



**UNIVERSITY  
OF LATVIA**

**FACULTY OF BUSINESS, ECONOMICS AND MANAGEMENT**

**ANTONINA MACKEVIČA**

**INCORPORATION OF RISK  
MANAGEMENT BEST PRACTICES INTO THE  
SECTOR OF EDUCATION**

**DOCTORAL THESIS**

Submitted for the Scientific Doctor's Degree (Ph.D.) in Social Sciences

Supervisor: Dr.oec., prof. Andrejs Geske

Riga, 2023

## TABLE OF CONTENTS

LIST OF ABBREVIATIONS .....	4
LIST OF FIGURES .....	6
LIST OF TABLES .....	7
ABSTRACT .....	8
INTRODUCTION.....	9
1. THEORETICAL APPROACH TO RISK MANAGEMENT.....	17
1.1. RISK CONCEPT AND DEFINITIONS.....	17
1.2. STAKEHOLDERS .....	18
1.3. WHO IS RESPONSIBLE FOR RISK MANAGEMENT? .....	20
1.4. KEY PILLARS OF SUCCESSFUL RISK MANAGEMENT .....	21
1.5. SUMMARY .....	51
2. RISKS IN THE SECTOR OF EDUCATION .....	53
2.1 PSYCHOSOCIAL RISK GROUP .....	53
2.2 INFORMATION SECURITY, CYBER AND PERSONAL DATA PROTECTION RISK GROUP .....	56
2.3 CORRUPTION RISK .....	63
2.4 LEGAL RISKS .....	64
2.5 EXTERNAL RISKS.....	65
2.6 REPUTATIONAL, RESILIENCE AND BUSINESS CONTINUITY RISKS .....	65
2.7 LIMITATIONS OF RISK MANAGEMENT .....	66
2.8 EFFECTIVE RISK MANAGEMENT PROGRAMME .....	68
2.9 SUMMARY .....	70
3. EMPIRICAL RESEARCH ON THE MANAGEMENT OF RISKS IN THE EDUCATIONAL SECTOR ...	72
3.1 METHODOLOGY AND ORGANISATION OF RESEARCH .....	72
3.2 RISK MANAGEMENT EFFECTIVENESS IN LATVIAN EDUCATIONAL INSTITUTIONS.....	78
3.3 INCIDENT REPORTING AND MANAGEMENT PRACTICES IN THE EDUCATIONAL INSTITUTIONS OF LATVIA ...	81
3.4 RISK ASSESSMENT.....	82
3.5 RISK ASSESSMENT ANALYSIS BY RISK GROUPS.....	87
3.6 RESPONSIBILITY FOR RISK MANAGEMENT WITHIN THE SECTOR OF EDUCATION .....	101
3.7 IMPROVING RISK MANAGEMENT PRACTICES IN THE SECTOR OF EDUCATION .....	102
3.8 INSURANCE.....	107

3.9 SUMMARY ON SURVEY 1 RESULTS.....	108
3.10 SURVEY 2 RESULTS .....	111
3.11 SUMMARY ON SURVEY 2 RESULTS.....	124
3.12 INTERVIEWS WITH RISK MANAGEMENT EXPERTS .....	125
3.13 SUMMARY OF INTERVIEWS WITH EXPERTS.....	131
CONCLUSION .....	133
RECOMMENDATIONS .....	138
REFERENCES.....	141
APPENDIX 1: RISK MANAGEMENT PLAN.....	161
APPENDIX 2: RISK ASSESSMENT REGISTER .....	162
APPENDIX 3: INCIDENT REGISTER .....	163
APPENDIX 4: RISK TAXONOMY.....	164
APPENDIX 5: BUSINESS CONTINUITY PLAN .....	169
APPENDIX 6: EMPIRICAL RESEARCH SURVEY 1 .....	170
APPENDIX 7: EMPIRICAL RESEARCH SURVEY 2.....	174

## **LIST OF ABBREVIATIONS**

BCBS	Basel Committee for Banking Supervision
BTA	Bow-Tie Analysis
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EBA	European Banking Authority
EU	European Union
FSA	Financial Services Authorities
GDPR	General Data Protection Regulation
IRM	The Institute for Risk Management
KCI	Key Control Indicators
KPI	Key Performance Indicators
KRI	Key Risk Indicators
LDA	Loss Distribution Approach
PDCA	“Plan-Do-Check-Act” cycles
RCSA	Risk and Control Self-Assessment
STAMP	Systems-Theoretic Accident Model and Processes

## LIST OF TERMS AND DEFINITIONS

- Risk** - the effect of uncertainty of objectives resulting in negative events, incidents and accidents.
- Risk management** – a set of technical, organizational, legal methods and measures aimed at reducing the probability and consequences of adverse events.
- Risk taxonomy** – comprehensive structure of categories of risk types.
- Risk coordinator ('risk champion')** – a person who has skills, competencies and authority to drive the risk management process, but who is not the risk owner.
- Accepted level of risk ('risk appetite')** - the amount of risk that the organisation is willing to take in pursuit of its strategic objectives. It is the level of risk that can be accepted without any additional risk prevention or mitigation actions.
- Risk culture** – the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose.
- Incident** - is the materialisation of a risk. It is defined by multiple authors as an event that is different from regularly followed routine due to failure in process or IT systems, human factor errors or external environment caused situations
- Key Risk Indicator (KRI)** – measures designed to monitor changes in the levels of risk exposure and contribute to the early warning signs that enable organisations to report risks, prevent crises and mitigate them in time.
- Operational risk** - is defined by the BCBS as the probability of loss from the actions of people (human errors, lack of confidence, internal fraud, etc.), deficiencies in processes (process gaps, lack of documented processes, lack of controls in processes), system downtimes (system bugs and errors, system's out-of-service, etc.) or external events (weather conditions, vendor behaviour, crisis, etc.).

## LIST OF FIGURES

Figure 1.1: Risk heatmap matrix example

Figure 1.2: Bow-tie tool's illustration

Figure 2.1: Risk management cycle

Figure 2.2: Driver question and range of responses example

Figure 3.1: Geographical representation of respondents who participated in the research

Figure 3.2: Break-down of respondents by their belonging to certain types of educational institutions in Survey 1

Figure 3.3: Break-down of respondents by their belonging to certain types of educational institutions in Survey 2

Figure 3.4: Break-down of respondents by their job role and position in Survey 1

Figure 3.5: Break-down of respondents by their job role and position in Survey 2

Figure 3.6: Risk effectiveness ratings by respondents

Figure 3.7 Risk effectiveness rated for different types of educational institutions

Figure 3.8 Incident reporting in educational institutions of Latvia

Figure 3.9 Risk assessment results derived by the research

Figure 3.10 Comparison of Criticality of risk and Risk control scores for psychosocial risks

Figure 3.11 Comparison of Criticality of risk and Risk control scores for IT and Information Security risks

Figure 3.12 Comparison of Criticality of risk and Risk control scores for External risks

Figure 3.13 Comparison of Criticality of risk and Risk control scores for Reputational risks

Figure 3.14: Distribution of respondent answers on question in Survey 1 "Who, in your view, should be responsible for the risk management in an educational institution?" (n=140)

Figure 3.15 Distribution of answers on question "What in your opinion is needed to better manage risks in the sector of education?"

Figure 3.16 Distribution of respondent answers whether their institution makes use of insurance

Figure 3.17 Interrelation of the top 6 risks as per Survey 2 results

Figure 3.18 Key consequences caused by the top risks

## LIST OF TABLES

Table 1.1 Risk mapping according to sources of risks and relevant stakeholders
Table 1.2: Examples of cause categories on levels 1-2. Source: Chapelle (2019)
Table 1.3: Risk assessment methodology example
Table 1.4: Risk assessment methodology example
Table 1.5. Incident reporting form example
Table 1.6: Categories of key risk indicators with examples
Table 1.7: Key risk indicator threshold examples
Table 1.8: KRI examples
Table 1.9: Steps for Key risk indicators
Table 2.1: KRI examples for Information Security. Source: Chapelle (2019)
Table 3.1 Measurement of risk management effectiveness by type of educational institution
Table 3.2 Risk rating scale methodology in empirical research questionnaire
Table 3.3 Descriptive statistics for “Criticality of risks” responses
Table 3.4 Independent Samples Test for “Criticality of risks” responses split by groups
Table 3.5 Descriptive statistics for “Effectiveness of risk management” responses
Table 3.6 Independent Samples Test for “Effectiveness of risk management” responses
Table 3.7: Correlation of “Inability to meet employment law requirements, poor work environment” risk with other risks
Table 3.8: Correlation of “Insufficient level of education quality provided” risk
Table 3.9: Correlation of “Closure of educational institution for any reason” with other risks
Table 3.10: Key consequences caused by the top risks
Table 3.11 Mitigation actions suggested by respondents of Survey 2 to manage the top risk
Tables 3.12 – 3.16 Interview results with experts in risk management
Table 4.1 Risk management plan for educational institutions
Table 5.1 Risk assessment register’s example
Table 6.1 Incident register’s example
Table 7.1 Registry of risks, causes and examples of mitigation actions for educational sector
Table 8.1 Example of Business Continuity and Resiliency Plan

## **ABSTRACT**

Risk management is gaining acknowledgement in organisational management due to the benefits it brings with it, such as ability of managers to forecast possible threats and plan the most appropriate prevention measures. Vulnerabilities and risks in the educational sector affect policy makers, education providers and education receivers. Weak risk management increases the likelihood of misaligned priorities, poor service delivery and financial losses. Risk management is crucial part of effective management of education, provision of qualitative educational services and fair distribution of financing in education. However, in Latvia this topic is only starting to gain attention of regulators and managers in the educational sector.

Psychosocial risk group is one of the largest risk group types for the sector of education and is related to the aspects of staff over-burning, lack of employee motivation, health problems due to stress, etc. Empirical research carried out in Latvia has shown that the top risks perceived by the education sector professionals in Latvia are relating to the psychosocial risks group.

The aim of this research is to analyse common risk management practices and tools in order to draw recommendations on incorporation of the risk management best practices into the management of education taking into consideration the specifics and needs of the educational sector in Latvia.

This research is based on analysis of existing worldwide research on risks and risk management practices within the educational sector and empirical study by way of questioning representatives of the sector of education in Latvia. Upon the results of the research, recommendations for risk management within the educational sector in Latvia will be drawn.

*Keywords: education, educational sector, risks, risk management, quality of education*



## INTRODUCTION

### **Research problem and the significance of the research**

Taleb (2020) in his famous work “The Black Swan” states, that the history is formed by unexpected anomalous events with high impact. The accent is placed on the words “unexpected” and “high impact”. The logic of the Black Swan event makes the unknown more important than the known, because the unknown shapes the history. The author of “The Black Swan” argues that historic events are retrospectively predicted, but before they have happened, no one could imagine such events within perspective predictions. Examples of the Black Swan events are the World War II, drowning of the “Titanic”, the Russian financial default, the September 11<sup>th</sup> bombing of New York World Trade Centre, the 2008 global Credit Crisis, the 2020 Coronavirus pandemic crisis worldwide, and so on. All these events were not predicted neither expected and all of them shaped the history, having great impact on history and society. Taleb (2020) offers as an experiment, to imagine that on September 10<sup>th</sup>, 2001 (day before the September 11<sup>th</sup> bombings) some impactful and risk averse lawmakers, following a consultation with risk managers, enforce a mandatory requirement to get all pilot cabins of airplanes to be equipped with bullet-proof doors to prevent terrorist attacks of airplanes to protect the World Trade Centre of New York. As a result of such law enforcement, the bombing of September 11<sup>th</sup> may not happen at all and society would significantly undervalue such requirement, airplane companies would complain that this is useless and expensive requirement and the lawmaker, who enforced such law, would be very unpopular. This is all due to human nature to underestimate unexpected risks and the unexpected events, what forms the essence of risk management (Taleb, 2020).

Rapid changes caused by globalization, IT advancements, changing demand perspectives and even the competition affect educational sector seamlessly. The World Bank in 2019 published a report “The changing nature of work” (World Bank, 2019), where the changes caused by technological advancements and globalisation have been analysed on the perspective of changing business environment, work and societies, however, there are no public strategic documents or risk assessments available in Latvia how the sector of education shall evolve in order to meet these challenges posed by the technical progress. Vulnerabilities and risks in the educational sector affect policy makers, education providers and education receivers and raise a fertile ground for negative unexpected events (Asian Development Bank, 2010; The Institute of Risk Management, 2002; The Institute of Risk Management, 2010). Weak risk management increases the likelihood of misaligned priorities, resource leakages, and poor service delivery. Effective risk management improves

strategic decision-making and increases availability of qualitative and fair education (Asian Development Bank [ADB, 2010; ADB, 2016; IRM, 2002; IRM, 2010).

The Covid-19 pandemic has provided an evidence of operational readiness in different sectors. For example, while in banking sector operations were stable from the start of the pandemic and decisions were taken fairly quickly (Kurens, 2020; De Bolle, Faye, 2021), the sector of education stagnated with lack of operating strategy for providing educational services during the lockdown (Hačatrjana, 2021; Blass, 2021; TVNET/LETA, 2020; Vaduguns, 2021). This is mainly due to the difference in regulatory requirements for the banking sector, where business continuity planning is a mandatory annual exercise, during which banks are required to simulate different risk scenarios and plan for operational continuity under any circumstances (Latvijas Banka, 2013; The Business Continuity Institute, 2016; Tedesco, Ing, 2021; Basel Committee of Banking Supervision, 2021). Experience of other sectors, such as medicine, banking, aeronautics, navigation and shipping, has proved that effectively integrated risk management practices serve as the base for effective planning and strategic alignment, helping to boost growth and ensure healthy development (Achampong, 2010; Beals, 2015; Beasley, 2013; Chapelle, 2019; Colins, 2013; Dionne, 2013; Meerts-Brandsma, 2017). Researching common risk management tools and approaches applied in different sectors, where this area is regulated, in line with the specifics of the sector of education, and developing recommendations for incorporating it into the sector of education in Latvia, may prove to be useful to improve the quality of education in the future.

During this research it was confirmed that risk management is gaining acknowledgement in organizational management due to the benefits it brings with it, such as ability of managers to forecast possible threats and plan the most appropriate prevention measures. Hence research about risk management and its integration into the educational sector may provide substantial benefit to the management of education practices and improve the quality of educational services by looking from another perspective. Quite often a problem or an issue are disguising and taking attention away from what has caused a problem or an issue. Risk management on the other hand studies the root cause for each problem first and then addresses the root cause in order to prevent or mitigate undesired consequences (Chapelle, 2019). In addition, risk management helps to identify and consider a combination of different types of events and impacts of those events, thus giving an organization a chance to correctly analyse opportunities and treats for strategic planning.

The Institute of Risk Management states: *“Risk management is a central part of any organisation’s strategic management. It is the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio”* (The Institute of Risk Management, 2002).

There is a broad range of risks to which education sector may be especially vulnerable if no risk management techniques and tools would be employed as demonstrated by the theoretical and empirical research performed during this research. Risk management techniques are not fully recognized and utilized for strategic planning and development of the education sector, as was proved by the empirical research performed for this study and discussed in detail in Chapter 3. As a result, weak risk management increases the likelihood of misaligned priorities, resource leakages, poor service delivery and deterioration of existing problems (Abraham, et.al, 2013; ADB, 2010; ADB, 2016; Beals, et.al., 2015; Beasley, 2013; Chapelle, 2019; Garnett, 2019).

The numerous risks specific to the educational sector based on theoretical and empirical research were compiled by author as a taxonomy of risks for the sector of in Appendix 4 during the course of this research and can be used by the institutions in risk assessments and for general guidance on what types of risk and risk manifestations exist. The significance of the research increased with the new findings provided in this study. For example, during the analysis of risks performed in scope of this research it was found that the ineffective government budget planning and treatment of teachers by managers of educational institutions cause lack of motivation among teachers, which in turn leads to deterioration of the quality of education. Government accreditation of educational institutions may be based on non-transparent criteria and bribes may be paid to officials in return for an accreditation certificate, as a result quality of education in the entire sector may suffer too. School officials may bypass proper criteria for teacher recruitment and promotion and employ “ghost” employees, what could lead to lack of qualified teaching staff and irrational decisions may be taken affecting safety and rights of students. There can be risks in procurement resulting in unexplained delays, bidding irregularities in favour of certain contractors, unjustified sole-source awards connected to bribes, what may lead to unsafe and insecure environment in an educational institution. Neglect can lead to confidential data leakages and personal data breaches of students and employees. In school construction - substandard, unsafe, and unstable buildings prone to rapid deterioration may be built as a result of neglect or corrupt practices and affect security of students and teachers. Education service providers, which receive per-student funding from the government, could inflate enrolment data in order to obtain higher payments, particularly in the absence of third-party validation of data, what would lead to waste of governmental funds (ADB, 2016). Violent behaviours of teachers, defined as a behaviour pattern inflicted from power differences that significantly harm students and have no legal, academic, or ethic purpose, may lead to reputational damage of educational institution or the entire educational sector. Violent acts from side of students threatens safety of students and teachers in the educational institutions (Mertoglu, 2015). Natural disasters,

environmental changes, strikes, armed attacks and national military threat may paralyse the provision of educational services entirely (UNICEF, 2021).

Understanding the risk environment in education sector and qualitatively managing identified risks could foster more transparency in management of education at all levels. Throughout the thesis is analysed how risk management can be useful for the effective management of education and provision of qualitative educational services. This study is aimed at putting together the most popular and working practices from other sectors in order to come up with recommendation how to incorporate risk management into the sector of education and what shall be taken into account.

**Object of research** - risk management in the sector of education.

**Subject of research** – analysing components of risk management and assessment of risks in scope of the management of education.

**The aim of research** is to analyse common risk management practices and tools in order to draw recommendations on incorporation of the risk management best practices into the management of education taking into consideration the specifics and needs of the educational sector in Latvia.

**Tasks of the research:**

1. To analyse risk management theory and risk management practices across different sectors and countries.
2. To investigate typical risks relevant for the sector of education.
3. To analyse awareness and understanding of risk management by stakeholders in educational sector of Latvia;
4. To assess level of maturity of risk management in the educational sector of Latvia and to determine to what extent risk management tools are utilised for risk management routine of educational institutions.
5. To assess existing risks within the educational sector of Latvia, effectiveness of its management, risk mitigation needs and problems obstructing effective risk management.
6. Upon the results of the research develop the risk taxonomy for sector of education, methodological templates for risk management tools, risk management guidelines and recommendations for educational service providers and regulatory authorities.

**Hypothesis:**

There is poor understanding of risk management in the educational sector in Latvia, low maturity of risk management in the educational institutions of Latvia and lack of capability and capacity to employ risk management tools. As a result, quality of education is affected by many not well-managed risks.

### **Theses for defence:**

- 1) Risk management is an essential element of the future management of education, but its importance is underestimated at present moment in the sector of education due to poor understanding of the topic.
- 2) Risks that need to be assessed and prioritized in terms of likelihood and seriousness, are not managed well in the sector of education in Latvia.
- 3) All large educational institutions and education governing bodies shall appoint a risk coordinator, who will be responsible for building and maintaining risk management framework and setting the acceptable level of risk, reporting to the management of educational institutions or governing bodies, where the strategic decisions take place.

### **Methods of research:**

1. Analysis of available theoretical material, including scientific research publications, non-scientific research articles, legislation acts, academic books and evaluation of practical applicability of theoretic concepts was performed in the first phase. The research was conducted by qualitative analysis of available theoretical material, which included academic books, scientific publications, non-scientific articles, governmental reports and news websites. The materials mainly were searched in electronic academic databases (EBSCO, ERIC, DOAJ, WoS), as well as in online news portals (News.lv, bbc.com, reuters.com), institutional websites (CERT.LV, mk.gov.lv, izm.gov.lv, dvi.gov.lv, knab.gov.lv) and by use of Internet search engine for additional information. The search words used in the electronic academic database catalogues were “risk management”, “risk management in education”, “risku vadība izglītībā”, “crisis management in schools”, “cyber security in educational sector”, “legal risks in education”, “lawsuits in education”, “fines and sanctions to education providers”, and other. Search words used in news portals were: “corruption in education sector”, “corruption in schools”, “violence in schools”, “crisis management in education”, “cyber security in education”, “fines and sanctions to education providers”, “korupcija izglītības sektorā”, “vardarbība skolās”, “krīzes vadība izglītībā”, “kiberdrošība Izglītības sektorā”, “sodi un sankcijas izglītības iestādēm”, and other. All abovementioned search word combinations were used in Internet search engine for additional information.

2. Qualitative methods, including analysis of policies in different educational institutions, practical analysis of risk management in institutions, the impact of existence and non-existence of risk management of the performance of educational institutions, comparison to educational institutions in other countries in regard to the extent and maturity of risk management, evaluation of risk culture in different educational institutions in Latvia by means of interviews and questionnaires.

All found academic books and publications were analysed for definition of risk management by different authors, the risk management approaches, risk theories, examples and practical application of risk management techniques in the educational sector across the world.

3. Quantitative methods: data was collected by ways of online surveys and interviews. Upon performing profound desktop study about risk management in the sector of education, the most notable risks were formulated and used in developing the questionnaire for educational sector stakeholders in Latvia, where respondents were asked to rate criticality of the formulated risks and level of controls for these risks according to provided methodology. Stakeholders within educational sector and risk experts were interviewed for profound analysis. Surveys were placed into online platform SurveyMonkey.com and distributed via social networks and e-mails, interviews with experts were held afterwards. Returned fully completed results were examined for this research. Online surveys were addressed to stakeholders of the sector of education to perform risk assessment and clarify opinions, understanding and practical usage of risk management within the management of education. It was important to analyse whether there is any correlation between the criticality of risk and its control risk level, as perceived by educational sector stakeholders, in order to draw the conclusion what is the most appropriate way for management of particular risk. SPSS and Excel were used to perform descriptive and inferential statistical analysis of the results. The results of online surveys were analysed by following methods: trend analysis, descriptive statistical analysis (mean, mode, median, frequency, severity), inferential statistical analysis in form of statistical significance and reliability scales (t-test, Cronbach's alpha), correlation analysis (Pearson correlation coefficient), followed by graphical display and visual analysis. The results were confirmed with several risk management experts in form of interviews.

#### **Scientific novelty of the research**

1. Holistic examination of risk management practices in different sectors where risk management is mature in the context of applying it to the sector of education.

2. Forming profound and holistic theoretical and practical overview of risk management beyond the scope of psychosocial and physical risks.

3. Researching best practices of risk management employed in other sectors, such as banking, medicine, shipping, etc., and in the sector of education of other countries, with purpose of applying the main principles into the management of education in Latvia.

#### **Practical novelty of the research**

1. Providing guidance and understanding of risk management concepts and approaches to accountable stakeholders in the sector of education.

2. Expanding the understanding of the key risks in the sector of education and the opportunities connected to managing these risks.

3. Developing risk management guidelines, templates and common risk taxonomy for the sector of education, which are provided with the results of this research in Appendix 4. Risk Management Handbook and Taxonomy of Risks, developed as a result of this thesis, can assist risk managers of educational institution and governing authorities.

### **Content and structure of dissertation**

Chapter 1 focuses on theoretical aspects of risk management. It will examine risk concept and definitions, purpose of risk management, roles and responsibilities of stakeholders, the key pillars of successful risk management and various risk management tools, techniques and approaches.

Chapter 2 examines the risks relevant for the educational sector. Based on desktop research by examining different authors it will be concluded which risks are prevalent in the sector of education. Risks are grouped and each group studied in a subchapter.

Chapter 3 describes the empirical study conducted within this research and its results. It will introduce the methodology of empirical study and provide descriptive statistics of the quantitative research results. Further on will follow the results of the empirical study, which will provide the answers to the research questions: what are the key risks in the educational sector of Latvia, how well are they managed, what should be improved and how it would be possible to integrate risk management into the management of education in Latvia. The results will be tested with reliability scales and statistical significance. Through the empirical study the conclusions will be made about how risk management could be integrated into the educational sector.

Chapters 4 and 5 summarise all of the above into conclusions and recommendations for educational institutions and governing authorities.

In the Appendix 1 and Appendix 4 are provided Risk Management Handbook and Risk Taxonomy, as well as other helpful templates for risk managers in educational sector, which can be utilised by educational sector's managers, employees and governing authorities.

### **Approbation of research results**

#### **a) Scientific publications:**

1. Jemeljanenko, A. (2018) Risk Management in the Educational Sector of Latvia. *Human, Technologies and Quality of Education: conference proceedings*, pp. 7-14, University of Latvia. Published in Web of Science database in April 2021. DOI: <https://doi.org/10.22364/htqe.2018.01>.
2. Jemeljanenko, A. (2018) Impact of EU General Data Protection Regulation on Management of Education, *Proceedings of the 60th International Scientific Conference of Daugavpils University, Part B - Social Sciences*, pp. 169-177. University of Daugavpils: Akadēmiskais Apgāds „Saule”.

ISBN 978-9984-14-864-9. Available at: [https://dukonference.lv/files/978-9984-14-864-9\\_60\\_konf\\_kraj\\_B\\_Soc%20zin.pdf](https://dukonference.lv/files/978-9984-14-864-9_60_konf_kraj_B_Soc%20zin.pdf).

