pārvaldības līmeņa grupā. Tas liecina, ka dinamisko spēju kvalitāti paaugstinošā ietekme DU novērtēšanā tiek atzīta un ir efektīva galvenokārt riska, atbilstības un drošības jomas profesionāļu vidū, kuri darbojas ar izpratni par pārvaldības praksēm.
3. Caurskatāmība DU novērtēšanā pozitīvi ietekmē DU līmeni un pilnībā mediē attiecības starp caurskatāmību un TPR. Tas norāda, ka caurskatāmība mazina nenoteiktību un veicina attiecību uzticību. Šī saistība galvenokārt novērojama plašākā darbinieku izlasē, savukārt pārvaldības līmeņa profesionāļi, vērtējot uzticamību, vairāk balstās uz objektīviem pierādījumiem nekā uz procesu caurspīdīgumu.
4. Ja DU novērtēšanas kritēriji ir caurskatāmi, caurskatāmība darbojas kā moderējošs faktors, kas vājina saikni starp DU un TPR. Trešās puses var manipulēt ar sniegtajiem signāliem,

radot mākslīgi paaugstinātu DU uztveri un tādējādi mazinot šīs uztvertās uzticības negatīvo ietekmi uz faktiskajiem TPR.
5. Caurskatāmība būtiski un pozitīvi ietekmē organizācijas spēju līmeni DU novērtēšanā.
6. Daudzveidīgu informācijas avotu izmantošana pozitīvi ietekmē DU līmeni.
7. Dažādu informācijas avotu izmantošana pozitīvi ietekmē organizācijas spējas DU novērtēšanā, kas apstiprināts, analizējot pilno datu kopu. Tomēr pārvaldības līmeņa grupā šī hipotēze netika apstiprināta, kas liecina, ka pieredzējušiem pārvaldības speciālistiem liels informācijas avotu skaits var radīt "troksni" un papildu saskaņošanas slogu, nevis stiprināt spējas.
8. Organizācijas spējas DU novērtēšanā būtiski un pozitīvi ietekmē trešās puses risku pārvaldības kopējo brieduma līmeni.

Pētījuma periods

Promocijas darba pētāmajai zinātniskajai literatūrai noteikti šādi laika ierobežojumi: pētījumi par DU aptver periodu no 2010. gada līdz 2024. gada septembrim, pētījumi par uzticības un risku pārvaldības saistību digitālajā vidē no 2000. gada līdz 2024. gada jūlijam, savukārt pētījumi par TPR no 2016. gada līdz 2024. gada oktobrim. Analīzē tika iekļauts viss atbilstošais zinātnisko rakstu un konferences publikāciju kopums no *Scopus* (Elsevier,2025) un *Web of Science* (Clarivate, 2024) datubāzēm, un sākotnējā literatūras atlasei netika noteikti laika ierobežojumi.

Promocijas darba izstrādes un pētījuma īstenošanas periods ilga no 2023. gada februāra līdz 2025. gada decembrim. Empīriskā daļa, kas ietvēra aptaujas un intervijas, tika īstenota no 2025. gada janvāra līdz 2025. gada jūlijam.

Pētījuma teorētiskā novitāte

Pētījuma teorētisko pamatu veido uzticības integratīvais modelis (angliski - *integrative model of trust*) (Mayer et al. 1995) un signalizēšanas teorija (angliski - *signalling theory*) (Spence 1973), kas iepriekš izmantotas uzticības un risku pārvaldības izpētē digitālajā vidē. Kā teorētiski jauns ieguldījums pētījumā uzticības un risku pārvaldības analīzē digitālajā kontekstā tiek integrēta informācijas asimetrijas teorija (angliski - *information asymmetry theory*) (Akerlof 1970) un dinamisko spēju teorija (angliski - *dynamic capabilities theory*) (Teece et al. 1997). Tas ļauj teorētiski pamatot un empīriski pārbaudīt, ka caurskatāmi DU novērtēšanas kritēriji un rezultāti var mazināt informācijas asimetriju attiecībās starp organizācijām un trešajām pusēm, veicinot DU pieaugumu un TPR samazināšanos, un ka organizācijas spējas DU novērtēšanā un pārvaldībā var stiprināt DU pozitīvo ietekmi uz TPR mazināšanu.

Turklāt promocijas darbs sniedz šādu teorētisko novitāti:

1. Veikta sistemātiska zinātnisko publikāciju analīze par DU, kuras rezultātā noteiktas sešas DU definīciju tematiskās grupas, atklājot šī koncepta daudzveidīgos akadēmiskos skatījumus un nozīmes.
2. Izstrādāta un validēta visaptveroša DU definīcija: "pārliecība, ka organizācija vai digitālā vide konsekventi demonstrē kompetenci un uzticamību, nodrošina augstu drošības līmeni un drošu sistēmas arhitektūru, īsteno godīgu un ētisku praksi, sniedz pozitīvu lietotāja pieredzi, ievēro pārvaldības un normatīvās prasības, kā arī nodrošina datu un darbību auditējamību un izsekojamību". Definīcija pamatojas uz 86 sistemātiskajā literatūras pārskatā analizētiem zinātniskiem darbiem un 42 noteiktajām DU definīcijām.
3. Sistemātiski noteikti 24 DU faktori, kas apkopoti četrās galvenajās kategorijās, veidojot visaptverošu ietvaru DU mērīšanai un pārvaldībai.
4. Noteiktas četras kategorijas, kas paplašina uzticības visaptverošo modeli (Mayer et al., 1995), papildinot to ar jaunu, digitālajam kontekstam raksturīgu kategoriju –atvērtību (angliski - *openness*).
5. Noteikts teorētisks pamatojums atšķirībai starp TPR un ar piegādātājiem, piegādes ķēdes dalībniekiem un pakalpojumu sniedzējiem saistītajiem riskiem. Šī nošķiršana pamatota ar četru sistemātisku literatūras pārskatu rezultātiem, argumentējot, ka minētie jēdzieni nav

sinonīmi, lai gan profesionālajā un zinātniskajā literatūrā tie bieži tiek lietoti kā savstarpēji aizvietojami.

Pētījuma praktiskā novitāte

1. Izstrādāts un empīriski pārbaudīts DU mērījuma ietvars, kas ietver deviņus validētus mērījuma indikatorus un konsolidētu faktoru struktūru, ko veido četrās uzticības dimensijās tādās kā spēja (angliski – *ability*), labvēlība (angliski – *benevolence*), integritāte (angliski – *integrity*) un atvērtība (angliski - *openness*). Šis mērījuma ietvars un tajā iekļautie indikatori ļauj praktiski novērtēt IKT trešo pušu DU.
2. Apkopots visaptverošs divpadsmit TPR saraksts, kas izstrādāts, pamatojoties uz sistemātisku literatūras pārskatu un strukturējot riskus septiņās kategorijās. Tas sniedz sistemātisku ieskatu risku daudzveidībā un sarežģītībā organizācijas sadarbībā ar trešajām pusēm.
3. Noteikti biežāk izmantotie un efektīvākie informācijas avoti DU novērtēšanā, kurus organizācijas var izmantot IKT trešo pušu DU izvērtēšanai.
4. Empīriski apstiprināts, ka augstāks DU līmenis saistīts ar zemāku līmeni 10 no 12 konkrētajiem TPR veidiem, savukārt, piegādes ķēdes kiberdrošības riskiem un ar partneriem saistītajiem faktoru riskiem nepieciešami papildu kontroles mehānismi ārpus uzticības veicināšanas pasākumiem.
5. Empīriski pierādīts, ka organizācijas dinamiskās spējas DU novērtēšanā un pārvaldībā pozitīvi ietekmē TPR pārvaldības brieduma līmeni. Vienlaikus caurskatāmība DU novērtēšanā stiprina organizācijas spējas, uzsverot skaidri definētu uzticamības kritēriju un dokumentācijas nozīmi.
6. Apstiprināts moderācijas efekts, kas parāda, ka augsts caurskatāmības līmenis DU novērtēšanā var radīt iespēju trešajām pusēm "manipulēt ar signālu", mākslīgi paaugstinot uztverto uzticības līmeni. Tas uzsver nepieciešamību pēc nepārtrauktas uzraudzības un papildu kontroles mehānismiem ārpus sākotnējā DU novērtējuma.
7. Izstrādāts *uz spējām balstīts DU ietvars pilnveidotai TPRP*, kura mērķis ir palīdzēt organizācijām paaugstināt DU novērtēšanas un pārvaldības briedumu. Ietvars sniedz praktisku ceļvedi, kā organizācijas spēju attīstību sasaistīt ar efektīvāku TPRP.
8. Pamatojoties uz ekspertu viedokļiem, izstrādāta pakāpeniska pierādījumu hierarhija, kas kalpo kā praktisks instruments novērtētājiem, nodrošinot visaptverošu un uzticamu IKT trešo pušu DU izvērtēšanu un mazinot dublējošas vai subjektīvas paziņojuma informācijas risku.
9. Pierādīts, ka caurskatāmība DU novērtēšanā stiprina organizācijas DU novērtēšanas un pārvaldības spējas, veicinot standartizāciju un ļaujot piegādātājiem savlaicīgi sagatavot atbilstošu dokumentāciju. Vienlaikus noteikts praktisks risks - pārmērīga caurskatāmība var vājināt uzticības un riska saikni, veicinot formālu prasību izpildi un "iepriekš sagatavotas atbildes". Tādēļ caurskatāmība jāpapildina ar saturisku izvērtējumu un neatkarīgu pārbaudi, lai mazinātu signalizēšanas riskus.
10. Sniegts praktisks ieskats finanšu iestādēm, gatavojoties turpmākajām regulatīvajām prasībām, tostarp DORA, pamatojoties uz ekspertu redzējumu par sagaidāmajām attīstības tendencēm nākamajos 3–5 gados.

Pētījuma metodoloģiskā novitāte

1. Pētījumā izstrādāta un empīriski validēta metodoloģija IKT trešo pušu pakalpojumu sniedzēju digitālās uzticamības novērtēšanai un mērīšanai. Metodoloģija balstās uz strukturētu uzticības faktoru un izmērāmu indikatoru kopumu, kas ļauj integrēt digitālo uzticību TPRP praksē.

Nozīmīgāko rezultātu aprobācija

Pētījuma rezultāti prezentēti trīspadsmit starptautiskās zinātniskajās konferencēs:

1. ASBBMC 2024 - 17th Annual Scientific Baltic Business Management Conference, 2024. gada 28.–30. maijs, Rīga, Latvija.
   Digital Trust in the Financial Sector: A Systematic Literature Review.

2. ICABE 2024 – 20th International Conference on Applied Business & Economics, 2024. gada 12.–14. septembris, Ščecina, Polija.
   Trust and Risk Management in Digital Settings: A Systematic Literature Review
3. SCEE 2024 – 65th Riga Technical University International Scientific Conference "Scientific Conference on Economics and Entrepreneurship", 2024. gada 11. oktobris, Rīga, Latvija.
   Examining the Role of Trust in Digital Risk Management Practices
4. FEMIB 2025 – 7th International Conference on Finance, Economics, Management and IT Business, 2025. gada 5.–6. aprīlis, Porto, Portugāle.
   Trust and Risk Management Interplay: A Review in the Digital Context
5. ASBBMC 2025 - 18th Annual Scientific Baltic Business Management Conference 2025, 2025. gada 28.–29. maijs, Rīga, Latvija.
   Digital Trust: Assessment Approaches and Communication Strategies
6. ESREL SRA-E 2025 - European Safety and Reliability & Society for Risk Analysis Europe Conference, 2025. gada 15.–19. jūnijs, Stavanger, Norvēģija.
   Third-Party Risk in Research: A Literature Review
7. ITSM 2025 - 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University, 2025. gada 9.–10. oktobris, Rīga, Latvija.
   Communicating and Assessing Digital Trust: Insights from Financial Institutions
8. SCEE'2025 – RTU 66th International Scientific Conference on Economics and Entrepreneurship, 2025. gada 16. oktobris, Rīga, Latvija.
   When Digital Trust Reduces Risk: ICT Third-Party Management in the Financial Sector
9. ComManTel 2025 - 4th IEEE International Conference on Computing, Management and Telecommunications, 2025. gada 14.–17. decembris, Madride, Spānija.
   Openness as a Catalyst for Organisational Capabilities in Digital Trust Assessment: Insights from the Financial Sector
10. 84th International Scientific Conference of the University of Latvia 2026, 15 April, 2026, Riga, Latvia
    Digital Trust Assessment Capabilities as a Driver of Third-Party Risk Management Maturity
11. 16th International Scientific Conference "BUSINESS AND MANAGEMENT 2026" of Vilnius Gediminas Technical University
    14 – 15 May, 2026, Vilnius, Lithuania
    From Compliance to Capability: The Evolving Role of Third-Party Risk Management in Strengthening Organisational Resilience
12. ASBBMC 2026 - 19th Annual Scientific Baltic Business Management Conference
    27 – 28 May 2026, Riga, Latvia
    Beyond Cybersecurity: The Category-specific Value of Digital Trust in Third-party Risk Management
13. 34th Annual Conference of the Society for Risk Analysis – Europe
    26 – 29 May 2026, Alicante, Spain
    a. Digital Trust and Third-Party Risk in the Financial Industry: The Moderating Roles of Transparency and Organisational Capabilities
    b. The Future Development of ICT Third-party Risk Management in the European Financial Industry

Publikācijas

Pētījuma galvenie rezultāti publicēti šādos zinātniskajos izdevumos:

1. Saveljeva, J. and Volkova, T. (2025), "A survey on digital trust: towards a validated definition", *Digital*, 5(2), 14. DOI: 10.3390/digital5020014.

2. Saveljeva, J. (2025), “Trust and risk management interplay: a review in the digital context”, in *Proceedings of the 7th International Conference on Finance, Economics, Management and IT Business (FEMIB 2025)*, Porto, Portugal, 5–6 April. Porto: SciTePress, pp. 189–196. DOI: 10.5220/0013344200003956.
3. Saveljeva, J. (2025), “Third-party risk in research: A literature review”, in *Proceedings of the 35th European Safety and Reliability Conference (ESREL2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025)*, Stavanger, Norway, June 15–19, 2025. Research Publishing, Singapore, pp. 267 – 274. DOI: 10.3850/978-981-94-3281-3_esrel-sra-e2025-p8074-cd
4. Saveljeva, J. (2025), “Digital trust in the financial sector: A systematic literature review”, in *Proceedings of the 17th Annual Scientific Baltic Business Management Conference (ASBBMC 2024)*, 28–30 May 2024, Riga, Latvia.
5. Saveljeva, J., Volkova T. (2025), “Communicating and assessing digital trust: Insights from financial institutions”, in *Proceedings of the 65th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITSM 2025)*, 9–10 October 2025, Riga, Latvia, pp 1- 6, DOI: 10.1109/ITMS67030.2025.11236559
6. Saveljeva, J., & Volkova, T. (2025), “Openness as a catalyst for organisational capabilities in digital trust assessment: Insights from the financial sector” in *Proceedings of the 4th International Conference on Computing, Management and Telecommunications (ComManTel 2025)*, Madrid, Spain, 14–17 December, pp. 88-92, DOI: 10.1109/ComManTel68363.2025.11368434
7. Saveljeva, J., & Volkova, T. (2026), “Category-specific effects of digital trust on third-party risks in the banking industry”*, The Journal of Risk Finance*, Vol. 27 No. 2 pp. 329–345, DOI: https://doi.org/10.1108/JRF-08-2025-0383
8. Saveljeva, J., & Volkova, T. (in press), “From Compliance to Capability: The Evolving Role of Third-Party Risk Management in Strengthening Organisational Resilience” in *Proceedings of the 16th International Scientific Conference “BUSINESS AND MANAGEMENT 2026” of Vilnius Gediminas Technical University,* 14-15 May 2026, Vilnius, Lithuania.

Citas publikācijas:

1. Peiseniece, L., Uvarova, I., Volkova, T., Saveljeva, J., Novicka, J., Polis, G., Kristapsone, S. and Vembris, A. (2025), “Integrating cybersecurity into sustainability management: current practices and future directions”, in *Proceedings of the 12th IEEE Conference on Technologies for Sustainability (SusTech 2025)*, Santa Ana, California, USA, 20–23 April. Piscataway, NJ: IEEE, pp. 1-2, DOI: 10.1109/SusTech63138.2025.11025583
2. Saveljeva, J., Uvarova, I., Peiseniece, L., Volkova, T., Novicka, J., Polis, G., Kristapsone, S. and Vembris, A. (2025), “Cybersecurity for sustainability: a path for strategic resilience”, in *Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience (CSR 2025)*, Chania, Crete, Greece, 4–6 August. Piscataway, NJ: IEEE, pp. 1–8, DOI: 10.1109/CSR64739.2025.11129980.
3. Saveljeva, J., Peiseniece, L., Volkova, T., Uvarova, I., Novicka, J., Polis, G., Kristapsone, S., & Vembris, A. (2026), “Integrating cybersecurity into sustainability: Emerging trends and the role of artificial intelligence”, in *Proceedings of the 5th International Conference on Novel & Intelligent Digital Systems (NIDS 2025)*, 24–26 September 2025, Athens, Greece. Lecture Notes in Networks and Systems, vol 1706. Springer, Cham., pp. 313-324, DOI: 10.1007/978-3-032-10827-2_25

Promocijas darba struktūra un apjoms

Promocijas darbs sastāv no ievada, trim nodaļām (kurās ietvertas vienpadsmit apakšnodaļas), secinājumiem, rekomendācijām un septiņiem pielikumiem. Darba kopējais apjoms ir 309 lappuses; tajā iekļauti 40 attēli un 40 tabulas. Bibliogrāfijā izmantoti 261 informācijas avoti.

1. nodaļas kopsavilkums: digitālās uzticības un trešās puses risku savstarpējā saistība

Uzticība jau vairākas desmitgades tiek atzīta par būtisku efektīvas risku pārvaldības elementu (Slovic 1993). Mayer et al. (1995) savā uzticības modelī iekļāva risku kā neatņemamu sastāvdaļu, norādot, ka uzticības un uztvertā riska līmenis situācijā ietekmē gatavību uzņemties risku attiecībās. Pētījums parādīja, ka augstāks uzticības līmenis palielina iespējamību, ka uzticētājs iesaistīsies attiecībās, kuras viņš uzskata par riskantām. Proti, ja uzticības līmenis pārsniedz uztvertā riska līmeni, uzticētājs ir gatavs uzņemties risku attiecībās.

Jāuzsver, ka Mayer et al. (1995) akcentēja uzticības daudzdimensionālo raksturu, iedalot to trīs dimensijās: spēja (angliski - *ability*), labvēlība (angliski - *benevolence*) un integritāte (angliski - *integrity*).

Zinātniskajā literatūrā visbiežāk tiek aplūkotas trīs uzticības formas: sociālā uzticība, DU un uzticība tehnoloģijām (Rychkova and Ghriba 2023). Sociālā uzticība nozīmē vienas puses gatavību būt ievainojamai otras puses rīcības dēļ (Mayer et al. 1995). Uzticība tehnoloģijām pamatojās pārliecībā, ka konkrētajai tehnoloģijai piemīt īpašības, kas nepieciešamas sagaidāmo rezultātu sasniegšanai situācijās, kur iespējamas negatīvas sekas (Rychkova and Ghriba 2023). DU, kas veidojas digitālajās mijiedarbībās un vidēs, atspoguļo pārliecību par digitāli mediētā kontekstā darbojošos dalībnieku, procesu un tehnoloģiju uzticamību. Šīs uzticības formas ir cieši saistītas ar organizāciju lēmumu pieņemšanu un tehnoloģiju ieviešanu (Rychkova and Ghriba 2023).

Pētījumi liecina, ka, izstrādājot tehnoloģiskos risinājumus, jāņem vērā uzticība visās trīs dimensijās. Jau 2017. gadā *Deloitte* globālās aptaujas rezultāti parādīja, ka vairāk nekā 50 % respondentiem būtiski palielinājās atkarība no trešajām pusēm, savukārt, tikai 20 % šo faktoru ņēma vērā, pilnveidojot savus risku pārvaldības mehānismus (Deloitte 2017). Jaunākie pētījumi norāda, ka būtisks izaicinājums noturības nodrošināšanā ir ar trešajām pusēm saistīto ietvaru un datu punktu nepietiekama integrācija (Deloitte 2023). Tas apstiprina informācijas asimetrijas teorijas piemērojamību TPR pārvaldības vidē un aktualizē nepieciešamību meklēt risinājumus šīs asimetrijas mazināšanai. Nobriedušas TPR pārvaldības prakses pakāpeniski pāriet no uz anketām veidtas pārvaldības uz sadarbībā un uzticībā pamatotu pieeju (Deloitte 2023).

Uzticība darbojas kā mehānisms, kas samazina sarežģītību lēmumu pieņemšanā (Lewis and Weigert 1985; Mclain and Hackman 1999), un ir saistīta ar precīzāku riska uztveri (Mclain and Hackman 1999). Vienlaikus uzticība ir kontekstuāla (Marsh 1994; Mayer et al. 1995) un atšķiras digitālajā un nedigitālajā vidē (Alpacan et al. 2011). Tādēļ organizāciju kontekstā nepieciešami atbilstoši DU novērtēšanas instrumenti.

Šīs nodaļas teorētiskais pamats veidots, ņemot vērā sešusm sistemātiskos literatūras pārskatus (SLR), kas veikti saskaņā ar PRISMA 2020 metodoloģiju (Page et al. 2021). Literatūras meklēšana veikta *Scopus* (Elsevier,2025) un *Web of Science* (Clarivate, 2024) datubāzēs, iekļaujot gan zinātniskos žurnālu rakstus, gan konferences publikācijas, ņemot vērā konferences darbu nozīmi jaunu digitālo tēmu attīstībā (Bates and Maack 2009).

1.1. Digitālās uzticības būtība un tās raksturlielumi

Neraugoties uz pieaugošo akadēmisko interesi, joprojām nepastāv vienota DU definīcija un tās raksturlielumu kopums (Pietrzak and Takala 2021; Tunkevichus and Rebiazina 2021; Chen et al. 2023). Tādēļ, lai iegūtu visaptverošu priekšstatu par DU konceptu, tika veikts sistemātisks literatūras pārskats. Literatūras meklēšana, izmantojot atslēgvārdu "digital trust", tika veikta 2024. gada 15. septembrī. Meklēšana tika ierobežota ar šādiem kritērijiem: 1) publikāciju nosaukumi, kopsavilkumi un atslēgvārdi; 2) zinātniskie raksti un konferences publikācijas; 3) publikācijas angļu valodā.

Kopumā *Scopus* (Elsevier, 2025) datubāzē tika noteikti 156 ieraksti, savukārt *Web of Science* (Clarivate, 2024) 84 ieraksti. Pēc dublikātu izslēgšanas atlasei palika 170 publikācijas. Pēc kopsavilkumu izvērtēšanas un pilntekstu analīzes teorētiskajai DU koncepta analīzei tika iekļauti 86 pētījumi - 27 konferences publikācijas un 59 zinātniskie raksti.

Esošās DU definīcijas

Vairāku publikāciju autori norāda, ka nepastāv vienota DU definīcija (Pietrzak and Takala 2021; Tunkevichus and Rebiazina 2021; Chen et al. 2023). Pētījuma rezultāti apstiprina šo atziņu - analizējot 86 zinātniskos darbus, tika noteiktas 42 atšķirīgas DU definīcijas.

Veiktā satura analīze ļāva klasificēt šīs definīcijas sešās tematiskajās grupās, kas apkopotas 1.1. tabulā.

1.1. tabula

DU definīciju sadalījums pa tematiskajām grupām

Groupas nr.	**Galvenā grupas tēma**
1. grupa (n=12)	Pārliecība par cilvēkiem, procesiem un tehnoloģijām drošas digitālās vides veidošanā
2. grupa (n=8)	Uzticība datu aizsardzībai, privātumam, drošībai un ētiskai informācijas apstrādei
3. grupa (n=8)	Uzticība tehnoloģiju tehniskajai kapacitātei un uzticamībai
4. grupa (n=7)	Uzticība kā psiholoģisks stāvoklis, kas ietver kognitīvos, emocionālos un pieredzes faktorus
5. grupa (n=4)	Uzticība kā veicinošs faktors digitālajās attiecībās, mijiedarbībā un biznesa tīklos
6. grupa (n=3)	Uzticība, kas pamatojas uz ētisku rīcību un kultūras principiem

Avots: autores veidots

DU galvenie raksturlielumi

Kopīgas izpratnes veidošanos par DU konceptu un tā raksturlielumiem apliecina tas, ka jau iepriekš veikti mēģinājumi tos noteikt , izmantojot sistemātiskas literatūras pārskata metodoloģiju. *Rychkova* un *Ghriba* (2023), analizējot blokķēdes literatūru, noteica 21 tehnoloģiski neitrālu uzticamības prasību, uzsverot digitālās, tehnoloģiskās un sociālās uzticības nozīmi organizāciju lēmumu pieņemšanā. Pamatojoties uz Mayer et al. (1995) izceltajiem uzticamības faktoriem, šīs prasības tika iedalītas trīs kategorijās: spēja, labvēlība un integritāte.

No 86 analizētajiem darbiem 36 publikācijās tika aprakstīti DU raksturlielumi, taču neviens no tiem nebija iekļauts *Rychkova* un *Ghriba* (2023) veiktajā sistemātiskajā pārskatā. Pamatojoties uz šīm publikācijām, tika noteikti 24 DU faktori, kas ir strukturēti četrās kategorijās un astoņās apakškategorijās.

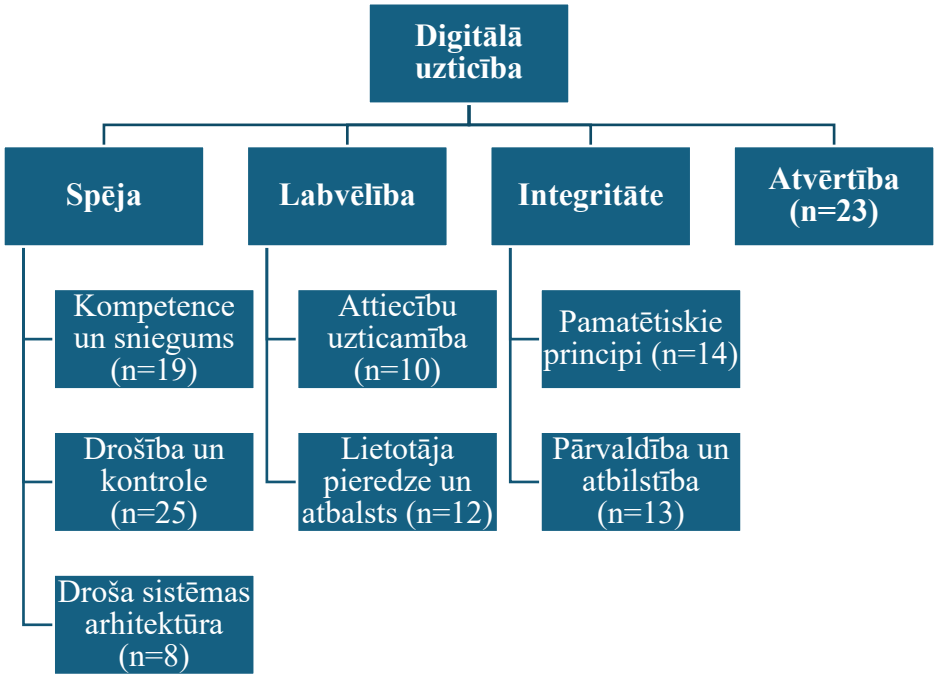
Ņemot vērā, ka pētījuma mērķis ir noteikt vispārīgi piemērojamus DU faktorus, kas nākotnē ļautu izstrādāt DU mērīšanas instrumentus, visi noteiktie faktori tika iedalīti trīs līmeņos:

1. Kategorija - pamatojas uz Mayer et al. (1995) sākotnēji izceltajiem uzticamības faktoriem;
2. Apakškategorija - atspoguļo attiecīgās kategorijas pamatelementus DU kontekstā;
3. Konsolidētie DU faktori - ņemot vērā, ka dažādi pētnieki ar atšķirīgiem jēdzieniem bieži aprakstījuši vienu un to pašu DU aspektu.

Analīze liecina, ka lielāko daļu noteikto faktoru var klasificēt trīs galvenajās kategorijās: 1. sistēmas vai organizācijas kompetence/spēja (*Spēja*), 2. organizācijas vai pakalpojumu sniedzēja pozitīvs nodoms attiecībā pret lietotājiem (*Labvēlība*), un 3. organizācijas atbilstība pieņemamiem standartiem un principiem (*Integritāte*). Tomēr atsevišķa DU faktoru grupa pilnībā neiekļaujas šajos trīs pīlāros.

Mūsdienu digitālajā vidē pastāv daudzi mehānismi, kas ļauj pārbaudīt uzticamību, izmantojot ārējus informācijas avotus vai apliecinājumus. Līdz ar to uzticamība kļūst demonstrējama un publiski pārbaudāma. Šo aspektu iespējams raksturot kā "atvērtību" (angliski – *Openness*), un tas pētījumā piedāvāts kā ceturtā DU faktoru kategorija.