3. Jemeljanenko, A., Mackeviča, L. (2018) Aspects in Higher Education Programme Development, 8. *International Young Researchers Academic Conference proceedings "Izaicinājumu un iespēju laiks: problēmas, risinājumi, perspektīvas"*, pp. 437-440. BSA: Daugavpils. Available at: [https://bsa.edu.lv/wp-content/docs/science/book/1718052018\\_sbornik.pdf](https://bsa.edu.lv/wp-content/docs/science/book/1718052018_sbornik.pdf)
4. Jemeljanenko, A., Geske, A. (2019) Management of Psychosocial risks in Latvia, *Proceedings of the International Scientific Conference "Society. Integration. Education"*, Vol. VI, May 24th-25th, 2019, pp. 215-223, Rezekne Academy of Technologies. DOI: <https://doi.org/10.17770/sie2019vol6.3789>
5. Jemeljanenko, A., Mackeviča, L. (2019) Incident reporting in Management of Education, *LU 77. International conference proceedings "Human, Technologies and Quality of Education"*, pp. 53-61, Education Management section, Rīga. Published in Web of Science database in April 2021. DOI: <https://doi.org/10.22364/htqe.2019.05>

**b) Scientific conferences:**

1. Jemeljanenko, A., Risk Management in the Educational Sector of Latvia. Human, Technologies and Quality of Education: 76<sup>th</sup> International Conference. Faculty of Pedagogy, Psychology and Arts, University of Latvia, 12 February 2018, Riga, Latvia.
2. Jemeljanenko, A., Impact of EU General Data Protection Regulation on Management of Education, 60th International Scientific Conference of Daugavpils University, Part B - Social Sciences, University of Daugavpils, 26 - 27 April 2018, Daugavpils, Latvia.
3. Jemeljanenko, A., Mackeviča, L., Aspects in Higher Education Programme Development, 8. International Young Researchers Academic Conference "Izaicinājumu un iespēju laiks: problēmas, risinājumi, perspektīvas", 17 – 18 May 2018, Baltic International Academy, Daugavpils, Latvia.
4. Jemeljanenko, A., Geske, A., Management of Psychosocial risks in Latvia. International Scientific Conference "Society. Integration. Education", Rezekne Academy of Technologies, 24-25 May 2019, Rezekne, Latvia.
5. Jemeljanenko, A., Mackeviča, L. (2019) Incident reporting in Management of Education. Human, Technologies and Quality of Education: 77<sup>th</sup> International Conference. Faculty of Pedagogy, Psychology and Arts, University of Latvia, 12-13 February 2019, Riga, Latvia.



## **1. THEORETICAL APPROACH TO RISK MANAGEMENT**

The aim of this chapter is to introduce general concepts of risk management, tools and techniques that can be applied for effective risk management, study the key stakeholders, their roles and responsibilities. This chapter's focus is on exploring and discussing the theory and nature of risk management. Risk management within the sector of education will be discussed in the following chapters based on the findings of this chapter.

### **1.1. Risk concept and definitions**

Walker (2019) defines risk as the probability to suffer losses. Chapelle (2019) defines risk as the effect of uncertainty of objectives resulting in negative events, incidents and accidents. Both authors mention and discuss financial and non-financial types of risk. Financial risks are market, credit, liquidity, currency risks, whereas non-financial are operational, reputational, regulatory compliance, legal and conduct risks.

Tufano (2011) states that Risk management within any organization helps to identify and consider a combination of different types of events and its impacts, thus giving an organization a chance to correctly analyse opportunities and treats for strategic planning. Clark, et. al. (2013), APPA (2018), Ariff et.al. (2014), Clyde-Smith (2014), Adams (1973) et. al. state that ensuring safe environment, effective and cost-efficient curriculum provision through assessing and mitigating involved risks is the core responsibility of educational institutions.

Successful management and administration of education institutions is not possible nowadays without utilising risk management concepts and techniques (Зaxaпoв, et.al., 2016). Risk management is crucial for decision-making as it helps to recognize threats at an early stage. Risk can be also defined as a threat that may pose implications for organization to meet its objectives (National Association of College and University Business Officers and the Association of Governing Boards of Universities and Colleges, [NACUBO and AGB], 2007), hence summarising the above definition, the key purpose of risk management can be defined as helping organisations to achieve established goals through structured dealing with threats and issues, which may disturb achievement of the strategic goals and the mission.

Asian Development Bank (ADB, 2010) sets out an overview of the risks to which the education sector globally is vulnerable, which are: lack of clearly defined processes and legal frameworks (e.g., in such important processes as admissions, recruitment, budgeting, procurement), misaligned priorities, bribery and corruption, weak financial management, poor internal culture, poor information systems, lack of relevant expertise on management level, poor security provision. Dunklee and Shoop (1993), in turn, analyse and discuss risks, mentioned in ADB(2010), related to personnel development

programmes and their compensations, environment and safety management, disputes and litigations, usage of institution's facilities and grounds by the community and risks pertained to the construction of buildings. Forlin (1995) states that the most undervalued risks are related to the educational environment, especially health and safety of employees and students. Clark, et al. (2016) further concludes that the interconnected risks are emerging, such as cyber, data management and privacy risks, terrorism and violence risks, infrastructure and facilities' management risks; and that a broader approach to risk management is required.

All above authors and theories discuss that risks can be generated from internal and external environment and therefore risk management in any institution is concerned with internal and external risks, which appear and shape internal and external environment in the educational system. In the external environment, for example, laws and regulations shape industry specific strategic planning, rules for textbook and supplies, set the framework for building and construction of educational institutions, defining co-operation partners and budgets. All of this can be disrupted by corruption and further impacts the internal environment of the educational institutions. Buildings and constructions may directly impact the quality and reputation of education as there the risk of student safety arises. Strategic planning on the industry level impact managers, who further set goals and objectives for their own organisations. Ability of managers to set goal correctly is impacted by their professional development. Goals and objectives shape internal attitudes and culture, which are also shaped by employees and their professionalism. Higher professionalism combined with correctly defined goals and objectives should shape positive internal attitudes and culture and vice versa. Risks of violence and bullying arising from unprofessionalism of teaching staff and negative internal culture, may have the detrimental impact on the quality of education, which in turn affects children and parents. Depending on the quality of education received, future society and external culture is formed, which in turn affects the economic environment. With higher quality of education there should be more positive effect on the society, culture and economic environment and vice versa. This further on may impact regulations and reforms in the sector. (Forlin, 1995; Clark, et.al., 2016; Moldovan, 2012; APPA, 2018; The Institute of Risk Management, 2002; ADB, 2010)

## **1.2. Stakeholders**

Stakeholder analysis is important in understanding the governance of the education sector. Governance tends to be more effective when there is:

(i) demand for accountability from stakeholders; and

(ii) supply of governance (where actors in power share information, take decisions within a clearly defined regulatory framework and transparently allocate resources, offer space for participation, and are accountable for their actions).

List of stakeholders in the sector of education looks as follows:

- a) policy makers, planners, and researchers;
- b) boards responsible for standards and accreditation;
- c) education and training providers;
- d) suppliers of textbooks and school supplies, equipment, facilities, and services to education and training providers;
- e) students, parents, and employers;
- f) development partners and investors;
- g) civil society organizations, including teacher unions, industry associations, and media; and
- h) oversight entities responsible for enforcing laws and regulations, such as the ombudsman, judiciary, and audit offices.

Examining the formal and informal relationships among stakeholders can help identify where risks may lie. Politicians, for example, may interfere in budgetary allocations and releases. Such interference can distract the focus of sector plans. Vested interests may influence large procurement projects because these provide opportunities for personal enrichment. Teacher deployment and promotion, for example, may be subject to family connections and favouritism. Those without connections may be assigned to remote locations. Parents may bribe school officials to ensure that their children will be admitted to the school of their choice. Teachers or examiners may collude with students by selling examination questions in advance or by manipulating examination results. (ADB, 2010; APPA, 2018; The Institute of Risk Management, 2002; Ariff, et.al., 2014; Clyde-Smith, 2014; Kirya, 2019)

Conclusion can be drawn from the information discussed above about who are the key stakeholders in the risk management within the educational sector. By taking the external environment, the stakeholders are: law makers, regulators, co-operation third-party partners provided food services and construction works, textbook authors and printing agencies and the society as such. External stakeholders are affected by the decisions taken in terms of what books will be demanded for the educational sector, what rules for food supplies or construction works will be made, how many students will be admitted to educational institutions, etc.

Internal stakeholders of the educational system are teachers, principals and managers of educational institutions and other non-teaching employees, students and their parents/guardians. Internal stakeholders are impacted by all the decisions related to safety, supplies, cost of education,

methodologies of education, which are decided often within the external environment by regulatory bodies.

All of the decisions taken within internal and external environment impact stakeholders on both sides. Final and biggest impact through the level and quality of education is created on the society. (The Institute of Risk Management, 2002; ADB, 2010; Scheer, et.al., 2014; APPA, 2018)

### 1.3. Who is responsible for risk management?

Basel Committee of Banking Supervision (2011) defines the following common sources of operational risk, which can be applied to the risk management within educational sector: people, systems, processes, external events and legal risks. The author mapped the risks mentioned in previous and further sections with stakeholders discussed above and the sources of operational risk, as provided the Table 1.1 below. It is important to note, that while trying to identify concrete stakeholders for different risk scenarios, it was identified that for each risk driver the stakeholder list would not change due to the fact that it is never possible to predict in what way exactly the risk will materialise and who would be affected as a result. Therefore, the Stakeholders list is common for all risk drivers and risk examples.

Table 1.1 **Risk mapping according to sources of risks and relevant stakeholders**  
(developed by author)

<b>Risk driver</b>	<b>Risk examples</b>	<b>Stakeholders</b>
People	Bullying and Violence in educational institutions; parent attitudes; corruption; inadequate strategic decision making; lack of motivation; confidentiality and privacy breaches.	- students, parents; - teachers, education and training providers; - policy makers, planners, researchers;
IT and Systems	Cyber-attacks; systems failure & downtimes; data leakage; confidentiality and privacy breaches	- boards responsible for standards and accreditation; - school suppliers;
Processes	Accreditation; corruption; changes in regulatory requirements and processes; overloading of employees; insufficient funding	- entities responsible for enforcing laws.
External Events	Nature disasters (e.g., floods); fire; terrorist attack; lack of financing due to crisis/changes; damages caused by suppliers; insufficient funding; lack of qualified staff; changes in regulations and political environment	
Legal and Compliance	Incompliance with relevant laws; new regulations; changes in law; lawsuits	

Such mapping of risks according to the risk sources and analysis of stakeholders provide a structured approach to the research of risk management of the organisation.

The role of each stakeholder is important in different situations:

- Students and parents may not comply with the rules and cause an incident: e.g., student may bring drugs, weapons or other unallowed subjects to the school, parent may be rude or violent to teaching staff;
- Students and parents may suffer from unstable IT systems, what does not allow to follow important updates and progress;
- Teachers may suffer from violent behaviour of other stakeholders or from not well-developed processes (e.g., communication with parents, air quality checks in the classrooms, requirements related to mandatory documentation, etc.)
- Lawmakers may be taking bribes, be incompetents and implement inadequate regulatory rules;
- Boards responsible for standards and accreditation may be bribed, may be incompetent or suffer from unstable IT systems, which does not correctly maintain their records;
- School suppliers may source goods of bad quality of poisonous food, as well as their staff may be unavailable due to epidemics or IT systems may crash and cancel all orders, what would result in not supplying ordered goods to institutions.

Thus, although the main responsibility in an institution for designing and implementation of the risk management framework and rules may seem to lie on the institution's management and governing bodies, there are number of aspects where every stakeholder is responsible for risk prevention and mitigation.

#### **1.4. Key pillars of successful risk management**

As concluded by the authors mentioned above, application of risk management techniques within the educational sector is important for quality improvement, transparency in educational institutions operations and effective decision-making and strategic planning. Risk management framework must be established in order to effectively manage risks. Risk management framework must include techniques and tools to identify, assess, monitor and mitigate risks, establish preventive and corrective controls, what will be described in further sections. Risk models and processes in this paper will be analysed in regard to applicability to educational sector. In this section, theory of the risk management and its application in practice will be analysed.

### 1.4.1 Risk Governance

Risk governance is the core of the risk management, as **it starts with clearly defining roles and responsibilities across the institution and transparent segregation of duties** (Chapelle, 2019; Walker, 2013). Clear policies and procedures are the backbone of risk governance, with defined responsibilities for different tasks, rules and principles followed in the institution and guidelines how certain tasks need to be executed. Communication of this internal regulation is very important to ensure implementation discipline. Decisions usually lie with the senior management (school administration or municipality), who may delegate mandates for decision making to certain established committees, where collegial decisions are officially taken based on reporting and escalation activities.

For the risk management to succeed in an organisation and to successfully gather required data on risks, incidents, customer complaints, etc., it is important for risk coordinators firstly to become accepted on the operational level. This requires ability to demonstrate the value that the risk management brings to the organisation. Before arguing the benefits of the risk management, risk coordinator should build the so-called “business case” for the risk management, which should include such advantages as reduction of large losses in the long-term, more efficiency, better stability for employees and customers and increase in productivity, etc., as with fewer incidents there will be less time required for reporting and for risk mitigation activities. Building such risk management framework, where the emphasis is put on managing the top risks associated with achievement of key objectives and respective prioritisation of risk management activities, brings most value to the organisation.

### 1.4.2 Risk Identification

Walker (2019), Leitch (2016), Chapelle (2019) discuss the risk identification tools and techniques. Risk identification focuses on risk event identification through risk cause analysis. Risk causes can be exposures to risk, vulnerabilities in controls, internal and external environment, as well as chains of causes and impacts. Operational risk according to definition provided by the Basel Committee for Banking Supervision (2011) is defined as the risk of losses resulting from inadequate or failed internal processes, human mistakes, technology and system downtimes and external factors, such as third-party vendors, external environment, natural disasters, politic environment, etc. Thus, there are four main causes defined for operational risk management in banks: People, Processes, Systems and External. *People* as a cause mean the risks arising from employees, e.g., insufficient competence, mistakes, poor motivation, fraud, incapacity to work, insufficient experience, poor engagement and work quality, etc. *Processes* stand for risks arising from not precisely defined roles and responsibilities, too complex or incorrectly designed internal processes, manual activities,

insufficient controls, etc. *Systems* stand for risks arising from IT systems and telecommunications, e.g., unavailability of an important system, slow performance of IT system, disconnection of telecommunications due to systems' issues, etc. *External* stand for risks associated with external environment, e.g., cyber-attacks, third-party service provider failures, weather disasters, pandemics, political decisions, regulatory actions, behaviour of parents and students that threatens achievement of objectives or leads to losses. Losses caused by actions of students can be also qualified as Process risk, if damaging actions were possible due to insufficient internal controls or as People risk, if it was allowed to happen due to lack of competence, engagement or experience of employees. Thus, these four criteria cover internal and external environments of educational institution and all stakeholders. Hence, author believes that classification as provided by Table 1.2 can be also applied in risk management within the sector of education:

**Table 1.2: Examples of cause categories on levels 1-2. Source: Chapelle (2019), p. 25**

Level 1	Level 2
People	Resources/Capacity
	Competence
	Engagement
	Experience
Process	Manual complexity
	Documentation
	Multiple input
	Automation
Systems	Availability
	Bug
	Capacity
	Performance
	Obsolescence
External events	Socio-political changes
	Regulatory
	Stakeholder interference
	Natural events
	Third party

Identified risks should be specific to the nature of operations of each concrete firm or institution. Author highlights that the most dangerous risks are those that are ignored and not known.

Kelliher et. al. (2016) claim that categorisation of operational risk should be as granular as possible to avoid ambiguity. The author therefore mentions the seven types of operational risk defined by Basel II, which in authors' view are too high-level and ambiguous. Authors call for breaking risk types into more granular levels to ensure transparency in selection of a certain type of operational risk. Thus, it is not sufficient to break down operational risk by cause categories, but it is also

important to study the type of loss operational risk causes in granular level. Kelliher et. al. (2016) suggests to clearly distinguish types of risk, e.g., operational, strategic, legal, etc. in order to have clear picture as to which risks need to be covered by capital planning tools in different categories. Risks of one type can be further broken down into sub-types, for example, in banking, operational risks are broken down into 7 sub-categories by Basel Committee for Banking Supervision (BCBS): internal fraud, external fraud, workplace safety and employment practices, compliant client, products and services practices, business disruptions and service failures, damage to physical assets and execution errors and process management mistakes. These categories on the high level would be suitable also for the educational institutions, with further sub-level categorisation specific to the sector of education. Losses arising from these events should also be categorised in the way, that will enable clear distinguishing of different types of losses and will help to group different losses for clear risk picture of individual organisation. Already budgeted costs, such as salaries of existing employees, involved in managing risk event, should not be considered as loss. On the other hand, salaries of new employees and consultants specifically hired to handle the risk event, should be counted as a loss (Kelliher, et. al., 2016).

Alberts and Dorofee (2009) and Beasley (2013) stress the importance to identify possible emerging operational risks – those which are not possible at the point of time, but maybe emerging to certain trends and developments.

#### 1.4.3 Risk Identification Tools

Chapelle (2019) provides overview of the approaches for risk identification. Top-down risk identification lies with senior management of an organisation and is focused on risks to the strategy, emerging risks, global trends and key threats to the organisation's strategy. Best practice is to facilitate top-down risk identification and assessment sessions at least 1-4 times per year. Alberts and Dorofee (2009) call top-down identification of risks as systemic risk management and highlight the importance of top-down risk identification linked to the key objectives and goal of an organisation. Through the systemic approach, the risk drivers that could halt or obstruct achievement of the key objectives should be identified and managed. Thus, against each objective should be developed a statement, what would help successful achievement of the objective and what would lead to failure, then these indicators of failure can be translated into the risk statements. It is important to analyse the environment and conditions surrounding the achievement of key objectives to be able to draw out potential risks. There can be multiple risks triggered by one risk driver, hence it is important to look at different risk drivers from different angles to identify all possible inherent risks.

Next approach described by Chapelle (2019) is bottom-up risk identification, which lies on the business process level or in regard to public organisations - on the operational level. Usually, such



process is organised at least once per year and involves all managers at the level of operations. Such process is called Risk Control Self-Assessment (RCSA). The process focuses on operational efficiency risks, organisation of processes, efficiency of systems, competency of staff, external risk factors, etc. It is important to exercise both top-down and bottom-up risk identification approaches, as Chapelle (2019) noted about using only bottom-up approach would lead to “failing to see a beach due to being very busy observing the grains of sand”.

In Appendix 2, Table 5.1 is provided an example how risk assessment’s register may look like and in Appendix 4, Table 7.1, are provided risk taxonomy and risk examples for educational sector. Sum of bottom-up and top-down risk identification tools should be used for the full risk universe of the organisation, as is provided by Appendix 4, Table 7.1.

Further Chapelle (2019) discusses that risk identification can be assisted by the use of “five why questions”, what means a sequence of questions leading to identification of causes and concrete risks. In addition, mapping performed tasks and processes to the existing controls may also assist in risk identification, as well as interviewing the key staff, who may be well be aware of any gaps leading to risks in the organisation.

One of the most popular risk identification tools according to author’s observations is usage of incident register, where already realised risks as internal or external incidents or near misses are analysed for future probability and losses. An example of such register of incidents is provided in Appendix 3, Table 6.1. This approach is most relevant for stable organisations, where the risk profile does not change for some years and hence it is possible to forecast future by analysis of the past events (Kelliher, et. al., 2016).

#### 1.4.4 Scenario Identification and Analysis

Scenario Identification Process according to Chapelle (2019), Walker (2013), Amin (2016) and Dutta & Babble (2014) is one of the key pillars in risk management and is very important tool in decision making. Scenario Identification usually focuses on extreme and severe risk event scenarios. Taleb (2020) states that in order to understand everyday risks it is crucial to focus on studying the extreme and rare risks; similar like with human beings, whose real nature and character become most prevalent in extreme conditions. Dutta & Babble (2014) highlight that Scenario Analysis has been used for a long time in engineering, medicine, management, defence, etc., hence it can be as successful be used in management of education.

Risk scenario assessment is down to assessing the level of risk event probability and level of its impact. Scenario identification process usually focuses on the low probability and high severity (impact) risk event scenarios. Dutta & Babbel (2014) characterize Scenario Analysis as having two important elements: assessment of the future state of a certain characteristic and knowledge about

current state of that characteristic. Amin (2016) mention that Scenario Analysis offers reasonable options of future environment developments. It is important to take in mind existing situation and assess various possibilities of future developments within a certain period of time (Dutta & Babbel, 2014). There are seven steps in this process according to Chappelle (2019):

1. Preparation of empirical evidence documents and split of roles and responsibilities – at this stage it is important to collect and consolidate external loss data (losses experienced by other similar organisations) to use during the session for scenario generation and to assign precise roles and responsibilities to all participants;
2. Brainstorming with stakeholders for generation of scenarios and selection of the most rare but plausible risk event scenarios for further assessment – at this stage participants generate specific risk events (scenarios) with supposedly high losses and with rare frequency;
3. Assessment of selected scenarios in regard to the risk probability (frequency) and impact (severity) – at this stage out of all generated risk event scenarios, participant choose the most plausible ones and assess its most plausible probability (how frequently selected scenario can happen, e.g., once in 10 years) and its total impact (probable financial loss by different categories – restitutions, write-offs, legal expenses, insurance recoveries, etc.);
4. Validation of selected assessed scenarios with help of pre-prepared empirical evidence – at this stage, assessed scenarios once again are checked against the pre-prepared external loss data for possible impact and probability;
5. Incorporation of the results into management plans – at this stage, all selected scenarios are assessed for the reaction, whether it will be accepted, mitigated or terminated/avoided. For those scenarios, which will be mitigated, risk mitigation plans are prepared and integrated with the management plans and for scenarios, which are chosen to be terminated or avoided, exit plans are prepared or risk insurance is budgeted into the annual budget plan;
6. Consolidation of all scenarios for further use – all scenarios with action plans, deadlines and precisely defined responsibilities are then consolidated for continuous follow-up;
7. Incorporation of the results into the calculations of the risk capital (specific for banking institutions) – at this stage results are incorporated into organisational internal model for calculating risk capital (e.g., Loss Distribution Approach), which calculates for cost of potential risk inherent to the organisation.

Scenario Analysis is especially useful for organisations, which have not experienced major loss events and incidents (Dutta & Babbel, 2014). It does not mean that such incidents and losses will not happen in the future. Scenario Analysis is a great tool to measure risk exposures inherent to an institution that can result in material loss sometime in the future (Dutta & Babbel, 2014). Thus,

Scenario Analysis is essential for successful risk management. Scenario Analysis is widely used in banking and finance, as well as in medicine, engineering, national defence, etc. (Dutta & Babble, 2014). In Appendix 2, Table 5.1 is provided an example how scenarios can be incorporated into the risk assessment's register and in Appendix 4, Table 7.1, are provided risk taxonomy and risk examples for educational sector, which can be used for scenario generation.

Scenarios and possible loss estimations can be derived by collecting data about material losses in other similar organisations and assessing whether the scenario would be relevant for the given organization and calibrating the losses accordingly taking in consideration specific organizational differences and goals (Dutta & Babble, 2014).

By utilizing Loss Distribution Approach (LDA) with Scenario Analysis results together with internal loss historical data and running it through the Monte Carlo simulation, it is possible to calculate price of the risk pertaining to certain organization.

As already mentioned above, for the Scenario Analysis it is important to gather in a series of workshops with subject matter experts to generate the scenarios. According to Dutta & Babbel (2014) and Amin (2016) external loss data can be used to start generating ideas and to validate proposed scenario losses. For example, facilitator may start by reading a pre-prepared scenario and asking participants to confirm whether such situation could happen with their institution. If yes, then next question would be about how much would be the total loss if such situation would happen with this particular organization. Then, frequency of an event would need to be assessed. Scenario Analysis should not over-rely on historical loss data of other institutions in order not to miss hypothetical scenarios specific to certain organization (Dutta & Babble, 2014).

Scenario should be perceived as sensitivity analysis of current environment to the future expected and unexpected events (Dutta & Babble, 2014). Scenario Analysis is based on assumptions of possible impact and frequency distributions. Appropriate risk mitigation actions may be developed by managers of educational institutions to prevent risk from happening in the future and making risk environment less sensitive to certain future developments.

Scenario Analysis differs from the risk assessment process mentioned previously with severity estimations: in Scenario Analysis the estimated losses should be much higher than in routine risk assessments and internal loss history, and the frequency of the events considered should be much rarer (Dutta&Babble, 2014; Amin, 2016; Chapelle, 2019).

#### 1.4.5 Risk Connectivity and Risk Networks

According to Chapelle (2019) good practice is to present risks in the register as a web, demonstrating the connectivity of different risks and interrelated mitigation actions. World Economic Forum provides the up-to-date map of global risks for the risk professionals each year, using the

representation of risks as a web. According to best practices observed by the author and as a simpler approach for small organisations, risks also can be organised into clusters for better prioritisation by the risk management unit. Risk clusters usually represent a cascade of different risks, one leading to another and provide a good overview of the risk profile relevant to certain organisation. An example of risk connectivity is provided in Appendix 4, Table 7.1 in form of risk taxonomy.

#### 1.4.6 Risk Appetite or the accepted level of risk

Chapelle (2019) and Walker (2013) define risk appetite as the amount of risk that the organisation is willing to take in pursuit of its strategic objectives. Risk appetite stays for the level of risk that can be accepted without any additional risk prevention or mitigation actions. Usually, in large companies, e.g., banks, a board of directors define the such acceptable level of risk, whereas framework establishment and monitoring of the accepted risk level is performed by the risk management functional unit. The purpose of risk appetite establishment is to assist management in decision-making and keep organisation's risk taking within certain boundaries.

Setting the acceptable level of risk for financial risks is quite straightforward: it is defined by the trade-off between the risk and return (or losses and profits), whereas for non-financial risks, such as operational, reputational and compliance risks, the benefits are often intangible and therefore not so straightforward. To ensure operating within the boundaries of risk appetite it is important to set controls, which will either prevent risks, minimise the losses or both. Acceptable risk level must have clear limits established as to when it should be considered that it is breached. There also should be clear governance structure with defined roles and responsibilities, what includes risk ownership and action plan what should be done in case the acceptable risk level limits are breached. According to author's observations and confirmed by Chapelle (2019), there are usually top-down and bottom-up approaches to setting the acceptable level of risk: what managers are thinking about risk tolerance in the organisation and what is actually happening in practice. Usually in theory the acceptable level of risk is more prudent and conservative, than in practice.

Risk management framework shall be based on the statement about the acceptable level of risk and subsequent development of key risk indicators – metrics that assist in measuring deviation from risk management limits and providing early warning signals, what will be discussed further in this study. The more advanced the acceptable level of risk statement is, and the more detailed the key risk indicators developed, the more mature becomes the risk management framework. Usually, the more essential is the activity, the lower is the acceptable level of risk. As PKF UK LLP (2011) put it, younger educational institutions take on more risks to grow and develop, whereas mature educational institutions with established reputation are more risk averse and tend to measure their risks with pre-

defined metrics and risk limits. Risk appetite may have significant differences in different organisations, depending on organisation's size, strategy, maturity level and risk environment.

In practice, excessive risk taking usually happens only for the risks, which are not identified, when risk assessment process is skipped or not properly performed, therefore as the analysis above demonstrates it is important to accomplish good quality risk identification and assessment processes on a regular basis.

#### 1.4.7 Risk and Control Self-Assessment (RCSA)

At least once per year or when any significant changes take place in an organisation, the risk-brainstorming workshop should be facilitated to perform risk assessment with line managers of lower level, where organisation-wide risks are identified and assessed according to established risk assessment methodology (Chapelle, 2019). The same approach can apply in all levels of educational institutions, where such risk assessment would be initiated and facilitated by a risk coordinator (e.g., appointed by municipality or employee with defined responsibilities for risk management) and involving managers of educational institution and teachers from different disciplines.

The process of risk and control self-assessment consists of the following steps (based on author's experience, Chapelle, 2019, Walker, 2013, Alberts and Dorofee, 2009):

1. Preparation of empirical evidence documents – at this stage it is important to collect internal loss data (losses historically experienced) to use during the workshop session for risk scenario generation;
2. Brainstorming with stakeholders for generation of risk scenarios – at this stage participants generate list of all possible risk events, which may happen to their area of responsibility;
3. Assessment of selected scenarios in regards to impact (severity) as represented by Table 1.3 and probability (frequency) as represented by Table 1.4 – at this stage all generated risk event scenarios are assessed by probability and impact to arrive at final risk score – methodology (example will be provided further below) for such risk assessment should be developed by organisation according to its acceptable level of risk (impact level and total risk score assessment should be directly linked to the acceptable level of risk);
4. Validation of selected assessed scenarios with help of pre-prepared empirical evidence – at this stage, it should be checked that all incidents, which appear to be in pre-prepared historical loss data are mentioned in the risk assessment and none of the inherent risks is missed from RCSA register;
5. Incorporation of the results into risk mitigation plans – at this stage, all selected scenarios are assessed for the reaction, whether it will be accepted, mitigated or terminated/avoided. For those scenarios, which will be mitigated, risk mitigation plans are prepared and for risks,

which are chosen to be terminated or avoided, exit plans are prepared or risk insurance is budgeted;

6. Consolidation of all scenarios for further use – all scenarios with action plans, deadlines and precisely defined responsibilities are then consolidated for continuous follow-up by the risk coordinator.

The following methodology is published by Chapelle (2019) as an example to use for assessing risk impact, risk probability and total risk level:

**Table 1.3: Risk assessment methodology example adapted from A. Chapelle (2019) book: impact scale per type. Source: A. Chapelle (2019), p.54**

<b>Impact rating</b>	<b>Financial</b>	<b>Service delivery</b>	<b>Customers and reputation</b>	<b>Regulatory</b>
<b>Extreme</b>	>25% of yearly budget	Critical service disruption with major impacts to internal and external stakeholders	Significant, possibly long-lasting damage to the firm's reputation and trust toward many stakeholders	Significant compliance breach leading to large fines and regulatory scrutiny.
<b>Major</b>	>5-25% of budget	Significant interruption of service leading to crisis management mode internally and customer detriment externally	Large number of customers or stakeholders impacted, to be actively addressed during incident and through post-incident remediation.	Compliance breach with or without fines, leading to lasting remediation programs with damage vis-à-vis the regulator.
<b>Moderate</b>	>0.5-5% of budget	Noticeable interruption of service but with no significant consequences for stakeholders besides inconvenience	Small reputation impact among limited number of customers and stakeholders, short-lived and addressed during incident management.	Some breach or delays in regulatory compliance necessitating immediate remediation but with no lasting impact.
<b>Low</b>	<0.5% of yearly budget	No interruption of service noticeable to external party	No impact outside of internal parties.	Minor administrative compliance breach not impacting the firm's reputation vis-à-vis the regulator.

Table 1.4: Risk assessment methodology example adapted from Chapelle (2019) book: likelihood scale. Source: Chapelle (2019), p.55

Qualitative rating	Frequency of occurrence	Probability of occurrence % (at 1-year horizon)	Definition	Guidance
<b>High</b>	1 year or less	>50%	Likely to occur within one year	More likely than not of happening within a year, historical evidence indicates that such event occurs once or more per year.
<b>Medium</b>	>1-5 years	10-50%	Likely to occur in the medium term	Likely to occur at least once in a five-year horizon (e.g., strategic plan horizon).
<b>Low</b>	>5-20 years	2.5-10%	Unlikely to occur in normal business circumstances	A remote possibility exists for such an event to occur, less than 10% chance of occurrence within a year.
<b>Rare</b>	>20 years	<2.5%	Should not happen, unless very rarely	Very unlikely, may occur in exceptional circumstances. Has not occurred yet in the company but the possibility should be envisaged.

For the educational institutions Beasley (2013) proposes the impact assessment scales, which are mainly based on measuring impact on funding, student application profile, faculty recruitment and retention, media attention and harm on reputation, peer ranking and fundraising goal achievement.

Alberts and Dorofee (2009), Chapelle (2019), Walker (2013) state that probability and impact must be assessed for each risk scenario described and total risk exposure then can be derived from the combination of probability and impact, which together establish the importance of risk. Year-on-year the results of such risk assessments can be compared, and risk controls can be evaluated by analysing the implementation of risk mitigation actions versus realised losses and incidents. During this process for all identified risk scenarios the total risk score is evaluated by multiplying probability and impact scores.

To visualise the risk assessment results, usually a risk matrix is used, where on one scale (x or y) is represented probability, on another scale (x or y) is represented impact, but the risk matrix is split into the areas from resulting risk levels, where green colour means acceptable level of risk, yellow colour means tolerable level of risk and red means intolerable level of risk (Alberts and Dorofee, 2009; Chapelle, 2019; Walker, 2013). The author has drawn an example of how this can be

drawn for visualisation in Figure 1.1. This type of heatmap as presented in Figure 1.1 can be drawn in different other ways as is most suitable for particular organisation and is dependent on institution's objectives and acceptable level of risk. For example, instead of 4x4 matrix, it is fine to draw it as 3x3, 5x5, 10x10, etc., as the main idea is to reflect connection of the scoring methodology for probabilities and impact. Colours may also be adjusted according to the risk appetite specific to particular unique organisation.

<b>4Catastrophic</b>				
<b>3 Major</b>				
<b>2 Moderate</b>				
<b>1 Minor</b>				
	<b>1 Unlikely</b>	<b>2 Possible</b>	<b>3 Probable</b>	<b>4 Highly probable</b>

Figure 1.1: Risk matrix example (developed by author)

As Risk matrix is prepared individually by each organisation according to their specific acceptable level of risk and objectives, the green, yellow and red areas in different organisation may take different quadrants. For example, for risk averse organisation there will be more yellow and red risk areas, whereas for less risk averse organisation there will be more green and yellow and less of the red areas. Each level of risk should have appropriate reaction by the management: accept the risk, mitigate or terminate/avoid. However, according to Alberts and Dorofee (2009), usually there are two strategies how to address all the identified risks, given that there may be a big number of risk scenarios identified and not all would be possible to monitor. The first strategy is to apply Pareto analysis to draw out top 10-20% of risk scenarios according to their combined probability and impact and the resulting risk exposure. These 10-20% then are constantly monitored and managed, but the rest 80-90% of risks are periodically reviewed for any changes in their resonance. The second strategy is to group the risk according to common characteristics and address the groups of risks rather than each



individual risk separately. However, this approach has its drawbacks, such as amount of effort required as well as being subject to bias and error while grouping.

It is especially important to assess at least material risks that may threaten daily operations of an institution (pandemic, fire, floods, weather disasters, terrorist attacks, war, etc.) and prepare risk mitigation action plans for such situations, hold instructions to all employees about their roles and responsibilities in such situations, rehearse course of actions through simulating different risk situations in real life and checking how smooth will be the response and what needs to be improved in the planning.

According to Kelliher, et. al. (2016), the risk of third-party failing is relevant for every company, which makes use of suppliers and service providers. The risk core may not be in fact of service non-delivery as such, as usually the third parties will indemnify their clients for incurred losses, but the risk is in disagreements between the parties that may arise in respect of who is liable for specific loss or failure, in cases when specific loss of failure is not covered by the agreement and in case of third-party insolvency, thus causing exposure to larger than expected losses. Kelliher, et. al. (2016) recommends attempting to collect data about third-party's operational loss history in order to get clear picture of third party's control framework and possible failure based on traces of past failures and effectiveness of introduced controls for risk mitigation, as well as analysis of causes that led to losses and strength of business continuity framework. Although, authors are stating, it may be challenging to obtain such data, new agreement with third parties could capture obligation of third parties to share this information with educational institutions. This data can serve as an important input into the annual RCSA process.

Mitigation action plans always must be prepared for the risks with highest total risk scores and for risks with extreme impact, even if the probability for such an event is very low. Mitigation action implementation should be followed-up on on-going basis until the next RCSA process (Chapelle, 2019; Walker, 2013). For convenience, risks are mapped on the Risk matrix and presented to the senior management and key stakeholders.

#### 1.4.8 Risk Mitigation

According to Chapelle (2019), Walker (2013), PKF (UK) LLP (2011) risks can be transferred (by outsourcing risky activity or buying an insurance), terminated (by ceasing the activity or changing strategy), treated (by applying relevant controls to bring it to acceptable level) or tolerated (by accepting without any further actions). Most often risks are treated with the risk mitigation activities called risk controls. Risk controls can be preventive, detective, corrective or directive, depending on its nature and position in the sequence of risk management framework (Chapelle, 2019). Controls usually are checked for validity by risk management functional unit or by an auditor. The main

prerequisite is that the function, which performs testing, must be fully independent. Usually, the common problems with the risk controls are that they are too optimistic, duplicative, unclear or responding to failures by adding the same type of additional controls as were before the failure. Prevention of risks should happen through efficient control design (Chapelle, 2019). It is important that risk controls and risk responses are designed in line with the acceptable level of risk (PKF (UK) LLP, 2011).

According to Chapelle (2019), realised loss events are of three types:

- *Slip* is the loss event that happened involuntarily due to disruption, tiredness, inattention, etc. and should be treated by addressing the root cause.
- *Mistake* is a result of voluntary action, when something is done to achieve a certain purpose, but the activity chosen is wrong due to flawed guidelines or lack of knowledge, which accordingly should be addressed to mitigate the risk.
- *Violations* are voluntary misdeeds, which should be addressed by applying relevant internal controls and sanctions.

According to PKF (UK) LLP (2011) risk control should not be excessive, otherwise they will lead to bureaucracy, failure of controls and over-complexity, what will make an institution ineffective and exposed to more risks.

#### 1.4.9 Root Cause Analysis and Action Plans

Root cause analysis is best performed by applying the Bow-Tie method, where the loss event lies in the middle, on the left side are located causes and on the right side are located consequences, as Figure 1.2 below demonstrates (Stemn and Bofinger, 2018; Chapelle, 2019).

According to Chapelle (2019) analysis starts with looking at the preventive controls, which fail and allow loss event to happen. By asking sequence of “why” questions, it is possible to come to the core of the problem. Then analysing the consequences in order to develop appropriate action plan continues the analysis. Corrective and detective controls lie on the right side after the loss event occurred and thus stronger controls are developed through comprehensive analysis of consequences and asking “what would happen if” at every stage.

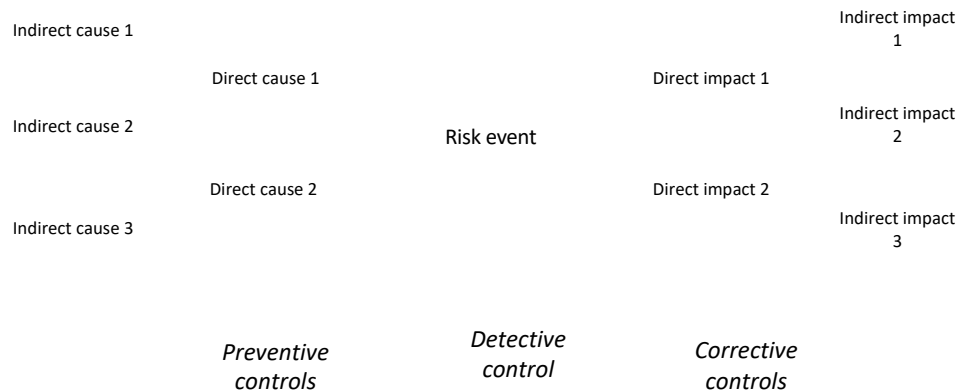


Figure 1.2: **Bow-tie tool's illustration (A. Chapelle, 2019)**

#### 1.4.10 Conduct, Culture and Data Processing

Conduct event is the one that breaches conduct regulatory requirements (Basel Committee of Banking Supervision, 2011; Chapelle, 2019). Culture consists of the key behaviours in the organisation. Risk culture is part of the corporate culture and risk management discipline across the organisation. Building risk culture through targeted risk training and risk management activities are the tools for achieving effective risk and conduct culture (Basel Committee of Banking Supervision, 2011; Chapelle, 2019). Data risk management is one of the most important risk management blocks related to risk culture for most of organisations, as the data processing law has become a necessity in the 21st century, following the abundant supply of smart digital devices and easy accessibility of Internet forms a big block for conduct and culture risk management. EU GDPR raises the control mechanisms for personal data processing and grants data subjects with rights to be aware and to be able to control who, why and how uses and processes their personal data (Martinez-Martinez, 2018). There were certain controls and risk management tools introduced to deal with conduct and culture risk management related to the data.

In relation to the sector of education, following the enforcement of GDPR it is not anymore allowed to publish personal data of students on school's website, such as photographs, personalised achievement greetings, lists of enrolled students. etc., without the consent of the data subjects or their guardians. Also, any communication performed by school should be based on specific legal grounds (e.g., security of child, provision of essential education services, consent from parents, etc.). Free

sharing of personal information without a proper justification is not permitted anymore and may be punished with radical fines (Datu Valsts Inspekcija, 2018; Gines, 2018; Morrison, 2018).

Institutions, in order to be compliant and build strong data risk culture, should be able to answer the three key questions in the documented way to ensure compliance with data protection regulation and to avoid the risk of breaching regulatory requirements (Datu Valsts Inspekcija, 2018; Morrison, 2018):

1. What is the purpose for data processing? Is it lawful and justified?
2. What data is needed to achieve the goal? Can it be done with less data?
3. What is the legal basis for data processing?

The key aspects that need to be considered in each and every educational institution are the following:

1. The data processing must be lawful, fair and transparent. When data is collected, it must be clear as to why that data is being collected and how the data will be used. If a data subject asks what personal data, we have about them and what is it used for, that information needs to be available.

2. Data minimization principle should be ensured: only the minimum required amount of data required for reaching the set purpose can be collected and stored. Unnecessary duplication of data should not be permitted.

3. Accurate and up-to-date processing principle require institutions to make sure information remains accurate, valid and fit for purpose.

4. Every institution, which acts as data controller or data processor, is responsible for data confidentiality, security and privacy (which extends to IT systems, paper records and physical security).

5. There are three specific criteria around the requirement to appoint a Data Protection Officer (DPO), where one or another will apply to all educational institutions, authorities and stakeholders, i.e.:

- a) where the processing is carried out by a public authority or body,
- b) where the “core activities” of the controller or processor consist of processing operations which require regular and systematic monitoring” of data subjects on a “large scale”,
- c) where the “core activities” of the controller or processor consist of processing on a “large scale” of “special categories of personal data” or data relating to criminal convictions and offences.

The DPO can be appointed full-time, part-time or as a shared or external consultant (Wheeler, 2017). There are certain requirements that should be considered in relation to appointment of DPO. Firstly, DPO should be in a position to perform his/her duties and tasks in an independent manner, however the Controller remains responsible for compliance with GDPR. Secondly, DPOs may not be

dismissed or penalized for performing his/her tasks and must be free from any conflicts of interests. The main duties of the DPO should be: informing and advising the controller or the processor and their employees of their data protection obligations, monitoring compliance with the Regulation, raising awareness among staff members and providing training, providing advice, where requested, as regards the data protection impact assessments (DPIAs), engaging with the Information Commissioner's Office or relevant Supervisory Authority (Demmel, Kuschewsky, 2017; Morrison, 2018).

In regard to processing of children's data, the institutions should be considered of the fact that up until reaching the age of adolescence, the child is under the guardianship of parents, therefore, the consent of the legal representative (parents), including for educational institutions, must be sought for the processing of the child's personal data (Datu Valsts Inspekcija, 2018; Morrison, 2018). It is important to note, that the consent of the data subject is a free, explicit statement of will by the data subject that allows the data subject to process his or her personal data in accordance with the information provided by the controller. In cases, where parents do not provide consent for processing of personal data, which does not fall within the scope of minimal needs for personal data processing for provision of education, children's data must be "anonymised" by, for example, numeric combinations, which have not specific meaning in relation to concrete child (Datu Valsts Inspekcija 2018). Furthermore, even when such consent is provided, the Controller is still liable for security of data. This especially relates to cases, when education providers communicate with parents and transmit data through digital and mobile channels, such as WhatsApp, Skype or e-mail. Although, this is permitted under GDPR with the according consent, the data controller will still be liable for data breach incidents and security related issues. These risks shall be addressed as part in internal risk culture, as well as documented in annual RCSA and other risk assessments, as described above.

#### 1.4.11 Incident Data Collection

Incident is the materialisation of a risk. It is defined by multiple authors as an event that is different from regularly followed routine due to failure in process or IT systems, human factor errors or external environment caused situations. Incident data collection is one of the most important risk management tools, as everything in risk management is built around and depends on the incident database (Chapelle, 2019). Incidents help to identify breaches and gaps in controls, assist in risk scenario identification process and risk assessments. The concept of incident management was established, and in some cases even is regulated by law, in such industries as banking, healthcare, aviation, construction, rail, energy, manufacturing, maritime, etc. (Margaryan and Littlejohn, 2016; Canham and Jun, 2018; Staender, 2011). In the education institutions of Latvia this practice is not widespread: according to empirical research results, only 1/3 of all respondents in this study,

discussed in Section 3, confirmed that their educational institutions use incident reporting as a tool for effective risk management.

According to author's professional observations and as discussed in most of the scientific publications referenced, incident reporting discipline in the organisation usually characterises organisation's risk culture. Time lags between date of discovering an incident and date of reporting demonstrate the reporting discipline and the risk culture. But often employees are reluctant to report incident either by lack of knowledge, lack of understanding of the purpose or too complicated reporting process.

Incidents, where losses are avoided by sheer luck, are called "near-misses" and are evaluated based on the potential losses that could have happened and are also included in the incident data set (Chapelle, 2019).

A lot of incidents have zero monetary losses, but are subject to non-financial losses, such as damage to reputation, waste of time and resources, etc., which can be very challenging to quantify. Therefore Chapelle (2019) recommends re-using the impact score used in the risk scenario assessment process in assessing potential impact of non-financial incidents. Although such practice may prove to be challenging for institutions with less mature risk management practices.

The risk management functional unit or a risk coordinator should organise reporting of incidents into as much as possible simple and purposeful process in order to encourage employees to diligently report incidents instead of avoiding such reporting. Co-operation should be fostered between risk coordinators and other employees in order to achieve transparency and stronger risk management discipline. Employees should be able to see that their act of reporting of an incident has led to certain improvements in the organisation and has added value, otherwise reporting can be perceived as demotivating and unnecessary burden.

Incidents with larger impact or potential impact should be reported to the management in order to assist decision-making and prioritisation at the higher administration level. Kelliher et. al. (2016) suggests grouping losses which are characterised by one cause and also high frequency and low impact losses characterised by different causes and aggregate those small losses into one in order to inform assumptions about the real impact of different «small» loss events.

BCBS issued Adverse Measurement Approach guidelines for banks, where the best recommended practice is to record three «reference dates» for each incident: date of occurrence, discovery and accounting date. It is needed in order to capture the time lags between event occurrence, its actual discovery and the emergence of losses, which can be used for future forecasting and better understanding of operational risk exposure (BCBS, 2011).

Incident database should be regularly (at least once a year) reviewed for quality and reconciled with other sources of information, such as accounting general ledger, media coverage reviews, legal provisions, etc. (Chapelle, 2019; Kelliher, et.al., 2016).

From the risk management perspective educational sector is exposed to a number of different risks which may result in serious incidents: student safety, research labs (e.g., chemical), food provision, new educational program introduction, change of methodology in teaching, budget allocation, selecting of co-operation partners, recruitment of teachers, accreditation process, power failure in educational institution, personal data leaks, and other. The cost of claims to education institution, not only financial, but also from a public image standpoint—can be significant. Educational institutions need to protect students, teachers, faculty, administration, support workers, contracted workers, community and their institution's reputation and budget. If educational institution's reputation is affected, a serious threat to future admissions, endowments, and financial strength is posed. Identifying and forecasting these risks via the incident reporting process is a common approach used by the risk managers in the corporate sector. Although the educational sector may face lower losses rather than the industrial sectors, effective incident management would help to ensure avoiding of financial losses and be prepared for any upcoming challenges.

Incident management as risk management tool is needed in order to improve organisation's performance and internal control environment; it is important to know what incidents occur in the organisation to be able to identify weakness points and possible breaches (Chapelle,2019). Occurrence of incidents is unavoidable and even a minor incident can provide valuable feedback for improvement of safety, quality and management in the organisation (Westhuizen, Stanz, 2017; Staender, 2011). Staender (2011), Margaryan and Littlejohn(2016) and Stemn and Bofinger (2018) discuss the concept of “learning from incidents”, which means that the organisation can learn from unexpected safety events to prevent similar such events that may happen in the future. This may be applicable not only to safety events, but any incidents, that cause any kind of losses. Nowadays the concept is applied in variety of industries, such as manufacturing, aviation, healthcare, transport, banking and finance, etc. (Margaryan and Littlejohn, 2016; Staender, 2011). Incident reporting provides the opportunity to reveal the weaknesses that allowed incident to happen and to act upon it to make required improvements (Staender, 2011; Chapelle, 2019).

The effective incident reporting process contains important steps, which include reporting of an incident, thorough investigation to identify and analyse the root causes of the incident and then drawing out recommendations and “learning points”, that are used for implementation of required changes in order to prevent the same incident from re-occurring (Staender, 2011; Margaryan and Littlejohn, 2016; Stemn and Bofinger, 2018). Staender (2011) compares incident reporting to the

storytelling and states that these reports can be collected by an organisation as documented experience used for applying necessary improvements.

Another important step in incident management is to communicate the required changes in human behaviour or processes to relevant responsible stakeholders, as without good communication implementation of changes (or mitigation actions) will not be effective and may not take place at all, if not addressed to the key responsible people in the organisation. The communication channels can be reports, internal regulations and manuals for employees, notice boards, notification e-mails, team discussions (Margaryan and Littlejohn, 2016). Stemm and Bofinger (2018) noted that learning from incidents is the key for achieving high levels of safety in organisations. Moreover, incident reporting is useful for scenario planning and analysis, which should be used for critical incident planning and management. Incident database can serve as a great input for risk modelling and risk scenario planning (Mazaheri and Montewka, 2015; Chapelle, 2019).

Studies of Margaryan and Littlejohn (2016) and Westhuizen and Stanz (2017) identified that there are problems with behaviour of reporting, i.e., incidents often are not reported because employees are reluctant to report due to the burden of completing incident report and consequent liability to get involved in the investigation or root causes. Lack of understanding of the incident causes or the importance of the incidents are additional reasons for avoiding reporting incidents. Also, often organisational ethics act as the key driver for reporting or not reporting the incidents (Westhuizen and Stanz, 2017).

Filtness and Goode (2015) performed research about usage of incident reporting system in hot air ballooning industry and came to conclusion that majority of respondents did not report incidents mainly due to lack of understanding of incident reporting process, when to report and how, as well as not seeing the significance of incidents to be reported. Another important aspect raised by majority of researchers is ease of incident reporting process: the simpler is the routine the more successful it becomes. Westhuizen and Stanz (2017) highlighted the perceived burden of incident reporting, which served as predicament for active reporting of incidents in air navigation industry. Hence, user-friendly simple system is an important factor in successful implementation of incident reporting in any organisation.

Staender (2011) in addition mentions the fear for reporting, as it may affect reporter's further career due to blaming culture. Filtness and Goode (2015) mention incident database as an important tool for holistic incident management for implementation of improvements and follow-up. In addition, aspects of privacy and usefulness are important, as often the reporters do not want to be recognised and there should be value in spending time into the reporting of incidents, what means



that it is expected that the incident will be investigated, followed up and conclusions for improvements will be drawn.