DU ir sarežģīts un daudzdimensionāls koncepts (Ferraro et al. 2023), tādēļ nav vienkārši noteikt, kuri faktori tās veidošanā ir nozīmīgāki par citiem. Veiktā analīze liecina, ka trīs nozīmīgākās digitālās uzticības faktoru apakškategorijas ir "drošība un kontrole" (n=25), "atvērtība" (n=23) un "kompetence un sniegums" (n=19). Pārējās apakškategorijas ir relatīvi mazāk pārstāvētas, tostarp "attiecību uzticamība" un "droša sistēmas arhitektūra". Visas noteiktās digitālās uzticības kategorijas un apakškategorijas attēlotas 1.1. attēlā.



1.1. attēls. DU faktoru kategorijas un apakškategorijas

Avots: autores veidots

Pamatojoties uz iepriekš analizētajām DU definīcijām un galvenajiem faktoriem, kas veido šo konceptu, autore piedāvā šādu digitālās DU: *digitālā uzticība ir pārliecība, ka organizācija vai digitālā vide konsekventi demonstrē kompetenci un uzticamību, nodrošina augstu drošības līmeni un drošu sistēmas arhitektūru, īsteno godīgu un ētisku praksi, sniedz pozitīvu lietotāja pieredzi, ievēro pārvaldības un normatīvās prasības, kā arī nodrošina datu un darbību auditējamību un izsekojamību*.

Ņemot vērā, ka pašlaik pastāv 42 atšķirīgas DU definīcijas un nav izveidojusies viena dominējoša pieeja, piedāvātās definīcijas pamatotības demonstrēšanai tiks izmantota koncepta validācijas metode.

DU definīcijas validācija

Skaidras un precīzas konceptuālās definīcijas ir būtiskas zinātnes attīstībai un turpmākai teorētiskajai pilnveidei (Podsakoff et al. 2016). Vēl jo svarīgāk ir izstrādāt formālu definīciju ar precīzu terminoloģiju, lai novērstu interpretācijas neskaidrības un atkārtotu argumentāciju (Sell 2018). Tādēļ piedāvātās definīcijas pamatotības pārbaudei tika izmantota satura validācijas metodoloģija (Colquitt et al. 2019; Hinkin and Tracey 1999).

Definīcijas satura validācijai tika izstrādāta aptaujas anketa, pamatojoties uz Hinkin un Tracey (1999) pieeju. Anketa sākotnēji tika pilotēta piecu respondentu grupā, lai iegūtu

atgriezenisko saiti un novērtētu tās atbilstību. Pēc tam tā tika izplatīta doktorantu un profesionāļu vidū, iegūstot 99 derīgas atbildes. Lai noteiktu, cik lielā mērā definīcija atbilst to veidojošajiem galvenajiem faktoriem, tika izmantota 5 punktu Likerta skala.

Validācijā izmantoto faktoru operacionalizētie apraksti pamatojas uz *Rychkova* un *Ghriba* (2023) piedāvātajiem faktoru raksturojumiem un apkopoti 1.2. tabulā. Pirmo trīs kategoriju (F1–F7) operacionalizācijai autore apkopoja attiecīgajās apakškategorijās ietverto faktoru aprakstus, kā tos definējuši *Rychkova* un *Ghriba* (2023). Savukārt, ceturtās kategorijas faktori (F8, F9) tika veidoti tieši, pamatojoties uz minēto autoru sniegtajiem aprakstiem.

1.2. tabula

Mērāmo indikatoru apraksts

Kods	**Kategorija**	**Faktors**
	1. kategorija: Spēja	
F1	1.1. Kompetence un sniegums	Organizācija demonstrē kompetenci un uzticami nodrošina pakalpojumu vai produktu sniegšanu.
F2	1.2. Drošība un kontrole	Organizācija nodrošina drošu piekļuvi, aizsargā datus un uztur to integritāti.
F3	1.3. Droša sistēmas arhitektūra	Organizācija izmanto drošu sistēmas arhitektūru un procesus, lai nodrošinātu efektivitāti, kontroli un integrāciju.
	2. kategorija: Labvēlība	
F4	2.1. Attiecību uzticamība	Organizācija demonstrē taisnīgumu, godīgumu un uzticamību, veidojot stabilu reputāciju.
F5	2.2. Lietotāja pieredze un atbalsts	Organizācija nodrošina pozitīvu lietotāja pieredzi un operatīvu atbalstu.
	3. kategorija: Integritāte	
F6	3.1. Ētikas pamatprincipi	Organizācija demonstrē integritāti, aizsargā datu privātumu un īsteno ilgtspējīgu praksi.
F7	3.2. Pārvaldība un atbilstība	Organizācija nodrošina pārvaldību un atbilstību normatīvajām prasībām un standartiem.
	4. kategorija: Atvērtība	
F8	4.1. Auditējamība	Organizācija nodrošina atbilstību, izmantojot sertifikāciju, auditus un uzraudzību.
F9	4.2. Izsekojamība	Organizācija nodrošina izsekojamību, sniedzot informāciju par datu izcelsmi.

Source: autores veidots, pamatojoties uz (Rychkova and Ghriba 2023)

Respondentu vērtējumam tika piedāvātas četras definīcijas: pirmā autores izstrādātā definīcija validācijas nolūkā; otrā analizētajā izlasē visbiežāk izmantotā definīcija, lai pārbaudītu, vai piedāvātā definīcija precīzāk atspoguļo koncepta būtību; trešā un ceturtā ar DU radniecīgiem jēdzieniem "kiberuzticība" (angliski - *cyber-trust*) un "tiešsaistes uzticība" (angliski - *online trust*) saistītās definīcijas.

1. definīcija: "Digitālā uzticība ir pārliecība, ka organizācija vai digitālā vide konsekventi demonstrē kompetenci un uzticamību, nodrošina augstu drošības līmeni un drošu sistēmas arhitektūru, īsteno godīgu un ētisku praksi, sniedz pozitīvu lietotāja pieredzi, ievēro pārvaldības un normatīvās prasības, kā arī nodrošina datu un darbību auditējamību un izsekojamību" (autores piedāvātā).

2. definīcija: "Digitālā uzticība ir ieinteresēto pušu pārliecība par dalībnieku, tehnoloģiju un procesu kompetenci uzticamu un drošu biznesa tīklu izveidē", (M. F. Mubarak and Petraite 2020, p. 3) visbiežāk izmantotā definīcija analizētajā izlasē.

3. definīcija: "Lietotāja pārliecība par programmatūras un aparatūras sistēmu (digitālo tehnoloģiju) uzvedības prognozējamību un uzticamību, kas izpaužas gatavībā deleģēt dažādus uzdevumus šīm sistēmām" (Vidiasova et al. 2020, citēts *Tunkevichus and Rebiazina* 2021, p. 433). Šī ir radniecīgā koncepta "kiberuzticība" (angliski – *cyber-trust*) definīcija.

4. definīcija: "Patērētāju uztvere par tīmekļa vietnes lietderību, drošību, privātumu, reputāciju un kvalitāti, kā arī par e-tirgotāju gatavību pielāgot pakalpojumus individuālām vajadzībām" (*Wu et al*. 2010, citēts *Tunkevichus and Rebiazina* 2021, p. 433). Šī ir radniecīgā koncepta "tiešsaistes uzticība" (angliski – *online trust*) definīcija.

Ņemot vērā, ka *Colquitt et al.* (2019) norāda, ka minimālais izlases apjoms 100 respondentu nodrošina pietiekamu rezultātu precizitāti, var secināt, ka izmantotā izlase ir pietiekama šī pētījuma mērķu sasniegšanai.

Pētījuma statistiskā analīze veikta, izmantojot *Jamovi* v. 2.6.26 (jamovi 2024) programmatūru. Autores piedāvātā definīcija - 1. definīcija (D1) - tika analizēta, izmantojot definicionālās atbilstības indeksu htc (angliski – *Hinkin Tracey correspondence*), kas aprēķināts pēc šādas formulas:

$$\text{htc} = \text{vidējais definicionālās atbilstības vērtējums} \diagup a$$

Saskaņā ar *Hinkin* un *Tracey* (1999), minimālā htc vērtība 4,2 apstiprina pietiekamu satura atbilstību. Savukārt, *Colquitt et al*. (2019) norāda, ka htc vērtība no 0,87 līdz 0,90 apliecina augstu satura atbilstību, bet vērtība no 0,84 līdz 0,86 liecina par vidēju, tomēr pietiekamu atbilstību. Kopumā *Jamovi* veiktā statistiskā analīze apstiprināja vidēju līdz augstu satura atbilstību (kopējais htc = 0,86).

Pēc tam līdzīgās (D2) un alternatīvās (D3, D4) definīcijas tika analizētas, izmantojot htd jeb *Hinkin Tracey* atšķirtspējas indeksu (angliski – *Hinkin Tracey distinctiveness*), kas aprēķināts pēc šādas formulas:

$$\text{htd} = \text{vidējā vērtība (paredzētās atbilstības vērtējums - orbitējošās atbilstības vērtējums)} / (a - 1)$$

, kur a ir vērtēšanas skalas punktu skaits.

Saskaņā ar *Colquitt et al*. (2019), htd vērtība no 0,18 līdz 0,26 norāda uz vidēju atšķirtspēju, bet no 0,27 līdz 0,34 uz augstu atšķirtspēju. Aprēķinu rezultāti rāda, ka 2. definīcija (D2), analizētajā izlasē vispopulārākā DU definīcijam uzrāda vidēju atšķirtspēju attiecībā pret jaunpiedāvāto definīciju (htd = 0,23). Līdz ar to var secināt, ka autores piedāvātā definīcija (D1) precīzāk atspoguļo DU konceptuālo būtību nekā esošā definīcija.

Savukārt 3. definīcija (D3), kiberuzticības (angliski – *cyber-trust*) definīcija, uzrāda augstu atšķirtspēju (htd = 0,27), bet 4. definīcija (D4), tiešsaistes uzticības (angliski – *online trust*) definīcija, demonstrē vidēju atšķirtspēju (htd = 0,24) salīdzinājumā ar piedāvāto D1. Pamatojoties uz šiem rezultātiem, var secināt, ka piedāvātā D1 atspoguļo tieši DU konceptu, nevis ar to radniecīgos jēdzienus.

DU mērīšana

Literatūras analīze liecina, ka vienota pieeja DU mērīšanai nepastāv, un tika noteiktas četras galvenās mērīšanas metodes. Visbiežāk izmantotā pieeja (n = 11) pamatojas uz daudzdimensionālām Likerta skalas aptaujām (ar vērtējuma diapazonu 1–4 (Svenson et al. 2024), 1–5 (Balci 2021) vai 1–7 (Mubarak et al. 2024)). Otrā metode izmanto sekundāros datus, piemēram, reputācijas vērtējumus, sertifikācijas apliecinājumus, atbilstības rādītājus, drošības incidentu datus un trešo pušu novērtējumus (Das et al. 2023; Kluiters et al. 2023). Trešā pieeja paredz tiešu uzticības uztveres mērīšanu, izmantojot vienu Likerta skalas jautājumu par to, cik lielā mērā pakalpojums vai pakalpojumu sniedzējs ir uzticams (Chen et al. 2022). Savukārt,

tehniski orientētos pētījumos DU tiek mērīta, izmantojot Industriālās revolūcijas 4.0 (angliski – *Industry 4.0*) konceptus vai uzticības arhitektūras dizaina pieejas (Akram and Ko 2014; Mubarak and Petraite 2020; Rane and Huang 2022).

Tomēr nevienā no analizētajiem pētījumiem netiek aplūkotas organizācijas spējas DU novērtēšanai. Ņemot vērā uzticības dinamisko raksturu (Oudina et al. 2024) un tās saistību ar riska uztveri (Mclain and Hackman 1999), dinamisko spēju koncepts (angliski – *dynamic capabilities*) (Teece et al. 1997) piedāvā atbilstošu teorētisko ietvaru. Pamatojoties uz Teece pieeju, dinamiskās spējas var iedalīt trīs funkcijās - uztveršanā (angliski - *sensing*), izmantošanā (angliski - *seizing*) un pārveidošanā (angliski - *reconfiguring*) (Jantunen et al. 2012), kas var veicināt organizācijas kapacitātes attīstību efektīvai DU novērtēšanai.

Iepriekšējie pētījumi par DU kā būtisku pakalpojumu sniedzēja atribūtu

Analizētie pētījumi liecina, ka DU organizāciju iekšējā kontekstā pētīta ierobežoti. Corsaro un D'Amico (2022) noteica DU kā būtisku dimensiju, kas ietekmē B2B attiecību pārmaiņas, kuras paātrinājusi digitālā transformācija. Empīriskie pierādījumi rāda, ka DU pozitīvi ietekmē atvērtās inovācijas sniegumu, un šo ietekmi mediē tehnoloģiskās absorbcijas spējas (Mubarak and Petraite 2020). Tāpat DU veicina ilgtspējīgu uz blokķēdi balstītu piegādes ķēžu attīstību, stiprinot caurskatāmību, kiberdrošību, atbildību un atbilstību regulatīvajām prasībām (Sharma et al. 2024).

B2B kontekstā DU palielina uztverto lietderību, apmierinātību un klientu lojalitāti (Balci 2021; Loh et al. 2024). Tā korelē arī ar korporatīvo digitālo atbildību (Jelovac et al. 2022) un no pārvaldības perspektīvas veicina uzņēmuma vērtības pieaugumu (Kluiters et al. 2023).

DU komunikācija

DU iespējams komunicēt, izmantojot tehnoloģiskus, reputācijas un signalizēšanas mehānismus. Blokķēde bieži tiek minēta kā instruments caurskatāmības, nemainīguma un pārbaudāmības stiprināšanai dažādās nozarēs (Piccininni et al. 2020; Kayhan 2022; Kobzan et al. 2018). Tomēr tehnoloģiskie risinājumi paši par sevi nav pietiekami DU nodrošināšanai, un pārmērīga paļaušanās uz atsevišķiem tehnoloģiskiem risinājumiem, neveidojot uzticību institūcijām un procesiem, var radīt pretēju efektu - neuzticēšanos. Tādēļ DU ir cieši saistīta arī ar institucionālo uzticību, pārvaldības kvalitāti un cilvēciskajiem faktoriem (Ferraro et al. 2023; Katete 2021).

Papildu uzticības signāli ir reputācija, sertifikācijas (piemēram, ISO 27001), iepriekšējā sadarbības pieredze un valsts institūciju apliecinājumi (Das et al. 2023; Deprez et al. 2016). DU var stiprināt arī partneru vai klientu vērtējumi un atsauksmes, kvalitatīva publiskā komunikācija, kā arī informācijas atklāšana par kiberdrošības investīcijām (Oukarfi and Sattar 2020; Mohlmann 2021; Kluiters et al. 2023). Klientu izglītošana par produktu arhitektūru un tehnoloģijām, kā arī kopienu veidošana ap organizāciju, papildus veicina DU komunikāciju (Levine 2019; Zolfaghari et al. 2023; Pivavarava and Koop 2024).

Informācijas asimetrijas teorija (Spence 1973) skaidro, kā nevienlīdzīga piekļuve informācijai ietekmē uzticību, un tā pētīta gan tradicionālajā, gan digitālajā vidē (Oukarfi and Sattar 2020; Sattar et al. 2022; Cerić 2021; Baumgaertner and Soluk 2023). Savukārt, signalizēšanas teorija (Spence 1973) pēta, kā viena puse stratēģiski komunicē informāciju, lai mazinātu nenoteiktību. Lai gan iepriekšējie pētījumi aplūkojuši uzticības komunikāciju, izmantojot vērtējumus vai blokķēdes risinājumus, DU novērtēšanas kritēriju caurskatāmība un vairāku neatkarīgu signālu savstarpējā papildināmība organizāciju sadarbībā ar trešajām pusēm joprojām ir nepietiekami izpētīta.

1.2. Uzticības pamati risku pārvaldībā

Uzticības un riska savstarpējā saistība jau ilgstoši ir pētniecības objekts, uzsverot šo jēdzienu ciešo savstarpējo saikni (Jøsang and Presti 2004). To apstiprina arī meklēšanas rezultāti *Scopus* (Elsevier,2025) datubāzē, izmantojot atslēgvārdus "risk management" AND "trust", ierobežojot meklējumu ar publikāciju nosaukumiem, kopsavilkumiem un atslēgvārdiem, kā arī iekļaujot zinātniskos rakstus un konferences publikācijas (meklēšana

veikta 2025. gada februārī). Rezultātā tika noteikti 2190 darbi, kas atbilda šiem kritērijiem. Analizētie dati liecina, ka interese par šo tematu sāka veidoties 20. gadsimta 90. gadu sākumā, kam sekoja izteikts pieaugums 2004. gadā un straujš interešu kāpums kopš 2020. gada.

Pēdējos gados Eiropas Savienība (ES) arvien lielāku uzmanību pievērš regulatīviem pasākumiem, lai stiprinātu risku pārvaldību digitālajā vidē (European Commission 2022b; 2022a). Tomēr risku pārvaldības sistēmas efektivitāte Eiropas kontekstā joprojām ir aktuāls jautājums (Ghazieh and Chebana 2021), jo tradicionālās risku mazināšanas pieejas arvien biežāk saskaras ar pieaugošiem kiberdrošības apdraudējumiem (Aslan et al. 2023), kas aktualizē nepieciešamību pēc efektīva risku pārvaldības ietvara (Luther et al. 2023). Jau agrākie pētījumi uzsvēruši uzticības nozīmi efektīvā risku pārvaldībā (Slovic 1993; Rousseau et al. 1998), norādot, ka uzticība var kalpot kā "sarežģītības mazināšanas" mehānisms lēmumu pieņemšanā un papildināt racionālas riska novērtēšanas pieejas (Lewis and Weigert 1985; Mclain and Hackman 1999).

Lai izpētītu, kā uzticība veicina risku pārvaldību digitālajā vidē, tika veikts sistemātisks literatūras pārskats, izmantojot atslēgvārdus trust AND "risk management" AND ("digital" OR "online" OR "cyber"). Meklēšana *Scopus* datubāzē (Elsevier, 2025) tika veikta 2024. gada 30. jūnijā (n = 272), bet *Web of Science* (Clarivate, 2024) 2024. gada 7. jūlijā (n = 55). Kopumā tika noteikta 281 unikāla publikācija, no kurām 45 (22 konferences publikācijas un 23 zinātniskie raksti) atbilda iekļaušanas kritērijiem, fokusējoties uz uzticības un risku pārvaldības korelāciju digitālajā kontekstā.

Atslēgvārdu un līdzparādīšanās analīze, izmantojot *VOSviewer* programmatūru (VOSviewer, 2025), parādīja, ka esošie pētījumi galvenokārt koncentrējas uz uztverto risku, uzvedības nodomu modeļiem, kiberdrošību un e-komercijas kontekstu. Tomēr uzticības daudzdimensionālā loma organizāciju līmeņa B2B digitālajā risku pārvaldībā joprojām ir nepietiekami izpētīta. Šī pētniecības plaisa pamato nepieciešamību padziļināti analizēt DU kā TPR noteicošo faktoru šī pētījuma ietvaros.

Galvenās teorētiskās perspektīvas par uzticību un risku

Atlasīto publikāciju analīze parādīja, ka nepastāv viena dominējoša teorija vai modelis, kas digitālajā kontekstā sistemātiski skaidrotu uzticības un riska savstarpējo saistību. Pētnieki izmantojuši dažādas teorijas un to kombinācijas, lai izstrādātu konceptuālos modeļus un analizētu šo attiecību dinamiku.

Visbiežāk piemērotā teorija bija Tehnoloģiju pieņemšanas modelis (angliski – *Technology Acceptance Model*, *TAM*) (Davis 1989) (n = 7), kam sekoja Plānotās rīcības teorija (angliski – *Theory of Planned Behaviour, TPB*) (Ajzen 1991) (n = 5). Tehnoloģiju pieņemšanas un izmantošanas vienotā teorija (angliski – *Unified Theory of Acceptance and Use of Technology, UTAUT*) (Venkatesh et al. 2003) (n = 3) un tās paplašinātā versija UTAUT2 (Venkatesh et al. 2012) (n = 2) tika izmantotas, lai skaidrotu uzvedības nodomu attiecībā uz tehnoloģiju ieviešanu. Savukārt, Pamatotās rīcības teorija (angliski – *Theory of Reasoned Action, TRA*) (Hansen et al. 2018) (n = 4) tika izmantota četros pētījumos, parasti kombinācijā ar TAM un TPB.

Papildus tika piemērots arī organizatoriskās uzticības integratīvais modelis (angliski – *Integrative Model of Organisational Trust*) (Mayer et al. 1995) (n = 4), kur uzticība konceptualizēta kā daudzdimensionāls konstrukts un kā mediējošs vai moderējošs mainīgais, kas samazina uztverto risku. Tāpat vairākos pētījumos (n = 4) tika izmantota signalizēšanas teorija (angliski – *Signalling Theory*) (Spence 1973), lai skaidrotu informācijas asimetrijas mehānismus.

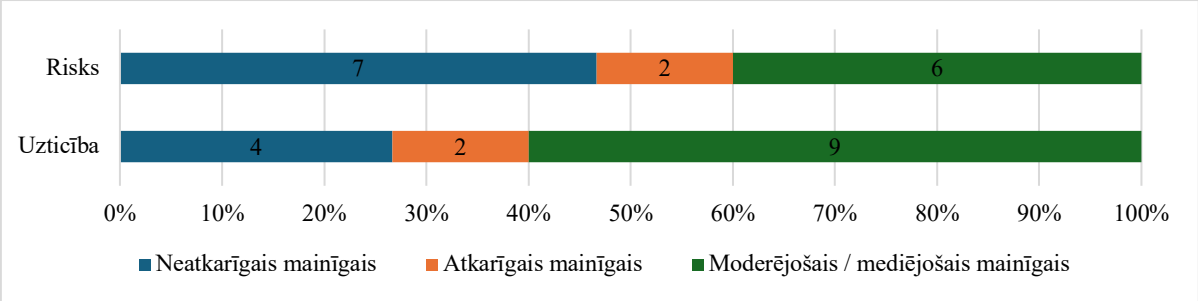
Iepriekšējās pētniecības metodoloģijas uzticības un risku pārvaldības izpētē digitālajā vidē

Analīze parādīja, ka lielākā daļa publikāciju (n = 31; 68,9 %) ir empīriskas, savukārt, desmit (22,2 %) ir konceptuālas un četras (8,8 %) ir teorētiskas. Dominējošā empīriskā metode ir aptauja (n = 19; 42,2 %), kas izmantota gan kvantitatīvā (n = 15), gan kvalitatīvā (n = 4) formā, visbiežāk piemērojot 5, 6 vai 7 punktu Likerta skalu. Modelēšana (n = 9; 20 %) un

nesistemātisks literatūras pārskats (n = 9; 20 %) tika izmantoti vienlīdz bieži. Intervijas pielietotas četros pētījumos (8,9 %), konstruktīvās pētniecības metodes - četros, savukārt, gadījuma izpētes un eksperimentālās metodes - divos pētījumos katra. Sešos pētījumos izmantota vairāku metožu pieeja, kopumā 45 publikācijās nosakot 51 metodoloģisko pielietojumu.

Apmēram trešdaļa pētījumu (n = 15; 33 %) pārbaudīja konceptuālos modeļus, izmantojot aptaujās pamatotu kvantitatīvo analīzi. Lielākā daļa pētījumu veikti uzņēmumu–patērētāju (B2C) kontekstā (n = 10; 66,7 %), kam seko personu–personu (angliski – *peer-to-peer, P2P*) (n = 2; 13,3 %), savukārt tikai viens pētījums (6,67 %) analizēja organizāciju līmeņa B2B kontekstu.

Konceptuālajos modeļos risks galvenokārt pozicionēts kā neatkarīgais mainīgais (n = 7; 46,7 %) vai kā moderējošs/mediējošs mainīgais (n = 6; 40 %), savukārt, uzticība pārsvarā analizēta kā moderējošs vai mediējošs mainīgais (n = 9; 60 %). Tikai vienā pētījumā tika analizēta uzticības ietekme uz risku (Zhang and Cozma 2022), turklāt uzticība tajā tika konceptualizēta kā viendimensionāls jēdziens. Riska un uzticības mainīgo sadalījums pēc to pozicionējuma konceptuālajos modeļos attēlots 1.2. attēlā.



1.2. attēls. Riska un uzticības sadalījums pēc mainīgo tipa konceptuālajos modeļos, %

Avots: autores veidots

Lielākajā daļā pētījumu (n = 11; 73 %) modeļu validācijai tika izmantota strukturālo vienādojumu modelēšana (angliski – *Structural Equation Modelling, SEM*) vai daļējo mazāko kvadrātu strukturālo vienādojumu modelēšana (angliski – *Partial Least Squares Structural Equation Modelling, PLS-SEM*). Kopumā rezultāti liecina, ka uzticības un riska savstarpējā saistība organizāciju digitālajā kontekstā joprojām ir nepietiekami izpētīta, īpaši attiecībā uz uzticību kā daudzdimensionālu neatkarīgo mainīgo, kas ietekmē risku (Marsh 1994; Dimitrakos 2001).

Uzticības loma risku pārvaldībā

Analizētie pētījumi apstiprina, ka uzticība un uztvertais risks ir savstarpēji saistīti un ietekmē viens otru: augstāks uzticības līmenis samazina uztverto risku un veicina pieņemšanu vai iesaisti, savukārt, augsts uztvertais risks mazina uzticību (Aldás-Manzano et al. 2009; Ksibi et al. 2023; San Martín and Camarero 2009; Putri et al. 2022). Uzticība arī veicina gatavību uzņemties risku finanšu, digitālās ekonomikas un koplietošanas ekonomikas kontekstā (Hansen et al. 2018; Mollazehi et al. 2024; Sun et al. 2016). Tomēr pārmērīga uzticība var radīt pārlieku pašpārliecinātību, samazinātu modrību un paaugstinātu ievainojamību (Bishop et al. 2020; Larsen et al. 2022; Terry Morris et al. 2020).

Apliecinājumu ietvari un jaunas tehnoloģijas, piemēram, blokķēde, ir pierādījušas spēju mazināt nenoteiktību un darījumu riskus, vienlaikus stiprinot uzticību (Ghaffarian et al. 2023; Hampton et al. 2021; Shaytura et al. 2021). Caurskatāma komunikācija un skaidrojama informācija (angliski – *explainable information*) papildus veicina uzticības veidošanos, savukārt, zems uzticības līmenis veicina riska izvairīšanās uzvedību (Ghaffarian et al. 2023; Windelberg 2016; McInnis et al. 2016; Setty 2018). Uzticības novērtējuma integrēšana lēmumu pieņemšanā paaugstina risku pārvaldības efektivitāti (Oudina et al. 2024; Yuan et al. 2010).

Visbeidzot, uzticības un riska uztvere ir kontekstuāli nosacīta un ietekmēta sociālajiem un kultūras faktoriem (Bhattacharya and Saha 2004; Windelberg 2016). Tas apstiprina, ka uzticības un riska attiecības ir sarežģītas un dinamiskas, nevis lineāras vai vienkārši cēloņsakarīgas.

Pieejas uzticības integrēšanai risku pārvaldībā

Analizētie pētījumi norāda uz vairākiem veidiem, kā digitālajā risku pārvaldībā integrēt uzticību. No pakalpojumu sniedzēja perspektīvas uzticību iespējams stiprināt, īstenojot augsta līmeņa drošības pasākumus (San Martín and Camarero 2009), nodrošinot caurskatāmu komunikāciju par risku pārvaldības praksi (Ghaffarian et al. 2023; Tehrani et al. 2020), veicinot kultūras saskaņotību (Bhattacharya and Saha 2004), palielinot tehnoloģiju caurskatāmību un skaidrojamību (angliski – *explainability*) (Ghaffarian et al. 2023), kā arī iesaistot lietotājus pakalpojumu izstrādē (McInnis et al. 2016; Zhang et al. 2016).

Organizāciju iekšienē uzticību iespējams integrēt, iekļaujot uzticības rādītājus un vērtēšanas sistēmas risku novērtējumos (Abdul-Rahman and Hailes 2000; Yuan et al. 2010), ko papildina neatkarīgi auditi un sertifikācijas (Hafver et al. 2021), kā arī ieviešot tehnoloģijas kuru pamatā ir izmantoti uzticamības principi(angliski – *trusted-by-design technologies*), piemēram, blokķēdi (Shaytura et al. 2021). Tomēr, ņemot vērā uzticības dinamisko raksturu (Oudina et al. 2024), nepieciešama nepārtraukta tās pārvērtēšana un uzraudzība, lai novērstu pārmērīgu paļaušanos (Larsen et al. 2022).

Literatūra liecina, ka uzticības integrēšana risku pārvaldībā prasa gan tehniskus, gan uz cilvēku orientētus risinājumus. Tomēr līdz šim nav izstrādāts standartizēts ietvars uzticības novērtēšanai vai tās sistemātiskai integrēšanai risku pārvaldībā. Turklāt dažādu DU raksturlielumu ietekme uz konkrētiem TPR joprojām ir nepietiekami izpētīta, kas pamato turpmāku izpēti šajā promocijas darbā.