There are a number of different methodologies how incidents can be analysed, learned lessons applied in practice and discovered risk effectively managed. Stemn and Bofinger (2018) highlight bow-tie analysis (BTA), mentioned earlier (Figure 1.2), as the most effective tool for learning from incidents, where the focus is on threats, consequences and required mitigation controls to prevent the threats from realising and to minimise the consequences. By focusing on the threats, it is possible to develop mitigation action plans that will control threats and prevent the incident, whereas by focusing on consequences, mitigation actions will minimise the impact of realised threats.

Canham and Jun (2018) in turn discuss the usability of Systems-Theoretic Accident Model and Processes (STAMP) concept, which consists of 8 key steps:

1. identification of threats related to incident;
2. identification of safety-related impediments related to the incident;
3. documentation of safety controls in place ought to control the threats;
4. determining possible events that lead to the incident and analysing frontline controls;
5. analysing higher-level controls and reasons why they allowed threats to realise and how;
6. studying overall communication and management problems that could have led to the incident;
7. looking for any recent changes that could have contributed to weakening of controls and contributed to the incident;
8. development of recommendations and mitigation action plans to strengthen controls and prevent incident from re-occurring in the future.

This approach is very comprehensive and being applied would provide very ample risk picture to the organisation, however its disadvantage is the amount of required time and effort, what most of the organisations would not be able to contribute in order to fulfil the entire process due to lack of capacity and resources.

Staender (2011) in his study discussed so-called “plan-do-check-act” (PDCA) cycles, concerned with the incidents that call for initiating of improvement process. This is simpler and less time-consuming approach, where it is possible to act upon the incident by planning concrete mitigation actions, implementing them and then performing follow-up on the effectiveness of controls. This is the most popular approach applied by the organisations due to its simplicity and effective use of resources. In combination with BTA approach discussed above, it would be possible to focus planned actions on threats or on consequences and thus mitigate the most painful problems that organisation is facing.

Stemn and Bofinger (2018) researched the consequences of not using incident reporting as a tool for learning and improving organisational performance and came to the following conclusion, that not paying attention to incident recording and learning from incidents leads to:

- regular repetition of similar incidents that wastes time and resources on frequent resolution of the same problem;
- transformation of insignificant incidents into significant and even crisis;
- incidents start to be accepted as normal course in daily routine, thus affecting long-term quality of provided services.

Stemn and Bofinger (2018) highlight that the key prerequisite for successful implementation of learning from incidents is internal culture focused on learning and self-improvement. In addition, organisations need to ensure qualitative collection of incidents and root causes, thorough investigation and developing efficient and well communicated improvement plans. According to Staender (2011), the following important factors serve as key prerequisites for successful implementation of incident reporting in any organisation:

1. comprehensive training of what should be reported and how;
2. continuing trainings on the importance and purpose of incident reporting, criteria for reporting, list of incident examples, user-friendly reporting form (an example provided in Table 1.5 below), clarity on how to report, dedicated person allocated for reported incident management, regular feedback on reported incidents, etc.

In addition, Staender (2011) state that an important role is in ensuring confidentiality of the person reporting an incident and assurance that the information will not be used against them.

The following type of register as presented in Table 1.5 can be used by the educational institutions to record all incidents that happen, including low impact incidents. This type of form would be easy to use, and the questions would guide the reporter on what needs to be recorded, what will subsequently assist in more comprehensive analysis if needed:

Table 1.5. **Incident reporting form example**

<b>Incident nr.</b>	It is important to allocate specific number for each separate incident for orientation purpose
<b>What happened?</b>	Short description of incident
<b>When and how was it discovered?</b>	Short description how the incident was discovered to reveal transparency or any breaches
<b>What are the root causes?</b>	Most important part to analyse why the incident happened and what caused it
<b>What are the consequences/losses?</b>	Description of financial and non-financial losses and consequences
<b>When and how did it start?</b>	Important to note to better understand root causes and possible additional breaches
<b>What mitigation actions are planned/executed?</b>	Here the focus can be on mitigating the root cause or the consequences
<b>Status</b>	Status of the mitigation actions and the incident itself, e.g., “closed, mitigation actions no needed”, or “open, mitigation actions in process”, or “closed, mitigation actions in process”, etc.

Threshold for reporting in educational institutions are not recommended to be set in order not to miss small but frequent events that impact the quality of education and general risk profile. Incidents can be recorded in a journal one by one or placed in Excel database with the same columns made vertical for recording many incidents on one sheet in order to have holistic summary for analysis and reporting. Example of such incident database or register is provided in Appendix 3, Table 6.1.

Drawback of incident loss database or register in risk management is that it is mainly backward-looking, often is incomplete and does not cover long period of time, as the practice of recording incidents is quite new. Incident loss database may not be sufficient for future risk forecasting, as historical incidents may be irrelevant in the future due to implemented controls and do not capture new and emerging risk exposures that have not yet manifested as incidents. Therefore, to overcome

this drawback in risk management programme, it is important to also perform annual risk control self-assessments (RCSA) and develop adverse risk scenarios for analysis and stress testing exercise withing the risk modelling process (Kelliher, et.al., 2016; Chapelle, 2019), all of which are discussed in other chapters of this study.

#### 1.4.12 Key Risk Indicators (KRI)

KRI play an important role in risk management as risk monitoring tool. KRIs translates the risk appetite into daily risk monitoring activities and measure potential impacts of risks and risk exposure for the organisation, serving as early warning signals. KRI provide objective and documented way of demonstrating whether the risk controls work and provide the management of an institution with regular information on changes in the risk profile of the institution and whether any risks are gaining more resonance, thus enable management to take actions before risks have realised into real losses. KRI can be any piece of data, that can perform the function of a metric to monitor identified risk exposure over time (Chapelle, 2019; Beasley, 2013;The Institute of Operational Risk [IRM], 2010).

KRI are often confused with Key Performance Indicators (KPI) and Key Control Indicators (KCI). KRI measure risk exposure of identified material risks relevant to the specific institution, whereas KPI measure achievement of objectives and KCI measure effectiveness of internal controls. KRI, KPI and KCI often overlap (Chapelle, 2019; IRM, 2010). KRI should be tied up to the acceptable level of risk setting and assist with an early warning signal that acceptable risk level limits may be breached soon. KRI is interlinked with RCSA, Risk Appetite, Scenario Analysis and other risk identification and assessment processes, and serves as a great tool for managerial decision-making, if developed and integrated correctly. However, IRM (2010) highlight, that it is not possible to develop a universal set of KRIs, that would be suitable for all organisations simultaneously, as KRI must be tailored to the most material risks inherent to an organisation, which usually differ according to the strategic objectives, acceptable level of risk, material risks, operational specifics and mission.

Chapelle (2019) state that KRI can be split into four categories: exposure, stress, failure, and causal, as represented in Table 1.6. Exposure KRI measure exposure to certain risks. Stress KRI measure overstretching of resources in the organisation. Failure KRI measure weaknesses and failures in risk controls. Causal KRI measure the causes of key risks.

Table 1.6: Categories of key risk indicators with examples. Source: Chapelle (2019), p.

147

Indicator type	Description	Examples
<b>Exposure indicators</b>	Monitor changes in an organisation's exposure to one or more risks, either in likelihood of occurrence or potential impact	Changes of resources exposed to risk, changes in political or regulatory environment
<b>Stress indicators</b>	Capture the stretch in organisational resources in human capital, equipment or IT	Rise in transactions handled per staff, long-term vacancies in small teams; percentage of machine time operated at capacity level, reduced buffer system capacity, overdue maintenance, missed intermediary deadlines, etc.
<b>Failure indicators</b>	KRIs derived from failing organisational performance and/or control weaknesses; typically captured by a KPI or KCI breaching their threshold.	Unconfirmed back-office transactions, incomplete client files, incomplete due diligence check (suppliers/staff), poor customer services ratings.
<b>Causal indicators</b>	Metrics that provide information about the causes and root causes of key risks.	Pay under market rate (for key man risk), financial pressure (for internal fraud), abnormal trading pattern (for rogue trading), abnormal behaviour pattern (for all types of fraud).

For effective monitoring, KRI thresholds must be set in accordance with the Risk Appetite thresholds (IRM, 2010), as demonstrated in Table 1.7. Thresholds are translated into three colours that call for certain action: green - do nothing, amber – monitor risk, red – act on risk. Upon breaching certain threshold, the KRI can be escalated to management for consideration and decision-making:

Table 1.7: Key risk indicator threshold examples. Adopted from IRM (2010)

Red	<ul style="list-style-type: none"> <li>➤ The value of KRI is too high/low suggesting that organisation may be exposed to significant risk.</li> <li>➤ Immediate action is required to manage risk(s) in question.</li> </ul>
Amber	<ul style="list-style-type: none"> <li>➤ The value of KRI is higher/lower than normal suggesting that the organisation may be exposed to an elevated and potentially significant level of risk.</li> <li>➤ Management attention is required to determine whether action needs to be taken in the near future.</li> </ul>
Green	<ul style="list-style-type: none"> <li>➤ The value of KRI is within normal parameters, suggesting that the organisation is not exposed to significant risk.</li> <li>➤ No action is required – the indicator and its associated risks are under adequate control.</li> </ul>

IRM (2010) split KRIs into “leading” indicators, “lagging” indicators and “current perspective” indicators. “Leading” indicators are those that provide forward-looking view (e.g., on emerging risks), “lagging” indicators are those that provide historical view on the risk and its development trends, “current perspective” indicators provide a picture of current risk exposure and may raise the “red flag” to address a certain issue immediately before it realised into a loss incident. Also, KRI can be split into three types according to IRM, 2010:

- “Specific focus indicators” – KRIs focused on specific risk exposure area;
- “General focus indicators” – KRIs that provide general impression of risk exposure in certain area of interest;
- “Common or generic indicators” – KRIs that can be used anywhere by simply adding some specific context.

IRM (2010) state that frequency of KRI monitoring is important: the more frequently the KRI is monitored, the better risk exposure picture it can provide. For example, frequent KRI can provide an indication whether exposure to certain risk is increasing or decreasing. Indicators that breach the limits defined via thresholds and denoted via the colour coding as described above.

The classic KRI examples are provided in Table 1.8 as published by Chapelle (2019):

**Table 1.8: KRI examples. Source: Chapelle (2019), p.154**

Classic KRI	Recommended
Sick days	<ul style="list-style-type: none"> <li>▪ Number of % rise in short leave (Mondays and Fridays) – signal of absenteeism</li> <li>▪ Number of long-term sick leave (&gt;3 months)/in small teams – risk of overstretch of resources</li> </ul>
Downtime	<ul style="list-style-type: none"> <li>▪ System interruption &gt; x minutes in a row over the last three months (x depending on the nature of the activity)</li> </ul>
Vulnerabilities	<ul style="list-style-type: none"> <li>▪ Critical vulnerabilities unpatched within policy deadlines</li> </ul>
Turnover rate	<ul style="list-style-type: none"> <li>▪ % of talent/high potential staff resigning over the last 3 months (lagging but more specific)</li> <li>▪ Number of talented individual underpaid/without substitute/unmanaged/expressing dissatisfaction at work</li> </ul>
Recommendations following a penetration test	<ul style="list-style-type: none"> <li>▪ Delays in action plans following the penetration test</li> </ul>
Customer complaints	<ul style="list-style-type: none"> <li>▪ Customer complaints unresolved within x days (x depending on the firm’s policy and tolerance for customer dissatisfaction)</li> </ul>

KRI are validated by looking into incident database. If number of incidents decreased due to acting on KRI red or amber warnings (as presented in Table 1.7) or if there were no incidents following green KRI (as presented in Table 1.7) – then the KRI are valid. If the red KRI (as presented in Table 1.7) do not foster any actions and reduction of incidents or if green KRI (as presented in Table 1.7) result in number of incidents, then the KRI are not valid.

KRIs assist in highlighting the risks before they turn into loss incidents (IRM, 2010). For example, personnel turnover can be tracked to evaluate level of staff expertise and experience, hence the quality of education provided, as well as employee relations and employee satisfaction. IRM (2010) highlight that KRIs must be quantifiable in terms of amount, percentage, ratio, number, etc. and the values of KRIs must be comparable over time.

Alberts and Dorofee (2009) introduce a concept of systemic approach to risk management, where KRI are set from the perspective of key objectives – the expected outcomes from certain activity used to measure the success. In their view, it is crucial to first define the key objectives of an organisation, then define critical factors, or drivers, that would put obstacles on achieving the key objectives. These factors will be the key risk indicators used for subsequent analysis of risks. Risk management has crucial role in achieving the objectives. As Alberts and Dorofee (2009) define distributed management environment, where management controls are shared by several organisations or different people for the same technology or process. In such environments the success directly depends on collaborative co-ordination of tasks and risk management. There is no as simple situation as single risk linked to a single cause, but instead risks may have many different causes. The risk indicators are directly linked to the key objectives of organisation and thus provide holistic view of the risks. Important to note here is that as drivers are derived from the key objectives, they need to be reviewed each time together with the objectives. Moreover, drivers should be developed for each life cycle of objective achievement: during the planning and development stage the objectives may differ from those during the execution stage, etc. This is very relevant for new institutions and those that introduce new programmes in their curriculum.

Table 1.9 provides a plan made by Chapelle (2019) for development of effective KRIs:

**Table 1.9: Steps for Key risk indicators. Source: Chapelle (2019), p.155**

1. Identify	Key risks to the organisation
2. Understand	Causes and root causes of these key risks
3. Recycle	KPIs and KCIs that can be treated and KRIs
4. Define	Missing metrics of key risk drivers
5. Design	Data capture, frequency, thresholds and reporting governance
6. Validate	The preventive nature of KRIs

According to IRM (2010) the data for KRI must be easy and cost-effective to collect in order to derive most value from the KRI monitoring process. Another important rule is that the data should be easy to interpret and understand to enable effective risk management and prompt decision-making. Finally, KRI must be easy to verify as incorrect or erroneous data un KRIs may lead to incorrect decisions.

To sum up, when setting the KRIs for an organisation, according to IRM (2010), the identified material risks should be taken into account, as well as availability of data for KRIs, costs of extracting the data for KRIs and what is the intended audience and purpose of the KRIs. It is also should be decided how often the KRIs will be reviewed and what will happen with those KRIs which are discontinued after the review. It is recommended to report KRIs in way of dashboards with use of colour coding in order to provide clear and simple overview of KRI trends and any breaches of thresholds.

#### 1.4.13 Risk Reporting

Important part in risk management is reporting, which aims to support decision-making and prioritising for the management. Golden rules for effective reporting according to Chapelle (2019) are the following:

1. cost of report preparation should not exceed the value that it creates;
2. reporter should know exactly how the information should or will be used;
3. the report must influence the decision-making of the management, even if it will only confirm the status quo and correctness of opinions.

Usually, the reporting should happen on monthly or at least quarterly basis and should provide information about the top incidents, the top risks, KRI monitoring results, risk appetite status and the risk mitigation action plans and status of previously reported activities to mitigate highest risks or recover largest losses.

Risk reporting has its own challenges, which include finding the right balance between too much and too little information in the report, deciding on what should and should not be reported and aggregating the risks.

There is no averaging in risk management for risks and incidents, as some incidents have very rare occurrence, but very large losses, whereas some incidents happen frequently, but with low or zero losses. Better measures than average are medians and quartiles, as well as it is proved useful to split expected losses from unexpected losses.

There are established risk reporting routines in large regulated corporate organisations, such as banks. Information flows from risk management experts to top management of organisation, then to



stakeholders and regulators. Regulators country by country collect such information from different financial institutions, consolidate and analyse it for strategic planning. Such integrated information about risks is further communicated to central EU authorities, which further use it for EU-wide planning. The same approach of data sharing can be applied in educational sector, which would significantly improve strategic planning on country level and distribute funds more fairly and efficiently.

IRM (2010) highlight the 5 features, which any risk report should include:

- relevance – the information in the report should be relevant and not too detailed;
- simplicity – reports should not be over-complicated with technical terms and complex formulas, but instead simplest graphs and tables should be used in reports to represent data without too much text;
- timeliness – it is important to produce the reports timely to ensure that data is relevant in particular point of time and is not overdue;
- accuracy – data in the reports should be precise and accurate to avoid wrong decisions and false snapshot of risk exposure;
- trending – the reports should provide the historical trends to enable comparability with present moment and indication of volatility;
- clear escalation procedures – it should be well understood when the recipients of the report need to escalate matters further;
- compliance – reporting must comply with any relevant regulations.

#### 1.4.15 Risk modelling

Risk modelling is one of key risk management practices in sectors with established risk management requirements and routines. Looking at the banking and insurance sectors, where the main requirements for risk modelling were established by BCBS, further adapted and complemented by European Banking Authority (EBA) and each country's Financial Services Authorities (FSA). Specifically, BCBS had first published global requirements in 2004 and finalised in 2006 as part of Basel II framework. Afterwards framework was reviewed, updated and supplemented on continuous basis, which led to Basel III framework, which is being enforced in 2022 with more comprehensive requirements for risk modelling in financial services industry.

In the framework for risk modelling in financial services firms, the notable part is the operational risk management modelling, which is the most applicable to the sector of education due to this risk type's non-financial nature and natural applicability to any sector, because the risk nature of operational risk type relates to the general operations and can be applied to any type of activity. As mentioned above, Operational risk is defined by the BCBS as the probability of loss from the

actions of people (human errors, lack of confidence, internal fraud, etc.), deficiencies in processes (process gaps, lack of documented processes, lack of controls in processes), system downtimes (system bugs and errors, system's out-of-service, etc.) or external events (weather conditions, vendor behaviour, crisis, etc.).

Risk modelling in the sector of education can be performed by the skilled risk coordinator, who would calculate potential cost of risks for the upcoming years by stressing loss data collected in previous years through incident reports, Scenario Analysis, RCSA and regular risk assessments. BCBS and EBA require banks to use at least three years of loss data as the minimum. Using more years of data provide more stable and reliable results.

Another useful source of information for modelling of stressed environment (stress tests) used in financial services operational risk management is incident losses of peer organisations. It is useful for calibrating severity distributions in internal loss datasets and to analyse incidents, which have not yet happened with the organisation in question, but have happened to similar organisations, scaled accordingly to the size of organisation in question, and preparing the mitigation plans in case the risk of suffering similar loss is adequately high (Kelliher, et.al., 2016). Such dataset should be structured in the same way as internal loss data and in the same way should be regularly reviewed for quality. It serves as a great input for brainstorming during risk scenario generation processes in annual and more regular risk assessments, Scenario Analysis, and further utilised in the risk modelling process.

Each organisation can build their own risk model, whereas the most popular for non-financial risk modelling is Loss Distribution Approach (LDA) (Dutta&Babbel, 2014; Chapelle, 2019).

#### 1.4.16 Project Risk Management

Changes in services, systems, operations and products usually caused by regulatory requirements (e.g., GDPR, educational reforms, pandemic related restrictions) or necessity for achievement of certain organisational goals, are organised as projects. Usual causes of risks in project management are: weak governance, inadequate deadlines, short-sighted budgeting, lack of synergies, poor internal competence, conflicted interests. Therefore, at the initial phase of project management, before the kick-off of the projects, project inherent risks should be identified and assessed by the project team together with the risk coordinator. Risk management functional unit or the risk coordinator at the initial stage should play the role of gatekeeper in project management and enforce sound decision-making process prior to launching a project. This can be effectively done by running a risk assessment at different stages of the project.

During the Risk Assessment process, when risk scenarios are identified, each and every risk scenario should be evaluated in regard to the probability of occurring (frequency) and the total negative impact that it will have, be it financial or non-financial consequences, direct or indirect

(Chapelle, 2019; Walker, 2013). Impact is usually assessed before taking into consideration any insurance cover and should be linked to the reality and risk drivers as much as possible.

Mitigation and monitoring plans should be developed at the initial stage of project life cycle. During the project life, monitoring and risk update reporting should take place on quarterly and half-yearly basis. During the project life the risk function should not intervene, but project managers should send regular updates on the risk level to all stakeholders, including risk function (Abraham, et.al., 2013; Chapelle, 2019).

During the life of a project, it is important to have holistic view on the project portfolio and identify any interdependencies that may hamper the project deliveries, such as reliance of different projects on the same resources or systems and dependency on deliveries by other projects. Such interdependencies need to be minimised in order to reduce the risk of poor or late project deliveries.

At the project closure stage debriefing on post-delivery review of risks, risk mitigation action status and lessons learned should be made with all stakeholders (Abraham, et.al., 2013; Chapelle, 2019).

Project risk management should follow the same methodology as RCSA; however, the risk impact scores can be based on the project budget rather than the acceptable level of risk. In addition, KRI can be developed for projects to monitor complexity, usage of resources, mitigation of residual risks, time, budget, project scope and stakeholder satisfaction (Abraham, et.al., 2013; Chapelle, 2019).

### **1.5. Summary**

Section introduced the concept of risk, risk management purpose, types of risks, key problems and issues and risk management tools and techniques, discussed in different sources of literature, as well as model developed by the author. Section covered the following concepts:

- Financial and non-financial risks threaten the achievement of strategic organisational goals;
- Risks shape external and internal environment of the educational sector;
- Stakeholder analysis play an important role in risk management process;
- Key pillars of successful risk management are: risk governance, risk identification, scenario analysis, risk networks, risk assessments, risk mitigation, root cause analysis, internal culture, data management, incident data collection, external loss data collection, key risk indicator monitoring, risk reporting, third-party risk management, risk monitoring, building value through risk management and project risk management;
- Risk management starts from defining objectives and strategic goals. Based on strategy, mission and goals, material and most relevant risks should be firstly identified, then assessed

and afterwards monitored and reported. Material risks are reviewed and re-assessed following changes in strategic objectives;

- Risk identification and risk assessment tools used on a regular basis can significantly strengthen the risk management of each educational institution by preparing them for facing all risks identified and assessed through the risk assessment and Scenario Analysis;
- Incident reporting is an important tool for learning from own failures and for risk effective management. Having an incident register in every educational institution would assist managers and officials to address the correct problems faced by concrete institutions and to analyse regional problems and correlation of incidents with other factors that would help to realise required developments;
- To manage risks successfully it is important to measure and report them. A tool that may be used for risk monitoring is KRI framework, organised in a dashboard for reporting;
- Risk management in educational institutions can be performed by the skilled risk coordinator appointed by local municipality and covering multiple schools within the municipality or appointed by each institution as full time employee.

## **2. RISKS IN THE SECTOR OF EDUCATION**

The aim of this chapter is to introduce the key risks and application of risk management theory into the sector of education. This chapter will provide an overview of different risk groups that are relevant for the sector of education as studied by various researchers, how the risks within those risk groups can be managed and will review the effective risk management model for the educational sector.

Starr (2012) highlights that risk involves the elements of social, cultural, ethical, political, legal, psychological, economic, environmental and technological nature. The author selected and analysed risk groups, which were most often analysed in the researched materials and, therefore, may have the highest level of relevance to the educational sector: psychosocial risks, information security risks, privacy and cyber security risks, risk of corruption, legal risks, external risks and reputational risks (Tufano, 2011; Clark, et al., 2013; Adams, 1973; ADB, 2010; Dunklee and Shoop, 1993, Forlin, 1995; Abraham, et.al., 2013). Risks within these risk categories are discussed in more details in this section.

Upon the results of the theoretical and practical research of risks, relevant to the sector of education, performed in scope of this dissertation, the author has developed the taxonomy of risks, provided in Appendix 4, which can be further utilised by the managers and risk coordinators in the sector of education.

### **2.1 Psychosocial risk group**

Rapid developments in the job market caused by globalisation and technological revolution resulted in changed risk factors in the work environment. For example, nowadays teachers in addition to classroom work must be able to provide all resources digitally via special dedicated online study platform, have to be able to operate well with technology and constantly update their knowledge about latest tools (Souto, et.al., 2018). Inability to meet job requirements or control circumstances at the workplace may cause work-related stress that takes the form of emotional and physical reactions (Kaļķis, 2008, 191; Fernet, et.al., 2016; Souto, et al. 2018). As a consequence of psychosocial risk realisation, employees are taking long periods of sick leave, underperform at work or constantly arrive late, burn out, in addition there are possible work-related incidents, damage of employer's image and reputation, often it is employer's responsibility to pay out compensations (Kaļķis, 2008, 192; Souto, et al., 2018; Guadix, et.al. 2015).

Psychosocial risks at work bring the highest threats for educational institutions, due to high probability and severe impact. In Latvia the problem is further amplified by employee's inability to

recognise these problems or lack of courage to openly discuss it with the direct manager in order to find mutually beneficial solution, as well as missing feedback culture. This further leads to distress in employees and its related problems, such as alcoholism, neurosis, oncology, psychosomatic disorders, theft, etc. (Kaļķis, 2008, 191-192).

Psychosocial risk group is one of the largest risk group types and is related to the aspects of staff over burning, lack of employee motivation, health problems due to stress, etc. Psychosocial risk factors, as identified by multiple researchers, are: frequent overtime, not involving employees in managerial decision-making, not ensuring sufficient information exchange for employees, unfavourable working conditions and organisational design of work (Kaļķis, 2008, 192; Souto et al., 2018). According to the results of empirical research performed for this thesis, which will be analysed in detail in Section 3 of this study, psychosocial risk group is the most significant for the sector of education. Empirical research carried out within the scope of this research and discussed in detail in Chapter 3 has shown that the top risks perceived by the education sector professionals in Latvia are overloading of employees and lack of employee motivation.

Work related stress can be caused by increasing job demands, employee's inability to cope with those, as well as employee may be lacking required skillset or motivation to perform at work according to set expectations. In addition to that, psycho-emotional type of work-related stress can be caused, if workplace does not meet employee's needs or there are unsatisfying relationships with colleagues and/or manager. For example, employee may be subject to psychological terror at work, bossing or mobbing, which are types of bullying at work, caused by employee's manager or colleagues respectively (Kaļķis, 2008, 191).