1.3. Trešās puses risku pārvaldība un tās ietvari

Finanšu iestādes saskaras ar vairākām risku kategorijām, no kurām nozīmīgākās ir kredītrisks, tirgus risks, operacionālais risks un likviditātes risks (Vashisht et al. 2022; Korneev et al. 2023). Operacionālais risks ietver kiberdrošības, cilvēkfaktora, tehniskos un TPR un ir cieši saistīts ar banku sistēmas stabilitāti. Lai gan tradicionālie risku pārvaldības ietvari ir labi nostiprināti, jaunākajos pētījumos arvien lielāka uzmanība tiek pievērsta jaunajiem riskiem, ko veicina digitālā transformācija, finanšu tehnoloģiju (fintech) attīstība un IT traucējumi (Gai et al. 2018), uzsverot nepieciešamību pastāvīgi pielāgot risku pārvaldības praksi (Minh Sang 2024). Kopš 2017. gada ar IKT saistītie TPR kļuvuši par būtisku bažu avotu Eiropas bankām, un nozares pārstāvji uzskata, ka arī 2025. gadā TPR saglabājas kā nozīmīgs risku virzītājspēks (Were 2025).

Lai izpētītu TPRP ietvarus, 2024. gada 12. oktobrī tika veikts sistemātisks literatūras pārskats meklējot vārdu kombināciju "third party risk" *Scopus* (Elsevier, 2025) (n = 108) un *Web of Science* (Clarivate, 2024) (n = 26) datubāzēs, nosakot 107 unikālas publikācijas. Pēc iekļaušanas un izslēgšanas kritēriju piemērošanas analīzē tika iekļauti 16 darbi (5 konferences publikācijas un 11 zinātniskie raksti). Publikācijas par TPR sāka parādīties 2016. gadā, sasniedzot maksimumu 2024. gadā. Pētījumi aptver dažādus nozares kontekstus un ģeogrāfiskās teritorijas.

Izmantojot *VOSviewer* (VOSviewer, 2025) programmatūru, tika veikta pilnā skaita līdzparādīšanās atslēgvārdu analīze, analizējot 63 atslēgvārdus, no kuriem 13 bija savstarpēji saistīti. Analīzē noteikti trīs tematiskie klasteri: (1) tehnoloģiskais klasteris, kas koncentrējas uz blokķēdi, šifrēšanu, lietu internetu (IoT), privātumu un drošību; (2) procesu orientētais klasteris, kas vērsts uz informāciju, risku un pašnovērtējumu; (3) nozarei specifiskais klasteris, kas akcentē būvniecību, inženieriju, integritāti un uz risku balstītu izpēti (angliski – *risk-based due diligence*). Lai gan izlases apjoms bija ierobežots, rezultāti parāda, ka TPR izpēte ir daudzdimensionāla un aptver tehnoloģiskos, procesuālos un nozares specifiskos aspektus, neaprobežojoties ar vienu jomu.

Kvalitatīvā analīze atklāja daudzdimensionālu pētniecības ainavu. Konceptuālie pētījumi (n = 6) koncentrējas uz inovatīviem instrumentiem un metodēm (Ramasubramaniam and Singh 2020; Fortner 2021; Mohta et al. 2024; Agrawal et al. 2024) vai uz regulatīvo un stratēģisko nepilnību noteikšanu (Jadwani et al. 2024; Neumannová et al. 2023). Empīriskie pētījumi (n = 10) piedāvā jaunus ietvarus, instrumentus un procesuālas pieejas vai izvērtē esošo TPRP praksi.

Sākotnējā analīze parādīja, ka profesionālajā un zinātniskajā literatūrā autori bieži lieto jēdzienu "TPR" kā sinonīmu "piegādātāja risks" (angliski - *vendor risk*) vai "piegādes ķēdes dalībnieka risks" (angliski - *supplier risk*). Tādēļ, lai precīzi izprastu TPR būtību un tā saistību ar līdzīgiem risku veidiem, šajā promocijas darbā veikti četri atsevišķi analītiski pētījumi, kas aprakstīti turpmāk.

TPR

Tikai sešās no analizētajām publikācijām tika sniegta skaidra TPR definīcija, un tikai viena no tām īpaši attiecās uz IKT jomu (Ramasubramaniam and Singh 2020). Pārējās definīcijas TPR raksturo plaši - kā riskus, kas izriet no attiecībām ar ārējām pusēm, tostarp piegādātājiem, piegādes ķēdes dalībniekiem, apakšuzņēmējiem, konsultantiem un kopuzņēmumu partneriem (Keskin et al. 2021; Roy et al. 2022; Mohta et al. 2024; Jadwani et al. 2024; Jallan and Ashuri 2020).

Definīciju daudzveidība liecina par vienotas izpratnes trūkumu attiecībā uz to, kas uzskatāms par trešo pusi un kādi riski ar to saistīti. Tas apgrūtina konsekventu TPR pārvaldības ietvaru izveidi un prasa pielāgot TPR tvērumu konkrētās organizācijas nozarei un darbības kontekstam. Lai gan daļa autoru TPR uzskata par sinonīmiem piegādātāja riskam (angliski – *vendor risk*) vai piegādes ķēdes dalībnieka riskam (angliski – *supplier risk*) (Schelegia and Fleşer 2021; Keskin et al. 2021), analizētās definīcijas norāda uz konceptuālām atšķirībām. Tādēļ šajā promocijas darbā TPR, piegādātāja risks un piegādes ķēdes dalībnieka risks netiek uzskatīti par savstarpēji aizvietojamiem jēdzieniem, un to atšķirības tiek precizētas turpmāk.

Piegādātāja risks

Sākotnējā analīze atklāja, ka nepastāv vienota piegādātāja riska definīcija. Tādēļ 2024. gada 23. oktobrī tika veikts sistemātisks literatūras pārskats, izmantojot vārdu kombināciju "vendor risk" *Scopus* (Elsevier, 2025) (n = 36) un *Web of Science* (Clarivate, 2024) (n = 6) datubāzēs. Pēc dublikātu izslēgšanas tika noteikti 36 unikāli avoti. Pēc kopsavilkumu izvērtēšanas un pilntekstu analīzes tika analizēti 19 darbi, kas ļāva noteikt septiņas atšķirīgas definīcijas.

Literatūras pārskatā atklātas divas galvenās perspektīvas: organizācijas skatījums (Natovich 2003; Keskin et al. 2021; John et al. 2024) un patērētāju skatījums (Tainyi et al. 2009; Mascha et al. 2011; Herrero and San Martín 2012; Pappas 2017). Lielākā daļa definīciju piegādātājus aplūko digitālajā vidē, tādējādi padarot šo jēdzienu īpaši attiecināmu uz ar IKT saistītām attiecībām.

Organizācijas perspektīvā definīcijās bieži iekļauti risku pārvaldības procesi, piemēram, piegādātāja izvēle, līgumu slēgšana un uzraudzība. Kopumā piegādātāja risks saistīts ar leģitimitāti un ētisku rīcību, iespējamiem zaudējumiem, privātuma un datu aizsardzības jautājumiem, kā arī darbības nepārtrauktību.

Piegādes ķēdes dalībnieka risks

Piegādes ķēdes dalībnieka risks, kas bieži tiek uztverts kā sinonīms piegādātāja riskam, tika analizēts, veicot sistemātisku literatūras pārskatu 2024. gada 12. oktobrī. Vārda kombināciju meklējums "supplier risk" Scopus (Elsevier, 2025) (n = 238) un Web of Science (Clarivate, 2024) (n = 69) datubāzēs pēc dublikātu izslēgšanas ļāva noteikt 243 unikālas publikācijas. Pētnieciskā aktivitāte būtiski pieauga pēc 2000. gadu sākuma, sasniedzot maksimumu 2021. un 2022. gadā (katru gadu – 25 publikācijas). Pēc kopsavilkumu izvērtēšanas un pilntekstu analīzes tika analizēti 47 darbi, no kuriem tikai 11 sniedza skaidras piegādes ķēdes dalībnieka riska definīcijas.

Definīcijas pārsvarā atspoguļo organizācijas perspektīvu un lielākoties saistītas ar tradicionālajām (ne digitālajām) nozarēm. Piegādes ķēdes dalībnieka risks galvenokārt tiek saistīts ar vides, operacionālajiem (piemēram, piegādes kavējumi, kvalitātes nepilnības, piegādes ķēdes traucējumi) un ētiskajiem riskiem (Lockamy 2011; Globočnik Žunac et al. 2019; Collier et al. 2022; Zhou et al. 2022; Leite et al. 2024; Puncreobutr and Puncreobutr 2024; Lau et al. 2024). Atšķirībā no piegādātāja riska, piegādes ķēdes dalībnieka risks ir cieši saistīts ar piegādes ķēdes darbības efektivitāti un augšupējo traucējumu ietekmi, padarot "piegādi" un "piegādes ķēdi" par centrāliem jēdzieniem tā konceptualizācijā.

Pakalpojumu sniedzēja risks

Tā kā TPR definīcijās pakalpojumu sniedzēji tiek minēti kā ārējās puses, kas var radīt risku, tika analizēts arī šis riska veids. Lai analizētu pakalpojumu sniedzēja risku, (kurā gadā???) 26. oktobrī tika veikts meklējums, izmantojot vārdu kombināciju "service provider risk", kā rezultātā tika noteiktas 17 unikālas publikācijas (Scopus n = 17; Web of Science n = 1) (Elsevier, 2025; Clarivate, 2024). Šis termins pirmo reizi parādījās 2007. gadā un neuzrādīja skaidru augšupejošu tendenci, sasniedzot maksimumu 2024. gadā ar četrām publikācijām. Pēc iekļaušanas kritēriju piemērošanas un pilntekstu analīzes tikai divi darbi tika atzīti par atbilstošiem.

Nevienā no šiem darbiem netiek sniegta tieša pakalpojumu sniedzēja riska definīcija. Vienā publikācijā (Mathew and Aundhe 2011) jēdziens "pakalpojuma sniedzēja risks" tika lietots kā sinonīms "piegādātajā riskam" ārpakalpojumu IKT kontekstā, savukārt otrā (Ray et al. 2013) tika minēts "pakalpojumu sniedzējā risks" stratēģisko ārpakalpojumu līgumu ietvarā, to nedefinējot. Analizējot minētos darbus, var secināt, ka pakalpojumu sniedzēja risks ir reti lietots jēdziens, ko noteiktos kontekstos iespējams uzskatīt par piegādātāja riska sinonīmu.

Risku pārvaldības cikls un TPRP ietvari

Iepriekšējie pētījumi liecina, ka esošie ietvari pilnībā neatbilst nozares prasībām TPRP jomā. Neumannová et al. (2023) noteica nepilnības ISO 27001:2013 standartā, norādot, ka esošie kontroles mehānismi pilnībā neaptver DORA prasības, īpaši attiecībā uz ārējiem partneriem un mākoņpakalpojumu piegādātājiem. Analizētie pētījumi nepiedāvā vienotu ietvaru un atšķiras detalizācijas pakāpē, sākot no augsta līmeņa modeļiem (Roy et al. 2022; Mohta et al. 2024) līdz detalizētām daudzposmu pieejām (Monev 2021).

Apvienojot analizētās pieejas, tika noteikti septiņi galvenie TPRP posmi: (1) pārvaldības struktūras un lomu noteikšana; (2) trešo pušu tvēruma definēšana un to klasifikācija pēc nozīmīguma; (3) risku novērtēšana, pamatojoties uz informācijas iegūšanu un novērtēšanas modeļa izstrādi; (4) līgumu slēgšana, iekļaujot risku mazināšanas nosacījumus; (5) nepārtraukta uzraudzība un atkārtota novērtēšana; (6) ziņošana un pārvaldības līmeņa uzraudzība; (7) nepārtraukta pilnveide un integrācija plašākā operacionālā riska pārvaldības ietvarā (Ramasubramaniam and Singh 2020; Monev 2021; Aliane and Zakariya 2023; Roy et al. 2022; Mohta et al. 2024).

Literatūrā tiek uzsvērtas arī atšķirīgas pieejas - tehnoloģiski orientēti risinājumi (piemēram, reāllaika risku noteikšana, automatizēta novērtēšana) pretstatā tradicionāliem instrumentiem, piemēram, anketām un klātienes auditiem. Efektīva TPRP prasa abu pieeju kombināciju (Aliane and Zakariya 2023; Monev 2021; Keskin et al. 2021).

TPR veidi

Deviņos pētījumos tika analizēti TPR veidi, kuru tvērums un detalizācijas līmenis atšķīrās. Pamatojoties uz šo pētījumu rezultātiem, tika noteiktas septiņas trešās puses risku kategorijas, kas apkopotas 1.3. tabulā.

1.3. tabula

TPR veidi

Kods	Kategorija	Iekļautie riski	Avots
R1	1. Regulējuma un atbilstības riski	Atbilstības un normatīvo prasību riski, tostarp atbilstība nodokļu regulējumam, sankcijām un citiem tiesiskajiem aspektiem	(Ramasubramaniam and Singh 2020; Roy et al. 2022; Mohta et al. 2024)
	2. Operacionālie riski		
R2.1	2.1.Vispārējie operacionālie riski	Riska faktori, kas saistīti ar trešās puses pārvaldību un pārvaldības ietvaru	(Ramasubramaniam and Singh 2020; Mohta et al. 2024).
R2.2	2.2. Piegādes ķēdes un sadarbības procesu problēmu izraisītie riski	Piegādes ķēdes traucējumi, izolēti procesi, ierobežota pārredzamība, uzsākšanas procesa izaicinājumi un neefektīva sadarbība	(Fortner 2021; Kähkönen et al. 2016).
R2.3	2.3 Koncentrācijas risks un nepārtrauktības plānošana	Pārmērīga atkarība no konkrētām trešajām pusēm vai nepietiekami alternatīvie risinājumi un nepārtrauktības pasākumi	(Jadwani et al. 2024; Abbasi et al. 2023).
R3	3. Finanšu riski	Finanšu riski, piemēram, augstas starpniecības izmaksas un citi izmaksu riski	(Abbasi et al. 2023; Kähkönen et al. 2016; Mohta et al. 2024).
	4. Drošības un privātuma riski		
R4.1	4.1. Piegādātāja un piegādes ķēdes kiberdrošības riski	Piegādātāju un piegādes ķēdes kiberdrošības ievainojamības	(Keskin et al. 2021; Mohta et al. 2024; Jadwani et al. 2024).
R4.2	4.2. Datu privātuma riski	Datu drošības pārkāpumi, datu noplūde un datu suverenitātes jautājumi	16/07/2026 10:13:00.
R5	5. Stratēģiskie riski	Riska faktori, kas saistīti ar atbilstību organizācijas biznesa mērķiem un stratēģijām, tostarp ārpakalpojumu stratēģijām	(Neumannová et al. 2023; Ramasubramaniam and Singh 2020).
	6. Ētiskie un sociālie riski		
R6.1	6.1. Reputācijas riski un interešu konflikts	Korupcijas, kukuļošanas un slepenas vienošanās riski	(Roy et al. 2022).
R6.2	6.2. Korporatīvā sociālā atbildība	Riska faktori, kas saistīti ar cilvēktiesībām un citiem sociālās atbildības aspektiem	(Roy et al. 2022; Kähkönen et al. 2016).
	7. Partneru un piegādes ķēdes riski		
R7.2	7.1. Ar partnera specifiskajiem faktoriem saistītie riski	Ģeogrāfiskā atrašanās vieta, nozare, partnera profils, tuvums amatpersonām, sadarbības pamatojums un līguma sarežģītība	(Roy et al. 2022; Kähkönen et al. 2016).

	7.2. Ceturtās un nākamā līmeņa puses riski	Riska faktori, kas saistīti ar piegādātājiem un apakšuzņēmējiem paplašinātajā piegādes ķēdē	(Ramasubramaniam and Singh 2020; Fortner 2021)

Avots: autores veidots

Noteikto risku daudzveidība apliecina TPR pārvaldības daudzdimensionālo raksturu. Īpaši jāuzsver, ka kiberdrošības un ar datiem saistīto risku biežā iekļaušana norāda uz digitālo apdraudējumu pieaugošo nozīmi, savukārt, ceturtās un nākamā līmeņa puses riski atspoguļo nepieciešamību pārvaldīt risku ietekmi visā paplašinātajā piegādes ķēdē.

1.4. Hipotēzes un pētījuma modelis

Promocijas darbā veiktā teorētiskā analīze ļāva formulēt pētnieciskās hipotēzes turpmākai empīriskai pārbaudei. H1 hipotēze tika izvirzīta pamatojoties uz organizācijas uzticības integratīvo modeli (Mayer et al. 1995). Tās apakšhipotēzes izstrādātas, pamatojoties uz noteikto trešās puses risku kategoriju analīzi:

H1: DU samazina TPR.

H1a: DU samazina regulējuma un atbilstības riskus.

H1b: DU samazina vispārējos operacionālos riskus.

H1c: DU samazina piegādes ķēdes un sadarbības procesu problēmas.

H1d: DU samazina koncentrācijas risku un nepārtrauktības plānošanas riskus.

H1e: DU samazina finanšu riskus.

H1f: DU samazina piegādātāja un piegādes ķēdes kiberdrošības riskus.

H1g: DU samazina datu privātuma riskus.

H1h: DU samazina stratēģiskos riskus.

H1i: DU samazina reputācijas riskus un interešu konflikta riskus.

H1j: DU samazina korporatīvās sociālās atbildības riskus.

H1k: DU samazina ar partnera specifiskajiem faktoriem saistītos riskus.

H1l: DU samazina ceturtās un nākamā līmeņa puses riskus.

Pieņēmums, ka organizācijas spējas DU novērtēšanā un pārvaldībā var pastiprināt DU negatīvo ietekmi uz TPR, izriet no dinamisko spēju teorijas (Teece et al. 1997) un ļāva formulēt šādu hipotēzi:

H2: DU ietekmi uz TPR mazināšanu moderē organizācijas spējas DU novērtēšanā un pārvaldībā.

Vēl viens šī pētījuma pieņēmums izriet no informācijas asimetrijas teorijas (Akerlof 1970). Tā paredz, ka DU novērtēšanas kritēriju un rezultātu caurskatāmība var mazināt informācijas asimetriju attiecībās starp organizācijām un trešajām pusēm. Tas, savukārt, var palielināt DU līmeni un samazināt TPR līmeni. Šis pieņēmums atspoguļots šādās hipotēzēs:

H3: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē DU līmeni.

H4: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā samazina TPR.

H5: DU darbojas kā mediators starp caurskatāmību DU novērtēšanā trešās puses piesaistes procesā un TPR līmeni.

H6: DU ietekmi uz TPR mazināšanu moderē caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā.

Turklāt minētās teorijas ļauj pieņemt, ka atklāta novērtēšanas kritēriju komunikācija trešās puses piesaistes procesā var kļūt par organizācijas rutīnu, kas palīdz noteikt novērtēšanas kritēriju vājās vietas, izmantot jaunu informāciju par piegādātājiem un savlaicīgi pilnveidot kontroles mehānismus. Šāda atkārtota un caurskatāma mijiedarbība pakāpeniski var veidoties par augstāka līmeņa spēju DU novērtēšanā. Tādējādi tiek izvirzīta šāda hipotēze:

H7: Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē organizācijas spējas DU novērtēšanā un pārvaldībā.

Turpmākās hipotēzes izriet no signalizēšanas teorijas (Spence 1973) un pieņēmumā, ka dažādi informatīvie signāli, ar kuriem tiek komunicēta DU, piemēram, ārējās sertifikācijas vai auditu rezultāti, var pozitīvi ietekmēt uztverto DU līmeni, kā arī pastiprināt DU negatīvo ietekmi uz TPR. Atbilstošās hipotēzes ir:

H8: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē DU līmeni.

H9: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā moderē DU ietekmi uz TPR mazināšanu.

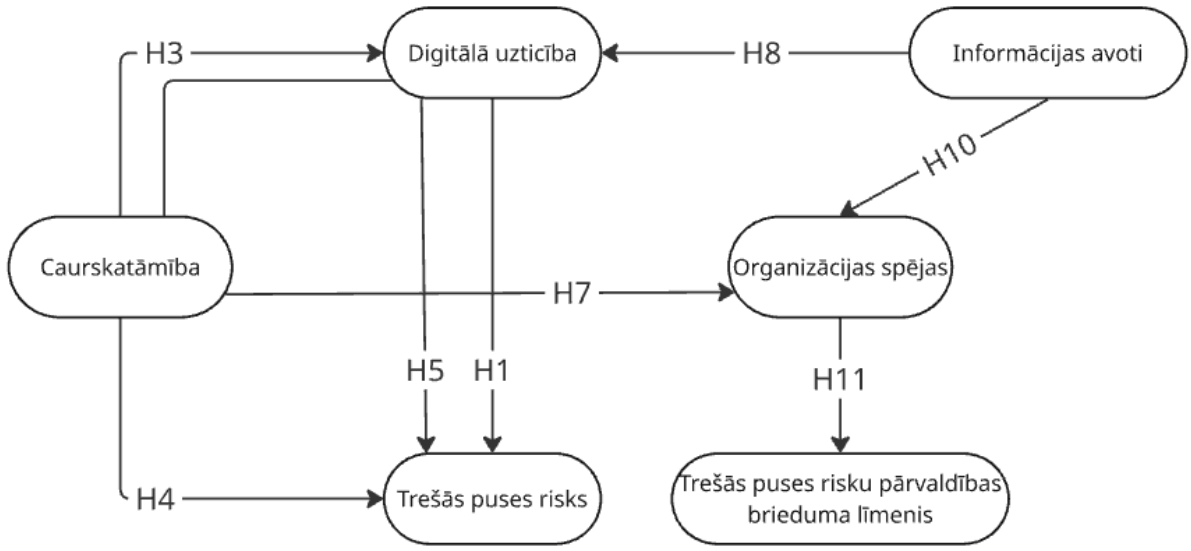
Līdzīgi kā caurskatāmības gadījumā, var pieņemt, ka konsekventa vairāku informācijas avotu izmantošana stiprina organizācijas spēju noteikt riskus, izmantot iespējas un pielāgot novērtēšanas pieejas. Plašāks DU indikatoru loks veicina novērtēšanas procesa pilnveidi un aktualizēšanu atbilstoši jaunajiem apdraudējumiem un praksēm. Tādēļ tiek formulēta šāda hipotēze:

H10: Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē organizācijas spējas DU novērtēšanā.

Noslēgumā šis pētījums izvirza pieņēmumu, ka organizācijas spēja novērtēt DU var pozitīvi ietekmēt kopējo TPRP brieduma līmeni. Saskaņā ar dinamisko spēju teoriju pilnveidota DU novērtēšanas rutīna uzlabo organizācijas spēju savlaicīgi noteikt vājās pazīmes piegādātāju rīcībā, izmantot korektīvus risinājumus un pielāgot līgumus vai kontroles mehānismus, pirms riski materializējas. Līdz ar to, jo attīstītāka ir organizācijas spēja novērtēt DU, jo strukturētāka, proaktīvāka un uz datiem veidota kļūst TPRP, kas atspoguļojas augstākā brieduma līmenī. Tādēļ tiek formulēta šāda hipotēze:

H11: Organizācijas spējas DU novērtēšanā un pārvaldībā pozitīvi ietekmē TPRP brieduma līmeni.

Pamatojoties uz izvirzītajām hipotēzēm, tika izstrādāts pētījuma modelis, kas attēlots 1.3. attēlā.



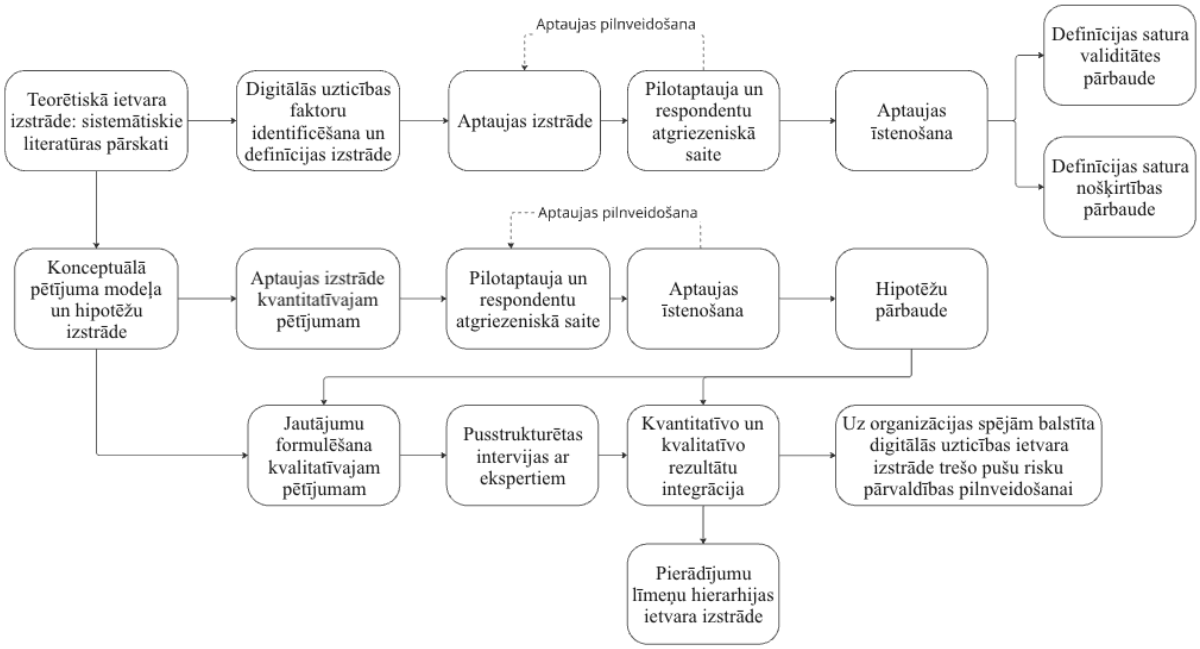
1.3. attēls. Pētījuma modelis

Avots: autores veidots

Apkopojot šī pētījuma teorētisko pamatu, tas izriet no organizācijas uzticības integratīvsā teorijas un signalizēšanas teorijā, kā arī papildina uzticības un risku pārvaldības izpēti digitālajā vidē ar informācijas asimetrijas teoriju un dinamisko spēju teoriju. Analīze veikta B2B līmenī un izvietota TPRP kontekstā. Turklāt šajā pētījumā TPR līmenis tiek aplūkots kā atkarīgais mainīgais - pieeja, kas iepriekšējos pētījumos izmantota tikai ierobežotā apjomā.

1.5. Pētījuma dizains un metodoloģija

Šī promocijas darba pētījuma dizains balstās uz jaukto metožu pieeju, kurā apvienota teorētiskā analīze, kvantitatīva empīriskā analīze un kvalitatīva rezultātu interpretācija. Šāda pieeja nodrošina metodoloģisko triangulāciju un palielina pētījuma rezultātu uzticamību. Pētījuma dizains ir atspoguļots 1.4. attēlā.



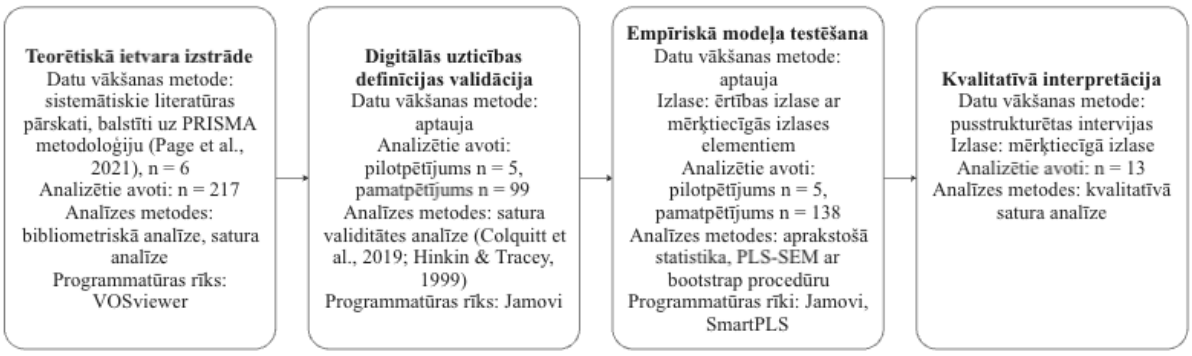
1.4. attēls. Pētījuma dizains

Avots: autores veidots

Pētījums sākas ar teorētiskā ietvara izstrādi, kas balstīta uz sistemātiskiem literatūras pārskatiem, izmantojot PRISMA metodoloģiju (Page et al. 2021). Kopumā tika veikti seši sistemātiski literatūras pārskati, lai analizētu esošo zināšanu kopumu par digitālo uzticību, trešo pušu risku pārvaldību un uzticības un risku pārvaldības savstarpējo saistību digitālajā vidē. Analīzē kopumā tika iekļautas 217 zinātniskās publikācijas.

Analizētajā literatūrā tika iekļautas zinātniskās publikācijas, kas indeksētas Scopus (Elsevier 2025) un Web of Science (Clarivate 2024) datubāzēs. Lai noteiktu pētījumu virzienus, publikāciju attīstības tendences un tematiskās grupas analizētajā literatūrā, tika veikta bibliometriskā analīze, izmantojot programmatūras rīku VOSviewer (VOSviewer 2024). Papildus teorētiskajā daļā tika izmantota satura analīze, lai analizētu digitālās uzticības galvenās raksturiezīmes, trešo pušu risku pārvaldību un tās ietvarus, kā arī atšķirības starp trešo pušu, piegādātāja, piegādes ķēdes dalībnieka un pakalpojumu sniedzēja riskiem un uzticības un risku pārvaldības savstarpējo saistību digitālajā kontekstā.