Work stress usually is caused by overtime work and can take two forms – physical (headaches, breathing problems, voice disorder, dry mouth, muscle tension, cardiovascular disorders) or psychological (aggression, concentration difficulties, fear, apathy, depression, increased number of incidents) (Kaļķis, 2008; Souto, et al., 2018).

According to Self-Determination Theory (Fernet, et al., 2016), employees engage in activities for a certain motive, which further affect their psychological state of well-being. Within the scope of Self-Determination Theory, employee motivation takes two forms of motivation: autonomous, when employees perform their job with pleasure out of intrinsic willingness connected to internal values and own feeling of importance of the performed job duties, and controlled, when duties are performed under external or internal pressure, such as for reward or to avoid certain unpleasant consequences (Fernet, et al., 2016). Autonomous motivation is positively correlated with psychological health, job satisfaction, high commitment to work; on the contrary, controlled motivation is associated with emotional exhaustion, work-related stress, burnout and workaholism (Fernet, et al., 2016). Self-

determination theory states that work environment plays the key role in determining the employee motivation. Looking from the perspective of Job Demand-Resource Model (Hakanen, et al., 2005), job demands, which are aspects of the job obstructing completion of tasks and resulting in employee's personal costs, such as disrupting behaviour of students, mainly cause controlled motivation, whereas job resources, which are aspects of the job boosting employee's ability to complete tasks and develop professionally, such as job recognition, cause autonomous motivation (Fernet, et. al., 2016).

Teachers are particularly vulnerable to emotional exhaustion, which frequently leads to over-burning, anxiety, chronic fatigue and sense of helplessness and reduction of autonomous motivation. According to the study of Fernet, et.al. (2016), teacher burnout was positively correlated with job demands, such as high workload and misbehaviour of students, and negatively with job resources, such as supervisory support. Commitment of teachers shows their degree of autonomous motivation that takes form of emotional attachment, association, and involvement with their profession. In addition to that, it was established that level of teacher satisfaction with their occupation and relative psychological investment in the job led to higher attentiveness of students and student achievements (Fernet, et. al., 2016). Controlled motivation, on the other hand, through obstructing basic psychological needs, leads to psychosomatic problems and work-related stress, reducing the commitment and performance of teachers (Fernet, et al., 2016).

Dombrovskis, et.al. (2011) distinguish intrinsic and extrinsic motives, where intrinsic are equivalent to autonomous motivation causes and extrinsic motives are corresponding with controlled motivation causes. Empirical study performed by Dombrovskis et al. (2011) revealed that in Latvia secondary school teachers are predominantly motivated by extrinsic motives, with economic motives taking the first place out of seven on the provided motives scale, indicating job dissatisfaction among secondary school teachers (Dombrovskis et al., 2011). Furthermore, significant positive correlation was found between economic motives of teachers in Latvia and level of their emotional exhaustion. This hinders the intrinsic motivation of teachers, leads to more formal relationships at work, professional de-valuation, inability to value professionalism of colleagues and instead perceiving colleagues more as competitors. Teachers perceive their profession to have low social status, what leads to further loss of intrinsic motivation, reduced performance and increased work-related stress levels (Dombrovskis, et al., 2011).

One more risk, which is caused by psychosocial risk factors, to which teachers are particularly exposed, is voice disorders, especially in large classes with higher number of students. With length of service this problem becomes more actual, thus elder more experienced teachers are more disposed to vocal tissue injuries (Trinite, 2016). Voice disorder is related to occupational risk especially relevant to teacher's profession. The risk factors leading to it are inadequate job resources, such as

poor classroom acoustics, overfilled classes, air quality, stressful situations requiring loud speaking, overtime work requiring voice overload, as well as emotional well-being of teachers at work (Trinite, 2016). The most exposed to this risk are music and sports teachers, according to the study performed by Trinite (2016). In addition, it was found that background noise level in the classroom is directly related to the teacher's stress level, leading to two-way explanation, that increased background noise raises stress level in teacher and increased stress level in teacher transfers to students and in return increase the noise levels. Thus, workload and level of stress have impact also on teacher's vocal health (Trinite, 2016).

## **2.2 Information Security, Cyber and Personal Data Protection Risk Group**

In years 1960-70, all available digital memory was limited to megabytes, the computers were able to process just hundred thousand of operations per second, there were no phones with built-in camera and no access to Internet. By contrast, in 21<sup>st</sup> century the simplest phone produced may process millions of operations per second and has gigabytes of digital memory, enabling everyone to have access to personal data and sensitive information from personal devices and process it for different purposes, which do not always have the good intention. Nowadays everyday user has a powerful weapon in their hands – mobile phone, tablet, portable computer, etc. In 1995 there were circa 16 million Internet users in the world, whereas in 2016 there were over 3.7 billion (Datu Valsts Inspekcija, 2018). Uncontrolled data processing is happening all over the world with use of more and more productive digital devices, turning the world into the digital village (Datu Valsts Inspekcija, 2018).

In March 2018 news exploded about 3<sup>rd</sup> party quiz application on Facebook called "thisisyourdigitallife" (originally built in 2014), developed by Russian American psychology professor, who had obtained data of users by scraping it from the profiles of people taking the quiz and also that of their friends. The data was handed over to political data firm Cambridge Analytica, which further used the data in political targeting and psychological profiling. Although only 270,000 people gave their consent to this quiz application, in reality circa 50 million users' data was collected for use in psychological profiling and micro targeting (Glaser, 2018; Hoffman, 2018).

This story is not one-off event. Martinez-Martinez (2018:186) quote Costas (2017), who proposes the term "digital capitalism" for the phenomena of markets being moved to digital platforms during the information age. It is suggested that "data", "the information" and the user profiles in social networks have become the products and the production resources used in advertising, profiling, market segmentation, behavioural advertising, and targeted marketing. The social network users and their social network profiles are used to make business (Martinez-Martinez, 2018). Personal data has



become key element in digital marketing and profiling across the world for majority of companies, what is compromising data subject privacy and security, without providing any control for data subjects of their personal data usage by third parties.

Information Security risk has acquired the greatest concern of risk managers in recent years and was rated as number one risk by Risk.net survey results seven years in a row from 2014 until 2021. According to the statistics provided by CERT.LV, solely during 2017 only in Latvia in total, were registered 477 252 endangered by cyber-attacks unique IP addresses. As CERT.LV points out, in almost all cases where infected equipment has become infected and have become robot network components (on average 15-20 thousand cases per month), users have not deliberately made harm, but the causes were non-updated software and lack of antivirus solutions. According to Cyber Security Strategy of Latvia (2019) due to the use of ICT solutions and digital technologies, cybercrime is growing faster than ever before, causing losses of at least € 265 billion per year in EU Member States and around € 900 billion per year worldwide.

Information Security incidents may lead to damage of reputation, financial losses and in some cases even may cause cease of business operations due to large data leaks or cyber-attacks (Chapelle, 2019). The main types of Information Security risk are cyber-attack, stolen, lost or unintentionally disclosed information and intentionally corrupted or deleted data following external attack (Chapelle, 2019).

In order to prepare for assessment of information security risks, it is important firstly to prepare information asset inventory by categorising information and documents according to confidentiality levels and revealing what information has the highest value. Next stage is to perform assessment of risks, by conducting information security risk assessment survey, identifying and assessing risk scenarios, as during the RCSA process, and mapping risks on RCSA matrix. Tail risk events such as cyber-attacks and large data leaks can be used in the Scenario Assessment Process (Chapelle, 2019).

Mitigation of information security risks is classified according to three dimensions of information: confidentiality, integrity and availability. There are two types of controls: behavioural and technical. Behavioural controls focus on human behaviour when it comes to handling and protecting confidential information, such as rules for conduct, awareness campaigns and trainings, password management, supervision, and sanctions. Technical controls include system architecture, login monitoring, encryption, passwords, etc.

Information Security KRI focus on effectiveness of information security controls and unexpected deviations from normality (e.g., exposure, traffic, staff behaviour). Table 2.1 provides an example of what KRIs can be developed for the Information Security risks:

Table 2.1: **KRI examples for Information Security. Source: Chapelle (2019)**

<b>Exposure KRI</b>	
	Spread of sensitive information
	Number of users/administrators in excess of the norm
	Number of third parties with data access
	Number of temporary workers and contractors with confidential data access
	Number of temporary workers and contractors with confidential data access
<b>Control failures KRIs</b>	
	Overdue vulnerability patching
	Overdue penetration tests/overdue resolution of penetration tests recommendations
	Software obsolesce
	Results of phishing tests, of password cracking attempts
	# Inadequate access and overdue revisions of access
<b>Stress KRIs</b>	
	% Change in # workload/change request/issues per IT managers
	% Vacancies in IT/cybersecurity teams
	Overcapacity usage of systems
<b>Causal KRIs</b>	
	Conduct metrics on employee compliance
	Breach of conduct and information rules on social media “Repeat offenders” (staff failing more than one phishing test) in sensitive data areas Devices or access cards lost/stolen

According to Cyber Security Strategy of Latvia (2014) and Clark, et. al. (2016), Cyber security risks are dangerous for educational sector from various angles:

- 1) Confidential data stored in educational institutions and educational authorities’ digital spaces may be at risk of being stolen, damaged or destroyed;
- 2) Digital devices used by educational institutions and authorities may be damaged by a virus and destroyed indefinitely causing severe financial damage.

According to Cyber Security Strategy (2019) number of cyber-attacks is growing for public administration institutions, through phishing, ransomware and malware downloading methods, data retrieval or integrity compromise. Latvia's cyberspace continues to face large-scale threats - phishing, extortion, and malware campaigns, attempts to break into systems, networks and websites, denial-of-service attacks on critical information systems and fraudulent e-mail and social engineering campaigns to retrieve personal or authentication data to discredit a specific person, company or institution or to commit crimes. According to Cyber Security Strategy (2019) in Latvia’s cyberspace, there are regular attempts to hack information systems and websites, fraudulent e-mail campaigns aimed at deceiving people and credentials, or infecting an information system with malware. Very often the reasons for data leakage and system hacking are insufficiently configured user information systems and insufficient knowledge of secure ICT solutions and digital technologies. In the 4th

quarter of 2018, a total of 203,455 compromised IP addresses were identified, of which 131,394 were found to have configuration vulnerabilities that could be used by cyber-attackers. Malicious code is also widespread and attempts to infiltrate information systems, exploiting vulnerabilities in users' information systems and subjecting their robotic networks to further malicious activity. Hence, cyber defence is an essential element of a comprehensive national defence system, in which public administrations and the private sector, as well as each individual, have an important role to play in achieving the common goal of cyber security and protection.

According to the Cyber Security Strategy of Latvia (2014), there is lack of academic study programs and scientific activities in the field of cyber security in Latvia, and in the respective field students studying abroad are not motivated to return to Latvia due to remuneration issues and lack of opportunities for professional development in Latvia. In 2019 the Latvian Ministry of Education published statistics about higher education study programmes, where Vidzeme High School and Banking High School offer master's degree programmes on Cyber Engineering (Vidzeme High School) and Cyber risk management (Banking High School). There are no more educational programmes in higher education institutions dedicated to cyber security. According to Cyber Security Strategy (2019) highlights that with the development of the Latvian economy, there is an increasing lack of specialists in various fields, especially ICT, which is not only a Latvian phenomenon, but also a pronounced situation elsewhere in the world. The lack of qualified staff leads to disproportionately high competition between entrepreneurs in attracting ICT specialists and compared to the public sector disproportionately high wages offered to ICT workers. The lack of ICT specialists makes public sector institutions uncompetitive in the fight for the necessary specialists and, accordingly, weakens the possibilities of maintaining and improving the public sector ICT resources. Accordingly, mitigation actions are defined on the State level in order to address this issue in way of an analysis how to attract ICT specialist to the public sector. In addition, value is found in sponsoring and fostering research projects in the area of ICT security. In order to promote the development of cyber security research, it is planned to use all available forms of support: provide grants for projects, support international cooperation projects, such as the European Defence Fund, include a section on cyber security in the national defence research program, etc.

According to Cyber Security Strategy of Latvia (2019) in order to tackle cyber security risks, it is important to carry out educational and information campaigns for the promotion of public awareness for cyber-security, cybercrime and existing threats, as well as international co-operation on cyber security topic, strengthening of society-critical ICT and related services management in Latvia and cyber risk mitigation. In order to make digital world more secure, it is important to raise the level of society's knowledge and promote understanding of ethical standards and moral

responsibility in the digital environment, starting with basic and secondary education. In cooperation with the non-governmental and private sector, it is necessary to organize regular informative campaigns, as well as constant display of information in the mass media. The author adds that it is crucial to encourage development and implementation of relevant specialisation programmes in higher education, include cyber security topics in the curriculum of secondary education and encourage practical application of cyber risk management techniques in the management of education (Clark, et. al., 2013; Abraham, et.al., 2013).

The EU GDPR strengthens and harmonises the rules for protecting privacy rights within and outside the European Union (EU) territory. Most importantly, with the introduction of the GDPR in 2018, the rights of the data subject are substantially strengthened, as described in Chapter 1.4.10. Consequently, the responsibilities of an education manager have become more comprehensive. One of the legal bases for processing personal data, which applies to the educational sector, is the legitimate interest of the data processor, but these interests are not absolute. Data processor must evaluate and inform the data subject, who can decide accordingly whether the legal interest is not excessive. This is a significant change, as data subjects are often not aware of the legal basis for the processing of their personal data. Presently, the presumption is that its proportionality with the privacy of the data subject must be assessed, namely that the legitimate interests of the controller (manager) do not exceed the fundamental rights and freedoms of the data subject. Consequently, data subjects will now be aware that the controller has a legal interest in processing the data. If the data subject sees it to be at some point disproportionate, he or she can object to it. If the manager is not ready to defend his position, it is likely that data processing will end (Chassang, 2017; Martinez-Martinez, 2018; Gines, 2018).

Martinez-Martinez (2018) noted that from the legal perspective it was always challenging to protect and secure personal data and information available and transferred on online platforms as opposed to the physical environment. Efficient and user-friendly electronic applications and management systems used in various processes requires the free and abundant circulation of data and information. The biggest challenge lies in providing full scope security, which would guarantee the fulfilment of rights and freedoms of online users in the face of malicious use of their digital trail or digital fingerprint (information that is left behind during interactions in digital environment) for cyber-crime purposes (e.g., cyber-bullying, scamming or phishing) (Martinez-Martinez, 2018).

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss or access to personal data. Furthermore, the Personal Data definition relates to all data that identifies a living individual: name, surname, personal ID number, physical characteristics (height, hair colour, clothes, etc.) or characteristics, which are not obvious (e.g., occupation, job

position, etc.). E-mail addresses that enable identification of the specific individual also qualify as personal data, e.g., e-mail address, which includes one's name, surname, or employer. Job title may also count as personal data as an identifier to identify a specific person, even though no name or surname is mentioned. Personal data may also be any fragmentary information that identifies specific person, for example: tall, middle-aged man, who lives in concrete flat number and works in school. The student's personal data also include their medical card, information about attendance and learning achievements. Sensitive personal data include information related to individual's biometric data (e.g., fingerprints), state of health, nationality, beliefs, assessment of student's behaviour, student's parents' personal data (Dzanuškāns, 2011). Personal data processing is any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means. Processing of personal data include such activities as reviewing documents containing personal data, copying of passport or other documents, transportation and erasure of documents, video surveillance, audio recording, storage of documents or information, etc.

According to EU GDPR (2016) Article 5, personal data shall be:

- 1) processed lawfully, fairly and in a transparent manner in relation to the data subject;
- 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- 4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- 5) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, in certain cases the data protection officer is required to be appointed ('integrity and confidentiality').

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Morrison 2018). Controller is responsible for the legality of the processing of personal data. EU GDPR (2016) Article 22 provides data subjects with rights to challenge automated decision-making and profiling and terminate such a request, if there are no adequate legal grounds provided by the data controller.

Data Processor is a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller (Morrison, 2018). When personal data processing services are outsourced, the Controller continues to be responsible for the legality of the processing of personal data. Controller cannot transfer this responsibility to the processor. The Processor, on the other hand, is responsible for the processing of personal data in accordance with the assignment concluded between the parties and the responsibilities set for a processor by the GDPR. For example, when a school as data controller outsources certain services, which require data processing by third parties, the school management will still be responsible for data protection and data security arrangements, including ensuring the personal data is processed lawfully and is not disclosed to third parties without legal grounds (Dzanuškāns, 2011; Datu Valsts Inspekcija, 2018).

The GDPR takes into account the technological developments and globalization, as well as the practices and possibilities of the digital commerce and digital marketing companies, providing the data subjects with their legally required security in processing of their personal data. Hence, the GDPR is an evolutionary milestone in field of privacy and personal data protection (Martinez-Martinez, 2018).

There are two essential things in regulatory requirements for personal data handling. First of all, the purpose of data processing must be legal. The second is having clear legal basis for data processing. All educational institutions must have Data Protection Officers appointed. It is imperative to raise the level of personal data security, so that data breach incidents are not discovered from the media or social networks. Institutions should be able to assess the incident, report to the supervisory authority and data subjects within 72 hours.

Managers and employees must understand how the data protection field is organized and managed in their institution.

There are a number of obstacles in getting compliant with GDPR, especially for educational sector. Much more of an obligation for institutions as data processors to think, justify and sufficiently document why particular data is needed and why it is legal to use it; to distinguish at which point the legal ground for particular way of data processing is not valid anymore; to ensure the security, legality, and integrity in data processing.

It is important to note that the data subject's rights are not absolute and common-sense principle should always be applied. It is important to remember in cases, where data processing is performed on grounds of consent, that data subject may withdraw consent at any time. Furthermore, the 72 hours requirement to inform supervisory authority if a personal data breach has realised highlights the need to understand the issue, act quickly and without delay.

Most important of all, that despite all challenges that GDPR brings, there are a number of wider scope

long-term benefits. Firstly, all institutions have to make and keep order in personal data processing. Secondly, privacy and security of all individuals, especially the most socially vulnerable category of people, children, has become more protected. Everyone is able to control what data about him or her companies hold and ensure that their privacy is not breached. Moreover, it is more difficult to manipulate with people's preferences - data subjects have full control over their personal data and will be able to take independent decisions, not being affected by targeted and psychologically profiled information inflows from data processors and controllers.

### **2.3 Corruption Risk**

Risk of corruption mainly is driven by unethical behaviour of responsible employees and school administrators, which in turn could be limited by lack of well-defined procedures and regulations governing purchasing of supplies, use of common textbooks, hiring service providers etc. Corruption risk affects the quality of education, as well as safety and wellbeing of students and teachers. Bribes result in weakening of the quality of education, non-implementation of relevant procedures, assessment criteria and certification results (Chr. Michelsen Institute, 2006; Hallack and Poisson, 2007).

Upon analysing available research publications (ADB, 2010; Chr. Michelsen Institute, 2006; Hallack and Poisson, 2007) and related news articles published in the Corruption Prevention and Combating Bureau of Latvia (KNAB.gov.lv), the State Police of Latvia website (vp.gov.lv) and local news websites (News.lv, tvnet.lv, delfi.lv), the following issues related to corruption risk were identified by the author:

- Absence or non-implementation of established processes and methods for reviewing teacher performance and teacher external engagements provides opportunities for corruption risk;
- Corruption may be the reason for reduced quantity of textbooks and low textbook quality;
- Deficient and unsafe materials may be used in school construction as a result of corruption;
- Corruption incidents may result in differing funding levels provided to similar educational institutions. Moreover, corruption incidents have resulted in more paperwork involved for schools applying for funding, in order to increase the controls over the corruption risk;
- Finally, corruption threatens development of educational sector and reduce overall quality of education curriculum.

Despite the cases mentioned above, according to empirical and desktop-based research combined performed for this study, it is challenging to find any valid recent statistics and evidence on corruption in the educational sector of Latvia.

## 2.4 Legal risks

Educational sector often is subject to regulatory reforms and other changes. In Latvia, education sector is not only the subject to local laws, but also to several common European Union (EU) laws. Education is strictly regulated and requires authorities and school administrators to closely follow changes legal requirements and stay compliant. Ensuring strong compliance would additionally foster better quality in provision of education (Abraham, et.al, 2013; ADB, 2010; Chr. Michelsen Institute, 2006; Clark, et al., 2013; Hallack and Poisson, 2007).

On the other hand, there also is a risk of frequent changes in regulations, which are difficult to follow, especially given that Latvian educational institutions are subject not only to local laws, but also to European Union regulatory requirements. Survey 2 performed in scope of empirical research for this thesis, as will be discussed in detail in the next section, revealed that changing regulations, educational reforms and changes in political environment serve as triggers for risks, such as overloading of employees and lack of needed competencies in educational institutions. The real outcomes of new or changed regulations usually become obvious only after a regulation came in force. This risk triggering other risks could be managed by simply applying general risk management techniques, such as risk assessment before implementation of changes and establishment of monitoring functions, which constantly follow changes in regulations and the compliance of each educational institution, clarifying roles and responsibilities for all stakeholders, all of this will be described in more details in further text of this thesis.

One of such regulations, which impacts all educational institutions, is the EU General Data Protection Regulation (GDPR) analysed earlier in sections 1.4.10 and 2.2. This regulation requires each institution, especially public, which processes large amounts of personal data, to appoint Data Protection Officer, what requires additional investment of funds and resources.

Non-compliance to regulatory requirements may cause legal liability for an educational institution in way of fines and compensations for breaches. Non-compliance with the reform requirements also can bring legal responsibility of an educational institution, which may further lead to loss of license and legal proceedings against the management. In addition, not having emergency and resiliency plans in place, legal responsibility may arise following major incidents resulting in injuries or deaths. If the educational institution has not done everything possible to plan and prevent such risks, it may be legally liable for the consequences.



## **2.5 External risks**

External risks may take form of pandemic, flood, fire, war, terrorist attacks, nature disasters, failures in supply management, sudden death of student or teacher, etc. There are real cases of the above listed risks materialising. For example, in 2014 in Jurmala Pumpuru Secondary School students and staff suffered from falling ceilings due to low quality of building works conducted at the school during the summer (tvnet.lv news, obtained online, 2017). This example demonstrates the risk of supplier negligence and low quality construction works. Whereas, due to Covid-19 global pandemic, the educational service provision was affected and quality of education deteriorated (Hačatrdžana, 2021; Blass, 2021; TVNET/LETA, 2020; Vaduguns, 2021). Floods and fires may leave students of certain schools without education for some time needed to resolve situation.

Disruptions caused by external factors, occurrence of which is not possible to control, can happen at any moment. It is important to be prepared and ready to face the incident, with clearly planned actions and appointed beforehand responsible persons, to enable organizations to continue functioning with as little interruption as possible (PKF UK LLP, 2011; ADB, 2010; Lehtonen, et.al., 2011).

In Latvia, the Ministries of Defence and of Education and Science have developed the Civil Protection Procedure (2011), but the Employer Confederation of Latvia published the Employer's Handbook (2010). Further documents are being published, such as EU Security and Defence Policy published in 2020, Latvian Cyber Security Strategy 2019-2022, etc. and targeted seminars are held by the Ministry of Defence and Ministry of Education to educate employers, teachers and the society.

## **2.6 Reputational, Resilience and Business Continuity risks**

Reputation is what stakeholders think about the firm or organisation based on their past experience with the firm/organisation, its behaviour and character. Along with information security, reputational risk is one of the top risks for many organisations. It can be controlled by way of interacting with stakeholders: being transparent and open with regulatory authorities, providing customer satisfaction with quality of services, achieving good financial results and stable prospects for investors, rewarding employees for their loyalty and commitment, fast handling of complaints etc. Good or bad reputation is fostered in day-to-day activities (Chapelle, 2019).

Resilience is the capacity to quickly recover from a crisis. Resilience risk management requires good crisis management, such as comprehensive business continuity plans developed following the assessment of risk scenarios, identifying top risks. Business Continuity Plans must be thoroughly tested and improved in order to secure resiliency.

To manage crisis effectively, recover quickly and stay resilient in tough circumstances, organisations need to demonstrate speed, competence and transparency. To achieve this, it is important, to hold regular risk assessment process, identify key risks and develop business continuity plans for high impact rare risk scenarios, such as pandemics, terrorist attacks, war, floods and fires, etc., as well as testing these plans by simulating real situations in order to find gaps and drawbacks in these plans. Example of business continuity and resiliency plan is provided in Annex 5, Table 8.1. Example of risk assessment register is provided in Appendix 2, Table 5.1.

## **2.7 Limitations of risk management**

Taleb (2020) argues that it is impossible to predict the unknown, calling this phenomenon as “the unknown unknown”, hence risk identification and risk probability assessment techniques are restricted with the limitations of human nature hence not all risks can be adequately identified and assessed, especially this refers to the Black Swan events – rare and very extreme. Taleb (2020) identifies five main problems with this:

1. confirmation error – human beings tend to take segments of a whole information set and make conclusions about the unknown and invisible by generalising their experience of what they have seen;
2. narrative distortion – human beings tend to build concise schemes based on stories, when the world in reality is very chaotic;
3. nature of human beings is not programmed to perceive and expect the rare extreme events, instead it tends to be optimistic and blind towards such events;
4. often there is a hidden evidence problem, which is being ignored. For example, those who died from Covid-19 were not questioned about their symptoms and how they felt in intensive therapy, those who drowned in “Titanic” tragedy did not give their evidence, disappeared archives hide from us some part of history, and so on;
5. human beings tend to “tunnelling” within zones of the certain uncertainty, what limits the ability to see all risks.