Pamatojoties uz sistemātisko literatūras pārskatu rezultātiem, tika izstrādāts konceptuālais pētījuma modelis un formulētas pētījuma hipotēzes. Literatūras analīze ļāva arī identificēt digitālās uzticības faktorus un izstrādāt holistisku digitālās uzticības definīciju. Lai pārbaudītu piedāvātās definīcijas uzticamību un skaidrību, tika veikta koncepta validācija, izmantojot satura validācijas metodoloģiju (Colquitt et al. 2019; Hinkin and Tracey 1999). Vispirms tika veikta pilotaptauja (n = 5), lai precizētu anketas jautājumu formulējumus, pēc kuras tika īstenots galvenais satura validācijas pētījums ar 99 respondentiem. Šajā posmā tika aprēķināts definicionālās atbilstības indekss (*htc*), lai novērtētu piedāvātās digitālās uzticības definīcijas atbilstību koncepta saturam, savukārt definicionālās atšķirtspējas indekss (*htd*) tika izmantots definīcijas nošķirtības novērtēšanai attiecībā pret citiem saistītiem konceptiem. Metodoloģiskā ietvara struktūra un galvenie pētījuma analītiskie posmi parādīti 1.5. attēlā.



1.5. attēls. Jaukto metožu metodoloģiskais modelis

Avots: autores veidots

Pētījuma kvantitatīvā daļa balstīta uz Baltijas valstu banku nozares darbinieku aptauju, kurā piedalījās speciālisti, kas tieši iesaistīti trešo pušu risku pārvaldībā. Aptaujas anketa tika izstrādāta, balstoties uz teorētisko ietvaru un literatūras analīzē noteiktajiem digitālās uzticības faktoriem. Lai pārbaudītu anketas jautājumu skaidrību un uzticamību, tika veikta pilotaptauja (n = 5). Respondentu sniegtā atgriezeniskā saite tika izmantota anketas pilnveidei pirms pamataptaujas. Aptaujā tika izmantota piecu punktu Likerta skala, un kopumā tika iegūtas 138 respondentu atbildes. Iegūtā izlase nodrošina 95 % ticamības līmeni ar 8,34 % izlases kļūdas robežu.

Respondentu atlase balstīta uz ērtuma izlasi, to papildinot ar mērķtiecīgas izlases elementiem, lai nodrošinātu, ka aptaujā piedalās respondenti ar pieredzi trešo pušu risku pārvaldībā. Iegūtie dati analizēti, izmantojot aprakstošās statistikas metodes programmatūrā *Jamovi* (jamovi 2024) un PLS-SEM ar bootstrap procedūru programmatūrā *SmartPLS* (Ringle et al. 2025).

PLS-SEM metode ir izvēlēta, jo tā ir piemērota sarežģītu konceptuālo modeļu analīzei, kuros ietverti vairāki koncepti un to savstarpējās attiecības, tostarp moderācijas un mediācijas efekti. Turklāt šī metode izvēlēta arī tādēļ, ka tā bieži izmantota empīriskajos pētījumos, kuros analizēta uzticības un risku pārvaldības savstarpējā saistība digitālajā vidē. Sistemātiskajā literatūras pārskatā, kas veikts šajā promocijas darbā, konstatēts, ka šī metode izmantota 73 % analizēto empīrisko pētījumu.

Lai padziļinātu empīrisko rezultātu interpretāciju un iegūtu plašāku priekšstatu par trešo pušu risku pārvaldības praksi Baltijas valstu finanšu sektorā, pētījumā tika izmantota arī kvalitatīvā pētniecības pieeja. Tās ietvaros tika veiktas daļēji strukturētas ekspertu intervijas ar finanšu iestāžu pārstāvjiem no Igaunijas, Latvijas un Lietuvas.Ekspertu atlase tika veikta, izmantojot mērķtiecīgu izlasi. Intervijās piedalījās 13 eksperti ar profesionālo pieredzi risku pārvaldībā, atbilstības nodrošināšanā, kiberdrošībā un piegādātāju pārvaldībā.

Kvalitatīvās analīzes mērķis ir papildināt un skaidrot aptaujas un modeļa testēšanas rezultātus. Ekspertu interviju analīzei tika izmantota kvalitatīvā satura analīze, lai izvērtētu ekspertu skatījumu uz digitālās uzticības novērtēšanas praksi, organizāciju spēju pārvaldīt digitālo uzticību, kā arī trešo pušu risku pārvaldības turpmāko attīstību finanšu sektorā. Interviju skaits tika noteikts, ievērojot teorētiskās piesātinātības principu, lai nodrošinātu pietiekamu izpētes dziļumu attiecībā uz pētījuma tematu.

Visbeidzot, kvantitatīvo un kvalitatīvo rezultātu integrācija ļāva izstrādāt uz spējām balstītu digitālās uzticības ietvaru trešo pušu risku pārvaldības pilnveidošanai. Turklāt, balstoties uz ekspertu interviju rezultātiem, tika izstrādāts pakāpeniskas pierādījumu hierarhijas ietvars, kas paredzēts, lai palīdzētu organizācijām uzlabot digitālās uzticības novērtējumu uzticamību un kvalitāti, izvērtējot IKT trešo pušu pakalpojumu sniedzējus.

2. nodaļas kopsavilkums: Trešās puses risku pārvaldības novērtējums finanšu sektorā

2.1. Baltijas banku nozares raksturojums

Finanšu sektors ietver vairumtirdzniecības, mazumtirdzniecības, formālās un neformālās institūcijas, kas sniedz finanšu pakalpojumus patērētājiem, uzņēmumiem un citām finanšu iestādēm (Department for International Development 2004). Tajā ietilpst kredītiestādes, maksājumu iestādes, apdrošināšanas sabiedrības, pensiju un ieguldījumu fondi, kā arī finanšu tehnoloģiju (FinTech) uzņēmumi (Spitzer and Sabol 2025; Arner et al. 2015).

Globālā finanšu pakalpojumu tirgus vērtība 2024. gadā tika lēsta aptuveni 33,5 triljonu Amerikas Savienoto Valstu (ASV) dolāru apmērā, ar prognozētu pieaugumu līdz 35,85 triljoniem ASV dolāru 2025. gadā (Benchmark International 2024; Research and Markets, n.d.). 2023. gadā Eiropas Savienības finanšu sektora (NACE Rev. 2 kods "K") neto apgrozījums sasniedza 2,45 triljonus eiro, savukārt Baltijas finanšu sektora neto apgrozījums bija 14 070 miljoni eiro, no kuriem Igaunijā – 4 127 miljoni, Latvijā – 3 155 miljoni un Lietuvā – 6 788 miljoni eiro (Eurostat 2025).

Kopumā Baltijas reģionā NACE koda "K" ietvaros darbojās 6 359 uzņēmumi, no kuriem tikai 7,38 % nodarbināja vismaz 10 darbiniekus un 3,98 % vismaz 20 darbiniekus, kas norāda uz mazo uzņēmumu dominanci (Eurostat 2025). Baltijas banku nozari veido 24 licencētas kredītiestādes un 16 ārvalstu kredītiestāžu filiāles ("Latvijas Banka," n.d.; "Lietuvos Bankas," n.d.; "Eesti Pank," n.d.), no kurām astoņas bankas darbojas visās trijās Baltijas valstīs, bet piecas lielākās iestādes kontrolē aptuveni 90 % tirgus daļas (Buch 2024).

Baltijas finanšu sistēmas ir cieši integrētas ar Ziemeļvalstu reģionu un raksturojas ar augstu digitalizācijas līmeni. Digitālā transformācija veicina finanšu tehnoloģiju inovāciju, pārveido vērtības ķēdes un pakalpojumu sniegšanas modeļus, uzlabo operacionālo efektivitāti un sekmē finanšu iekļaušanu (Mavlutova et al. 2022; Ellex 2025).

2.2. Trešās puses risku pārvaldības izaicinājumi banku nozarē

Digitalizācija paplašina finanšu iestāžu tirgus iespējas, taču vienlaikus rada jaunus apdraudējumus, tostarp kiberuzbrukumus un noziedzīgi iegūtu līdzekļu legalizācijas riskus, tādējādi palielinot TPRP nozīmi (Buch 2024). Baltijas banku nozare darbojas stingri regulētā ES ietvarā, kura mērķis ir nodrošināt stabilitāti un noturību (Korneev et al. 2023).

Centrālais normatīvais akts, kas regulē ar IKT saistītos TPR, ir Digitālās darbības noturības akts (DORA), kas piemērojams no 2025. gada janvāra (European Commission 2022b). DORA nosaka stingras prasības IKT risku pārvaldībai, tostarp TPR novērtēšanai, līgumiskajiem aizsardzības mehānismiem, koncentrācijas riska analīzei, apakšuzņēmēju iesaistes kontrolei, IKT reģistru uzturēšanai, iziešanas stratēģijām un datu aizsardzības pasākumiem. Tas izriet no uz Eiropas Banku iestādes Pamatnostādnēm par ārpakalpojumu līgumiem (European Banking Authority 2019), kas izveidoja pamatu ārpakalpojumu dzīves cikla pārvaldībai un pašlaik tiek pārskatītas, lai tās saskaņotu ar DORA un paplašinātu tvērumu arī uz ar IKT nesaistītiem TPR (European Banking Authority 2025).

Nozares dati apstiprina šī jautājuma nozīmīgumu: 74,6 % finanšu iestāžu TPR ierindo starp būtiskākajiem operacionālajiem riskiem, savukārt 46 % apšauba savu pašreizējo prakšu efektivitāti (Operational Riskdata eXchange Association 2025). Ņemot vērā bankām izvirzītās stingrās regulatīvās prasības (Enria 2023) un banku nozares centrālo lomu Baltijas valstu ekonomikās (Mavlutova et al. 2022), šis pētījums koncentrējas uz Baltijas banku nozari. Turklāt, ņemot vērā TPRP prakses attīstības stadiju un nesen ieviestās prasības IKT TPRP, sagaidāms, ka banku nozare ieņems vadošo lomu šo prakšu ieviešanā, savukārt banku nozares profesionāļiem būs nepieciešamās zināšanas un prasmes šo risku efektīvai pārvaldībai.

2.3. Digitālās uzticības ietekme uz trešās puses riskiem Baltijas bankās

Sākotnēji analīzes vienība tika noteikta organizācijas līmenī, koncentrējoties uz kopējo TPR un DU piegādātājiem. Tomēr validācijas procesā, apspriežoties ar trim Baltijas nefinanšu risku profesionāļiem, tika konstatēts, ka pat organizācijās ar definētu vai integrētu TPRP brieduma līmeni trūkst portfeļa līmeņa skatījuma uz TPR un nav iespējams novērtēt kopējo DU līmeni IKT piegādātājiem. Tādēļ analīzes vienība tika pārcelta uz atsevišķas trešās puses līmeni.

Atbilstoši tam tika pārstrādāta aptauja, pilotēta ar pieciem banku risku pārvaldības profesionāļiem un uzsākta 2025. gada 30. aprīlī. Tā tika izplatīta Baltijas finanšu sektorā, izmantojot nejaušo un sniega bumbas izlases metodi, tostarp tieši uzrunājot aptuveni 250 profesionāļus, izplatot informāciju *LinkedIn* platformā, caur Baltijas finanšu un risku pārvaldības asociācijām, kā arī mērķtiecīgi sazinoties ar licencētu kredītiestāžu un filiāļu darbiniekiem. Kopumā tika nosūtīti vairāk nekā 200 uzaicinājumi saziņai un 80 tiešie ziņojumi.

Uzrunātā mērķauditorija ietvēra risku, atbilstības, IT, audita un drošības jomas profesionāļus, kas atspoguļo TPRP fragmentēto pārvaldības struktūru (Ncontracts 2025). Saņemtā atgriezeniskā saite apstiprināja ierobežotu atbildības un izpratnes līmeni organizācijās, kas saskan ar ORX datiem, kuri liecina, ka TPRP centralizācija joprojām nav pilnībā īstenota (Operational Riskdata eXchange Association 2025). Aptauja bija atvērta līdz 2025. gada 15. jūnijam un tika saņemtas 157 atbildes no banku nozares darbiniekiem. Salīdzinoši pieticīgais atsaucības līmenis atbilst nozares datiem, kas liecina, ka 73 % iestāžu piegādātāja riska pārvaldībai ir atvēlēti divi vai mazāk pilna laika darbinieki (Ncontracts 2025).

Dalība tika ierobežota ar Baltijas valstu finanšu sektora pārstāvjiem. Pēc vienas ģeogrāfiski neatbilstošas atbildes (Zviedrija) izslēgšanas analīzē tika iekļautas 156 atbildes. Papildu datu kvalitātes pārbaudes atklāja identiskas atbildes DU faktoros (n = 10) un TPR kategorijās (n = 8). Šīs atbildes tika izslēgtas, un gala izlasi veido 138 atbildes. Papildus tika veikts Harmana viena faktora tests, lai novērtētu iespējamo kopējās metodes nobīdi, ņemot vērā, ka visi mainīgie tika iegūti, izmantojot pašnovērtējuma aptauju (Podsakoff et al. 2003). Pirmais faktors izskaidroja 26,6 % no kopējās dispersijas, kas ir zem ieteiktā 50 % sliekšņa. Tas norāda, ka kopējās metodes radītā nobīde, visticamāk, būtiski neietekmē pētījuma rezultātus. Tādējādi pētījums tiek veikts ar 95 % ticamības līmeni un 8,34 % kļūdas robežu (Calculator.net, 2025).

Lielākā daļa respondentu bija no Latvijas (n = 59; 42,8 %), kam seko Lietuva (n = 45; 32,6 %) un Igaunija (n = 32; 23,2 %), kā arī divi respondenti ar darbības tvērumu visās trijās Baltijas valstīs (1,4 %). Kopumā tika norādīti 28 amati, kas tika apvienoti piecās grupās: IT (n = 46; 33,3 %), biznesa un komercfunkcijas (n = 40; 29,7 %), risku pārvaldība (n = 23; 16,7 %), atbilstība un drošība (n = 17; 12 %) un operācijas un atbalsts (n = 12; 9 %). Šāds sadalījums norāda uz dažādu iesaistīto pušu pārstāvniecību IKT TPRP.

Attiecībā uz TPRP briedumu (saskaņā ar *Capability Maturity Model Integration Institute* noteikto 1–5 līmeņu skalu), 84,1 % (n = 116) novērtēja savu organizāciju vismaz 3. līmenī (“Definēts”), vidējais brieduma līmenis bija 3,57, mediāna – 4, kas norāda uz tendenci virzīties uz kvantitatīvi pārvaldītām praksēm (CMMI Institute, n.d.). Šie rezultāti apstiprina izlases atbilstību turpmākai IKT TPR analīzei.

Respondentiem tika lūgts izvēlēties vienu IKT trešās puses pakalpojumu sniedzēju, ar kuru viņi ir tieši iesaistīti sadarbībā, un vispirms novērtēt tā DU līmeni, pirms izvērtēt TPR, lai mazinātu kopīgās metodes kļūdas risku (angliski - *common method bias*). Tika izmantota 5 punktu Likerta skala (1 = pilnībā nepiekrītu; 5 = pilnībā piekrītu), ar iespēju izvēlēties “N/A”, ja informācija nebija pieejama. DU tika operacionalizēta deviņās apakškategorijās, kas apvienotas četrās kategorijās: spēja, labvēlība, integritāte un atvērtība. Katra no tām tika mērīta ar diviem apgalvojumiem, pamatojoties uz teorētiskajā ietvaru.

Analīzei tika aprēķinātas vidējās vērtības apakškategoriju, kategoriju un kopējā DU līmenī. Datu normalitātes pārbaudei tika izmantots Šapiro–Vilka tests, bet aprakstošā statistika aprēķināta, izmantojot *Jamovi* programmatūru (jamovi 2024). Rezultāti liecina, ka respondenti kopumā augstu novērtēja izvēlēto IKT trešo pusi kā uzticamu (kopējais vidējais = 4,11), un

līdzīgas vidējās vērtības tika konstatētas spējai (4,09), labvēlībai (4,07), integritātei (4,19) un atvērtībai (4,11). Vidējā standartnovirze bija 0,82, kas norāda uz iekšēju konsekvenci, savukārt Šapiro–Vilka testa rezultāti (W = 0,750–0,945; p < .001) apliecina datu nenormālu sadalījumu. Atsevišķas iztrūkstošās vērtības tika konstatētas galvenokārt atvērtības kategorijā (auditējamība un izsekojamība), tomēr tās būtiski neietekmēja turpmāko analīzi.

Nākamajā aptaujas blokā tika vērtēts organizācijas saskarsmes līmenis ar IKT TPR. Riski tika novērtēti piecu punktu skalā (1 = ļoti zems; 5 = ļoti augsts), neparedzot atbildes iespēju "N/A", jo neatbilstība tika interpretēta kā ļoti zems risks. Pamatojoties uz teorētisko ietvaru, tika operacionalizētas septiņas TPR kategorijas un piecas apakškategorijas (kopā – divpadsmit TPR), kas tika vērtēti atsevišķi, jo tie pārstāv atšķirīgus risku veidus un nav apvienojami.

Kopumā novērtētais TPR līmenis bija vidēji zems (vidējais = 2,19), kas atbilst pieņēmumam, ka finanšu iestādes parasti sadarbojas ar salīdzinoši zema riska IKT pakalpojumu sniedzējiem. Augstākā vidējā vērtība tika konstatēta koncentrācijas un nepārtrauktības plānošanas riskam (R2.3; vidējais = 2,68), bet zemākā – korporatīvās sociālās atbildības riskam (R6.2; vidējais = 1,73).

Šapiro–Vilka testa rezultāti (W = 0,756–0,945; p < .001) arī šajā blokā liecina par nenormālu sadalījumu. Standartnovirzes svārstījās no 0,948 līdz 1,227, atspoguļojot atšķirības starp vērtētajām IKT trešajām pusēm. Tā kā respondenti vērtēja jau esošus pakalpojumu sniedzējus, norādītie riski lielākoties atspoguļo iekšējo risku līmeni pēc preventīvo kontroles mehānismu ieviešanas. Aktuālās TPR prioritātes finanšu sektorā tika padziļināti analizētas ekspertu intervijās.

Turpmākajā aptaujas blokā tika analizēta DU novērtēšanas kritēriju skaidrība un pieejamība IKT trešajām pusēm, kā arī izmantoto informācijas avotu caurskatāmība. Respondenti vērtēja trīs autora izstrādātus apgalvojumus (TRAN1, TRAN2 un TRAN3) piecu punktu Likerta skalā (1 = pilnībā nepiekrītu; 5 = pilnībā piekrītu), lai noskaidrotu, vai trešās puses ir informētas par DU novērtēšanas kritērijiem un vai šāda caurskatāmība veicina atbilstību organizācijas uzticības prasībām, tādējādi atspoguļojot aģentūras teorijas lomu attiecībās starp DU un TPR.

Kopumā respondenti sliecās piekrist, ka DU novērtēšanas process ir caurskatāms (vidējais = 3,71; mediāna = 4,00). Atsevišķu apgalvojumu vidējās vērtības svārstījās no 3,57 līdz 3,93, standartnovirze – no 0,928 līdz 0,949, kas norāda uz salīdzinoši vienmērīgām atbildēm. Šapiro–Vilka tests apstiprināja nenormālu sadalījumu (W = 0,838–0,938; p < .001). Šie rezultāti liecina par kopumā caurskatāmu DU novērtēšanas praksi aptaujātajās organizācijās.

Nākamais jautājumu kopums bija vērsts uz to, lai noteiktu, kuri informācijas avoti visbiežāk tiek izmantoti un uzskatīti par efektīviem IKT trešo pušu DU novērtēšanā, proti, kā IKT trešās puses komunicē savu DU. Četri apgalvojumi (SOU1–SOU4), kas izstrādāti, pamatojoties uz teorētiskajā analīzē noteiktajām DU komunikācijas metodēm, tika vērtēti piecu punktu Likerta skalā (1 = pilnībā nepiekrītu; 5 = pilnībā piekrītu). Papildus respondentiem bija iespēja atklātā jautājumā norādīt citus izmantotos informācijas avotus.

Rezultāti liecina, ka visbiežāk izmantotais informācijas avots DU novērtēšanā ir pakalpojumu sniedzēja risinājuma dokumentācija, tostarp tehniskie un arhitektūras apraksti (vidējais = 4,06), kam seko reputācijas apliecinājumi (vidējais = 3,93). Partneru un klientu vērtējumi un atsauksmes tika izmantoti retāk (vidējais = 3,14), savukārt blokķēdes tehnoloģijas izmantošana kā uzticības indikators bija reta (vidējais = 2,49). Standartnovirzes robežās no 0,983 līdz 1,426 norāda uz atšķirībām novērtēšanas praksē starp organizācijām. Šapiro–Vilka tests apstiprināja nenormālu datu sadalījumu (W = 0,807–0,903; p < .001).

Atvērtā jautājuma atbildēs (n = 23) tika noteikti 39 praksē izmantoti informācijas avoti, kurus autore apkopojusi vārdu mākonī 2.1. attēlā. Tie ietvēra ISO 27001 sertifikātus, auditētus finanšu pārskatus, valsts reģistru datus, kredītbiroju un tiesu lietu informāciju, iekšējo ieinteresēto pušu atsauksmes, iepriekšējo sadarbības pieredzi, iekšējās politikas (piemēram, drošības un datu aizsardzības politiku), darbības nepārtrauktības plānus, pakalpojumu līmeņa

līgumus, datu apstrādes līgumus, iekšēji izstrādātas anketas, drošības skenēšanas un drošības ievainojamību testēšanas rezultātus, publiski pieejamu informāciju, gadījumu analīzes, demonstrācijas sesijas un trešās puses personāla kompetences novērtējumu. Šie rezultāti apliecina, ka organizācijas DU novērtēšanā izmanto plašu un daudzdimensionālu informācijas avotu kopumu.

2.2. attēls. Vārdu mākonis ar DU novērtēšanā izmantotajiem informācijas avotiem

Avots: autores veidots

Noslēdzošais aptaujas bloks tika īstenots organizācijas līmenī, un tā mērķis bija novērtēt, cik plaši organizācijas ievieš DU novērtēšanas un pārvaldības praksi attiecībā uz IKT trešajām pusēm. Apgalvojumi tika izstrādāti, ņemot vērā dinamisko spēju ietvaru: uztveršanā (angliski – *sensing*; SEN1 un SEN2), izmantošanā (*angliski* – seizing; SEI1 un SEI2) un pārveidošanā (angliski – *reconfiguring*; REC1 un REC2), pielāgojot to DU novērtēšanas kontekstam. Tika izmantota piecu punktu skala (1 = vispār netiek īstenots; 5 = pilnībā īstenots).

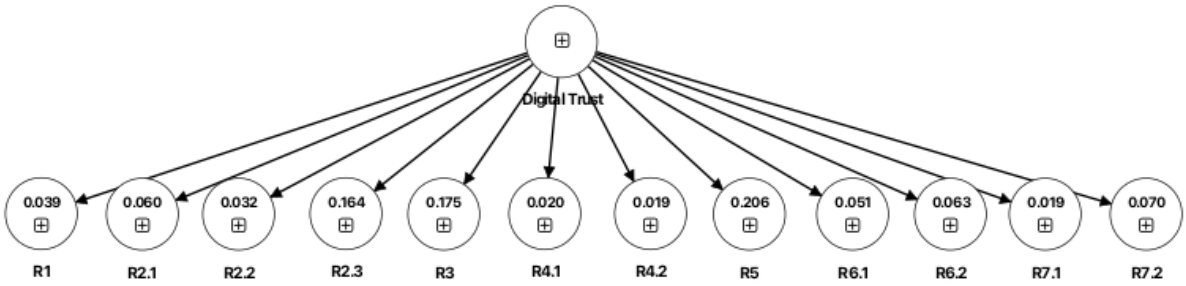
Rezultāti liecina, ka respondentu pārstāvētajās organizācijās izteiktāk attīstītas ir spējas izmantošanā un pārveidošanā (abos gadījumos vidējais = 3,72), savukārt spējas uztveršanā ir nedaudz mazāk attīstītas (vidējais = 3,58). Jo īpaši vairāk īstenota ir ar uzticību saistītās informācijas apkopošana un analīze (SEN1; vidējais = 3,86), DU datu integrēšana risku pārvaldībā un piegādātāju izvēles procesā (SEI1; vidējais = 3,92), kā arī novērtēšanas metožu pastāvīga pilnveide (REC1; vidējais = 3,91). Savukārt, mazāk attīstīta ir nepārtraukta uzticības līmeņa izmaiņu uzraudzība (SEN2; vidējais = 3,30), formālu rīcības protokolu izstrāde (SEI2; vidējais = 3,52) un ieguldījumi tehnoloģijās un kompetencēs (REC2; vidējais = 3,53).

Standartnovirzes (0,785–1,05) norāda uz mērenu rezultātu konsekvenci starp organizācijām. Šapiro–Vilka tests apstiprināja datu nenormālu sadalījumu ($W = 0,838–0,945$; $p < .001$).

Turpmāk statistiskie aprēķini tika veikti, izmantojot *SmartPLS* v.4.1.1.4 (Ringle et al. 2025). Visos modeļos vispirms tika piemērots *PLS-SEM* algoritms ar faktoru svēruma shēmu, pēc tam veikta *bootstrap* procedūra ar ceļu svēruma shēmu (angliski - *path weighting scheme*), izmantojot 5 000 apakšizlases un vienpusēju testu, ņemot vērā, ka hipotēžu virziens bija iepriekš noteikts.

1. modeļa izstrāde un analīze

1. modelis (attēlots 2.2. attēlā) tika izstrādāts, lai pārbaudītu DU ietekmi uz katru TPR veidu atsevišķi.



2.1.attēls. 1. modeļa shēma ar aprēķinātajām R^2 vērtībām
Avots: autores veidots

Digitālā uzticība (shēmā – *Digital Trust*) tika modelēta kā viens reflektīvs konstrukts, kas ietver 18 mērāmus rādītājus, ar kuriem tika mērīti deviņi faktori. *Heterotrait–monotrait* attiecības (HTMT) analīze parādīja nepietiekamu diskriminanto derīgumu, modelējot DU kā četras atsevišķas kategorijas vai patstāvīgus faktorus, jo vairākas *HTMT* vērtības pārsniedza ieteikto 0,85 slieksni (Franke un Sarstedt 2019). Tādēļ DU tika saglabāta kā vienots augstāka līmeņa konstrukts. Savukārt, TPR tika iekļauti kā atsevišķas novērojamas riska kategorijas, lai izvērtētu DU ietekmi uz katru konkrēto riska veidu. Pēc tam visi mainīgie tika pārbaudīti attiecībā uz modeļa atbilstību.

Attiecībā uz **ārējām slodzēm** (angliski – *outer loadings*) septiņi no 18 DU rādītājiem pārsniedza ieteikto 0,708 robežvērtību (Hair et al. 2020), bet pārējie bija zem šī līmeņa. Šāds rezultāts skaidrojams ar DU daudzdimensionālo raksturu, jo to veido deviņas apakškategorijas. Tā kā šo rādītāju izslēgšana nebija nepieciešama, lai uzlabotu iekšējo saskaņotību, uzticamību vai konverģento derīgumu, visi rādītāji tika saglabāti mērījumu modelī (Hair et al. 2021a).

Konstrukta uzticamības (angliski – *construct reliability*) rādītāji apliecināja augstu iekšējo saskaņotību: Kronbaha alfa sasniedza 0,929, bet **saliktā uzticamība** (angliski – *composite reliability*) – 0,937, kas būtiski pārsniedz 0,7 slieksni. **Konverģentais derīgums** (angliski – *convergent validity*), kas mērīts ar vidējo izskaidroto dispersiju (angliski – *average variance extracted*, *AVE*), bija nedaudz zem ieteicamā līmeņa (0,455), tomēr tuvs 0,5, kas norāda uz pieņemamu kopīgās dispersijas apjomu starp rādītājiem.

Diskriminantais derīgums (angliski – *discriminant validity*) starp DU un TPR kategorijām tika apstiprināts ar HTMT attiecību, jo visas vērtības bija zem 0,85, apliecinot skaidru latento mainīgo nošķirumu. **Kolinearības rādītāji** (angliski - *collinearity statistics***)** neuzrādīja multikolinearitātes risku, jo visas vērtības bija būtiski zem 10 (maksimālā – 3,011). Kopumā mērījumu modelis demonstrēja pieņemamu uzticamību un derīgumu turpmākai strukturālajai analīzei.

Pēc tam tika interpretēti iekšējā modeļa analīzes rezultāti, lai novērtētu izskaidrojošo spēju un DU ietekmi uz TPR. Ņemot vērā mazāko statistiski nozīmīgo ceļa koeficientu (β = – 0,138), izlases apjoms nodrošināja pietiekamu statistisko jaudu (0,80), lai noteiktu efektus 10% nozīmīguma līmenī (Hair et al. 2021b).

Saskaņā ar Hair et al. (2011), R^2 interpretācija būtiski atkarīga no pētījuma konteksta. Lai gan vispārpieņemts ir uzskatīt R^2 vērtības 0,75, 0,50 un 0,25 attiecīgi par augstām, vidējām un zemām, dažās sociālo zinātņu nozarēs jau 0,20 R^2 vērtība tiek vērtēta kā augsta. Savukārt Falk un Miller (1992) norāda, ka adekvātai modeļa atbilstībai R^2 vērtībai jābūt vismaz 0,10 vai lielākai.