The biggest problem with risk management in the sector of education may be related to generalisation of risks. For example, taking an example from Taleb (2020), Thanksgiving Day Turkey would have one thousand days when she was well fed and lived in comfort, historical data had no evidence that something may go wrong in the future, however one day she gets killed in order to be served and eaten at the Thanksgiving Day. Taleb (2020) draws here a parallel with human perception of risks: people tend to judge that nothing bad will happen based on historical data and perception of past experience. Alternatively, people are afraid to fly on airplanes due to perceived statistics of

airplane crashes, whereas in reality airplanes crash much more rarely than cars. In educational institutions in Baltics high-impact loss events happen rarely and observing the latest history, before the Covid-19 pandemic, one would never say that something disastrous could happen and risk management was not taken seriously as a discipline that would bring any benefit apart from waste of resources, whereas Covid-19 pandemic proved this perception wrong – majority of educational institutions proved to be weak and not resilient towards a pandemic, unable to ensure continuity of educational processes immediately via remote platforms. It took weeks and for some months to re-start operations with low quality distance learning arrangements, which caused high stress for students and teachers and resulted in lower marks for many students (Hačatrjana, 2021; Blass, 2021; TVNET/LETA, 2020; Vaduguns, 2021). Human limitation is in unwillingness to believe in something, what was not experienced previously. Weak faith in risk management within the sector of education and inability to believe in unknown makes it difficult to «sell» the benefits of risk management to employees and managers of educational sector. On the other hand, benefits of planning for high-impact events are of greatest value, which can save the sector and all its stakeholders from larger losses when something disastrous will happen.

Another aspect, as highlighted by Taleb (2020) is that each event is unique, and it is not possible to make precise forecasts. Despite all the risk planning, human beings cannot predict what may happen whichever models they use, as the world is chaotic and unpredictable. However, planning of known risk events, which are possible to predict, may help to reduce the impact of unknown loss events (which are not possible to predict) and be more prepared in the face of uncertainty. Although it is never possible to forecast the actual probability of risk events, it is easier to predict possible impact of different events. Thus, in view of the author, it is critically important to plan and prepare for range of scenarios and be ready to adopt action plans of «known» scenarios for an «unknown» scenario, which was not planned at all. Taleb (2020) also highlighted that it is important to focus on mitigating possible losses, rather than try to predict probability of risk events. Thus, as also Taleb (2020) puts it, it is possible to draw a map of risk events, highlight those risk areas with the highest possible losses, and focus on those most risky areas to mitigate the impact. Murphy, et.al. (2016) in their analysis identified the following risk mitigation tools in education provision context: effective lesson plans, curriculum guidelines, safety rules, lesson objectives, skill progressions, first aid kits, emergency action plans, appropriate equipment, inventories of equipment and facilities, activities conducted away from hazardous areas, supervision of students, certification of teachers, communication and posting of guidelines for emergency actions plans and emergency exit procedures.

## 2.8 Effective risk management programme

Abraham, et.al. (2013), Beasley (2013), Chappelle (2019) define the following risk management cycle as shown in Figure 2.1:



Figure 2.1: Risk management cycle

Figure 2.1 makes visual representation of the risk management process according to the statements by authors listed above. It shall start from defining the strategy, mission or key objectives, then next goes identification of risks processes, which is followed by the risk assessment. Residual and significant risks are monitored through key risk indicators, acceptable level of risk threshold, follow-up on risk mitigation action and escalated when risk becomes intolerable. After a certain period (usually one-two years), the cycle starts again from the definition of strategy and objectives.

Alberts and Dorofee (2009) in their systemic risk management approach discussion propose a framework for efficient risk management with the following key drivers: objectives, preparation, execution, environment, resilience, results. By addressing each of them, it is possible to implement strong risk management programme in any type of an institution:

➤ **Objectives:** in this stage it is important to draw out a strategy - define the mission, vision, goals and objectives to which an institution is striving during a certain period of time. It is important

to avoid any aggressive schedules, underfunding and too complex or high-risk technologies in pursuing of the objectives.

➤ Preparation: in the preparation stage it is important to define precise roles and responsibilities, sequence correctly all activities into processes, identify dependencies and interrelationships among different activities, develop artefacts in way of instructions, written procedures, decision-making guidelines, templates, define what technologies should be used in each process and develop metrics for measuring the success.

➤ Execution: in this stage concrete people are tasked with concrete exercises, technologies are supporting processes which it needs to support, assets used to execute the plan (information, technologies, facilities) are being assessed and overseen. Success and progress being measured with the defined metrics during the previous stage.

➤ Environment: it is important to be aware and to manage the environment, which includes organisational structure, culture, politics, communication styles and infrastructure. Environment plays an important role in how tasks are being executed and on the overall success, hence should not be ignored and should be well understood for effective implementation of tasks.

➤ Resilience: organisations must be ready to withstand unexpected events and respond quickly in emergency. Hence, organisations should plan effectively in order to be able to withstand and manage potential risk events and changing conditions. Resilience aspect enables employees of an organisation to handle unusual and unexpected situations that would hamper achievement of objectives and should be part of the risk management;

➤ Result: in this part in respect to the management of educational institution the factors resulting to the results part are about the understanding of the requirements and understanding what the envisioned final result upon achievement of set objectives would be and what the unwanted result would be, hence factors influencing the final result need to be analysed from the perspective of the risk management.

In order to determine risk causes, according to Alberts et.al. (2009), it is important to find relationships between the above-described drivers and pinpoint the possible risks. For example, risk factors relating to the “Result” driver could be prevented on the stage of “Preparation”. Also, by addressing “Environment” risk drivers it is possible to mitigate the risks relating to “Result” part.

The simplest approach is to draw a table and define statements, as Figure 2.2 demonstrates, which would represent successful and unsuccessful achievement of objectives. Then formulate these statements as questions with “yes” or “no” answer options, or add additional options as “Likely”, “Unlikely”, etc. In this way it would be possible to identify the risky areas at an early stage. Example is provided in the Figure 2.2 below:

Driver Question	Answer				
Is the process being used to develop an educational programme is efficient?	No	Likely no	Equally likely	Likely yes	Yes
Consider: process design, roles and responsibilities, measurements and controls, process effectiveness and efficiency, life cycle, training, employee competences	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 2.2: **Driver question and range of responses example (Alberts and Dorofee, 2009)**

Similar to the example provided in Figure 2.2, it is possible to build it in a way as to answer options would have defined weights of points to quantify the results and attribute to it risk scores. Also, it is beneficial to consider conditions affecting the driver and the answers, as it could be possible to mitigate risks by addressing the conditions. Failure of objective achievement can be seen as threat or risk, which should be analysed further. Beasley (2013) suggests finding relationships between the core success drivers and strategic initiatives and formulate the questions in way to determine what are the required conditions, factors, assets needed to achieve the successful achievement of strategic objectives and what are the conditions, factors, drawbacks, that would lead to failing to achieve the strategic objectives.

According to Alberts, Dorofee (2009) it is important to document conditions and events leading to positive outcomes and leading to negative outcomes, fostering the positive conditions and mitigating the negative conditions. Beasley (2013) highlights that it is especially important to understand well the driver’s fostering development and achieving objectives and strategic mission. Risk needs to be identified through the strategic lens and managers need to manage risk keeping in mind the long-term strategic mission, as risk management is focused on identifying the threats that could hamper achievement of strategic goals.

## 2.9 Summary

Section analysed various risk clusters most relevant for the sector of education and how these risks can be managed in order to bring value to the sector of education:

- Risks of the highest level of relevance to the educational sector are psychosocial risks, information security risks, privacy and cyber security risks, risk of corruption, legal risks, external risks and reputational risks. Appendix 4 provides more detailed taxonomy of risks for the sector of education;
- Psychosocial risks rated as the top important risks for the educational sector.

- Overloading of employees is the category of job demands, if looking from the perspective of Job Demand-Resources Model. In combination with low job controls on the employee side and lack of recognition of employee's effort it causes work-related stress and burnout.
- Positive correlation was discussed between economic motives of teachers in Latvia and level of their emotional exhaustion - driven by intrinsic economic motives, teachers are exposed to risk of demotivation, high level of stress, formal relationships at work and perceiving colleagues as competitors;
- Information Security risk was rated as number one risk by Risk.net survey results seven years in a row from 2014 until 2021, whereas CERT.lv revealed that cybercrime causes losses of at least € 265 billion per year in EU Member States and around € 900 billion per year worldwide;
- For the educational sector Information Security and Cyber risk mainly poses the threat to confidentiality and integrity of stored personal data and resiliency of digital devices used in educational process;
- Corruption risk affects the quality of education, development of educational sector, safety and wellbeing of students and teachers and efficiency of processes by raising bureaucracy and reducing level of trust;
- Legal liability is a risk to suffer financial loss from not following regulatory requirements, not having adequate resiliency plans, privacy policies and not complying to health and safety requirements;
- External risks are most difficult to control due to independent cause of threat, e.g., pandemics, flood, fire, war, terrorist attacks, nature disasters, failures in supply management, sudden death of student or teacher, etc.
- Reputational risks stand as one of the top risks for any organisation and can be controlled by being more transparent, resilient and strong in crisis management;
- Risk management is limited to confirmation error, narrative distortions, human nature, hidden evidence problem and "tunnelling" within the certainty zones;
- Effective and systemic risk management cycles are risk management processes focused on achievement of strategic goals.
- Systemic risk management approach includes the following key drivers: objectives, preparation, execution, environment, resilience, results. By addressing each of them, it is possible to implement strong risk management programme in any type of an institution.

### 3. EMPIRICAL RESEARCH ON THE MANAGEMENT OF RISKS IN THE EDUCATIONAL SECTOR

The aim of this chapter is to provide practical research results in order to support theoretical part discussed in previous chapters with empirical data, answer the research questions, prove the research hypothesis and achieve the aim of the research. Chapter will introduce the methodological approaches used for data collection and analysis, present the results using descriptive and inferential statistics, as well as qualitative data analysis techniques. Mainly the chapter will discuss the key risks in the sector of education, level of awareness and understanding of risk management in the sector of education, ways how key risks could be mitigated and what needs to be improved for more efficient risk management in the sector of education in Latvia. In the end conclusions and recommendations will be drawn mainly based on the data and results discussed in this chapter.

#### 3.1 Methodology and organisation of research

In order to check the validity of research hypothesis and achieve the aim of the research, empirical research was conducted in form of online surveys with key stakeholders from the sector of education in Latvia and interviews with experts in risk management. Surveys for stakeholders from the sector of education were placed into online platform SurveyMonkey.com generating online links and allowing participants to stay anonymous. Link to the survey was distributed via social networks, e-mail to the Association of Education Leaders in Latvia and e-mailed to 1600 e-mail addresses of educational institutions of Latvia (secondary schools, colleges, universities, pre-school institutions) as published in database [www.mykoob.lv](http://www.mykoob.lv). In addition, 10 printed questionnaires were distributed to students of Pedagogy and Psychology Faculty, who work in educational institutions, at the premises of the University of Latvia.

There were three parts of practical research. Initial survey (further in text - **Survey 1**) consisting of 10 questions was carried out from October 2018 until June 2019, where the main focus was on assessment of 32 risks by respondents and their view on risk management. Answer options were provided in most answers and respondents had to choose which ones are relevant for them. In the second part a second questionnaire (further in text - **Survey 2**) was distributed to the same respondents and responses were collected during July 2019 with request to provide some more detailed explanations to the trends, which resulted from analysis of the first questionnaire results. The aim was to determine view of the respondents about the consequences of these risks, how they could be managed and whether risk management is important and possible to implement in the sector of education. There were no answer options provided and respondents had to write open answers in free



form, providing their justification about the top risks, consequences and mitigation actions. If Survey 1 was structured as multiple-choice survey, then Survey 2 was structured as an interview with open-ended questions and answers. Survey 1 template is provided in Appendix 6 and Survey 2 template is provided in Appendix 7. Finally, interviews with risk experts from Finance Sector were held in October 2022 in order to validate the statements and findings of this research.

In addition to the abovementioned surveys and recorded interviews, the author, who is Risk Management expert in Finance Sector and also is a former lecturer of Risk Management course on the faculty of Pedagogy and Arts in the University of Latvia in autumn semesters of academic years 2017/2018, 2018/2019 and 2019/2020, collected additional evidence through professional discussions at workplace, risk management workshops with the students studying Risk Management as part of their bachelor's degree programmes (there were four streams of students with on average 9 students per class within the years while this research was ongoing). In addition, author held a verbal interview with director of the school attended by the author's child about risk management in schools in general, main risks and risk management needs. These discussions with students, risk management colleagues and school director will be used as additional evidence to formal surveys and interviews.

Following qualitative review of returned questionnaires, it was established that a total of 235 respondents participated in multiple-choice style Survey 1 and 41 respondents in open-question style Survey 2; all of respondents have direct relation to educational sector from different parts of Latvia - majority were managers and leaders of educational institutions (50%), most of the responses (85%) were received from schools: primary (grades 1-4), basic (grades 1-7 and 1-9) and secondary (grades 10-12). This is the target audience needed for this research, as this dissertation's hypothesis is based on assumption that there is neither capacity nor awareness and expertise for risk management in the sector of education in Latvia (*"H0: There is poor understanding of risk management in the educational sector in Latvia, low maturity of risk management in the educational institutions of Latvia and lack of capability and capacity to employ risk management tools. As a result, quality of education is affected by many not well-managed risks"*). Thus, the sample of respondents who participated in the surveys perfectly fit for proving or disapproving the hypothesis set for this research, as it is represented by directors and teaching staff of educational institutions across the country (97% of respondents), who are closest to the management of education in practice. As it was established in section 1.3, every stakeholder is responsible for risk management, although the responsibility mistakenly may seem to lie on the institution's administration. As section 1.2 established teachers and school directors are the key stakeholders in the sector of education, where school directors are responsible for risk management on high level (governance) and teachers are responsible on operational level. Parents of students are also key stakeholders as much as students, and are

responsible for risk management from the angle of complying to rules and risk management framework established by an educational institution (more details in sections 1.2 and 1.3), hence parents were not excluded from the respondent sample, as they represent only 7% of respondents and are very close to risk management practical implementation by educational institutions.

### 3.1.1. Geographical characteristics of respondents

Survey 1 completed 235 respondents, out of which 110 were located in the capital of Latvia, Riga (47%). 46 out of 235 respondents (19%) were located in larger towns, such as Cesis, Liepaja, Daugavpils, Rezekne, Jelgava, etc. 49 respondents (21%) were located in smaller towns (Dagda, Ludza, Talsi, Gulbene, Pļaviņas, Alūksne, etc.). 30 respondents (13%) were located in villages. Overall respondents are evenly located across all regions of Latvia and represent different groups of representatives from educational sector (directors, teachers, other employees of educational institutions, coaches, etc.). Hence collected data is considered to be representative enough for the entire country. Figure 3.1 visualises geographical representation of respondents who took part in Survey 1.



**Figure 3.1: Geographical representation of respondents who participated in the research**

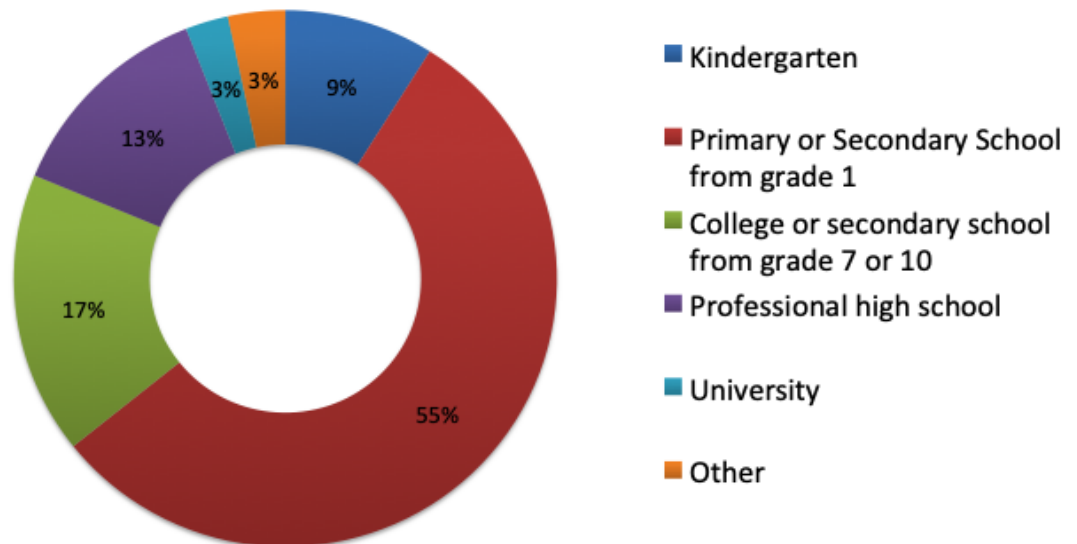
Survey 2 completed 41 respondents from the sample of Survey 1 respondents. Geographical representation data was not collected for Survey 2, as it was sent to the same respondents, who completed Survey 1, thus it is assumed that it replicates that as of Survey 1.

3.1.2. Classification of respondents by role in the educational sector and attachment to certain type of educational institution.

Respondents in both, Survey 1 and Survey 2, were asked to select their position and type of educational institution they belong to.

In Survey 1, 129 out of 235 respondents (55%), indicated that they belong to school that starts from grade 1 (Primary, Basic or Secondary School). At the same time, 40 respondents out of 235 (17%) replied that they belong to school type that starts from grade 7 or grade 8, such as college or secondary school. Hence these two groups of respondents further in the research will be taken as one group, as they represent the largest part of all respondents (169 respondents or 72% from the sample) and belong to the type of educational institution defined in this study as “school”. 30 respondents (13%) stated that they belong to professional high schools, 21 respondent (9%) belong to kindergarten and only 7 respondents (3%) replied that they represent universities. Out of all 235 respondents, in addition 7 respondents (3%) belong to other types of educational institutions, such as interest education, for example, sport and IT clubs and distance learning schools. Figure 3.2 provides visual representation of belonging of respondents to different educational institution in Survey 1.

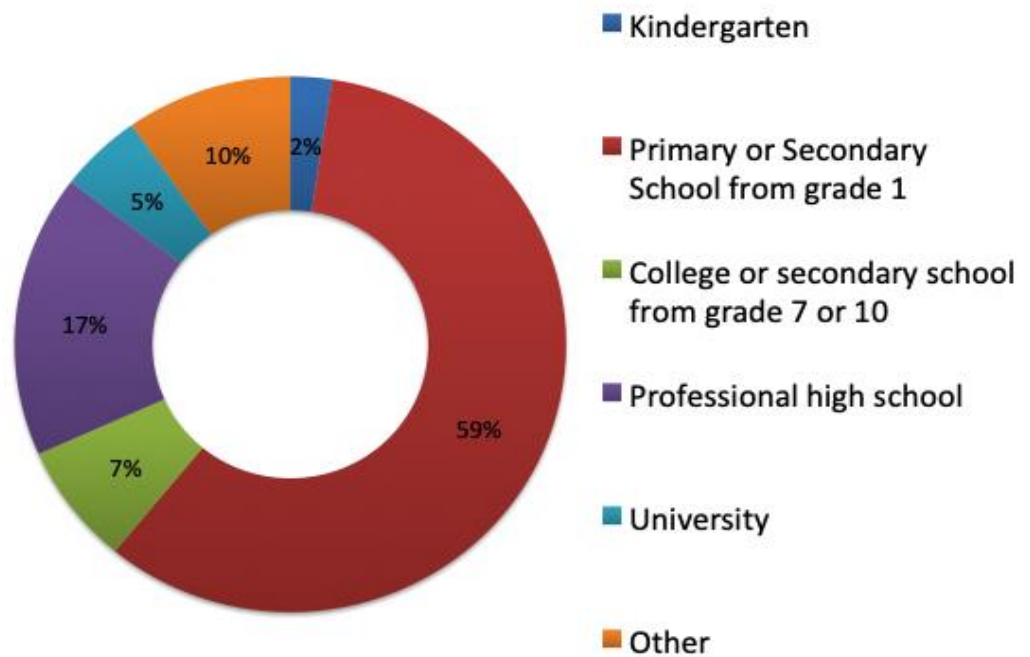
**Breakdown of respondents by type of educational institution**



**Figure 3.2: Break-down of respondents by their belonging to certain types of educational institutions in Survey 1**

In Survey 2, 24 respondents out of 41 (59%), indicated that they belong to school that starts from grade 1 (Primary, Basic or Secondary School). 7 respondents out of 41 (17%) indicated that they represent professional high school. 4 respondents (10%) indicated that they belong to other types of educational institution, mainly special education institutions. Only 3 respondents out of 41 (7%) replied that they belong to college or secondary school that starts from grade 7 or 10. Only 2 respondents were from university type of institution and 1 respondent from pre-school educational institution. Figure 3.3 provides visual representation of belonging of respondents to different educational institution in Survey 2.

**Breakdown of respondents by type of educational institution in Survey 2**



**Figure 3.3: Break-down of respondents by their belonging to certain types of educational institutions in Survey 2**

The next question was about the role of the respondents in the educational sector, whether they are managers of educational institutions, teachers, support employees, parents, etc. Figure 3.4 provides visual representation of the break-down of respondents by their job role and position in Survey 1 and Figure 3.5 provides break-down of respondents by their job role and position in Survey 2.

In Survey 1, 117 respondents out of 235 (50%) replied that they are managers or deputy managers of different educational institutions. Of those, 66 out of 117 (56%) work in schools that start from grade 1 and 19 out of 117 (16%) work in schools that start from grades 7 or 10, thus a total of 85 out of these 117 respondents (72%) are managers or deputy managers of various types of schools. 17 out of 117 (15%) are managers of professional high schools and 6 (5%) are managers of other educational institutions, such as interest clubs and distance learning schools. 9 out of 117 (8%) are managers of pre-school educational institutions.

76 respondents out of 235 (33%) indicated that they are teachers. Out of those 76 respondents who replied that they are teachers, 48 (63%) indicated that they work in schools that start from grade 1 and 14 (18%) indicated that they work in schools that start from grades 7 or 10. Thus out of 76 teachers who took part in Survey 1, 82% work in various types of schools. On the other hand, 7 out of 76 (6%) teachers belong to professional education institutions, 5 out of 76 (4%) indicated that they belong to pre-school educational institutions and 2 out of 117 (2%) belong to universities.

17 respondents out of 235 (7%) were parents of students studying in schools and professional education institutions. 14 respondents out of 235 (6%) stated that they are employees in educational institutions, representing schools, professional education institutions and university. Remaining 11 respondents out of 235 (4%) represent interest education and teaching assistants. Please see Figure 3.4 below for visual representation.

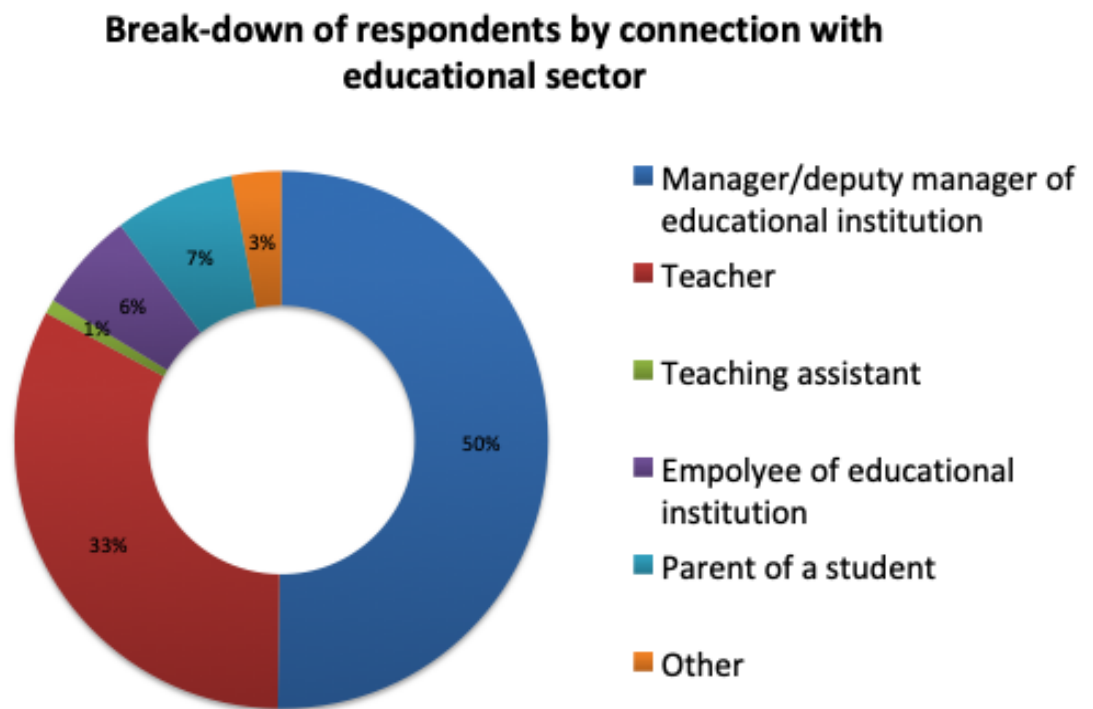


Figure 3.4: Break-down of respondents by their job role and position in Survey 1

In Survey 2, 22 out of 40 respondents (55%) are managers or deputy managers of educational institutions. Of those, 12 (55%) are managers/deputy managers in schools, 6 (27%) are managers/deputy managers in professional education institutions, 3 (14%) are managers in other types of educational institutions such as special education, and only 1 (4%) was representative from pre-school educational institution.

14 out of 40 respondents (35%) who completed Survey 2 indicated that they are teachers. Of those, 11 (73%) work in schools that start from grade 1, 3 (20%) work in schools or colleges that start from grade 7 or 10 and 1 (7%) in university. The remaining 4 respondents out of 40 (10%) were support employees at university and school and interest education representatives. Please see Figure 3.5 below for visual representation.