Interpretējot R^2 vērtības, jāņem vērā, ka TPRP ir attīstības posmā esoša joma, kurai nav noteiktu un vispārpieņemtu R^2 robežvērtību. Tādēļ, pamatojoties uz analīzes rezultātiem, var secināt, ka DU piemīt pietiekama prognozējošā spēja attiecībā uz koncentrācijas risku un nepārtrauktības plānošanas risku (R2.3; 0,164), finanšu riskiem (R3; 0,175) un stratēģiskajiem riskiem (R5; 0,206), nodrošinot pietiekamu statistisko jaudu efekta noteikšanai.

DU ir statistiski nozīmīga negatīva ietekme uz 10 no 12 TPR. Spēcīgākā negatīvā saistība konstatēta ar koncentrācijas risku (R2.3), finanšu riskiem (R3) un stratēģiskajiem riskiem (R5). Neliela līdz mērena negatīva ietekme konstatēta attiecībā uz ceturtās un nākamā līmeņa puses riskiem (R7.2), vispārējiem operacionālajiem riskiem (R2.1), reputācijas un interešu konflikta riskiem (R6.1) un korporatīvās sociālās atbildības riskiem (R6.2). Mazāka ietekme konstatēta uz regulatīvajiem un atbilstības riskiem (R1), piegādes ķēdes un sadarbības procesu riskiem (R2.2) un datu privātuma riskiem (R4.2).

DU nav statistiski nozīmīgas ietekmes (≥ 95% ticamības līmenī) uz piegādātāja un piegādes ķēdes kiberdrošības riskiem (R4.1) un ar partnera specifiskajiem faktoriem saistītajiem riskiem (R7.1), un šī saistība uzskatāma kā indikatīva un turpmākas izpētes vērta. Pēdējo var skaidrot ar stingrām noziedzīgi iegūtu līdzekļu legalizācijas novēršanas (NILLN), sankciju un datu aizsardzības prasībām, kas ierobežo sadarbību ar augsta riska jurisdikcijām, savukārt kiberdrošības risku gadījumā statistiskās nozīmības trūkums prasīja papildu ekspertu diskusiju.

Tādējādi autore secina, ka rezultāti **apstiprina visas apakšhipotēzes** par DU tiešo ietekmi uz TPR veidiem, izņemot **noraidītās hipotēzes H1f un H1k**. Rezultāti apkopoti 2.1. tabulā.

2.1. tabula

1. modeļa strukturālie rezultāti

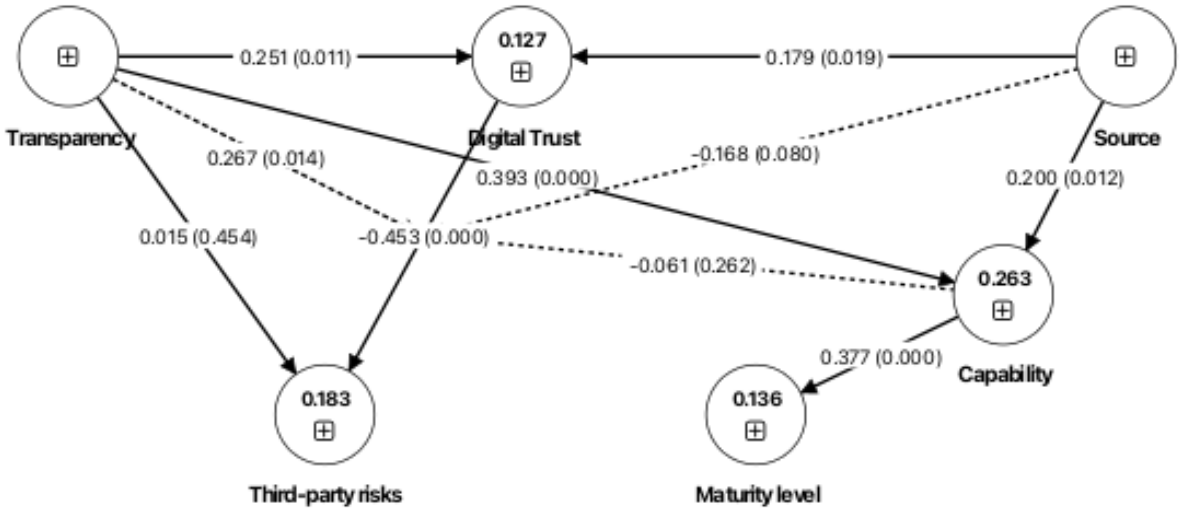
	R^2	Ceļa koeficients	p-vērtība		R^2	Ceļa koeficients	p-vērtība
R1	0.039	-0.199	0.017	R4.2	0.019	-0.138	0.050
R2.1	0.060	-0.246	0.002	R5	0.206	-0.454	0.000
R2.2	0.032	-0.179	0.013	R6.1	0.051	-0.227	0.006
R2.3	0.164	-0.405	0.000	R6.2	0.063	-0.250	0.002
R3	0.175	-0.419	0.000	R7.1	0.019	-0.137	0.068
R4.1	0.020	-0.140	0.057	R7.2	0.070	-0.265	0.002

Avots: autores veidots

2. modeļa izstrāde un analīze: pilnā datu kopa

Turpmāk tika izstrādāts 2. modelis, lai pārbaudītu pārējās hipotēzes. DU (shēmā un rezultātos – **Digital Trust**) tika modelēta tāpat kā 1. modelī - kā viens reflektīvs konstrukts. TPR (shēmā un rezultātos – **Third-party risks**) tika modelēts kā reflektīvs mainīgais, kas ietver visus 12 TPR veidus. Caurskatāmība DU novērtēšanā (shēmā un rezultātos – **Transparency**) tika specificētā kā reflektīvs konstrukts, kas vērtē DU novērtēšanas kritēriju skaidrību un pieejamību. Organizācijas spējas (shēmā un rezultātos – **Capability**) tika modelētas kā viens reflektīvs konstrukts ar sešiem rādītājiem, nevis sadalītas uztveršanā, izmantošanā un pārveidošanā, jo netika konstatēta pietiekama diskriminantā validitāte starp šīm dimensijām.

Informācijas avoti (shēmā un rezultātos – **Source**) tika modelēti kā reflektīvs latentais mainīgais, kas ietver četrus informācijas avotu veidus, savukārt TPRP brieduma līmenis (shēmā un rezultātos – **Maturity level**) tika iekļauts kā atsevišķs novērojamais rādītājs. 2. modeļa shēma attēlota 2.3. attēlā.



2.3. attēls. 2. modeļa shēma ar aprēķinātajām koriģētajām R^2 vērtībām, ceļa koeficientiem un p-vērtībām

Avots: autores veidots

Mērāmo rādītāju **ārējo slodžu** vērtības kopumā bija līdzīgas kā 1. modelī. Lielākā daļa organizācijas spēju un caurskatāmības rādītāju pārsniedza ieteicamo 0,708 robežvērtību. TPR rādītāji daļēji bija virs, daļēji nedaudz zem šīs robežvērtības (zemākā vērtība R3 = 0,597), kas tika pieņemts, ņemot vērā šo risku daudzdimensionalitāti. No informācijas avotu rādītājiem trīs pārsniedza 0,708 robežvērtību, savukārt, SOU4 bija nedaudz zem tās (0,614), kas tika uzskatīts par pieņemamu.

Uzticamības un validitātes rādītāji apstiprināja mērījumu kvalitātes atbilstību. Kronbaha alfa koeficients četriem konstruktēm pārsniedza 0,7, savukārt, informācijas avotu konstrukts bija nedaudz zem šīs robežvērtības (0,663), tomēr, noapaļojot, tas tika uzskatīts par pieņemamu. **Kompozītās uzticamības** rādītāji pārsniedza 0,7, bet *AVE* vērtības dažiem konstruktēm bija tuvu vai nedaudz zem 0,5, tomēr liecināja par pietiekamu **konverģento validitāti**. *HTMT* attiecības apstiprināja **diskriminanto validitāti**, jo visas vērtības bija zem 0,85. **Kollinearitātes** rādītāji bija būtiski zem robežvērtības 10, apliecinot modeļa noturību.

Pēc tam tika izvērtēta modeļa atbilstība. Analīze parādīja pietiekamu prognozējošo spēju visiem latentajiem mainīgajiem, un visaugstākā prognozējošā spēja tika konstatēta organizācijas spēju līmenim (R^2 adj. = 0,263) un TPR līmenim (R^2 adj. = 0,182). Turpmāk tika veikta *bootstrap* procedūra, un rezultāti apkopoti 2.2. tabulā.

2.2. tabula

2. modeļa strukturālie rezultāti

	Digital Trust		**Third-party risks**		**Capability**		**Maturity level**	
R^2 adj.	0.127		0.183		0.263		0.136	
	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība
Digital trust			-0.453	0.000				
Capability							0.377	0.000
Transparency	0.251	0.011	0.015	0.454	0.393	0.000		
Source	0.179	0.019			0.200	0.012		

Avots: autores veidots

Atbilstoši veiktajai analīzei DU ir statistiski nozīmīga negatīva ietekme uz TPR (β = -0,452; p = 0,000), tādējādi **apstiprinot H1**, ka DU samazina TPR.

Caurskatāmība DU novērtēšanā uzrāda nelielu, bet statistiski nozīmīgu pozitīvu ietekmi uz DU (β = 0,251; p = 0,011), **apstiprinot H3**. Tomēr caurskatāmībai nav tiešas statistiski nozīmīgas ietekmes uz TPR (β = 0,014; p = 0,458); tās ietekme ir pilnībā mediēta ar DU (β = -0,114; p = 0,023). Līdz ar to **H4 tiek noraidīta**, savukārt **H5**, kas paredz, ka DU mediē attiecības starp caurskatāmību un TPR, **tiek apstiprināta**.

Vienlaikus caurskatāmība statistiski nozīmīgi moderē DU ietekmi uz TPR (β = 0,267; p = 0,014), **apstiprinot H6**, tomēr augstāks caurskatāmības līmenis var mazināt DU negatīvās ietekmes uz riskiem spēku. 2. modeļa moderācijas un mediācijas analīzes rezultāti apkopoti 2.3. tabulā.

2.3. tabula

2. modeļa mediācijas un moderācijas analīzes rezultāti

Analīze	**Ceļa koef.**	**p-vērtība**
Capability x Digital Trust -> Third-party risks	-0.061	0.262
Source x Digital Trust -> Third-party risks	-0.168	0.080
Transparency x Digital Trust -> Third-party risks	0.267	0.014
Transparency -> Digital Trust -> Third-party risks	-0.114	0.023
Source -> Capability -> Maturity level	0.075	0.043
Transparency -> Capability -> Maturity level	0.148	0.001

Avots: autores veidots

Daudzveidīgu informācijas avotu izmantošana uzrāda nelielu, bet statistiski nozīmīgu pozitīvu ietekmi uz DU (β = 0,179; p = 0,019), **apstiprinot H8**, tomēr tā statistiski nozīmīgi nemoderē DU un TPR attiecības (β = -0,168; p = 0,080), kā rezultātā **H9 tiek noraidīta.**

Gan caurskatāmība (β = 0,393; p = 0,000), gan informācijas avotu izmantošana (β = 0,200; p = 0,012) pozitīvi ietekmē organizācijas spējas DU novērtēšanā, **apstiprinot H7** un **H10**. Savukārt organizācijas spējas uzrāda mērenu pozitīvu ietekmi uz TPRP brieduma līmeni (β = 0,377; p = 0,000), tādējādi **apstiprinot H11**. Caurskatāmības un informācijas avotu izmantošanas ietekme uz brieduma līmeni ir neliela, bet statistiski nozīmīga, un tā ir mediēta ar organizācijas spējām.

Tomēr organizācijas spējas statistiski nozīmīgi nemoderē DU ietekmi uz TPR (β = -0,063; p = 0,258), kā rezultātā **H2 tiek noraidīta**. Iespējamais skaidrojums saistāms ar atšķirīgiem mērījuma līmeņiem: DU un TPR tika vērtēti trešās puses līmenī, savukārt, organizācijas spējas – organizācijas līmenī, turklāt respondentiem varēja nebūt pilnīga pārskatāmība par organizācijas mēroga DU pārvaldības praksēm.

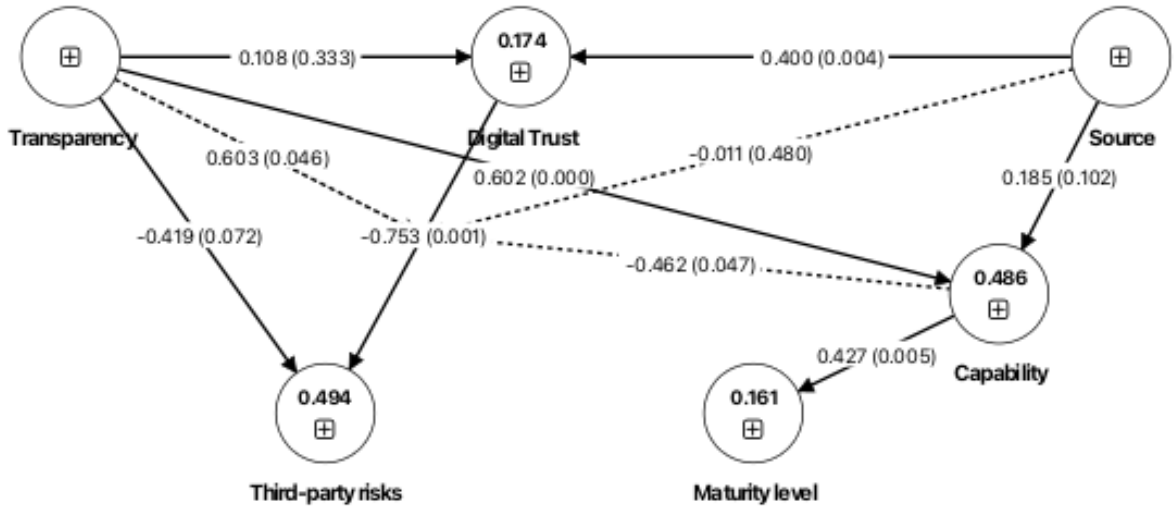
2. modeļa izstrāde un analīze: pārvaldības līmeņa grupa

Papildu tika veikta papildu analīze, izmantojot 2. modeli ar atlasītu respondentu apakškopu, kuri bija iesaistīti organizācijas līmeņa DU novērtēšanā un uzraudzībā (risku vadītāji un atbilstības/drošības funkciju pārstāvji; n = 40). Šī apakškopa turpmāk tiek apzīmēta kā **pārvaldības līmeņa grupa**, lai pārbaudītu iepriekš formulēto pieņēmumu.

Mērāmo rādītāju **ārējo slodžu** vērtības bija salīdzināmas ar pilnās datu kopas rezultātiem un saglabājās pieņemamās robežās, arī gadījumos, kad tās bija zem 0,7, ņemot vērā organizācijas spēju, informācijas avotu, DU un TPR daudzdimensionalitāti. **Uzticamības un validitātes** rezultāti kopumā bija līdzīgi pilnajai izlasei. Vienīgais konstrukts, kura uzticamības rādītāji bija zem ieteicamajām robežvērtībām, bija informācijas avoti (Kronbaha alfa = 0,642; kompozītā uzticamība = 0,637). ***AVE*** **vērtības** konstruktiem "informācijas avoti" (0,491) un "TPR" (0,470) bija nedaudz zem 0,5, tomēr, noapaļojot, tās tika uzskatītas par pieņemamām.

Diskriminantā validitāte (*HTMT*) apstiprināja visu konstruktus konceptuālo nošķirtību (vērtības zem 0,85). **Kollinearitāte** nebija problemātiska, jo visi VIF rādītāji bija

zem 10, lai gan relatīvi augstākas vērtības tika konstatētas RC1 (8,012), TR1 (7,014) un AU (6,963).



2.4. attēls. 2. modeļa shēma (pārvaldības līmeņa grupa) ar aprēķinātajām koriģētajām R^2 vērtībām, ceļa koeficientiem un p-vērtībām

Avots: autores veidots

2. modelis, izmantojot pārvaldības līmeņa grupas datus (2.4. attēls), uzrāda būtiski augstāku un spēcīgu prognozējošo spēju attiecībā uz DU negatīvo ietekmi uz TPR līmeni (R^2 adj. = 0,494 salīdzinājumā ar R^2 adj. = 0,183 pilnajā datu kopā), kā arī attiecībā uz informācijas avotu un DU novērtēšanas caurskatāmības ietekmi uz organizācijas spējām (R^2 adj. = 0,486 salīdzinājumā ar R^2 adj. = 0,263 pilnajā datu kopā). 2. modeļa strukturālie rezultāti, izmantojot pārvaldības līmeņa grupas datus, apkopoti 2.4. tabulā.

2.4.tabula

2. modeļa strukturālie rezultāti (pārvaldības līmeņa grupa)

	Digital Trust		**Third-party risks**		**Capability**		**Maturity level**	
R^2 adj.	0.174		0.494		0.486		0.161	
	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība	Ceļa koef.	p-vērtība
Digital trust			-0.753	0.001				
Capability							0.427	0.005
Transparency	0.108	0.333	-0.419	0.072	0.602	0.000		
Source	0.400	0.004			0.185	0.102		

Avots: autores veidots

Veiktā analīze pārvaldības līmeņa grupas datu kopai apstiprināja šādus rezultātus, kas tika iegūti arī, testējot pilno datu kopu:

- **H1** tika pārliecinoši **apstiprināta** - DU samazina TPR ar vēl augstāku prognozējošo spēju ($\beta = –0,753$; $p = 0,001$), tādējādi nostiprinot secinājumu, ka negatīvā saistība starp uzticību un uztverto risku, kā to aprakstījuši Mayer et al. (1995), darbojas arī digitālajā B2B kontekstā, iesaistot IKT pakalpojumu sniedzējus.

- **H4** atkārtoti tika **noraidīta** (β = –0,419; p = 0,072), apstiprinot, ka caurskatāmība DU novērtēšanā trešās puses piesaistes procesā tieši nesamazina TPR, kuri, šķiet, saglabājas neatkarīgi no caurskatāmības līmeņa.
- **H6** tika **apstiprināta** ar spēcīgāku moderācijas efektu (β = 0,603; p = 0,046), norādot, ka caurskatāmība vājina DU negatīvo ietekmi uz TPR. Šis secinājums ir pretrunā ar informācijas asimetrijas teoriju, bet atbalsta signalizēšanas teoriju, liecinot, ka, izprotot novērtēšanas kritērijus, IKT trešās puses var stratēģiski pārvaldīt signālus, lai radītu augstāku uzticamības priekšstatu - šo skatījumu apstiprināja arī ekspertu intervijas.
- **H7** tika **apstiprināta** ar spēcīgu pozitīvu ietekmi (β = 0,602; p = 0,000), apliecinot, ka caurskatāmība stiprina organizācijas spējas DU novērtēšanā un pārvaldībā.
- **H8** tika **apstiprināta** (β = 0,400; p = 0,004), parādot, ka daudzveidīgu informācijas avotu plaša izmantošana pozitīvi ietekmē DU līmeni, saskanot ar signalizēšanas teoriju.
- **H9** tika **noraidīta** (β = –0,011; p = 0,480), jo informācijas avoti nemoderēja attiecības starp DU un TPR.
- **H11** tika **apstiprināta** (β = 0,427; p = 0,005), norādot, ka organizācijas spējas DU novērtēšanā un pārvaldībā pozitīvi ietekmē TPRP brieduma līmeni, tādējādi atbalstot dinamisko spēju teoriju šajā kontekstā.

2. modeļa mediācijas un moderācijas analīzes rezultāti pārvaldības līmeņa grupā apkopoti 2.5. tabulā.

2.5. tabula

2. modeļa mediācijas un moderācijas analīzes rezultāti (pārvaldības līmeņa grupa)

Analīze	**Ceļa koef.**	**p-vērtība**
Capability x Digital Trust -> Third-party risks	-0.462	0.047
Source x Digital Trust -> Third-party risks	-0.011	0.480
Transparency x Digital Trust -> Third-party risks	0.603	0.046
Transparency -> Digital Trust -> Third-party risks	-0.081	0.341
Source -> Capability -> Maturity level	0.079	0.148
Transparency -> Capability -> Maturity level	0.257	0.010

Avots: autores veidots

Pārvaldības līmeņa apakšgrupā vairāki rezultāti atšķīrās no pilnās datu kopas. Hipotēze **H2** tika **apstiprināta**, konstatējot statistiski nozīmīgu un tuvu spēcīgam negatīvu moderācijas efektu (β = –0,462; p = 0,047). Tas norāda, ka respondentu vidū, kuriem ir pārskatāmība par organizācijas līmeņa pārvaldības praksēm, spēcīgākas organizācijas spējas DU novērtēšanā pastiprina DU mazinošo ietekmi uz uztvertajiem TPR.

Savukārt hipotēzes, kas saistītas ar caurskatāmību trešās puses piesaistes procesā, **netika apstiprinātas**. **H3** (β = 0,108; p = 0,333) un **H5** (β = –0,081; p = 0,341) nebija statistiski nozīmīgas, kas liecina, ka pilnajā izlasē novērotie caurskatāmības efekti pārvaldības līmeņa respondentiem netika atkārtoti konstatēti. Iespējamais skaidrojums ir saistīts ar to, ka pārvaldības līmeņa speciālisti parasti ir iesaistīti DU novērtēšanas procesu izstrādē un uzraudzībā, nevis konkrētu trešo pušu attiecību operatīvā vadībā. Līdz ar to caurskatāmība piesaistes procesā viņu skatījumā var būt mazāk tieši saistīta ar uztverto uzticību un risku.

Visbeidzot, arī **H10** tika **noraidīta** (β = 0,185; p = 0,102). Daudzveidīgu informācijas avotu izmantošana šajā apakšgrupā statistiski nozīmīgi neietekmēja organizācijas spējas DU novērtēšanā un pārvaldībā. No dinamisko spēju teorijas perspektīvas tas var atspoguļot atšķirību starp informācijas resursu pieejamību un institucionalizētu spēju tos integrēt un pārveidot. Atšķirības starp abām izlasēm tika padziļināti analizētas ekspertu intervijās. Pilns hipotēžu testēšanas rezultātu kopsavilkums sniegts 2.6. tabulā.

2.6. tabula

Hipotēžu testēšanas rezultāti

Kods	Hipotēze	Modelis	Izlase	Efekta veids	Rezultāts
H1	DU samazina TPR	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Apstiprināta
H1a	DU samazina regulējuma un atbilstības riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1b	DU samazina vispārējos operacionālos riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1c	DU samazina piegādes ķēdes un sadarbības procesu problēmas.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1d	DU samazina koncentrācijas risku un nepārtrauktības plānošanas riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1e	DU samazina finanšu riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1f	DU samazina piegādātāja un piegādes ķēdes kiberdrošības riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Noraidīta
H1g	DU samazina datu privātuma riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1h	DU samazina stratēģiskos riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1i	DU samazina reputācijas riskus un interešu konflikta riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1j	DU samazina korporatīvās sociālās atbildības riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H1k	DU samazina ar partnera specifiskajiem faktoriem saistītos riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Noraidīta
H1l	DU samazina ceturtās un nākamā līmeņa puses riskus.	1. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
H2	DU ietekmi uz TPR mazināšanu moderē organizācijas spējas DU novērtēšanā un pārvaldībā.	2. modelis	Pilnā izlase	Moderācija	Noraidīta
			Pārvaldības līmeņa grupa	Moderācija	Apstiprināta
H3	Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē DU līmeni.	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Noraidīta
H4	Augstāks caurskatāmības līmenis DU novērtēšanā	2. modelis	Pilnā izlase	Tiešā ietekme	Noraidīta

	trešās puses piesaistes procesā samazina TPR.		Pārvaldības līmeņa grupa	Tiešā ietekme	Noraidīta
H5	DU darbojas kā mediators starp caurskatāmību DU novērtēšanā trešās puses piesaistes procesā un TPR līmeni.	2. modelis	Pilnā izlase	Mediācija	Apstiprināta
			Pārvaldības līmeņa grupa	Mediācija	Noraidīta
H6	DU ietekmi uz TPR mazināšanu moderē caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā.	2. modelis	Pilnā izlase	Moderācija	Apstiprināta
			Pārvaldības līmeņa grupa	Moderācija	Apstiprināta
H7	Augstāks caurskatāmības līmenis DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē organizācijas spējas DU novērtēšanā un pārvaldībā.	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Apstiprināta
H8	Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē DU līmeni.	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Apstiprināta
H9	Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā moderē DU ietekmi uz TPR mazināšanu.	2. modelis	Pilnā izlase	Moderācija	Noraidīta
			Pārvaldības līmeņa grupa	Moderācija	Noraidīta
H10	Daudzveidīgu informācijas avotu izmantošana DU novērtēšanā pozitīvi ietekmē organizācijas spējas DU novērtēšanā.	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Noraidīta
H11	Organizācijas spējas DU uzticības novērtēšanā un pārvaldībā pozitīvi ietekmē TPRP brieduma līmeni.	2. modelis	Pilnā izlase	Tiešā ietekme	Apstiprināta
			Pārvaldības līmeņa grupa	Tiešā ietekme	Apstiprināta

Avots: autores veidots

Apkopojot iegūtos rezultātus, hipotēžu pārbaudes rezultāti apstiprina, ka digitālā uzticība samazina trešo pušu riskus, lai gan šīs ietekmes raksturs atšķiras atkarībā no risku veidiem un respondentu grupām. Rezultāti arī apliecina, ka organizācijas spējas DU uzticības novērtēšanā un pārvaldībā ieņem būtisku lomu digitālās uzticības novērtēšanas sasaistē ar augstāku trešo pušu risku pārvaldības brieduma līmeni. Vienlaikus atšķirīgie rezultāti attiecībā uz caurskatāmību un informācijas avotiem norāda, ka DU nav atkarīga tikai no informācijas pieejamības, bet arī no organizācijas spējas šo informāciju interpretēt un integrēt risku pārvaldības praksēs. Tādēļ novērotās atšķirības starp pilno izlasi un pārvaldības līmeņa grupu tika tālāk analizētas ekspertu intervijās.

3. nodaļas kopsavilkums: Kvalitatīvie ieskati par digitālo uzticību un trešās puses riskiem: secinājumi un rekomendācijas

Pēc kvantitatīvās analīzes un hipotēžu testēšanas pētījums tika turpināts ar kvalitatīvo posmu, kura ietvaros tika veiktas daļēji strukturētas intervijas ar nozares ekspertiem. Šī posma mērķis bija apspriest sākotnējos rezultātus, iegūt papildu ieskatus uz spēju attīstību balstīta DU ietvara izstrādei TPRP pilnveidošanai, kā arī analizēt TPRP turpmākās attīstības tendences Baltijas banku nozarē.

Intervijās piedalījās eksperti, kuri tieši iesaistīti IKT trešo pušu attiecību pārvaldībā un risku vadībā Latvijā, Lietuvā un Igaunijā. Tika pārstāvētas dažādas ieinteresēto pušu perspektīvas, tostarp IT riski, nefinanšu riski, informācijas drošība, atbilstība, trešo pušu attiecību pārvaldība, iepirkumi un juridiskās funkcijas. Lai gan daļa Baltijas banku ietilpst Ziemeļvalstu finanšu grupās, neviens no ekspertiem nenorādīja, ka IKT TPRP būtu pilnībā deleģēta mātesbankām. Teorētiskā piesātinātība tika sasniegta Baltijas ekspertu grupas ietvaros.

Izlase apzināti tika ierobežota ar profesionāļiem, kuri ikdienā ir atbildīgi par IKT TPR novērtēšanu un pārvaldību. Uzraudzības iestāžu un konsultāciju uzņēmumu pārstāvji netika iekļauti, jo viņi šos riskus vērtē no ārēja skatpunkta, nevis tieši iesaistās to operatīvā pārvaldībā.

Intervijas tika veiktas attālināti, izmantojot *Microsoft Teams* platformu, laika posmā no 2025. gada 18. jūlija līdz 1. augustam. Ekspertu saraksts, pārstāvētās valstis un amati ir apkopoti 3.1. tabulā.

3.1. tabula

Intervijās piedalījušos ekspertu saraksts

	Kods	**Valsts**	**Amats**
Eksperts 1	E1	Latvija	Trešo pušu attiecību pārvaldnieks
Eksperts 2	E2	Lietuva	IT risku vadītājs
Eksperts 3	E3	Lietuva	Nefinanšu risku vadītājs
Eksperts 4	E4	Latvija	IT risku vadītājs
Eksperts 5	E5	Latvija	Informācijas drošības vadītājs
Eksperts 6	E6	Igaunija	Trešās puses risku vadītājs
Eksperts 7	E7	Lietuva	Trešo pušu attiecību pārvaldnieks
Eksperts 8	E8	Latvija	Atbilstības vadītājs
Eksperts 9	E9	Igaunija	Informācijas drošības vadītājs
Eksperts 10	E10	Lietuva	Informācijas drošības vadītājs
Eksperts 11	E11	Igaunija	IT risku vadītājs
Eksperts 12	E12	Latvija	Jurists
Eksperts 13	E13	Igaunija	Iepirkumu vadītājs

Avots: autores veidots

Dalība bija brīvprātīga un anonīma; tika saņemta informēta mutiska piekrišana, lai izvairītos no personas datu uzglabāšanas. Interviju ieraksti tika atšifrēti, manuāli rediģēti, anonimizēti un pārskatīti. Pirms katras intervijas tika sniegta īsa ievadprezentācija par pētījuma dizainu, modeli un pētnieciskajiem jautājumiem. Pētījumā izlasē tika iekļauti 13 eksperti no dažādām Baltijas valstīm un banku institūciju funkcijām.

3.1. Trešās puses risku kategoriju kvalitatīvās analīzes atziņas un hipotēžu pārbaude

Eksperti visbiežāk kā nozīmīgākos IKT TPR noteica piegādātāja un piegādes ķēdes kiberdrošības riskus (R4.1) un regulatīvos un atbilstības riskus (R1), īpaši DORA regulējuma

kontekstā. Tiem sekoja datu privātuma riski (R4.2) un ceturtās un nākamā līmeņa puses riski (R7.2).

Lai gan attiecībā uz drošības un privātuma riskiem aptaujas un ekspertu viedokļi sakrita, regulatīvie riski un ceturtās/nākamā līmeņa puses riski aptaujas rezultātos netika novērtēti kā visaugstākie. Šo atšķirību var skaidrot ar aptaujas metodoloģiju - respondenti vērtēja jau esošos IKT pakalpojumu sniedzējus, attiecībā uz kuriem preventīvie pasākumi jau ir ieviesti, tādējādi atspoguļojot drīzāk atlikušos, nevis sākotnējos riskus.

Eksperti vienprātīgi norādīja, ka koncentrācijas un nepārtrauktības nodrošināšanas riski (R2.3) var būt augstākie pēc to sākotnēja līmeņa. Galvenie iemesli ir Baltijas IKT tirgus monopolizācija (piemēram, telekomunikāciju jomā), priekšroka lieliem un nostiprinātiem piegādātājiem, kā arī regulatīvais spiediens, tostarp DORA prasības, kas netieši veicina piegādātāju konsolidāciju.

Zemais korporatīvās sociālās atbildības riska (R6.2) novērtējums tika skaidrots ar tā uztverto mazāko aktualitāti ES bāzētiem IKT pakalpojumu sniedzējiem, ierobežotu sankciju piemērošanas praksi, kā arī iespējamu šo risku nepietiekamu pārbaudi vai nenovērtēšanu.

Pamatojoties uz ekspertu viedokļiem, organizācijām savās TPRP programmās būtu jāprioritizē:

1. Drošības un privātuma riski (R4.1 un R4.2),
2. Piegādes ķēdes pakļautība ceturtās un nākamā līmeņa puses atkarībām (R7.2),
3. Regulatīvās un atbilstības prasības, īpaši DORA kontekstā (R1).

Savukārt, aptaujas rezultāti norāda uz relatīvi augstākiem sākotnējiem risku līmeņiem šādās kategorijās, kurām būtu jānodrošina nepārtraukta uzraudzība visā trešās puses pārvaldības ciklā:

1. Koncentrācijas un nepārtrauktības plānošanas riski (R2.3; vidējais = 2,68),
2. Piegādes ķēdes un procesu riski (R2.2; vidējais = 2,51),
3. Stratēģiskie riski (R5; vidējais = 2,33),
4. Piegādātāja un piegādes ķēdes kiberdrošības riski (R4.1; vidējais = 2,32) un datu privātuma riski (R4.2; vidējais = 2,31).

Minētais apliecina, ka līdzsvarotai TPR prioritāšu noteikšanai nepieciešams apvienot gan kvantitatīvās analīzes rezultātus, gan ekspertu kvalitatīvos vērtējumus.

Hipotēžu testēšanas rezultātu apspriešana ar ekspertiem

Eksperti kopumā piekrita tam, ka netika konstatēta statistiski nozīmīga saistība starp DU un piegādātāja un piegādes ķēdes kiberdrošības riskiem (**H1f**). Galvenais skaidrojums bija, ka kiberdraudi ir ārēji determinēti un stohastiski ("nevis vai, bet kad"), un pat nobrieduši vai augsti uzticami piegādātāji saglabā ievainojamību. DU bieži tiek vērtēta pirms līguma noslēgšanas (pakalpojuma kvalitāte, pārvaldība, nepārtrauktība), savukārt, kiberdrošības ekspozīcija ir atkarīga no dinamiski mainīgiem ārējiem draudiem. Eksperti arī norādīja uz iespējamu uztveres nobīdi anketā minētos uzticības novērtējumos – augsts uzticības vērtējums ne vienmēr atspoguļo faktisko kiberrisku līmeni.

Attiecībā uz **H2** (DU ietekmes uz TPR moderēšana ar organizācijas spējām DU novērtēšanā un pārvaldībā) eksperti piekrita, ka šādām spējām teorētiski būtu jāpastiprina DU riska mazinošā ietekme. Atšķirības starp pilno izlasi un pārvaldības līmeņa grupu tika skaidrotas ar lomu redzamību: otrās līnijas funkcijas (risku pārvaldība, atbilstība, juridiskā funkcija) pārredz visu dzīves ciklu un pārvaldības mehānismus kopumā, savukārt pirmās līnijas pārstāvji redz tikai atsevišķus procesa posmus. Daļa ekspertu uzsvēra arī "teorijas un prakses plaisu", proti, pārvaldības līmeņa darbinieki pieņem, ka ietvari darbojas atbilstoši izstrādātajam modelim, kamēr operatīvie darbinieki reaģē uz faktisko izpildi praksē.

Saistībā ar **H3** (caurskatāmības pozitīvā ietekme uz DU) eksperti uzskatīja par ticamiem abus kvantitatīvās analīzes rezultātus. Caurskatāmība var palielināt uztverto uzticību operatīvā līmeņa darbiniekiem, savukārt pārvaldības līmeņa pārstāvji vairāk paļaujas uz verifikāciju, nevis procesa atklātību. Vienlaikus tika pausts brīdinājums, ka pārmērīga caurskatāmība var

ļaut piegādātājiem "pielāgoties" novērtēšanas kritērijiem un mākslīgi paaugstināt uztverto uzticamību.

H5 (DU mediējošā loma starp caurskatāmību un TPR) noraidījums lielākoties tika atbalstīts. Eksperti norādīja, ka caurskatāmība var palielināt uztverto uzticību, taču ne obligāti samazina faktisko riska ekspozīciju, jo piegādātāji var optimizēt dokumentāciju, lai "izturētu pārbaudi". Turklāt riska vērtējuma pamatā joprojām ir pierādījumi, un papildu informācijas atklāšana dažkārt pat var paaugstināt notiekto risku līmeni.

Attiecībā uz **H10** (informācijas avotu izmantošanas ietekme uz organizācijas spējām DU novērtēšanā) pārvaldības līmeņa eksperti uzsvēra, ka izšķiroša nozīme ir nevis informācijas avotu daudzumam, bet to kvalitātei un efektīvai izmantošanai. Pēc noteikta bāzes līmeņa sasniegšanas papildu avoti sniedz ierobežotu pievienoto vērtību. Daži eksperti deva priekšroku vienam uzticamam "zelta avotam" salīdzinājumā ar vairākiem fragmentētiem informācijas avotiem.

Visbeidzot, **H9** (informācijas avotu moderējošā ietekme uz DU un TPR attiecībām) noraidījumu eksperti atbalstīja. Viņu ieskatā papildu informācijas avoti var precizēt uzticības novērtējumu, taču nemaina strukturālos riskus. Riska samazināšanai nepieciešami uzlaboti kontroles mehānismi vai konkrēti riska mazināšanas pasākumi, nevis tikai plašāka informācijas pieejamība.

Teorētiskie secinājumi

Hipotēžu testēšanas rezultāti kopā ar ekspertu intervijām sniedz pamatojumu šajā promocijas darbā izmantoto teorētisko ietvaru piemērojamībai, kā arī izgaismo to ierobežojumus.

Lielākā daļa rezultātu attiecībā uz H1 un tās apakšhipotēzēm apstiprina Integrēto organizatoriskās uzticības modeli (Mayer et al., 1995): augstāks DU līmenis ir saistīts ar zemāku TPR, īpaši tajās risku kategorijās, kur pakalpojumu sniedzēja rīcība, kontroles mehānismi un pārvaldība tieši ietekmē riska iznākumu (piemēram, regulatīvie, operacionālie un piegādes ķēdes riski). Vienlaikus prognozēšanas spēja ir ierobežota attiecībā uz riskiem, ko galvenokārt nosaka ārēji vai strukturāli faktori (piemēram, pakļautība kiberdraudiem, ģeopolitiskie riski). Tas apliecina, ka uzticība kā apzināta riska uzņemšanās attiecībās ne vienmēr nozīmē izmērāmu riska samazinājumu.

H2 guva daļēju apstiprinājumu attiecībā uz organizācijas spēju (Teece et al., 1997) moderējošo lomu. Organizācijas spējas DU novērtēšanā un pārvaldībā moderē DU un TPR attiecības tikai pārvaldības līmeņa grupā. Ekspertu komentāri norādīja uz lomu redzamības faktoru – otrās līnijas funkcijas ir labāk pozicionētas, lai novērtētu spēju ietekmi uz riska mazināšanu. H7 tika apstiprināta abās izlasēs, apliecinot, ka strukturētos novērtēšanas procesos iestrādāta caurskatāmība stiprina organizācijas spējas.

H10 tika apstiprināta pilnajā izlasē, bet noraidīta pārvaldības līmeņa grupā, kas liecina, ka spējas DU novērtēšanā un pārvaldībā nav atkarīgas no informācijas avotu daudzuma, bet gan no spējas tos kvalitatīvi izvērtēt un savstarpēji salāgot. H11 tika apstiprināta, apliecinot, ka attīstītas DU novērtēšanas prakses veicina TPRP briedumu.

Rezultāti attiecībā uz H3, H4, H5 un H6 sniedz padziļinātu ieskatu organizācijas atklātības lomā potenciālo IKT pakalpojumu sniedzēju piesaistes procesā kā informācijas asimetrijas mazināšanas mehānismā (Akerlof, 1970). Caurskatāmība tieši nesamazina TPR (H4 noraidīta), un tās mediējošā ietekme (H5) nav vienāda abās izlasēs. Apstiprinātais moderācijas efekts (H6) norāda, ka atklātība var pat vājināt DU riska mazināšanas efektu, jo piegādātāji pielāgo savu informācijas sniegumu noteiktajiem kritērijiem, ne vienmēr uzlabojot faktiskās spējas. Tas izaicina informācijas asimetrijas teorijas pieņēmumus un vairāk saskan ar signālu teoriju (Spence, 1973).

Visbeidzot, H8 apstiprina, ka vairāku informācijas avotu izmantošana palielina uztverto DU līmeni, tomēr H9 tika noraidīta abās datu kopās – papildu informācijas avoti paši par sevi nesamazina TPR. Eksperti skaidroja, ka plašāka informācija var vienlaikus gan stiprināt

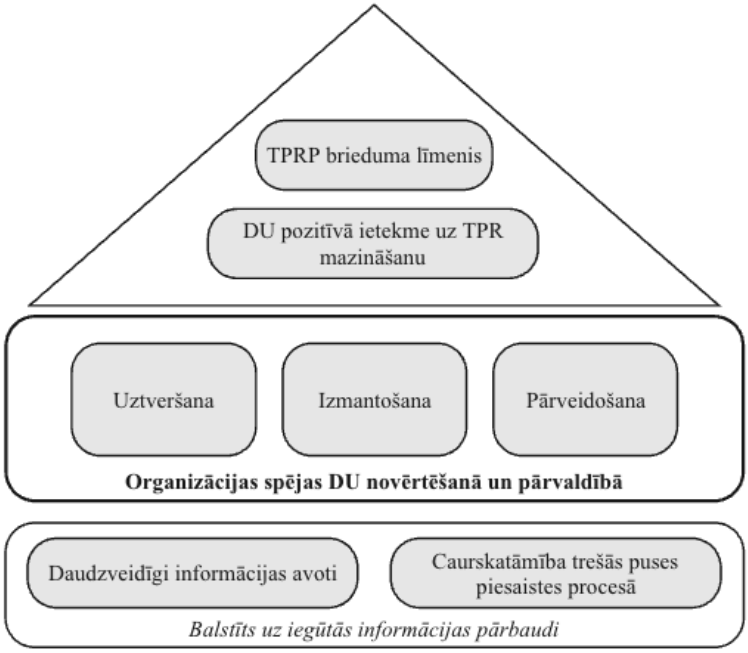
uzticību, gan atklāt jaunus problemātiskus aspektus, tādējādi nemainot faktisko riska pakļautības līmeni.

3.2. Spējās pamatots digitālās uzticības ietvars pilnveidotai trešās puses risku pārvaldībai

Eksperti vērtēja pašreizējo organizāciju spēju līmeni DU novērtēšanā un pārvaldībā kā sākotnēju - lielākā daļa intervēto to novietoja 1. vai 2. līmenī piecu līmeņu skalā. Augstāks brieduma novērtējums (3.–4. līmenis) biežāk tika sniegts no informācijas drošības jomas pārstāvju puses, kuriem parasti ir strukturētākas pieejas trešo pušu uzticamības izvērtēšanai.

Statistiskā analīze apstiprināja, ka spēcīgākas organizācijas spējas DU novērtēšanā būtiski pastiprina DU risku mazinošo ietekmi un palielina DU novērtējumu ticamību plašākā TPRP ietvarā. Turklāt augstāks DU spēju līmenis ir tieši saistīts ar augstāku TPRP brieduma pakāpi, veicinot efektīvāku nefinanšu risku pārvaldības pārvaldību.

Lai atbalstītu organizācijas DU novērtēšanas un pārvaldības brieduma pilnveidē, kā arī stiprinātu DU efektivitāti TPR mazināšanā, pētījumā ir izstrādāts "Uz spējām balstīts DU ietvars pilnveidotai TPRP", kas attēlots 3.1. attēlā.



3.1. attēls. Uz spējām balstīts DU ietvars pilnveidotai TPRP

Avots: autores veidots

Ietvara struktūra pamatojas uz trim galvenajām komponentēm:

1. **Spēju attīstības priekšnosacījumi** - nepieciešamie informācijas avoti DU novērtēšanai un caurskatāmība DU novērtēšanas procesā trešās puses piesaistes posmā.
2. **Spējas DU novērtēšanai un pārvaldībai** – trīs dinamisko spēju pīlāri (uztveršana, izmantošana un pārveidošana), kas nodrošina informācijas apstrādi un izmantošanu.
3. **Pilnveidotu DU prakšu rezultāti** – ietvara rezultātā sasniedzams augstāks TPRP brieduma līmenis un efektīvāka DU ietekme uz TPR mazināšanu.

Tādēļ turpmākajās sadaļās vispirms tiek aplūkoti priekšnosacījumi, kas nepieciešami ietvara darbībai.

Daudzveidīgu informācijas avotu nozīme

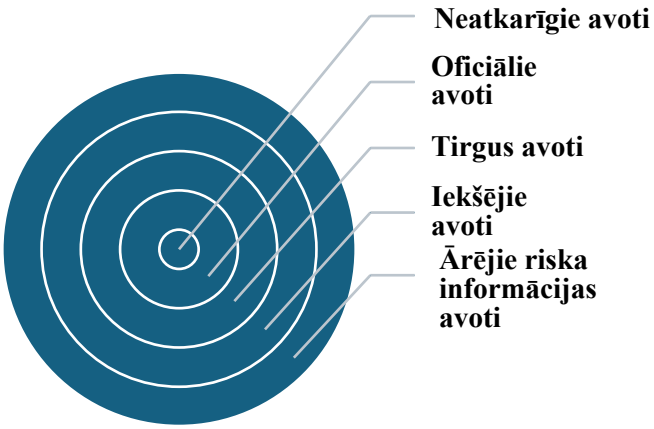
Eksperti uzsvēra, ka daudzveidīgu informācijas avotu izmantošana var uzlabot DU novērtēšanas kvalitāti, taču izšķiroša nozīme ir šo avotu kvalitātei, neatkarībai un spējai tos efektīvi integrēt. Organizācijām būtu jāizveido uzticams, no pierādījumiem izrietošs

pamatavotu kopums, jāizvairās no dublējošas vai "trokšņainas" informācijas un jānodrošina, ka vērtētāji spēj kvalitatīvi analizēt un savstarpēji salāgot iegūtos datus.

Eksperti noteica vairākas būtiskas informācijas avotu grupas DU novērtēšanā:

1. Neatkarīgie avoti – audita ziņojumi, sertifikāti, drošības ievainojamību testēšanas rezultāti, incidentu vēsture (augstākais pārliecības līmenis).
2. Oficiālie avoti – publiskie reģistri, sankciju saraksti, regulatīvais statuss, ES uzraudzība.
3. Tirgus avoti – partneru un klientu atsauksmes (ar nepieciešamību izvērtēt iespējamo aizspriedumu risku).
4. Iekšējie avoti – piegādātāja sniegtā dokumentācija, anketas, arhitektūras apraksti, līgumi.
5. Ārējie riska informācijas avoti – negatīvā mediju informācija, NILLN, ESG (vides, sociālo un pārvaldības aspektu skrīnings).

Ekspertu noteiktie daudzveidīgie informācijas avoti DU novērtēšanai var tikt apvienoti vienotā, holistiskā IKT trešās puses pakalpojumu sniedzēja profilā, kas attēlots 3.2. attēlā.



3.2.attēls. IKT trešās puses pakalpojumu sniedzēja holistisks profils
Avots: autores veidots

Aptaujas rezultāti apstiprina, ka finanšu iestādes jau izmanto daudzveidīgus informācijas avotus, taču eksperti iesaka prioritizēt neatkarīgus un no rezultātiem izrietošus pierādījumus, nevis pašu piegādātāju sniegto informāciju. Blokķēdes tehnoloģija netika noteikta kā būtisks DU signāls, visticamāk tās ierobežotās piemērojamības un uzticības daudzdimensionālās būtības dēļ.

Pamatojoties uz ekspertu atziņām, tiek piedāvāta pakāpeniska pierādījumu hierarhija (angliski - *tiered evidence hierarchy*):

- **A līmenis** (uz rezultātiem balstīta pārbaude) – neatkarīgi auditi, drošības ievainojamību testēšanas rezultāti, incidentu atklāšana.
- **B līmenis** (faktos balstīta pārbaude) – oficiālie reģistri, finanšu pārskati, atzīti sertifikāti.
- **C līmenis** (papildinoši pierādījumi) – skrīninga platformas, partneru atsauksmes, piegādātāja materiāli (nepieciešama savstarpēja pārbaude).

Caurskatāmības nozīme spēju stiprināšanā

Hipotēzes H7 statistiskā pārbaude apstiprina, ka caurskatāmība DU novērtēšanā trešās puses piesaistes procesā pozitīvi ietekmē organizācijas spējas DU novērtēšanā un pārvaldībā. Caurskatāmību iespējams īstenot, izmantojot skaidri definētus un dokumentētus novērtēšanas kritērijus (piemēram, strukturētas padziļinātās izpētes anketas), pieejamu un saprotamu izvērtēšanas procesu, kā arī savstarpēji saskaņojot uzticības gaidas ar IKT trešajām pusēm.

Eksperti norādīja, ka caurskatāmība stiprina spējas, jo tā veicina:

- standartizāciju un atkārtojamību, nodrošinot salīdzināmu pierādījumu apkopošanu;
- piegādātāju iesaisti, uzlabojot dokumentācijas kvalitāti un procesa efektivitāti;
- sadarbības kvalitāti, palielinot taisnīgumu, atsaucību un iesniegtās informācijas pilnīgumu.

Tomēr caurskatāmība veicina spēju attīstību tikai tad, ja:

- tā tiek apvienota ar saturisku izvērtēšanu un neatkarīgu pārbaudi;
- pierādījumu novērtēšanu regulē dokumentēta metodoloģija (vērtēšanas sistēma, izlases pieeja, papildu jautājumi);
- komandām ir pietiekamas kompetences un laiks paplašināta pierādījumu kopuma analīzei.

Vienlaikus eksperti brīdināja, ka pārmērīga caurskatāmība var veicināt formālu atbilstības izpildi, kritēriju pielāgošanu formālai atbilstībai, mākslīgi paaugstinātu uzticamības uztveri vai šķietamu atbilstību, kā arī atturēt daļu piegādātāju no sadarbības.

Pamatprocess: trīs spēju elementi

Pamatojoties uz ekspertu intervijām un dinamisko spēju teoriju, pētījumā tiek izstrādātas trīs pamatspējas DU novērtēšanai un pārvaldībai ar mērķi paaugstināt TPRP brieduma līmeni un mazināt IKT TPR.

1. Uztveršana: DU signālu noteikšana, izpratne un uzraudzība

Šī spēja raksturo organizācijas spēju sistemātiski apkopot, interpretēt un laikus konstatēt izmaiņas signālos un pierādījumos, kas saistīti ar trešās puses uzticamību. Tā ietver:

- daudzavotu informācijas apkopošanu (neatkarīgie, oficiālie, tirgus un piegādātāja avoti);
- nepārtrauktu un notikumos pamatotu uzraudzību (veiktspēja, incidenti, regulatīvās izmaiņas);
- sistemātisku pierādījumu pārbaudi un izcelsmes izvērtēšanu;
- jauno risku un tendenču analīzi.

2. Izmantošana: DU atziņu integrēšana TPRP lēmumu pieņemšanā

Šī spēja nodrošina uztveršanas posmā iegūto atziņu praktisku izmantošanu, integrējot tās lēmumu pieņemšanas sistēmās un risku pārvaldības procesos. Tā ļauj organizācijai pieņemt savlaicīgus un pamatotus lēmumus attiecībā uz trešajām pusēm, tostarp:

- uz riskiem pamatotas uzraudzības intensitātes pielāgošanu;
- uzticībā pamatotu piegādātāju izvēli un TPRP pārvaldības mehānismu piemērošanu;
- strukturētu incidentu un novēršanas pasākumu īstenošanu.

3. Pārveidošana: novērtēšanas pieeju pielāgošana un pilnveidošana laika gaitā

Šī spēja vērsta uz nepārtrauktu pilnveidi, sistemātiski mācoties no iepriekšējām novērtēšanām un attiecīgi uzlabojot metodes, rīkus un pārvaldības pieeju. Tā nodrošina, ka DU novērtēšanas ietvars attīstās un sasniedz augstāku brieduma līmeni, ietverot:

- DU novērtēšanas ietvara standartizāciju;
- sistemātisku zināšanu un datu pārvaldību.

Noslēgumā eksperti uzsvēra arī procesu salāgotības nozīmi - vadības spēju saskaņot uztveršanas, izmantošanas un pārveidošanas procesus (Eurico Soares De Noronha et al. 2024).

Organizācijas dinamiskās spējas DU novērtēšanā un pārvaldībā ir attēlotas 3.3. attēlā.

3.3. attēls. Organizācijas dinamiskās spējas DU novērtēšanā un pārvaldībā

Avots: autores veidots

DU novērtēšanas un pārvaldības spēju salāgošana paredz nepārtrauktu izmantoto metožu, rīku un kompetenču izvērtēšanu un pilnveidi. Tas ietver ieguldījumus tehnoloģijās un ārējā ekspertīzē, pierādījumu kvalitātes un novērtēšanas efektivitātes uzraudzību, kā arī validāciju vai novērtēšanas modelis konsekventi sasaista augstāku uzticības līmeni ar zemāku atlikušo risku. Tāpat nepieciešama saskaņota pieeja starp galvenajām funkcijām (piemēram, TPRP, informācijas drošību, IT risku pārvaldību), lai nodrošinātu vienotu izpratni par DU.

3.3 IKT trešo pušu risku pārvaldības turpmākā attīstība Baltijas banku nozarē

Eksperti tika aicināti sniegt viedokli par TPRP turpmāko attīstību Baltijas banku nozarē. TPRP ir salīdzinoši jauna joma ES finanšu sektorā, un nākamo 3–5 gadu laikā sagaidāma turpmāka regulatīvā attīstība. Lai gan pamatprasības attiecībā uz IKT trešajām pusēm, visticamāk, būtiski nemainīsies, eksperti paredz lielāku prasību standartizāciju visā ES, skaidrāku interpretāciju, koplietojamus veidlapu paraugus un iespējamu centralizētu kritisko piegādātāju datubāzi uzraudzības iestāžu pārraudzībā. Regulējums, visticamāk, vairāk akcentēs ieviešanas kvalitāti un esošo prakšu briedumu, kā arī paplašināsies uz noteiktiem ne-IKT pakalpojumu sniedzējiem, pastiprinās uzmanību ESG riskiem un padziļinās ceturtās un nākamā līmeņa pušu uzraudzību.

Lai sagatavotos šīm izmaiņām, organizācijām ieteicams:

- formalizēt detalizētus TPRP procesus, procedūras un rīcības plānus;
- paplašināt reģistrus, iekļaujot ceturtās un nākamā līmeņa puses, lai kartētu apakšuzņēmēju ķēdes;
- integrēt ar ESG saistītas prasības anketās un līgumos.

Pārvaldības līmenī sagaidāma lielāka TPRP redzamība valdes līmenī, augstāks brieduma līmenis un specializētu TPRP lomu un komandu izveide. Pašlaik vērojams resursu ierobežojums, taču tiek prognozēta plašāka automatizācijas un mākslīgā intelekta risinājumu ieviešana. Tāpat būs nepieciešama ciešāka starpfunkcionāla sadarbība (iepirkumi, atbilstība, juridiskā funkcija, biznesa struktūrvienības) un vienota izpratne par TPR.

Sagaidāmas arī tirgus izmaiņas: trešās puses stiprinās atbilstības kompetenci DORA prasību izpildē, iespējams, izmantojot to kā konkurences priekšrocību, savukārt, finanšu iestādes pieprasīs augstākas kvalitātes dokumentāciju. Vienlaikus var pieaugt atbilstības izmaksas. DORA regulējums var dot priekšrocības lieliem piegādātājiem, potenciāli palielinot koncentrācijas risku, kamēr mazākiem pakalpojumu sniedzējiem un tālāk pārdevējiem var rasties grūtības.

Noslēgumā eksperti paredz pakāpenisku TPRP tipa regulējuma paplašināšanos ārpus finanšu sektora, īpaši uz kritiskās infrastruktūras nozarēm (enerģētika, ūdensapgāde, transports, telekomunikācijas) un, iespējams, arī uz lieliem uzņēmumiem, ņemot vērā savstarpēji saistītās piegādes ķēdes, kiberrisku pakļautību un DORA un NIS2 regulējuma savstarpējo saskaņošanu.

Secinājumi

Promocijas darbā tika analizēta DU ietekme uz TPR Baltijas banku nozarē. Galvenie pētījuma secinājumi ir šādi:

1. Pētījuma teorētiskais devums sniedz konceptuālu skaidrojumu DU jēdzienam, izstrādājot un validējot jaunu definīciju, kas balstīta uz 42 esošo definīciju sistemātisku analīzi un to klasifikāciju sešās tematiskajās grupās. Tika konsolidēti 24 DU faktori un strukturēti četrās kategorijās: spēja, labvēlība, integritāte un jaunieviestā kategorija – atvērtība. Definīcijas satura validācija apstiprināja tās atbilstību noteiktajiem faktoriem (kopējais htc = 0,86), apliecinot, ka tā precīzāk atspoguļo DU daudzdimensionālo būtību nekā līdz šim populārākā definīcija.
2. Pētījums sniedz skaidru teorētisku nošķīrumu starp TPR un saistītajiem jēdzieniem - piegādātāja risku, piegādes ķēdes dalībnieka risku un pakalpojumu sniedzēja risku, kurus literatūrā bieži lieto kā sinonīmus. Darbā TPR definēts kā visaptverošs risku veids un strukturēts septiņās kategorijās: (1) regulatīvie un atbilstības riski, (2) operacionālie riski, (3) finanšu riski, (4) drošības un privātuma riski, (5) stratēģiskie riski, (6) ētiskie un sociālie riski un (7) partneru un piegādes ķēdes riski.
3. Šī pētījuma pamat-hipotēze (H1), ka DU samazina TPR, tika pārliecinoši apstiprināta gan pilnajā darbinieku izlasē ($\beta = -0{,}452$; $p = 0{,}000$), gan pārvaldības līmeņa grupā ($\beta = -0{,}753$; $p = 0{,}001$), apliecinot, ka augsts DU līmenis būtiski veicina zemāku kopējo TPR līmeni B2B kontekstā IKT pakalpojumu sniedzēju attiecībās. Detalizētā analīze apstiprināja šo negatīvo ietekmi desmit no divpadsmit konkrētajiem risku veidiem, tostarp koncentrācijas, finanšu, stratēģiskajiem un datu privātuma riskiem. Tomēr statistiski nozīmīga ietekme netika apstiprināta attiecībā uz piegādātāja un piegādes ķēdes kiberdrošības riskiem (H1f) un ar partneru specifiskajiem faktoriem saistītajiem riskiem (H1k), kas liecina, ka konkrēti tehniskie un ģeopolitiskie riski prasa papildu risku pārvaldības pasākumus.
4. DU ietekmi uz TPR mazināšanu pastiprina organizācijas spējas (H2), taču šis rezultāts ar spēcīgu negatīvu moderācijas efektu ($\beta = -0{,}462$; $p = 0{,}047$) tika apstiprināts tikai to darbinieku grupā, kuri ir informēti par pārvaldības līmeņa praksēm (riska, atbilstības un drošības profesionāļi), bet pilnajā izlasē tika noraidīts.
5. Organizācijas caurskatāmībai DU novērtēšanā ir atšķirīga nozīme atkarībā no konteksta, kas izaicina informācijas asimetrijas teorijas piemērošanu. Lai gan pilnajā darbinieku izlasē caurskatāmība pozitīvi ietekmē DU (H3; $\beta = 0{,}251$; $p = 0{,}011$), kas liecina, ka operatīvā līmeņa darbinieki to izmanto nenoteiktības mazināšanai, šī saistība tika noraidīta pārvaldības līmeņa grupā. Turklāt moderācijas efekta (H6) apstiprināšana abās izlasēs ar pozitīviem (vājināšanas) ceļa koeficientiem ($\beta = 0{,}267$ un $\beta = 0{,}603$) liecina, ka trešās puses var izmantot augstu caurskatāmības līmeni, lai "manipulētu ar signālu" un radītu mākslīgu uzticamības uztveri, kas ne vienmēr rezultējas risku samazinājumā.
6. Darbā tika apstiprināts, ka dinamiskās organizācijas spējas (H11) DU novērtēšanā būtiski un pozitīvi ietekmē TPRP brieduma līmeni ($\beta = 0{,}377$; $p = 0{,}000$), demonstrējot praktisku saikni starp šo spēju attīstību un organizācijas TPRP līmeņa paaugstināšanu. Savukārt, šīs spējas pozitīvi ietekmē caurskatāmība (H7) (apstiprināta abās izlasēs) un plaša daudzveidīgu informācijas avotu izmantošana (H10) (apstiprināta pilnajā izlasē).
7. Nozares profesionāļu visbiežāk izmantotie informācijas avoti bija pakalpojuma aprakstošā dokumentācija (vidējais = 4,06) un reputācijas apliecinājumi (vidējais = 3,93), piemēram, ISO 27001 sertifikāti un audita ziņojumi.
8. Pētījums apstiprināja DU mediējošo lomu attiecībās starp caurskatāmību un risku, apstiprinot H5 pilnajā izlasē. Šis secinājums norāda, ka caurskatāmība pati par sevi tieši nesamazina risku (H4 tika noraidīta), bet netieši veicina risku mazināšanu, veidojot augstāku DU līmeni, kas savukārt mazina riskus.
9. Metodoloģiskais lēmums analizēt datus, izmantojot divas atsevišķas izlases (pilno darbinieku izlasi un pārvaldības līmeņa grupu), atklāja būtiskas atšķirības H2, H3, H5 un

H10 rezultātos. Šī analīze divās atsevišķās izlasēs sniedza pierādījumus tam, ka spēju, caurskatāmības un informācijas izmantošanas nozīme un loma TPRP ietvarā ir atkarīga no lomas organizācijā.