**Break-down of respondents by connection with educational sector in Survey 2**

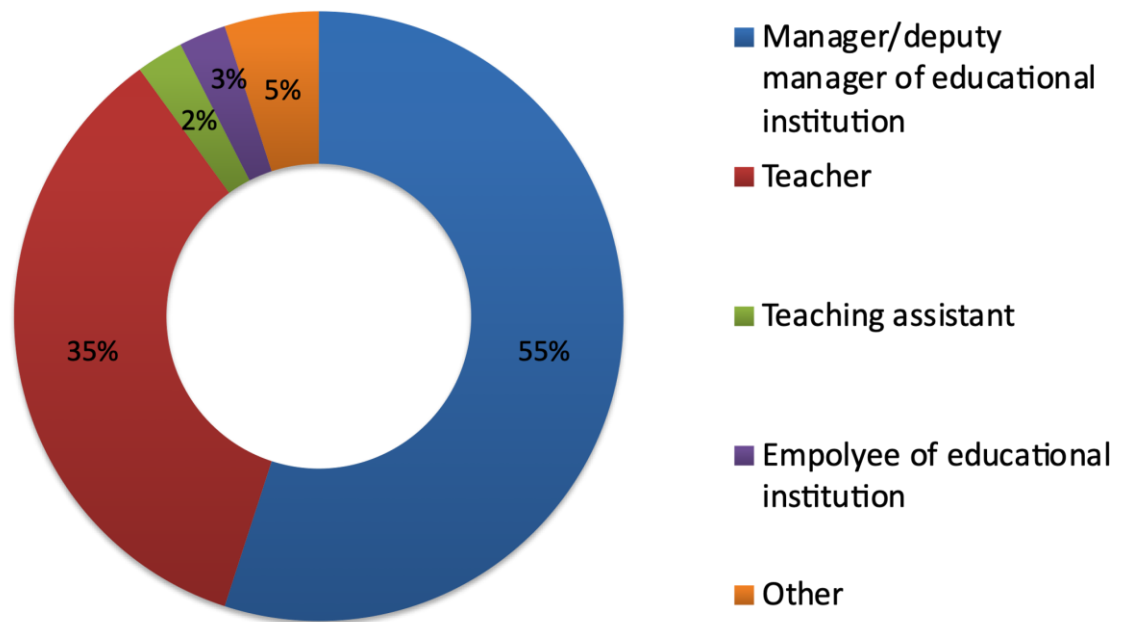


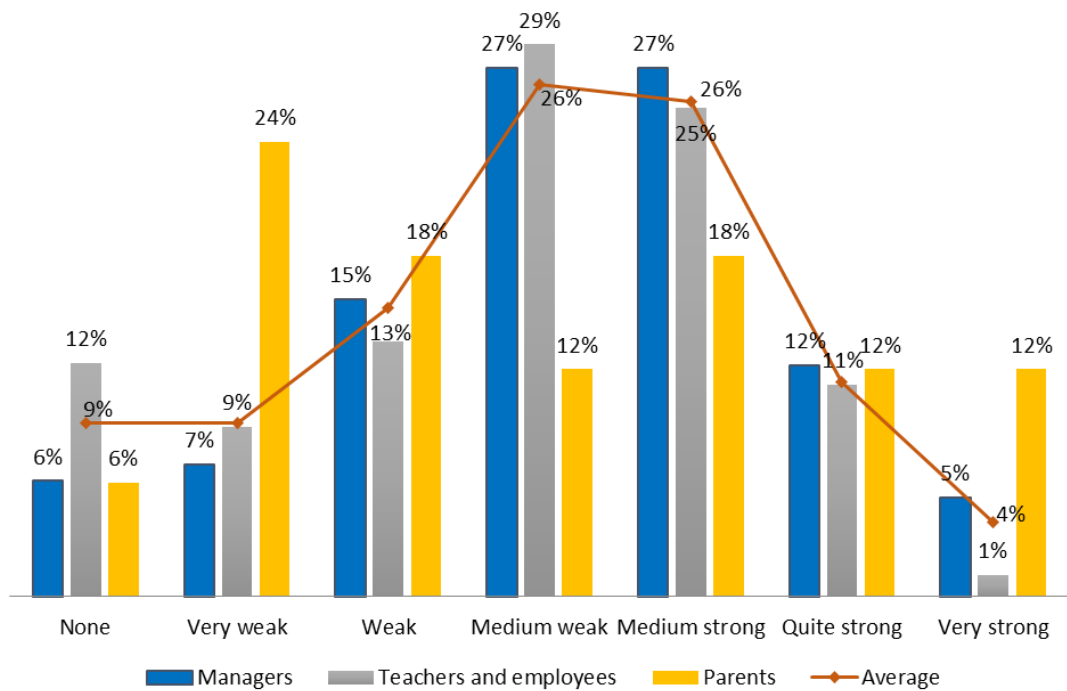
Figure 3.5: Break-down of respondents by their job role and position in Survey 2

### 3.2 Risk management effectiveness in Latvian educational institutions

In Survey 1 respondents were asked to rate the effectiveness of risk management in the educational institutions to which they belong to on the scale from 0 to 6, where 0 score stands for “none or very poor risk management” and 6 stands for “very strong risk management”. Figure 3.6 below provides histogram of average answers of all respondents and compares it to average answers

of different respondent groups. It is seen that on average respondents tended to choose middle number, between 3 and 4 out of 6, leading to mean ( $\mu$ ) score 2.99 (n=235). This result provides evidence about uncertainty of respondents on how risks are managed in the organisation they belong to and possible cognitive bias choosing the numbers in the middle when not sure which is the correct answer. For this research, such result indirectly supports the initial hypothesis, that there is low

### Effectiveness of risk management in related educational institution



awareness about risk management in the sector of education, what could trigger such a result.

Figure 3.6: Risk effectiveness ratings by respondents in Survey 1

On the other hand, taking results of different groups of respondents, provide additional evidence of cognitive bias in the answers of respondents. Managers of educational institutions tend to evaluate risk management in their educational institutions more positively with the mean ( $\mu$ ) score 3.21 (n=117): 5% of them rated risks management effectiveness in their organisation with score “6”, equally 27% rated with scores “4” and “3”, only 6% of managers chose score “0”.

On the other hand, the results of teachers and employees are more negative, with the mean ( $\mu$ ) score of 2.79 (n=94): 12.8% chose score “0”, 28.7% chose score “3”, 24.5% chose score “4” and only 1.1% chose score “6”.

The results of parents are most uneven, which is understandable that for parent such rating is most difficult and at the same time, there was very small sample of parents in this study. On average,

majority of parents selected option “1 – risk management is very weak” in relation to their educational institution. Mean ( $\mu$ ) score for parents’ ratings is 2.94 (n=17).

It was quite hard for most stakeholders of educational sector to evaluate effectiveness of risk management in the educational institution they belong to and as a result majority of respondents subjectively selected scores closest to the middle avoiding more extreme scores. The conclusion can be made that the risk management awareness and culture may not be at the sufficiently high level in the educational institutions of Latvia and require focused training and raising of awareness.

On the other hand, it was interesting for the author to check and compare how risk management effectiveness was rated for different types of educational institutions and whether there are any extremes or trends. Hence, the author compared schools (primary, basic, secondary, colleges and gymnasiums) with high schools, professional schools and universities and with pre-school educational institutions in Table 3.1. The results did not show any extremes and average scores stayed around the middle value:

**Table 3.1 Measurement of risk management effectiveness by type of educational institution (Survey 1)**

Type of educational institution for which risk management effectiveness is measured	Mean value ( $\mu$ )	Number of respondents (n)
Schools (primary, basic, secondary, colleges, gymnasiums)	3.0	170
High schools, professional schools and universities	2.8	36
Pre-school	3.1	21

Looking more closely at individual results and distribution across the scale, it was observed that more respondents chose scores on the left side of the scale (0-3). Figures 3.10 - 3.12 below provide more detailed view about how scores were distributed. However, due to much lower number of respondents for high-school, professional schools, universities and pre-school, it is hard to make any specific conclusions. At the same time, more than half of all respondents represent different types of schools and their result is considered to be fully reliable, providing evidence that there is no common view on how effective is the risk management, but majority inclining to rate it with medium scores. Picture 3.7 provides a summary of these results. Skewness to the left side is observed for schools and universities, providing an evidence that risk management effectiveness according to the respondents, is not efficient in these educational institutions.



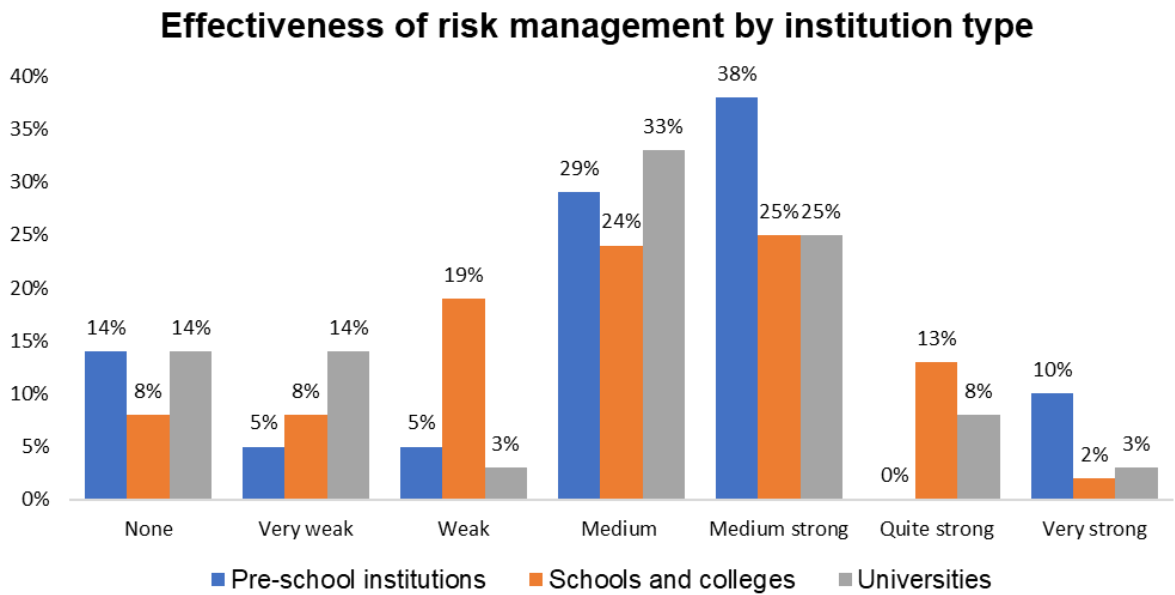


Figure 3.7 Risk effectiveness by different types of educational institutions (Survey 1)

### 3.3 Incident reporting and management practices in the educational institutions of Latvia

Survey 1 contained one question, where respondents were asked to answer whether the education institution to which they belong performs collection and registration of incidents. As it was described in sections 1.3 and 1.4.11 it should be responsibility of all stakeholders to report an incident to centrally appointed person who should collect incident data in special incident and risk database, and incident reporting should be integrated as end-to-end documented process in each institution. The question about incident reporting was structured as multiple choice with the following options:

1. Yes, incidents are registered in the incident database;
2. No, incidents are not registered;
3. I do not know;
4. Please specify if neither of the options applies (space was provided for the comment).

Figure 3.8 demonstrates the results of this question and how the answers got distributed:

Do you register incidents in your educational institutions?

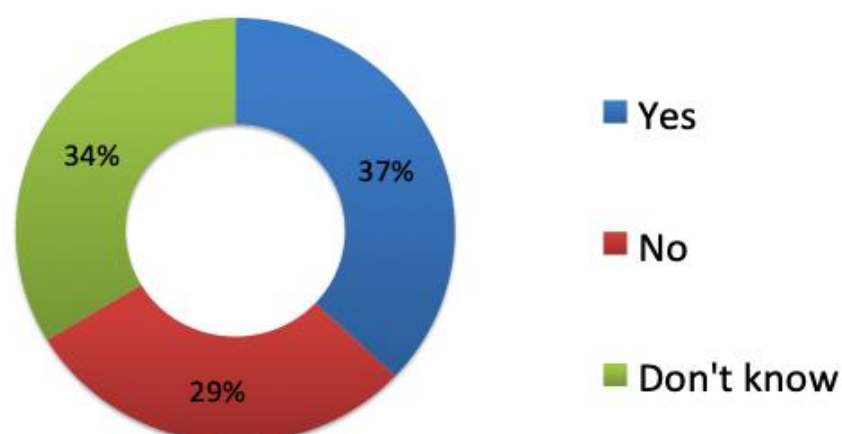


Figure 3.8 **Incident reporting in educational institutions of Latvia (Survey 1)**

As it can be seen, only 37% (n=87) of respondents provided confident answer that incidents are recorded in their educational institution. Some of those answers indicated additional information that not all, but several cases that meet certain criteria (e.g., serious trauma caused to student at school that result in calling an ambulance, school closure due to emergency situation, etc.) are recorded in internal register. 29% (n=69) of respondents confirmed that in their educational institutions there is no incident reporting routine and 34% (n=79) responded that they do not know whether incidents are recorded, what means that incident reporting awareness is not practiced in their institutions and therefore it is assumed that incidents are not recorded in their institutions, as the key prerogative for incident reporting and management is awareness of employees about such requirement.

Hence, empirical research results demonstrated the low awareness of respondents about incident reporting and low usage of this management tool in the educational institutions of Latvia. Nevertheless, majority of respondents highlighted the importance of risk management for their organisation while answering other questions analysed further below.

### 3.4 Risk assessment

**Methodology:** In order to perform risk assessment, risks that are most relevant to the sector of education were selected based on literature review and analysis in the theoretical part of this study and brainstorming sessions with students studying Risk Management course on the Pedagogy, Psychology and Arts faculty in the University of Latvia, who also were employed at the time of this research in different types of educational institutions.

Survey 1 mainly consisted of the assessment of 32 risks from two dimensions: risk criticality in relation to respondent's educational institution and risk management effectiveness by their

educational institution. Table 3.2 demonstrates the scales developed by author which were applied in the risk assessment completed by the respondents in Survey 1:

Table 3.2 **Risk rating scale methodology in empirical research questionnaire**

Criticality of risk		Effectiveness of management	
1	Risk is not at all significant	1	Risk is not managed at all
2	Risk is neutral	2	Risk is very poorly managed
3	Risk is slightly significant	3	Risk is managed, but very weakly
4	Risk is very significant	4	Risk is well managed
5	Risk is critically significant	5	Risk is managed to the highest standard

Upon collection of results, risks were grouped according to their type, forming the following **groups**: psychosocial risks, IT and information security risks, external risks and reputational risks. Reliability of scale was tested with Cronbach’s alpha for all risks and for each group of risks. In the end, correlation between risks and groups of risks was measured taking Pearson’s correlation coefficient.

Ratings allocated by respondents for each risk on two dimensions (risk criticality and management effectiveness) were assumed as individual risk scores for each dimension and average score from all responses was taken as final risk score for each risk on two dimensions: risk criticality and risk management effectiveness.

Data was analysed mainly by use of MS Excel and SPSS to perform comparative evaluation of risk criticality and management and whether there are any relationship trends between the two dimensions.

**Results:** Figure 3.9 provides graphical summary of risk assessment results for all risks sorted by highest risk criticality scores in order to see what risks are perceived as most critical by the respondents. It is interesting to note that where risk was assessed as more critical, management of effectiveness was assessed as very low and vice versa, thus creating “scissors” effect between risk criticality and level of its management.

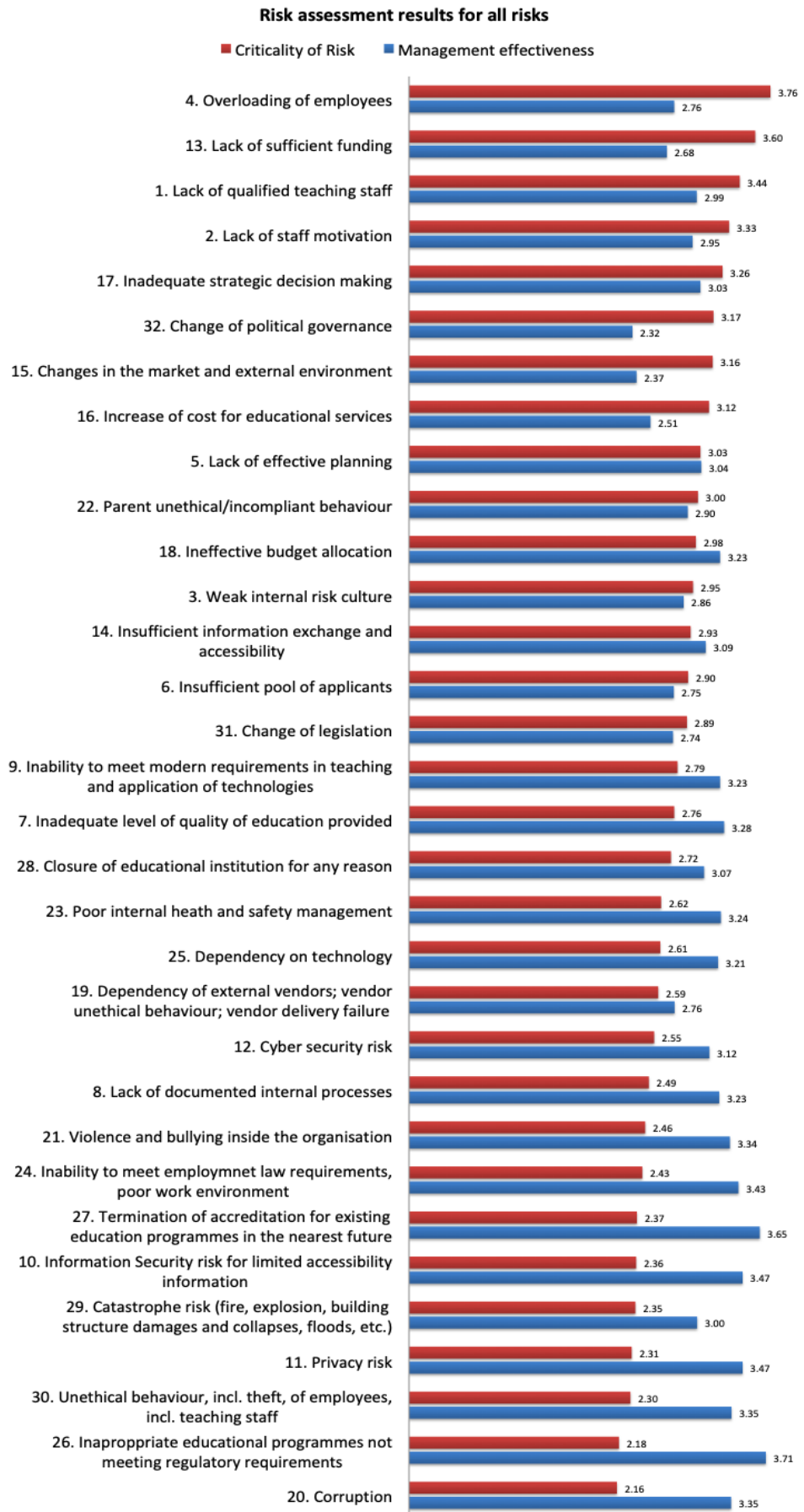


Figure 3.9 Risk assessment results derived by the research (Survey 1)

Thus, according to the survey results, the most topical risks in the educational sector in Latvia are:

1. Employee overload (average 4 points out of 5)
2. Insufficient funding (average 3.8 points out of 5)
3. Lack of employee motivation (average 3.5 points out of 5)
4. Lack of qualified staff (average 3.5 points out of 5)
5. Wrong strategic decision making (average 3.5 points out of 5)
6. Changes in the political environment and legislation (average 3.4 points out of 5).

For deeper analysis of risk assessment results, it was decided in addition to check and compare differences in answers of two biggest groups of respondents: managers of educational institutions and teachers. In order to have a better overview, author grouped assessed risks into risk groups, as was described above. Then author compared the assessment results for different risk groups of two major respondent groups by use of Student's t-test to check to how much extent the answers of these two groups differ for different types of risks. Table 3.3 provides the descriptive statistics of the results when respondent groups were split into two major groups and all risks were split into four major groups when assessing the "Criticality of risks":

**Table 3.3 Descriptive statistics for "Criticality of risks" responses comparison with Student's t-test split by groups**

What is your role in the educational sector: 1 - manager 2 - teacher, teaching assistant, other employee		N	Mean	Std. Deviation	Std. Error Mean
Psychosocial	1	117	2.7912	.64205	.05936
	2	101	2.9646	.75144	.07477
ICT and IS	1	117	2.3868	.70520	.06520
	2	101	2.4703	.78045	.07766
External	1	117	2.9434	.57200	.05288
	2	101	2.9468	.72787	.07243
Reputational	1	117	2.5773	.65151	.06023
	2	101	2.8119	.77088	.07671

Table 3.4 provides the Student's t-test results for the abovementioned groups of respondents in assessing the criticality of risks:

**Table 3.4 Independent Samples Test for “Criticality of risks” responses split by groups**

		Independent Samples Test								
		Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Interval of the	
									Lower	Upper
Psychosocial	Equal variances assumed	2.649	.105	-1.838	216	.067	-.17343	.09437	-.35944	.01258
	Equal variances not assumed			-1.817	197.975	.071	-.17343	.09547	-.36169	.01483
ICTandIS	Equal variances assumed	.793	.374	-.830	216	.407	-.08354	.10064	-.28191	.11482
	Equal variances not assumed			-.824	203.493	.411	-.08354	.10140	-.28347	.11638
External	Equal variances assumed	4.742	.031	-.039	216	.969	-.00341	.08813	-.17710	.17029
	Equal variances not assumed			-.038	188.788	.970	-.00341	.08968	-.18030	.17349
Reputational	Equal variances assumed	4.459	.036	-2.436	216	.016	-.23463	.09634	-.42451	-.04475
	Equal variances not assumed			-2.406	196.828	.017	-.23463	.09753	-.42696	-.04230

From the above t-test results presented in Table 3.4 it can be concluded that there are statistically significant differences in answers for the two respondent groups in their assessment of psychosocial and reputational risks: with 90% confidence there are statistically significant differences in the assessment of criticality of psychosocial risks between teachers and managers and with 95% confidence there are statistically significant differences in the assessment of criticality of reputational risks between teachers and managers. According to the data derived, teachers tend to rate these risks as more critical than managers. On the other side, there is no statistical difference in assessing the criticality of ICT/IS and External risks by these two major groups of respondents.

The same exercise was performed in order to determine whether there are any significant differences between the opinions of two major respondent groups in assessing the effectiveness of risks. Table 3.5 presents the descriptive statistics of the results when respondent groups were split into two major groups and all risks were split into four major groups when assessing the “Effectiveness of risk management”:

**Table 3.5 Descriptive statistics for “Effectiveness of risk management” responses comparison with Student’s t-test split by groups**

What is your role in the educational sector: 1 - manager 2 - teacher, teaching assistant, other employee	N	Mean	Std. Deviation	Std. Error Mean	
					Psychosocial
	2	101	3.0481	.64848	.06453
ICT and IS	1	117	3.3397	.72104	.06666
	2	101	3.3119	.79247	.07885
External	1	117	2.5630	.73670	.06811
	2	101	2.7339	.72428	.07207
Reputational	1	117	3.3031	.58716	.05428
	2	101	3.1904	.56627	.05635

Table 3.6 provides the Student’s t-test results for the abovementioned groups of respondents in assessing the effectiveness of risk management:

**Table 3.6 Independent Samples Test for “Effectiveness of risk management” responses split by groups**

Independent Samples Test										
		Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Interval of the	
									Lower	Upper
Psychosocial_Eff	Equal variances assumed	3.244	.073	1.792	216	.075	.14483	.08082	-.01446	.30412
	Equal variances not assumed			1.769	196.180	.078	.14483	.08185	-.01660	.30625
ICTandIS_Eff	Equal variances assumed	.928	.336	.272	216	.786	.02786	.10254	-.17424	.22997
	Equal variances not assumed			.270	204.128	.788	.02786	.10325	-.17572	.23144
External_Eff	Equal variances assumed	.166	.684	-1.721	216	.087	-.17088	.09928	-.36657	.02481
	Equal variances not assumed			-1.723	212.362	.086	-.17088	.09916	-.36634	.02459
Reputational_Eff	Equal variances assumed	.179	.673	1.436	216	.152	.11269	.07845	-.04194	.26731
	Equal variances not assumed			1.440	213.340	.151	.11269	.07824	-.04154	.26691

From the above t-test results it can be concluded that there are statistically significant differences in answers for the two respondent groups in their assessment of risk management effectiveness for psychosocial and external risks with 90% confidence that there are statistically significant difference in the assessment of effectiveness of management for the risks in these risk groups between teachers’ and managers’ responses. According to the data derived, teachers tend to rate management of psychosocial risks with lower scores (weaker risk management) than managers, but management of external risks with higher scores (stronger risk management) than managers did. On the other side, there is no statistical difference in assessing the effectiveness of risk management for ICT/IS and Reputational risks by these two major groups of respondents.

Another observation, which can be concluded from the above results, is that teachers tend to rate reputational risks higher in terms of criticality, than managers, but the effectiveness of risk management assessed by teachers and managers has no statistically significant difference. In addition, criticality of external risks is rated without statistically significant differences by teachers and managers, but the effectiveness of risk management is rated with statistically significant differences for external risks group is rated by teachers as more effective, than the same is rated by managers.

In the next sub-chapters, more detailed analysis of each risk group will be performed.