10. Pamatojoties uz ekspertu viedokli, pašreizējais organizāciju spēju līmenis DU novērtēšanā un pārvaldībā Baltijas banku nozarē kopumā ir raksturojams kā agrīnā posmā, parasti 1. vai 2. līmenī.
11. Sagaidāmās izmaiņas regulētajā sektorā akcentēs TPRP prakšu briedumu, ieviešanas kvalitāti un kompetenci, prasot organizācijām izstrādāt detalizētus procesu aprakstus un rīcības scenārijus, lai sagatavotos uzraudzības pārbaudēm.
12. DORA prasību ietekmē paredzamas izmaiņas IKT trešo pušu tirgus struktūrā, potenciāli dodot priekšrocības lieliem globāliem piegādātājiem un prasot papildu resursu piešķiršanu, tostarp specializētas TPRP lomas un paaugstinātu automatizācijas līmeni finanšu iestādēs.

Rekomendācijas

Praktiskie ieteikumi

1. Ņemot vērā, ka pētījumā konstatēts, ka augstāks DU līmenis samazina TPR, organizācijām ieteicams formalizēt DU novērtēšanu un pārvaldību kā risku mazināšanas kontroli. Vienlaikus ieteicams ierobežot paļaušanos uz uzticību kā aizvietotāju kiberdrošības apliecinājumam vai partnerim raksturīgo faktoru izvērtēšanai, jo šajās jomās ir nepieciešama atsevišķa pārbaude.
2. Organizācijām ieteicams stiprināt TPRP briedumu, attīstot dinamiskās spējas DU novērtēšanai un pārvaldībai. Tas ietver pierādījumu sistemātisku apkopošanu un pārbaudi no dažādiem avotiem, uzticības indikatoru iekļaušanu lēmumu pieņemšanas procesos, kā arī novērtēšanas instrumentu regulāru pilnveidošanu, lai nodrošinātu vienotu pieeju un atkārtojamību visā organizācijā.
3. Organizācijām ieteicams atklāti dalīties ar DU novērtēšanas kritērijiem, lai atbalstītu spēju attīstību, vienlaikus uzraugot "pielāgotu atbilžu" risku un nodrošinot neatkarīgu pārbaudi, lai sniedzamā informācija patiesi atspoguļotu reālo praksi.
4. Novērtējot IKT trešo pušu DU, organizācijām vajadzētu izvairīties no paļaušanās uz vienu informācijas avotu. Tā vietā ieteicams kombinēt sertifikātus, risinājuma dokumentāciju, tirgus signālus un trešo pušu atzinumus, vienlaikus nodrošinot darbinieku apmācības, lai viņi spētu apvienot dažādus un reizēm pretrunīgus datus vienotā uzticības novērtējumā.
5. Lai uzlabotu uzticības novērtējumu kvalitāti, organizācijām ieteicams prioritizēt pierādījumus pēc to uzticamības, nevis apjoma. Neatkarīgai, no rezultātiem izrietošai pārbaudei (A informācijas avotu līmenis) jābūt primārajam novērtējuma pamatam, ko papildina faktos balstīta validācija no oficiāliem avotiem (B informācijas avotu līmenis). Pašdeklarēta vai kontekstuāla informācija (C informācijas avotu līmenis) izmantojama piesardzīgi un tikai kā papildinājums augstākas kvalitātes pierādījumiem.
6. Organizācijām ieteicams formalizēt uzticības novērtēšanas procesus un attīstīt uztveršanas, izmantošanas un pārveidošanas spējas, vienlaikus panākot vienotu izpratni starp pārvaldības un operacionālajām lomām, izmantojot vienotu novērtēšanas ietvaru.
7. Ņemot vērā, ka caurskatāmība samazina risku tikai caur uzticību, ko tā palīdz veidot (H5), organizācijām būtu jākoncentrējas uz sadarbības stiprināšanu, nevis jāuztver caurskatāmība kā formāla procedūra. Ja caurskatāmība stiprina labvēlības un integritātes uztveri, risks mazinās. Savukārt, ja tā tiek īstenota tikai kā formāla atbilstības izpilde, būtiska risku mazināšana nenotiek.
8. Ņemot vērā, ka pārvaldības līmeņa lomas uzsver pierādījumus, bet procesu īstenotāji biežāk paļaujas uz attiecību uzticību, organizācijām ieteicams šos skatījumus saskaņot, izmantojot vienotus ietvarus un vienotus informācijas avotus. Centralizēti uzticamības pierādījumi, piemēram, vērtēšanas ieraksti un pārbaudīti pierādījumi, palīdz sinhronizēt lēmumu pieņemšanu un mazināt sadrumstalotu novērtēšanu starp komandām.
9. Lai atbilstu mainīgajām regulatoru prasībām, organizācijām ieteicams paplašināt TPRP praksi, kartējot apakšuzņēmējus un nākamā līmeņa pušu atkarības, formalizējot detalizētas operacionālās rokasgrāmatas, kā arī integrējot ESG apsvērumus padziļinātā pārbaudē (angliski – *due diligence*). Automatizācijas un mākslīgā intelekta risinājumu izmantošana kļūs arvien nozīmīgāka, lai tiktu galā ar pieaugošo sarežģītību un pastiprinātu regulatoru uzraudzību.

Ieteikumi turpmākajiem pētījumiem

1. Ņemot vērā TPRP agrīno attīstības posmu Baltijas banku nozarē, ieteicams veikt garengriezuma pētījumu, lai izpētītu DU ietekmes uz TPR dinamiku, kā arī šo organizāciju brieduma pieaugumu laika gaitā.
2. Starpnozaru pētījums finanšu sektorā varētu parādīt, kā organizācijas lielums, tās briedums vai regulējuma intensitāte ietekmē attiecības starp DU un TPR.

3. Lai palielinātu rezultātu vispārināmību, turpmākie pētījumi varētu pārbaudīt noteiktās sakarības citos regulējuma režīmos, kultūras normās un digitalizācijas līmeņos, veicot salīdzinošus pētījumus dažādās ES valstīs vai salīdzinot rezultātus ar ASV, Āzijas vai jaunattīstības tirgiem.
4. Lai mazinātu pašnovērtējuma aizspriedumus, turpmākajos pētījumos ieteicams iekļaut objektīvus datus, piemēram, auditu rezultātus, incidentu ziņojumus, veiktspējas rādītājus, darbību žurnālus vai ārēji pārbaudītus uzticības indikatorus.
5. Turpmākie pētījumi varētu analizēt DU un risku dinamiku visas organizācijas trešo pušu ekosistēmas ietvarā, nevis koncentrēties uz vienām attiecībām, un kā analīzes vienību izmantot organizācijas TPR portfeli.
6. Pamatojoties uz interviju secinājumiem, turpmākie pētījumi varētu izmantot gadījumu izpētes, etnogrāfiju vai rīcībpētniecību, lai analizētu, kā DU spējas tiek attīstītas, operacionalizētas un laika gaitā iestrādātas organizācijas rutīnās.
7. Turpmākie pētījumi varētu paplašināt piedāvāto ieteikumu praktisko pielietojamību, izstrādājot prioritizēšanas ietvarus, kas pielāgoti mazākām finanšu iestādēm ar ierobežotiem finanšu un organizatoriskajiem resursiem.
8. Tā kā korporatīvās sociālās atbildības riski ekspertu vērtējumā tika atzīti par vieniem no vismazāk nobriedušajiem un vismazāk skaidri izprastajiem, turpmākie pētījumi varētu koncentrēties uz auditējamu digitālo ESG metriku izstrādi, kas ir piemērotas IKT pakalpojumu sniedzējiem.

Noslēguma atziņas

Promocijas darbā tika sniegtas atbildes uz visiem pētījuma jautājumiem un tika izpildīti visi pētījuma sākumā izvirzītie uzdevumi. Pētījumā apvienota teorētiskā analīze, kvantitatīvā modelēšana un ekspertu intervijas nodrošināja vispusīgu priekšstatu par digitālās uzticības nozīmi trešo pušu risku pārvaldībā.

Lai gan pētījuma empīriskā daļa veltīta Baltijas valstu banku nozarei, kur normatīvā regulējuma prasības un tehnoloģiskā attīstība veido īpaši piemērotu pētījuma vidi, šajā promocijas darbā iegūtās konceptuālās atziņas pārsniedz šo ģeogrāfisko un nozares ietvaru. Pētījumā noskaidrotās saistības starp digitālo uzticību un trešo pušu riskiem atspoguļo plašākas likumsakarības, kas raksturīgas digitālajai videi un organizāciju sadarbībai ar IKT pakalpojumu sniedzējiem. Tādēļ izstrādātais konceptuālais ietvars un metodoloģiskā pieeja digitālās uzticības novērtēšanai var būt izmantojama arī citās nozarēs, dažādos normatīvā regulējuma kontekstos un organizatoriskajos kontekstos, kuros organizācijas sadarbojas ar ārējiem IKT pakalpojumu sniedzējiem.

Pētījumā noteiktās trešo pušu risku kategorijas veido strukturētu klasifikāciju, kas var būt aktuāla dažādās nozarēs un organizatoriskajos kontekstos. Tādēļ tās var uzskatīt par vispārīgi piemērojamām organizācijām, kas savā darbībā izmanto trešo pušu pakalpojumus.

Tādējādi promocijas darbs veido pamatu turpmākajiem akadēmiskajiem pētījumiem un praktiskajai attīstībai digitālās uzticības un trešo pušu risku pārvaldības jomā. Tajā iegūtās atziņas var palīdzēt organizācijām pilnveidot digitālās uzticības novērtēšanas praksi un stiprināt trešo pušu risku pārvaldību.

Bibliography used in the summary / Kopsavilkumā izmantotais literatūras saraksts

1. Abbasi, M., J. Prieto, A. Shahraki, and J. M. Corchado. 2023. “Industrial Data Monetization: A Blockchain-Based Industrial IoT Data Trading System.” *Internet of Things (Netherlands)* 24. Scopus. https://doi.org/10.1016/j.iot.2023.100959.
2. Abdul-Rahman, A., and S. Hailes. 2000. “Supporting Trust in Virtual Communities.” *Proc. Annu. Hawaii Int. Conf. Syst. Sci.* 2000-January. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85094162508&partnerID=40&md5=07a90713207ea1a535184152f578700b.
3. Agrawal, P., P. Durge, R. K. Kushwaha, G. Kaur, G. K. Gupta, and S. Maheshwari. 2024. “Securing the Internet of Things: A Blockchain Paradigm.” Paper presented at 2024 International Conference on Innovations and Challenges in Emerging Technologies, ICICET 2024. *Int. Conf. Innov. Challenges Emerg. Technol., ICICET*. Scopus. https://doi.org/10.1109/ICICET59348.2024.10616308.
4. Ajzen, Icek. 1991. “The Theory of Planned Behavior.” *Organizational Behavior and Human Decision Processes* 50 (2): 179–211. https://doi.org/10.1016/0749-5978(91)90020-T.
5. Akerlof, George A. 1970. “The Market for ‘Lemons’: Quality Uncertainty and the Market Mechanism.” *The Quarterly Journal of Economics* 84 (3): 488. https://doi.org/10.2307/1879431.
6. Akram, RN, and RKL Ko. 2014. “Digital Trust - Trusted Computing and beyond: A Position Paper.” *Proc. - IEEE Int. Conf. Trust, Secur. Priv. Comput. Commun., TrustCom*, 884–92. WOS:000380562600115, pp. 884–92. Scopus. https://doi.org/10.1109/TrustCom.2014.116.
7. Aldás-Manzano, J., C. Lassala-Navarré, C. Ruiz-Mafé, and S. Sanz-Blas. 2009. “Key Drivers of Internet Banking Services Use.” *Online Information Review* 33 (4): 672–95. WOS:000270768100003, pp. 672–95. Scopus. https://doi.org/10.1108/14684520910985675.
8. Aliane, N., and A. Zakariya. 2023. “Enhancing Cyber Security Resilience in the Industrial Sector: A Comprehensive Framework for Third-Party Risk Management.” *International Journal of Cyber Criminology* 17 (2): 262–83. Scopus. https://doi.org/10.5281/zenodo.4766716.
9. Alpcan, T., A. Levi, and E. Savas. 2011. “Digital Trust Games: An Experimental Study.” In *Lect. Notes Comput. Sci.*, edited by JS Baras, J. Katz, and E. Altman, 7037 LNCS. WOS:000306390000015, pp. 182–200. Scopus. https://doi.org/10.1007/978-3-642-25280-8_15.
10. Arner, Douglas W., Janos Nathan Barberis, and Ross P. Buckley. 2015. “The Evolution of Fintech: A New Post-Crisis Paradigm?” *SSRN Electronic Journal*, ahead of print. https://doi.org/10.2139/ssrn.2676553.
11. Aslan, Ömer, Semih Serkant Aktuğ, Merve Ozkan-Okay, Abdullah Asim Yilmaz, and Erdal Akin. 2023. “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions.” *Electronics* 12 (6): 1333. https://doi.org/10.3390/electronics12061333.
12. Balci, G. 2021. “Digitalization in Container Shipping: Do Perception and Satisfaction Regarding Digital Products in a Non-Technology Industry Affect Overall Customer Loyalty?” *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE* 172 (November). WOS:000704400900017. Scopus. https://doi.org/10.1016/j.techfore.2021.121016.
13. Bates, Marcia J., and Mary Niles Maack, eds. 2009. “Grey Literature.” In *Encyclopedia of Library and Information Sciences, Third Edition*, 0 ed. CRC Press. https://doi.org/10.1081/E-ELIS3-120043732.

14. Baumgaertner, Laura Doriane, and Jonas Soluk. 2023. “Trust and Information Asymmetry: How Intermediaries Affect Asymmetric Innovation Collaborations.” *Academy of Management Proceedings* 2023 (1): 12230. https://doi.org/10.5465/AMPROC.2023.12230abstract.
15. Benchmark International. 2024. “Global Financial Industry Report.” December 17. https://www.benchmarkintl.com/insights/global-financial-industry-report/.
16. Bhattacharya, K. K., and S. Saha. 2004. “Trust Dimensions in E-Retailing: A Strategic Exploration.” *IEEE Int Eng Manage Conf* 2: 825–28. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-17644387597&partnerID=40&md5=3e39f71a22f513246ea3b98a9bd19c6b.
17. Bishop, L. M., P. L. Morgan, P. M. Asquith, G. Raywood-Burke, A. Wedgbury, and K. Jones. 2020. “Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design.” In *Lect. Notes Comput. Sci.*, edited by Moallem A., 12210 LNCS. Springer. Scopus. https://doi.org/10.1007/978-3-030-50309-3_4.
18. Buch, Claudia. 2024. “Financial Integration in the Baltics: Lessons in Resilience and Transformation.” April 10. https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp241004~9588c58d39.en.html.
19. Calculator.net. 2026. “Sample Size Calculator.” https://www.calculator.net/sample-size-calculator.html.
20. Cerić, Anita. 2021. “Reducing Information Asymmetry and Building Trust in Projects Using Blockchain Technology.” *Journal of the Croatian Association of Civil Engineers* 73 (10): 967–78. https://doi.org/10.14256/JCE.3310.2021.
21. Chaudhuri, A. 2021. “TRANSFORMATION WITH TRUSTWORTHY DIGITAL: POLICY DESIDERATA FOR BUSINESSES IN POST COVID-19 WORLD.” *EDPACS* 63 (1): 1–8. Scopus. https://doi.org/10.1080/07366981.2020.1806443.
22. Chen, J. K. C., P. K. Lin, H. Aminah, H. Rizaldy, and D. Dinh. 2022. “How Digital Payment Applications and Digital Trust Response Industry 5.0.” *ACM Int. Conf. Proc. Ser.*, 369–74. Scopus. https://doi.org/10.1145/3568834.3568906.
23. Chen, X., B. Li, D. Song, and M. Wang. 2023. “Influences of Risk-Aversion Behavior and Purchasing Option in a Cross-Border Dual-Channel Supply Chain.” *International Transactions in Operational Research*, ahead of print. Scopus. https://doi.org/10.1111/itor.13345.
24. Clarivate. 2024. “Web of Science.” https://www.webofscience.com.
25. CMMI Institute. n.d. “CMMI Levels of Capability and Performance.” Accessed June 22, 2025. https://cmmiinstitute.com/learning/appraisals/levels.
26. Collier, Z. A., U. Guin, J. Sarkis, and J. H. Lambert. 2022. “Decision Model with Quantification of Buyer-Supplier Trust in Advanced Technology Enterprises.” *BENCHMARKING-AN INTERNATIONAL JOURNAL* 29 (10): 3033–56. WOS:000730397000001, pp. 3033–56. Scopus. https://doi.org/10.1108/BIJ-06-2021-0336.
27. Colquitt, Jason A., Tyler B. Sabey, Jessica B. Rodell, and Edwyna T. Hill. 2019. “Content Validation Guidelines: Evaluation Criteria for Definitional Correspondence and Definitional Distinctiveness.” *Journal of Applied Psychology* 104 (10): 1243–65. https://doi.org/10.1037/apl0000406.
28. Corsaro, D., and V. D’Amico. 2022. “How the Digital Transformation from COVID-19 Affected the Relational Approaches in B2B.” *Journal of Business and Industrial Marketing* 37 (10): 2095–115. WOS:000803068900001, pp. 2095–115. Scopus. https://doi.org/10.1108/JBIM-05-2021-0266.
29. Das, D., S. Banerjee, P. Chatterjee, and U. Ghosh. 2023. “A Comprehensive Analysis of Trust, Privacy, and Security Measures in the Digital Age.” *Proc. - IEEE Int. Conf. Trust,*

Priv. Secur. Intell. Syst. Appl., TPS-ISA, 360–69. WOS:001174354000041, pp. 360–69. Scopus. https://doi.org/10.1109/TPS-ISA58951.2023.00051.
30. Davis, Fred D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology." *MIS Quarterly* 13 (3): 319. https://doi.org/10.2307/249008.
31. Deloitte. 2017. *Overcoming the Threats and Uncertainty Third-Party Governance and Risk Management (TPGRM).* https://www2.deloitte.com/kz/en/pages/risk/articles/eerm-survey-report.html.
32. Deloitte. 2023. *Navigating the Headwinds Enhancing Agility to Regain Momentum Global Third-Party Risk Management Survey 2023*. https://www.deloitte.com/global/en/services/risk-advisory/research/gx-third-party-risk-management-survey.html.
33. Deloitte. 2024a. "Future of Digital Trust." https://www2.deloitte.com/de/de/pages/risk/articles/future-of-digital-trust.html.
34. Deloitte. 2024b. "Third-Party Risk." https://www2.deloitte.com/cy/en/pages/governance-risk-and-compliance/articles/third-party-risk.html.
35. Department for International Development. 2004. "The Importance of Financial Sector Development for Growth and Poverty Reduction." Policy Division, August.
36. Deprez, JC, C. Ponsard, and N. Matskanis. 2016. "A Goal-Oriented Requirements Analysis for the Collection, Use and Exchange of Electronic Evidence across EU Countries." *Proc. - IEEE Int. Requir. Eng. Conf. Workshops, REW*, 106–13. WOS:000405493000019, pp. 106–13. Scopus. https://doi.org/10.1109/REW.2016.31.
37. Dimitrakos, Theo. 2001. "System Models, e-Risks and e-Trust." Paper presented at Towards The E-Society: E-Commerce, E-Business, and E-Government, The First IFIP Conference on E-Commerce, E-Business, E-Government (I3E 2001).
38. "Eesti Pank." n.d. Accessed June 15, 2025. https://www.eestipank.ee/.
39. Ellex. 2025. *Baltic Fintech Legal Outlook 2025*. https://ellex.legal/wp-content/uploads/2025/02/baltic-fintech-legal-outlook-2025.pdf.
40. Elsevier. 2025. "Scopus." https://www.scopus.com.
41. Enria, Andrea. 2023. "The Role of Banks in Mitigating Systemic Risks Arising in the Non-Bank Financial Sector." June 20. https://www.bankingsupervision.europa.eu/press/speeches/date/2023/html/ssm.sp230620~ecce24f124.en.html.
42. Eurico Soares De Noronha, Matheus, Diandra Maynne Ferraro, Leonardo Reis Longo, and Scarlet Simonato Melvin. 2024. "The Orchestration of Dynamic Capabilities in Cleantech Companies." *Innovation & Management Review* 21 (1): 15–27. https://doi.org/10.1108/inmr-08-2021-0144.
43. European Banking Authority. 2019. *Final Report on EBA Guidelines on Outsourcing Arrangements*. https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf.
44. European Banking Authority. 2025. "The EBA Launches Consultation on Its Draft Guidelines on Third-Party Risk Management with Regard to Non-ICT Related Services." August 7. https://www.eba.europa.eu/publications-and-media/press-releases/eba-launches-consultation-its-draft-guidelines-third-party-risk-management-regard-non-ict-related.
45. European Commission. 2022a. "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive

(EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA Relevance).” https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
46. European Commission. 2022b. “Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA Relevance).” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.
47. Eurostat. 2025. “Enterprise Statistics by Size Class and NACE Rev. 2 Activity (from 2021 Onwards).” May 14. https://doi.org/10.2908/SBS_SC_OVW.
48. Falk, R. F., and N. B. Miiler. 1992. *A Primer for Soft Modeling*. University of Akron Press.
49. Ferraro, C., MA Wheeler, JI Pallant, SG Wilson, and J. Oldmeadow. 2023. “Not so Trustless after All: Trust in Web3 Technology and Opportunities for Brands.” *BUSINESS HORIZONS* 66 (5): 667–78. WOS:001060955600001, pp. 667–78. Scopus. https://doi.org/10.1016/j.bushor.2023.01.007.
50. Fortner, Z. A. 2021. “Mitigating Third-Party Risks: The Benefits of Extending Quality to the Supply Chain.” *Pharmaceutical Technology Europe* 45 (9): 56–60. Scopus.
51. Franke, George, and Marko Sarstedt. 2019. “Heuristics versus Statistics in Discriminant Validity Testing: A Comparison of Four Procedures.” *Internet Research* 29 (3): 430–47. https://doi.org/10.1108/intr-12-2017-0515.
52. Gai, Keke, Meikang Qiu, and Xiaotong Sun. 2018. “A Survey on FinTech.” *Journal of Network and Computer Applications* 103 (February): 262–73. https://doi.org/10.1016/j.jnca.2017.10.011.
53. Ghaffarian, S., F. R. Taghikhah, and H. R. Maier. 2023. “Explainable Artificial Intelligence in Disaster Risk Management: Achievements and Prospective Futures.” *International Journal of Disaster Risk Reduction* 98. Scopus. https://doi.org/10.1016/j.ijdrr.2023.104123.
54. Ghazieh, Louai, and Nadia Chebana. 2021. “The Effectiveness of Risk Management System and Firm Performance in the European Context.” *Journal of Economics, Finance and Administrative Science* 26 (52): 182–96. https://doi.org/10.1108/JEFAS-07-2019-0118.
55. Giacchero, Andrea, and Jacopo Moretti. 2021. “A Possible Holistic Framework to Manage ICT Third-Party Risk in the Age of Cyber Risk.” *Risk Management Magazine* 16 (1): 30–42. https://doi.org/10.47473/2020rmm0082.
56. Globočnik Žunac, A., V. Kordoš, and S. Zlatić. 2019. “RISK MANAGEMENT IN THE PROCESS OF USING THE EXTERNAL SERVICE SUPPLIER.” *Proceedings on Engineering Sciences* 1 (2): 195–202. Scopus. https://doi.org/10.24874/PES01.02.017.
57. Grammarly. 2026. *Grammarly*. Released. https://www.grammarly.com/.
58. Hafver, A., C. Ferreira, C. Agrell, et al. 2021. “On the Meaning of Assurance.” In *Proc. Eur. Saf. Reliab. Conf.*, edited by Castanier B., Cepin M., Bigaud D., and Berenguer C. Research Publishing, Singapore. Scopus. https://doi.org/10.3850/978-981-18-2016-8_465-cd.
59. Hair, Joe F., Matt C. Howard, and Christian Nitzl. 2020. “Assessing Measurement Model Quality in PLS-SEM Using Confirmatory Composite Analysis.” *Journal of Business Research* 109 (March): 101–10. https://doi.org/10.1016/j.jbusres.2019.11.069.
60. Hair, Joe F., Christian M. Ringle, and Marko Sarstedt. 2011. “PLS-SEM: Indeed a Silver Bullet.” *Journal of Marketing Theory and Practice* 19 (2): 139–52. https://doi.org/10.2753/mtp1069-6679190202.
61. Hair, Joseph F., G. Tomas M. Hult, Christian M. Ringle, Marko Sarstedt, Nicholas P. Danks, and Soumya Ray. 2021a. “Evaluation of Reflective Measurement Models.” In *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*, by Joseph F. Hair, G. Tomas M. Hult, Christian M. Ringle, Marko Sarstedt, Nicholas P. Danks, and

Soumya Ray. Classroom Companion: Business. Springer International Publishing. https://doi.org/10.1007/978-3-030-80519-7_4.
62. Hair, Joseph F., G. Tomas M. Hult, Christian M. Ringle, Marko Sarstedt, Nicholas P. Danks, and Soumya Ray. 2021b. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*. Classroom Companion: Business. Springer International Publishing. https://doi.org/10.1007/978-3-030-80519-7.
63. Hampton, C., S. G. Sutton, V. Arnold, and D. Khazanchi. 2021. "Cyber Supply Chain Risk Management: Toward an Understanding of the Antecedents to Demand for Assurance." *Journal of Information Systems* 35 (2): 37–60. WOS:000683742700003, pp. 37–60. Scopus. https://doi.org/10.2308/ISYS-19-050.
64. Han, SQ, JP Ulhoi, and H. Song. 2024. "Digital Trust in Supply Chain Finance: The Role of Innovative Fintech Service Provision." *JOURNAL OF ENTERPRISE INFORMATION MANAGEMENT*, ahead of print, July 26. WOS:001275666300001. Scopus. https://doi.org/10.1108/JEIM-07-2022-0238.
65. Hansen, J. M., G. Saridakis, and V. Benson. 2018. "Risk, Trust, and the Interaction of Perceived Ease of Use and Behavioral Control in Predicting Consumers' Use of Social Media for Transactions." *Computers in Human Behavior* 80: 197–206. Scopus. https://doi.org/10.1016/j.chb.2017.11.010.
66. Herrero, A., and H. San Martín. 2012. "Effects of the Risk Sources and User Involvement on E-Commerce Adoption: Application to Tourist Services." *Journal of Risk Research* 15 (7): 841–55. WOS:000306320800009, pp. 841–55. Scopus. https://doi.org/10.1080/13669877.2012.666758.
67. Hinkin, Timothy R., and J. Bruce Tracey. 1999. "An Analysis of Variance Approach to Content Validation." *Organizational Research Methods* 2 (2): 175–86. https://doi.org/10.1177/109442819922004.
68. ISACA. 2024. "Digital Trust." https://www.isaca.org/digital-trust.
69. Jadwani, B., S. Parkhi, and P. K. Mitra. 2024. "Operational Risk Management in Banks: A Bibliometric Analysis and Opportunities for Future Research." *Journal of Risk and Financial Management* 17 (3). Scopus. https://doi.org/10.3390/jrfm17030095.
70. Jallan, Y., and B. Ashuri. 2020. "Text Mining of the Securities and Exchange Commission Financial Filings of Publicly Traded Construction Firms Using Deep Learning to Identify and Assess Risk." *Journal of Construction Engineering and Management* 146 (12). Scopus. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001932.
71. jamovi. 2026. *The Jamovi Project*. V. 2.7. Released. https://www.jamovi.org.
72. Jantunen, Ari, Hanna-Kaisa Ellonen, and Anette Johansson. 2012. "Beyond Appearances – Do Dynamic Capabilities of Innovative Firms Actually Differ?" *European Management Journal* 30 (2): 141–55. https://doi.org/10.1016/j.emj.2011.10.005.
73. Jelovac, D., C. Ljubojevic, and L. Ljubojevic. 2022. "HPC in Business: The Impact of Corporate Digital Responsibility on Building Digital Trust and Responsible Corporate Digital Governance." *Digital Policy, Regulation and Governance* 24 (6): 485–97. WOS:000663591900001, pp. 485–97. Scopus. https://doi.org/10.1108/DPRG-11-2020-0164.
74. John, N., P. Nwaguru, M. G. D. Okon, U. Tommy, and M. Bariate. 2024. "Managing Materials Vendor Risks for Improved Project Operational Performance: The Role of Risk-Oriented Culture." *Brazilian Journal of Operations and Production Management* 21 (2). WOS:001230623700004. Scopus. https://doi.org/10.14488/BJOPM.1957.2024.
75. Jøsang, Audun, and Stéphane Lo Presti. 2004. "Analysing the Relationship between Risk and Trust." In *Trust Management*, edited by Christian Jensen, Stefan Poslad, and Theo Dimitrakos, vol. 2995, edited by Gerhard Goos, Juris Hartmanis, and Jan Van Leeuwen. Lecture Notes in Computer Science. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-24747-0_11.

76. Kähkönen, A. K., K. Lintukangas, J. Hallikas, and P. Evangelista. 2016. “Responsible Buying Practices in Supply Risk Management.” *International Journal of Integrated Supply Management* 10 (3–4): 309–29. Scopus. https://doi.org/10.1504/IJISM.2016.081282.
77. Katete, G. 2021. “Digital Elections and the Problem of Liquid Trust in the Kenyan Electoral Management Institution.” *INTERNATIONAL JOURNAL OF AFRICAN RENAISSANCE STUDIES* 16 (1): 165–76. WOS:000675086700001, pp. 165–76. Scopus. https://doi.org/10.1080/18186874.2021.1949363.
78. Kayhan, H. 2022. “Ensuring Trust In Pharmaceutical Supply Chains By Data Protection Through A Design Approach To Blockchains.” *Blockchain in Healthcare Today* 5. Scopus. https://doi.org/10.30953/bhty.v5.232.
79. Keskin, O. F., K. M. Caramancion, I. Tatar, O. Raza, and U. Tatar. 2021. “Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports.” *Electronics (Switzerland)* 10 (10). WOS:000654838900001. Scopus. https://doi.org/10.3390/electronics10101168.
80. Kluiters, L., M. Srivastava, and L. Tyll. 2023. “The Impact of Digital Trust on Firm Value and Governance: An Empirical Investigation of US Firms.” *SOCIETY AND BUSINESS REVIEW* 18 (1): 71–103. WOS:000819032800001, pp. 71–103. Scopus. https://doi.org/10.1108/SBR-07-2021-0119.
81. Kobzan, T., A. Biendarra, S. Schriegel, T. Herbst, T. Müller, and J. Jasperneite. 2018. “Utilizing Blockchain Technology in Industrial Manufacturing with the Help of Network Simulation.” *Proc. - IEEE Int. Conf. Industr. Inf., INDIN*, 152–59. WOS:000450180200022, pp. 152–59. Scopus. https://doi.org/10.1109/INDIN.2018.8472011.
82. Korneev, Volodymyr, Oleksandr Dziubliuk, Andriy Tymkiv, Volodymyr Antkiv, and Nataliia Kucherenko. 2023. “Banking Sector Stability and Economic Development: Assessment of Risks and Efficiency.” *Economic Affairs* 68 (3). https://doi.org/10.46852/0424-2513.3.2023.33.
83. Ksibi, S., F. Jaidi, and A. Bouhoula. 2023. “A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach.” *Proc. Int. Conf. Syst. Syst. Eng.: Socio-Tech. Perspec., SoSE* 28 (1): 107–27. Scopus. https://doi.org/10.1007/s11036-022-02042-1.
84. Larsen, M. H., M. S. Lund, and F. B. Bjørneseth. 2022. “A Model of Factors Influencing Deck Officers’ Cyber Risk Perception in Offshore Operations.” *Maritime Transport Research* 3. WOS:001027914500010. Scopus. https://doi.org/10.1016/j.martra.2022.100065.
85. “Latvijas Banka.” n.d. Accessed June 15, 2025. https://www.bank.lv/.
86. Lau, A. K. W., P. K. C. Lee, and T. C. E. Cheng. 2024. “The Relationships between Ethical Codes of Conduct, Ethical Supplier Risks, and Financial Performance: A Buyer-Supplier Perspective.” *Production Planning and Control*, ahead of print. Scopus. https://doi.org/10.1080/09537287.2024.2359547.
87. Leite, M. S. A., F. P. Arantes, A. C. Bornia, L. M. F. e Silva, K. V. D. Santos, and J. F. R. Júnior. 2024. “A New Tool for Evaluating Supply Risk Management.” *Production* 34. Scopus. https://doi.org/10.1590/0103-6513.20240005.
88. Levine, L. 2019. “Digital Trust and Cooperation with an Integrative Digital Social Contract.” *JOURNAL OF BUSINESS ETHICS* 160 (2): 393–407. WOS:000497511200006, pp. 393–407. Scopus. https://doi.org/10.1007/s10551-019-04201-z.
89. Lewis, J. David, and Andrew Weigert. 1985. “Trust as a Social Reality.” *Social Forces* 63 (4): 967. https://doi.org/10.2307/2578601.
90. “Lietuvos Bankas.” n.d. Accessed June 15, 2025. https://www.lb.lt/.

91. Lockamy, III A. 2011. “Benchmarking Supplier Risks Using Bayesian Networks.” *Benchmarking* 18 (3): 409–27. Scopus. https://doi.org/10.1108/14635771111137787.
92. Loh, HS, JL Lee, YM Gu, HS Chen, and HL Tay. 2024. “The Effects of Digital Platforms on Customers’ Satisfaction in International Shipping Business.” *REVIEW OF INTERNATIONAL BUSINESS AND STRATEGY* 34 (2): 231–44. WOS:001144154300001, pp. 231–44. Scopus. https://doi.org/10.1108/RIBS-07-2023-0072.
93. Luther, Benjamin, Indra Gunawan, and Nam Nguyen. 2023. “Identifying Effective Risk Management Frameworks for Complex Socio-Technical Systems.” *Safety Science* 158 (February): 105989. https://doi.org/10.1016/j.ssci.2022.105989.
94. Marsh, Stephen. 1994. “Formalising Trust as a Computational Concept.” PhD, University of Stirling.
95. Mascha, M. F., C. L. Miller, and D. J. Janvrin. 2011. “The Effect of Encryption on Internet Purchase Intent in Multiple Vendor and Product Risk Settings.” *Electronic Commerce Research* 11 (4): 401–19. WOS:000296473300003, pp. 401–19. Scopus. https://doi.org/10.1007/s10660-011-9080-6.
96. Mathew, S. K., and M. D. Aundhe. 2011. “Identifying Vendor Risks In Remote Infrastructure Management Services.” *Journal of Information Technology Case and Application Research* 13 (4): 32–50. Scopus. https://doi.org/10.1080/15228053.2011.10856216.
97. Mavlutova, Inese, Aivars Spilbergs, Atis Verdenhofs, Andris Natrins, Ilja Arefjevs, and Tatjana Volkova. 2022. “Digital Transformation as a Driver of the Financial Sector Sustainable Development: An Impact on Financial Inclusion and Operational Efficiency.” *Sustainability* 15 (1): 207. https://doi.org/10.3390/su15010207.
98. Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. “An Integrative Model of Organizational Trust.” *The Academy of Management Review* 20 (3): 709. https://doi.org/10.2307/258792.
99. McInnis, B., D. Cosley, C. Nam, and G. Leshed. 2016. “Taking a Hit: Designing around Rejection, Mistrust, Risk, and Workers’ Experiences in Amazon Mechanical Turk.” *Conf Hum Fact Comput Syst Proc*, 2271–82. WOS:000380532902027, pp. 2271–82. Scopus. https://doi.org/10.1145/2858036.2858539.
100. Mclain, David L., and Katarina Hackman. 1999. “Trust, Risk, and Decision-Making in Organizational Change.” *Public Administration Quarterly* 23 (2): 152–76.
101. Minh Sang, Nguyen. 2024. “Evolution and Future Directions of Banking Risk Management Research: A Bibliometric Analysis.” *Banks and Bank Systems* 19 (2): 1–14. https://doi.org/10.21511/bbs.19(2).2024.01.
102. Mo, Z., Y. Liu, C. Lu, and J. Yu. 2023. “Influences of Industrial Internet Platform Firms’ ESG Performance and Digital Leadership on User Firms’ Innovation Performance: The Mediating Role of Inter-Firm Trust.” *Journal of Digital Economy* 2: 204–20. Scopus. https://doi.org/10.1016/j.jdec.2024.01.002.
103. Mohlmann, M. 2021. “Unjustified Trust Beliefs: Trust Conflation on Sharing Economy Platforms.” *RESEARCH POLICY* 50 (3). WOS:000609875700003. Scopus. https://doi.org/10.1016/j.respol.2020.104173.
104. Mohta, Y., U. Singh, and A. Arya. 2024. “NLP-Enabled Bot for Managing Third-Party Risk.” In *Proc. - Int. Conf. Comput. Intell. Comput. Appl., ICCICA*, edited by Gupta S.C., Gandhi A.B., Mehla S., and Lakhina U. Institute of Electrical and Electronics Engineers Inc. Scopus. https://doi.org/10.1109/ICCICA60014.2024.10584983.
105. Mollazehi, A., I. Abuelezz, M. Barhamgi, K. M. Khan, and R. Ali. 2024. “Do Cialdini’s Persuasion Principles Still Influence Trust and Risk-Taking When Social Engineering Is Knowingly Possible?” In *Lect. Notes Bus. Inf. Process.*, edited by Araújo J., de la Vara J.L., Santos M.Y., and Assar S., vol. 513. Springer Science and Business Media Deutschland GmbH. Scopus. https://doi.org/10.1007/978-3-031-59465-6_17.

106. Monev, V. 2021. “The ‘Self-Assessment’ Method within a Mature Third-Party Risk Management Process in the Context of Information Security.” Paper presented at 2021 35th International Conference on Information Technologies, InfoTech 2021 - Proceedings. *Int. Conf. Inf. Technol., InfoTech - Proc.* Scopus. https://doi.org/10.1109/InfoTech52438.2021.9548373.
107. Mubarak, MF, M. Ghobakhloo, R. Evans, G. Jucevicius, SA Prestianawati, and M. Mubarik. 2024. “Metaverse Adoption in the Manufacturing Industry: Impact on Social and Environmental Sustainability Performance.” *ASIA-PACIFIC JOURNAL OF BUSINESS ADMINISTRATION*, ahead of print, September 4. WOS:001303367100001. Scopus. https://doi.org/10.1108/APJBA-02-2024-0043.
108. Mubarak, MF, and M. Petraite. 2020. “Industry 4.0 Technologies, Digital Trust and Technological Orientation: What Matters in Open Innovation?” *TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE* 161 (December): 120332. WOS:000598794000009, p. 120332. Scopus. https://doi.org/10.1016/j.techfore.2020.120332.
109. Natovich, J. 2003. “Vendor Related Risks in IT Development: A Chronology of an Outsourced Project Failure.” *Technology Analysis and Strategic Management* 15 (4): 409–19. Scopus. https://doi.org/10.1080/0953732030001360 15.
110. Ncontracts. 2025. *Ncontracts 2025 Third-Party Risk Management Survey*.
111. Neumannová, A., E. W. N. Bernroider, and C. Elshuber. 2023. “The Digital Operational Resilience Act for Financial Services: A Comparative Gap Analysis and Literature Review.” In *Vienna University of Economics & Business*, edited by Papadaki M., Rupino da Cunha P., Themistocleous M., and Christodoulou K., 464 LNBIP. Springer Science and Business Media Deutschland GmbH. WOS:001308340700040, pp. 570–85. Scopus. https://doi.org/10.1007/978-3-031-30694-5_40.
112. OpenAI. 2026. *ChatGPT: An AI Language Model*. Released. https://chatgpt.com/.
113. Operational Riskdata eXchange Association. 2025. *Top Risk Review H1 2025*. https://orx.org/resource/top-risk-review-h1-2025.
114. Oudina, Z., M. Derdour, A. Dib, and M. A. Yaakoubi. 2024. “Identifying and Addressing Trust Concerns in Cyber-Physical Systems for the Oil and Gas Industry.” *Ingenierie Des Systemes d’Information* 29 (2): 469–78. Scopus. https://doi.org/10.18280/isi.290208.
115. Oukarfi, S., and H. Sattar. 2020. “Asymmetric Information and E-Tourism: Literature Review.” In *Adv. Intell. Sys. Comput.*, edited by Y. Bi, R. Bhatia, and S. Kapoor, vol. 1037. Springer Verlag. WOS:000637312900093, pp. 1263–74. Scopus. https://doi.org/10.1007/978-3-030-29516-5_93.
116. Page, Matthew J., Joanne E. McKenzie, Patrick M. Bossuyt, et al. 2021. “The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews.” *Systematic Reviews* 10 (1): 89. https://doi.org/10.1186/s13643-021-01626-4.
117. Papic, A., KK Radoja, and D. Szombathelyi. 2022. “CYBER SECURITY AWARENESS OF CROATIAN STUDENTS AND THE PERSONAL DATA PROTECTION.” In *University of JJ Strossmayer Osijek*, edited by ML Simic. WOS:000838669300039.
118. Pappas, N. 2017. “Risks and Marketing in Online Transactions: A Qualitative Comparative Analysis.” *Current Issues in Tourism* 20 (8): 852–68. Scopus. https://doi.org/10.1080/13683500.2016.1187586.
119. Piccininni, M., JL Rohmann, G. Logroscino, and T. Kurth. 2020. “Blockchain-Based Innovations for Population-Based Registries for Rare Neurodegenerative Diseases.” *FRONTIERS IN BLOCKCHAIN* 3 (May). WOS:000678829900001. Scopus. https://doi.org/10.3389/fbloc.2020.00020.

120. Pietrzak, P., and J. Takala. 2021. “Digital Trust– Asystematic Literature Review.” *Forum Scientiae Oeconomia* 9 (3): 59–71. Scopus. https://doi.org/10.23762/FSO_VOL9_NO3_4.
121. Pivavarava, AV, and C. Koop. 2024. “Digital Practices for Consumer E-Participation in Economic Regulation and the Role of Organisational Capacity.” *JOURNAL OF EUROPEAN PUBLIC POLICY*, ahead of print, June 21. WOS:001257054700001. Scopus. https://doi.org/10.1080/13501763.2024.2367065.
122. Podsakoff, Philip M., Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.” *Journal of Applied Psychology* 88 (5): 879–903. https://doi.org/10.1037/0021-9010.88.5.879.
123. Podsakoff, Philip M., Scott B. MacKenzie, and Nathan P. Podsakoff. 2016. “Recommendations for Creating Better Concept Definitions in the Organizational, Behavioral, and Social Sciences.” *Organizational Research Methods* 19 (2): 159–203. https://doi.org/10.1177/1094428115624965.
124. Puncreobutr, V., and B. Puncreobutr. 2024. “Risk Management of Universities in the Age of Digital Disruption.” *ST THERESA JOURNAL OF HUMANITIES AND SOCIAL SCIENCES* 10 (1): 162–75. WOS:001231132400003.
125. Putri, NR, E. Yuliati, KB Mulyono, YA Rahman, and DP Astuti. 2022. “The Effect of Perceived Risk on Customer’s Behavioral Intention of Digital Gold Platform: The Moderating Role of Trust.” Paper presented at ICE-BEES 2021. *University of Indonesia*. WOS:001186728800095. https://doi.org/10.4108/eai.27-7-2021.2316918.
126. PwC. 2024. “Digital Trust and Cybersecurity.” https://www.pwc.com/my/en/services/digital/digital-trust-and-cybersecurity.html.
127. Ramasubramaniam, V., and A. K. Singh. 2020. “Addressing Key Pain Points to Develop a Mature Third-Party Risk Management Program.” *ISACA Journal* 3: 46–52. Scopus.
128. Rane, T., and JW Huang. 2022. “Blockchain-Based Digital Trust Mechanism: A Use Case of Cloud Manufacturing of LDS Syringes for COVID-19 Vaccination.” *Journal of Integrated Design and Process Science* 26 (2): 103–29. WOS:000939719400001, pp. 103–29. Scopus. https://doi.org/10.3233/JID-210021.
129. Ray, B. K., S. Tao, A. Olkhovets, and D. Subramanian. 2013. “A Decision Analysis Approach to Financial Risk Management in Strategic Outsourcing Contracts.” *EURO Journal on Decision Processes* 1 (3–4): 187–203. Scopus. https://doi.org/10.1007/s40070-013-0013-6.
130. Research and Markets. n.d. “Financial Services Market Report 2025.” Accessed November 6, 2025. https://www.researchandmarkets.com/reports/5939673/financial-services-market-report.
131. Ringle, C. Christian M., Sven Wende, and Jean-Michael Becker. 2025. *SmartPLS*. V. 4.1.1.4. Released June 18. https://www.smartpls.com.
132. Rousseau, Denise M., Sim B. Sitkin, Ronald S. Burt, and Colin Camerer. 1998. “Not So Different After All: A Cross-Discipline View Of Trust.” *Academy of Management Review* 23 (3): 393–404. https://doi.org/10.5465/amr.1998.926617.
133. Roy, V., D. Desjardins, C. Fertel, and C. Ouellet-Plamondon. 2022. “Methodology for Conducting Third-Party Risk-Based Due Diligence in the Construction and Civil Engineering Industry.” *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction* 14 (4). WOS:000853929300007. Scopus. https://doi.org/10.1061/(ASCE)LA.1943-4170.0000553.
134. Rychkova, I., and M. Ghriba. 2023. “Trustworthiness Requirements in Information Systems Design: Lessons Learned from the Blockchain Community.” *Complex Systems Informatics and Modeling Quarterly* 2023 (35): 67–91. Scopus. https://doi.org/10.7250/csimq.2023-35.03.

135. San Martín, S., and C. Camarero. 2009. “How Perceived Risk Affects Online Buying.” *Online Information Review* 33 (4): 629–54. WOS:000270768100001, pp. 629–54. Scopus. https://doi.org/10.1108/14684520910985657.
136. Sattar, H., M. Elatrachi, and S. Oukarfi. 2022. “Information Asymmetry and E-Tourism: An Empirical Study in Morocco.” In *Lect. Notes Networks Syst.*, edited by Arai K., 438 LNNS. Springer Science and Business Media Deutschland GmbH. Scopus. https://doi.org/10.1007/978-3-030-98012-2_11.
137. Schelegia, E. P., and T. Fleşer. 2021. “Automated Supplier Risk Evaluation System.” In *J. Phys. Conf. Ser.*, edited by Sandu A.V., Abdullah M.M.A.B., Vizureanu P., Nabialek M., Ghazali C.M.R., and Sandu I., vol. 1960. no. 1. IOP Publishing Ltd. Scopus. https://doi.org/10.1088/1742-6596/1960/1/012003.
138. Sell, Jane. 2018. “Definitions and the Development of Theory in Social Psychology.” *Social Psychology Quarterly* 81 (1): 8–22. https://doi.org/10.1177/0190272518755335.
139. Setty, E. 2018. “Young People’s Attributions of Privacy Rights and Obligations in Digital Sexting Culture.” *International Journal of Communication* 12: 4533–52. Scopus.
140. Sharma, V., R. Agrawal, and VK Manupati. 2024. “Blockchain Technology as an Enabler for Digital Trust in Supply Chain: Evolution, Issues and Opportunities.” *INTERNATIONAL JOURNAL OF SYSTEM ASSURANCE ENGINEERING AND MANAGEMENT*, ahead of print, August 15. WOS:001291219800001. https://doi.org/10.1007/s13198-024-02471-z.
141. Shaytura, S. V., L. A. Olenev, A. A. Nedelkin, A. M. Minitaeva, K. V. Ordov, and V. M. Feoktistova. 2021. “Blockchain in Technogenic Safety and Risk Management.” *International Journal of Emerging Technology and Advanced Engineering* 11 (12): 72–78. Scopus. https://doi.org/10.46338/ijetae1221_08.
142. Slovic, Paul. 1993. “Perceived Risk, Trust, and Democracy.” *Risk Analysis* 13 (6): 675–82. https://doi.org/10.1111/j.1539-6924.1993.tb01329.x.
143. Spence, Michael. 1973. “Job Market Signaling.” *The Quarterly Journal of Economics* 87 (3): 355. https://doi.org/10.2307/1882010.
144. Spitzer, Kai Gereon, and Maja Sabol. 2025. “European System of Financial Supervision.” April. https://www.europarl.europa.eu/factsheets/en/sheet/84/european-system-of-financial-supervision-esfs-.
145. Sun, Q., M. Gibbert, T. T. Hills, and E. Nowak. 2016. “Are Financial Advisors Money Doctors or Charlatans? Evidence on Trust, Advice, and Risk Taking in Delegated Asset Management.” In *Proc. Annu. Meet. Cogn. Sci. Soc., CogSci*, edited by Papafragou A., Grodner D., Mirman D., and Trueswell J.C. The Cognitive Science Society. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139186557&partnerID=40&md5=bc9e52309734c3317c9571925c412f27.
146. SupplyWisdom. 2025. *Risk Management in a Technology-Driven World*. https://21542732.fs1.hubspotusercontent-na1.net/hubfs/21542732/-%20Sales%20Enablement%20Folder%202024/Supply%20Wisdom%20-%20Survey%20Results%202024%20-%20Risk%20Management%20in%20a%20Technology%20Driven%20World.pdf?__hstc=74024525.95a6eeb7a25b38614c71e7ddd887b51c.1725040239177.1725040239177.1725393336780.2&__hssc=74024525.1.1725393336780&__hsfp=3801953514&__hstc=74024525.359d31a35439a9a1e448ca734a5cb619.1701879591866.1719511920188.1719525418069.227&__hssc=74024525.1.1719525418069&__hsfp=3530606189&submissionGuid=2279a213-57d0-4615-847f-5d5cead256ad.
147. Svenson, F., M. Peuser, F. Çetin, D. C. Aidoo, and M. A. Launer. 2024. “Decision-Making Styles and Trust across Farmers and Bankers: Global Survey Results.” *Decision Analytics Journal* 10. Scopus. https://doi.org/10.1016/j.dajour.2024.100427.

148. Tainyi, L., C. H. Chen, and H. P. Lu. 2009. “Fixed Income Investors on the Acceptance of E-Commerce: An Empirical Study.” *Int. Conf. Inf. Sci. Eng., ICISE*, 2932–35. Scopus. https://doi.org/10.1109/ICISE.2009.597.
149. Teece, David J., Gary Pisano, and Amy Shuen. 1997. “Dynamic Capabilities and Strategic Management.” *Strategic Management Journal* 18 (7): 509–33. https://doi.org/10.1002/(SICI)1097-0266(199708)18:7%253C509::AID-SMJ882%253E3.0.CO;2-Z.
150. Tehrani, P. F., N. von Kalckreuth, and S. Lamprecht. 2020. “Toward an Integrative Model of Trust for Digital Emergency Communication.” In *Proc. Int. ISCRAM Conf.*, edited by Hughes A.L., McNeill F., and Zobel C.W., vols. 2020-May. Information Systems for Crisis Response and Management, ISCRAM. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118609002&partnerID=40&md5=b95f1d5c7b359a237c0d458392574811.
151. Terry Morris, A., J. M. Maddalon, and P. S. Miner. 2020. “On the Moral Hazard of Autonomy.” *AIAA IEEE Dig Avionics Syst Conf Proc* 2020-October. Scopus. https://doi.org/10.1109/DASC50938.2020.9256682.
152. Tunkevichus, EO, and VA Rebiazina. 2021. “CONSUMER DIGITAL TRUST: THE MAIN TRENDS AND RESEARCH DIRECTIONS.” *ROSSIISKII ZHURNAL MENEDZHMENTA-RUSSIAN MANAGEMENT JOURNAL* 19 (4): 429–50. WOS:001124544200003. https://doi.org/10.21638/spbu18.2021.403.
153. Urbano, Joana, Ana Paula Rocha, and Eugénio Oliveira. 2013. “A Socio-Cognitive Perspective of Trust.” In *Agreement Technologies*, edited by Sascha Ossowski, vol. 8. Law, Governance and Technology Series. Springer Netherlands. https://doi.org/10.1007/978-94-007-5583-3_23.
154. Vashisht, Shailja, Mahesh Sarva, and Hardeep Singh Mundi. 2022. “Risks Measurement in Banking: A Bibliometric and Content Analysis.” *International Social Science Journal* 72 (246): 955–77. https://doi.org/10.1111/issj.12371.
155. Venkatesh, Morris, Davis, and Davis. 2003. “User Acceptance of Information Technology: Toward a Unified View.” *MIS Quarterly* 27 (3): 425. https://doi.org/10.2307/30036540.
156. Venkatesh, Thong, and Xu. 2012. “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology.” *MIS Quarterly* 36 (1): 157. https://doi.org/10.2307/41410412.
157. Vidiasova, Lyudmila, Iaroslava Tensina, and Elena Bershadskaya. 2020. “Cyber-Social Trust in Different Spheres: An Empirical Study in Saint-Petersburg.” In *Digital Transformation and Global Society*, edited by Daniel A. Alexandrov, Alexander V. Boukhanovsky, Andrei V. Chugunov, Yury Kabanov, Olessia Koltsova, and Ilya Musabirov, vol. 1242. Communications in Computer and Information Science. Springer International Publishing. https://doi.org/10.1007/978-3-030-65218-0_1.
158. VOSviewer (VOSviewer). 2024. “VOSviewer.” https://www.vosviewer.com//.
159. Windelberg, M. 2016. “Objectives for Managing Cyber Supply Chain Risk.” *International Journal of Critical Infrastructure Protection* 12: 4–11. Scopus. https://doi.org/10.1016/j.ijcip.2015.11.003.
160. World Economic Forum. 2024. “Earning Digital Trust.” March 25. https://initiatives.weforum.org/digital-trust/earning-trust.
161. Wu, Guohua, Xiaorui Hu, and Yuhong Wu. 2010. “Effects of Perceived Interactivity, Perceived Web Assurance and Disposition to Trust on Initial Online Trust.” *Journal of Computer-Mediated Communication* 16 (1): 1–26. https://doi.org/10.1111/j.1083-6101.2010.01528.x.
162. Yuan, D., T. Lu, X. Yang, and L. Yan. 2010. “A Theory Analysis and Model Research on E-Commerce Credit Risk Management.” *Proc. Int. Conf. E-Bus. E-Gov., ICEE*, 2006–9. Scopus. https://doi.org/10.1109/ICEE.2010.507.

163. Zhang, Y., Z. Zhang, and J. Ren. 2016. “Transform Farming with the Help of Social Media a Pioneering Chinese Community Supported Agriculture (CSA) Farm and Its Micro Blog Usage.” Paper presented at Pacific Asia Conference on Information Systems, PACIS 2016 - Proceedings. *Pac. Asia Conf. Inf. Syst., PACIS - Proc.* Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85011022648&partnerID=40&md5=a2371fee33eff1d4fb8b91ea1403d001.
164. Zhghenti, T., and V. Chkareuli. 2021. “ENHANCING ONLINE BUSINESS SECTOR: DIGITAL TRUST FORMATION PROCESS.” *MARKETING AND MANAGEMENT OF INNOVATIONS*, no. 2: 87–93. WOS:000667238800007. https://doi.org/10.21272/mmi.2021.2-07.
165. Zhou, R., T. H. Bhuiyan, H. R. Medal, M. D. Sherwin, and D. Yang. 2022. “A Stochastic Programming Model with Endogenous Uncertainty for Selecting Supplier Development Programs to Proactively Mitigate Supplier Risk.” *OMEGA-INTERNATIONAL JOURNAL OF MANAGEMENT SCIENCE* 107 (February). WOS:000745846200005. Scopus. https://doi.org/10.1016/j.omega.2021.102542.
166. Zolfaghari, A., K. Thomas-Francois, and S. Somogyi. 2023. “Consumer Adoption of Digital Grocery Shopping: What Is the Impact of Consumer’s Prior-to-Use Knowledge?” *British Food Journal* 125 (4): 1355–73. Scopus. https://doi.org/10.1108/BFJ-02-2022-0187.