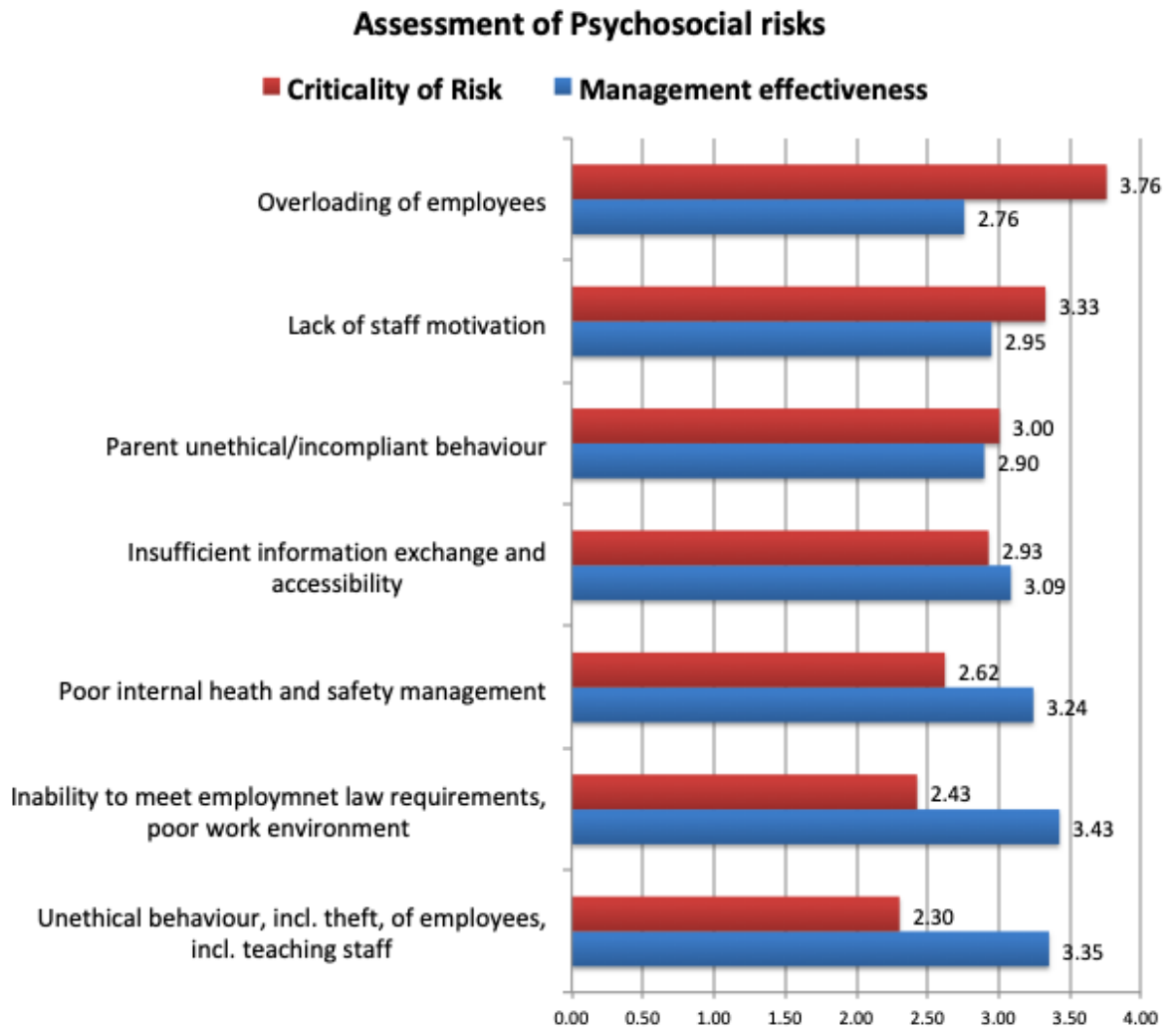
### **3.5 Risk assessment analysis by risk groups**

#### 3.5.1 Psychosocial risks

Reliability of the psychosocial risk scales were tested with the Cronbach’s alpha and the result of .853 validated the reliability of obtained results. Obtained results revealed that psychosocial risks are considered as significant, but not critical by the respondent sample in Survey 1 (average score:

2.94 – risk is slightly significant). Notably, that level of controls for majority of risks was rated opposite in proportion to risk criticality: the more significant is the risk, the weaker are the controls, and vice versa. Average score of control effectiveness for the psychosocial risk groups is 3.04 – risk is managed, but insufficiently.

Figure 3.10 provides graphical summary of respondent risk assessment results for psychosocial risk group sorted by highest risk criticality scores in order to see what risks the respondents perceive as most critical.



**Figure 3.10 Comparison of Criticality of risk and Risk control scores for Psychosocial risk group (Survey 1)**

Several psychosocial risks received the highest scores among all other risk types:

- Risk of “employee overloading” rated as the highest among the psychosocial risk group and among all the 32 risks evaluated. Average score of “Overloading of employees” risk is 3.76, what means that majority of respondents marked the risk as “very significant”. Overloading of employees usually results in exhaustion, over-burning, problems with health and decrease in autonomous



motivation. Average score of existing controls for this risk is 2.76, what means that educational institutions manage it as much as possible, but there are no strong controls or there is no possibility to implement strong controls. Such result provides evidence of the “scissors” between risk criticality and management of risk: risk is quite critical, but its management is rated as quite poor. Thus, such score provides a clear lack of risk management and of well-established risk controls. This serves as evidence, that introduction of risk management practices in the educational institutions should be relevant to strengthen the controls to improve risk management effectiveness. This risk is most correlated with “Lack of effective planning” risk (Pearson correlation .429) and with “Weak internal risk culture” (Pearson correlation .428). Hence, addressing planning and internal risk culture should help to mitigate risk of employee overloading to some extent.

- “Lack of staff motivation” risk was rated as second most important risk in the group, with average criticality score 3.33 (risk is significant), indirectly confirms the above and might be the consequence of the above risk (overloading of employees). Dombrovskis et al. (2011) revealed in their research that teachers in Latvia are lacking autonomous motivation, what has been further confirmed by this research results. The level of control for this risk was rated at 2.95, what means that the management of this risk quite weak. This risk correlates well with “Weak internal risk culture” (Pearson correlation coefficient .467) and with “Lack of qualified teaching staff” (Pearson correlation coefficient .431). Hence, it is important to work in internal culture and hiring qualified teaching staff to keep motivation of employees at a higher level.

- “Unethical behaviour of employees” risk received the lowest score in the psychosocial risks group (2.3 – risk is neutral). This can be interpreted as that there are implemented strong controls to manage the risks and the social climate at work is not at its worst in Latvian educational institutions, what makes employees feel quite emotionally safe at work. At the same time, this risk also holds an element of the conflict of interests, as respondents have to rate themselves and their colleagues on this topic, but managers – their managed educational institutions. On the contrary, risk of “Parent unethical/incompliant behaviour” is rated on average as 3.0 (risk is slightly significant). Risk of unethical behaviour of parents also has quite weak management level (2.9) according to respondents, whereas risk of employee unethical behaviour looks to be controlled more effectively (3.35). This can be explained by fact that behaviour of employees is internal risk, which is easier to control, whereas behaviour of parents is external risk, which is more difficult to control. On the other hand, as many respondents were managers, it was emotionally easier for them to answer more positively when rating risk related to behaviour of employees in educational institution, which they are managing.

▪ “Accessibility and exchange of information” risk received the score for criticality of risk 2.93 (risk is slightly significant) and 3.09 (risk is managed, but insufficiently) for the level of risk management effectiveness. It can be interpreted that the risk is not having high priority and therefore it is not expected to invest a lot of energy in its management. However, information provision and exchange increase organisational transparency and serves as job resource for employees. Thus, this factor should be paid more attention to and the risk controls should be increased by way of sharing information more openly and allowing employees to share their feedback when there is such.

▪ “Internal health and safety risk” was rated as having slightly significant criticality (2.62 – risk is slightly significant) and good controls (3.24 – risk is managed to as much extent as possible), what means that risk is rather more neutral than significant and is managed well. Health and safety aspects are the job resources that provide to employees feeling of safety and being cared about. This risk includes the quality of air in the classrooms that affects teachers’ vocal health, fire safety, physical safety, etc. This risk should have strong controls by way of implementing required by law policies and checks, regular fire tests, air tests, etc. The students studying Risk Management course at the University of Latvia raised this risk as one of the most poorly managed in universities. Students had a task to evaluate and discuss health and safety risk criticality and management effectiveness in three types of educational institutions: pre-schools, schools and universities. The conclusion was same for all four streams of students: risk is managed quite well in pre-schools, slightly worse in schools and most unmanaged in universities. Such conclusion was explained by fact that in most schools and pre-schools there are introduced safety measures such as door codes, closure of doors during lessons, etc., whereas there are no entry controls at universities in Latvia. Students also raised concern that they have not evidenced fire safety tests and trainings at university, whereas such tests they experienced when they were studying or working at schools and pre-schools. Thus, more attention should be brought to managing this risk, as it depends mainly on internal controls and has interdependence with external funding.

▪ Criticality of “Inability to meet employment law requirements, poor work environment” was rated as the second lowest among psychosocial type of risk controls (2.43 – risk is neutral), and the management effectiveness score for this risk is quite high (3.43 – risk is managed well to as much extent as possible). Provided that 54% of respondents completing the survey were managers of educational institutions or their deputies, and that the highest scores were given by managers, such criticality score demonstrates slight concern of the educational sector managers on their ability to follow all the complex employment law requirements and increasing requirements of employees. Hence, regulators should communicate requirements in clear and concise way and ensure provision of all necessary resources to enable educational institutions to realise them. Interesting fact is that this

risk has the highest Pearson correlation coefficient (.677) with the risk of “Poor internal health and safety management”, thus managing health and safety well within the organisation should play a vital role in managing the risk or poor work environment and non-compliant employment practices. As the Table 3.7 demonstrates, this risk is also correlated with a number of other risks examined:

**Table 3.7: Correlation of “Inability to meet employment law requirements, poor work environment” risk with other risks (Survey 1)**

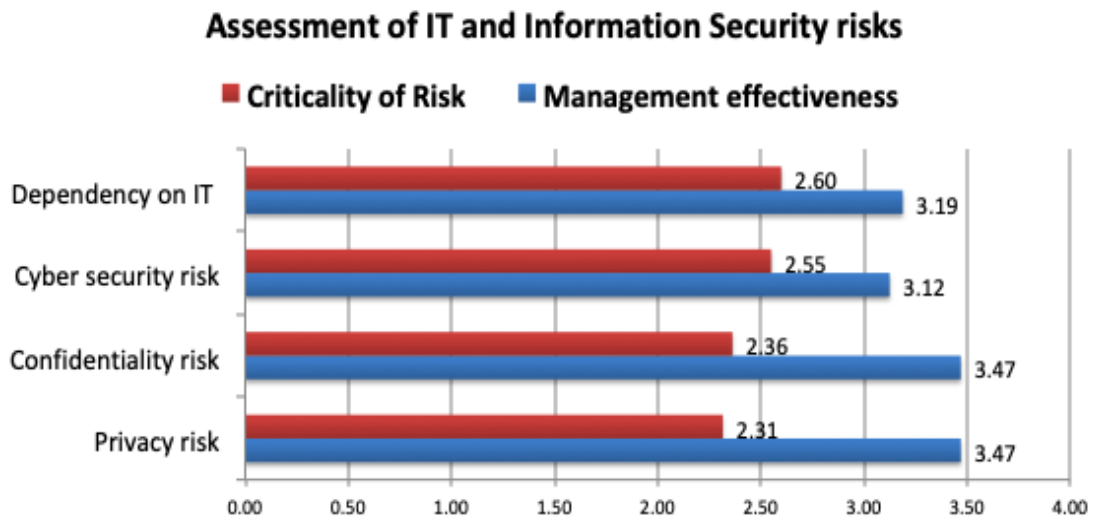
Risk title	Pearson correlation coefficient
Poor internal health and safety management	.677
Inappropriate educational programmes not meeting regulatory requirements	.638
Violence and bullying risk	.624
Corruption	.601
Confidentiality risk	.562
Inadequate level of quality of education provided	.550
Privacy risk	.542
Lack of effective planning	.505
Inadequate strategic decision making	.499

Some of the above correlations can be observed as a consequence or a cause of the risk in question. For example, with poor working environment in line would be logically to assume corruption risk, inappropriate educational programs and lack of care for privacy and confidentiality issues. Poor working environment can be caused by lack of effective planning and inadequate strategic decisions, as well as insufficient internal documentation. Hence focusing on addressing these key causes, that risk should be taken under control by management of educational institution.

### 3.5.2 IT and Information Security (including privacy and cyber) risks

Reliability of the Information security risk scales were tested with the Cronbach’s alpha and the result of .786 validated the reliability of obtained results. Obtained results revealed that IT and Information security risks are considered to have neutral significance by the respondent sample in Survey 1 (average risk criticality score: 2.46 – risk is neutral). Respondents rated risk management effectiveness for this risk group much higher, what may explain the low-risk criticality score: average score of control effectiveness for the IT and Information Security risk group is 3.31 – risk is managed to as much extent as possible.

Figure 3.11 provides graphical summary of the risk assessment results by stakeholders for IT and Information security risk group sorted by highest risk criticality scores in order to see what risks the respondents perceive as most critical.



**Figure 3.11 Comparison of Criticality of risk and Risk control scores for IT and Information Security risk group (Survey 1)**

- The most topical risk according to the respondents of Survey 1 in this risk group is “Dependency on IT” risk with average criticality score 2.6 – risk is slightly significant. The essence of this risk lies in the idea that nowadays IT started to play huge role in everyday life: all people have mobile phones, personal computers, etc., what makes businesses and critical service providers, such as educational institutions, heavily dependent on technologies and vulnerable to IT downtimes, electricity shortages, loss of Internet and third-party IT service provider failures. In line with relatively low risk criticality score, respondents consider that this risk managed as good as it could be, with risk management effectiveness average score 3.19 – risk is managed to as much extent as possible. This risk also is not correlated to other risks in this risk group. This brings to a conclusion, that in overall, educational institutions in Latvia are not heavily dependent on technologies and thus are not vulnerable to IT downtimes. Existing residual risk is well managed. However, given that the Survey was conducted in years 2018-2019, the situation might have changed following the pandemic forced transition from classroom teaching to online teaching.

- Despite the GDPR rules enforced in 2018 respondents rated Privacy risk as the lowest in this risk group with 2.31 score – risk is neutral. It is possible, that this risk is undervalued by the respondents, as Privacy risk is hard to understand and hard to estimate its possible impact. Respondents also rated risk management effectiveness for Privacy risk as one of the highest – 3.47 – risk is well managed. It is possible that the GDPR and its implementation brings such feeling to the

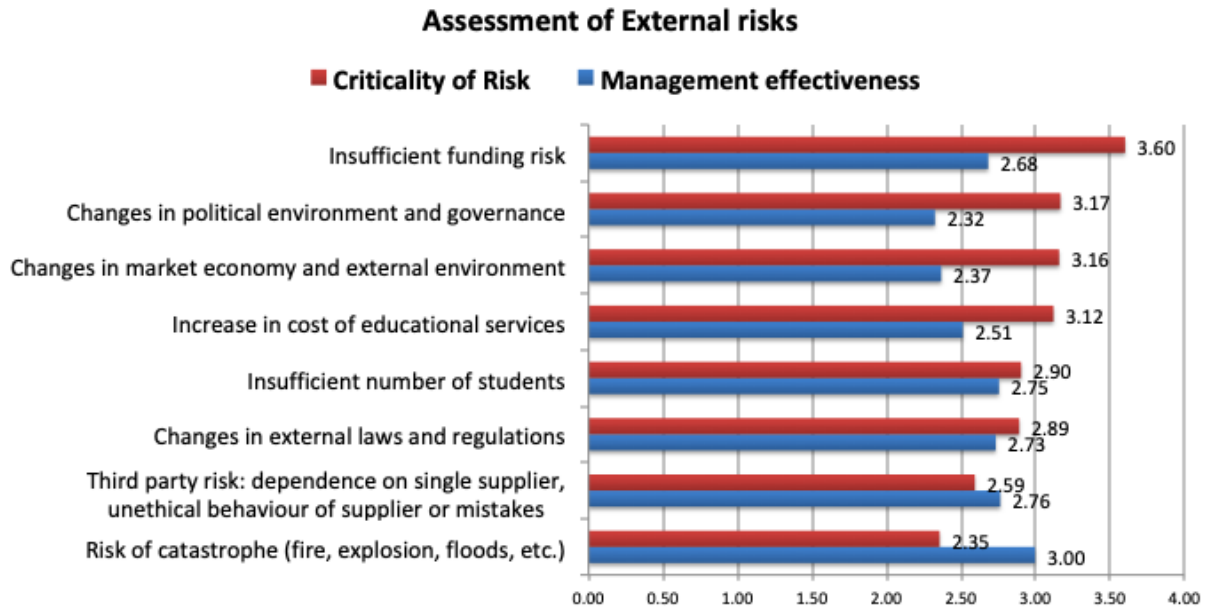
respondents and makes the risk to be perceived as not very important and well managed, when in reality it may not be so. Hence, apart from evaluation of respondents for this risk it is needed to study the statistics of actual privacy breaches in educational institutions and fines imposed by regulator on the educational institutions in Latvia. However, for such information to become available in trustable dataset, more years need to be passed to collect trustable incident and loss data.

- Similar to privacy risk is the risk of leaking confidential and restricted access information – the Confidentiality risk. Respondents gave slightly higher criticality score to the Confidentiality risk – 2.36 – risk is neutral, but the average risk management effectiveness score is exactly the same as of Privacy risk – 3.47 – risk is well managed. Pearson correlation with Privacy risk is .765, which is the highest correlation in this risk group, proving the interdependence for these two risks.

- Cyber security risk was ranked as second most important risk in this risk group with average criticality score of 2.55 – risk is slightly significant. Pearson correlation with Privacy risk is .637, what allows concluding there is correlation between these two risks, although Cyber security risk is ranked as more significant. The average risk effectiveness score for this risk is 3.12 – risk is managed to as much extent as possible. In overall educational institutions are not considered being vulnerable to cyber security risk and managing residual risk well.

### 3.5.3 External risks

Reliability of the External risks scales were tested with the Cronbach's alpha and the result of .743 validated the reliability of obtained results. Obtained results revealed that External risks are considered to have slightly significant criticality by the respondent group in Survey 1 (average risk criticality score: 2.97 – risk is slightly significant). Average score of control effectiveness for the External risks group is 2.64 – risk is managed to as much extent as possible. Summary of the results are presented in Figure 3.12:



**Figure 3.12 Comparison of Criticality of risk and Risk control scores for External risk group (Survey 1)**

- The most critical risk in this risk group is considered to be “Insufficient funding risk” with average score of 3.6 – risk is very significant and risk management effectiveness score of 2.68 – risk is managed to as much extent as possible. This may mean that it is not well understood how to manage this risk and respondents subjectively provided the rating that everything what is known as possible is done but accept that not to the full extent. Risk of insufficient funding may be seemed to be highly related to “Insufficient number of students risk”, however Pearson correlation for these two risks appears to be just .194 according to Survey 1. On the other hand, highest correlation of this risk in this risk group is seen with “Increase in cost of educational services” (.479).

- “Changes in the political environment” risk is considered by the respondents as the next most critical risk in this risk group with the risk criticality score of 3.17 – risk is slightly significant and risk effectiveness score of only 2.32 – risk is poorly managed. The educational institutions hardly can manage political risk, hence the low-risk management effectiveness score. Risk management score for this risk is the lowest among all 32 risks in all risk groups, meaning that this risk has weakest controls and has weakest risk management. At the same time, this risk is one of the most impactful on the sector of education - changing political environments often are connected to educational reforms, causing the most significant changes in the sector of education, what constitutes the core of this risk.

- Very similar situation is with the “Changes in the market economy and the external environment” risk: risk criticality score is 3.16 (risk is slightly significant) and risk management effectiveness score of 2.37 (risk is poorly managed). This can be explained in the same way as with

the political risk - educational institutions cannot influence the market economy and the external environment, however changes in the market economy may have significant impact on the educational institutions: from changes in funding to changes in number of applicants and students, to changes in compensation of employees and changes in internal culture. Well correlated (Pearson correlation score - .514) with the above risk (“Changes in the market economy and the external environment”) is the risk of “Increase in the cost of educational services”, which has average risk criticality score of 3.12 (risk is slightly significant) and average risk management effectiveness score of 2.51 (risk is managed as much as possible, but not sufficiently). Increasing costs of the educational services are connected to funding, number of students and demand for educational services, political and economic environment. Hence, this risk to some extent is hard to manage by the educational institutions, but possible to reduce its impact by mitigating risk of insufficient number of students and risk of underfunding.

- “Insufficient number of students” and “Changes in regulations” risks rated similarly with average risk criticality scores 2.90 and 2.89 respectively – risk is slightly significant. These two risks have very low correlation between themselves (.132) and “Insufficient number of students” risk best correlates with the risk “Unethical behaviour of employees, internal fraud and theft” (.422). “Insufficient number of students” and “Changes in regulations” risks also rated very similar on average risk management effectiveness score – 2.75 and 2.73 respectively (risk is managed as much as possible, but not sufficiently). “Changes in regulations” risk is difficult to manage as it is not much dependent on educational institutions, but on the other side it can be managed well if educational institutions get a chance to discuss and comment upcoming regulatory projects and these views would be considered before enforcing a new regulation. “Insufficient number of students” risk can be managed by raising quality of education, continuously upgrading qualifications of teaching personnel, maintaining high level of service and keeping fees competitively low.

- “Third party risk” in this research and survey means the risk of over-dependency on suppliers, risk of unethical supplier delivery and supplier not fulfilling obligations. This risk was rated as one of the least significant, with average score of 2.59 – risk is slightly significant. The risk management effectiveness score average rating given by the respondents was 2.76 - risk is managed as much as possible, but not sufficiently. To mitigate this risk, it is important to timely sign clear and transparent agreements with the suppliers ensuring a penalty in case of failure from supplier side, as well as it is important to have workarounds as plan B in place. An example of supplier failure is the incident when in Sigulda’s primary schools several kids were poisoned by eating fruits in the kindergarten (LETA, 2019). The third-party risk was found to be best correlated with “Corruption” risk (.518) and with

“ineffective budget planning” risk (.522), which is very logical, as with thorough budget planning and prevention of corruption the third-party risk can be partially managed.

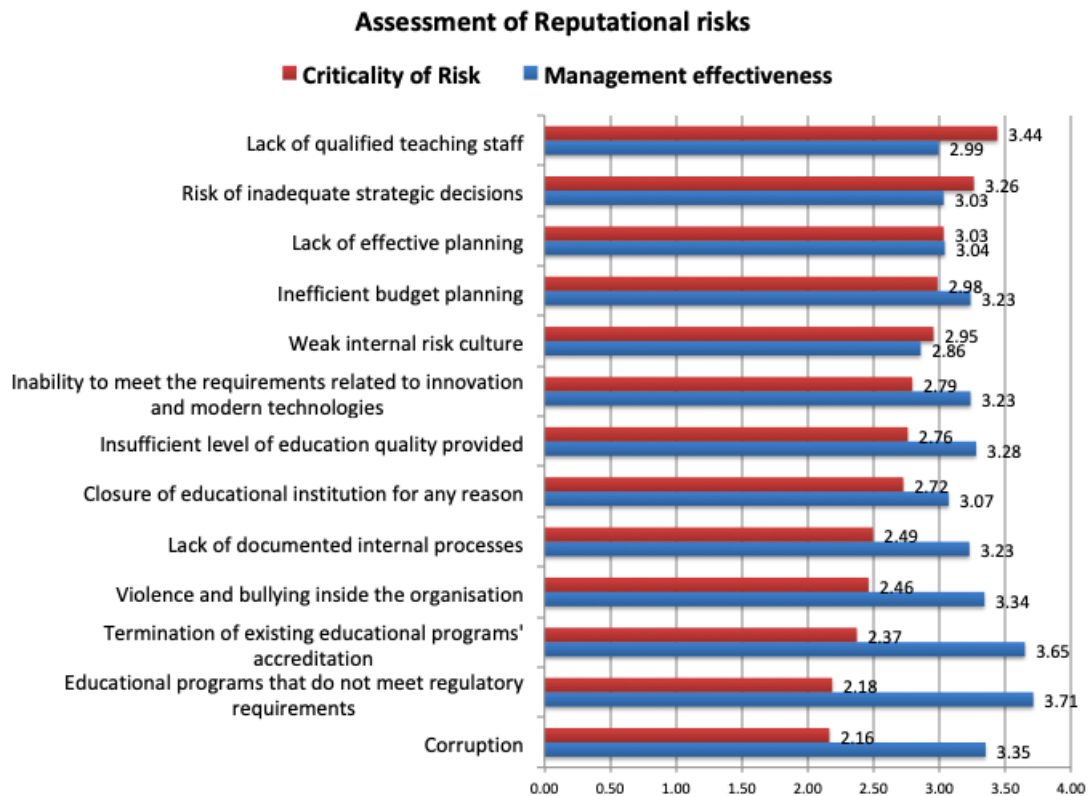
- The risk of catastrophe was rated with lowest criticality score – 2.35 (risk is neutral) and highest in this group risk management score (3.0 – risk is managed to as much extent as possible). This is the perception of respondents that risk of fire, floods and other types of catastrophes is very low due to existing strong controls, e.g., fire alarms, anti-flood systems, etc. As already observed above, respondents rated risks as less significant when they feel that strong controls are in place, which is reflected in risk management effectiveness score. However, this risk can be underestimated due to its rare nature and human tendency to expect positive events rather than negative events, thinking that the worst should never happen “with me”, but happens somewhere else “with others”.

- Pandemic risk was not provided as an option in the survey, because it was not well understood by the respondents at the time of the survey (2018-2019) and thus was excluded from the risk assessment. The fact of poor understanding of the pandemic risk by the respondents serves as indirect evidence that the effectiveness of this risk management was very poor at the time and risk not considered as significant at all, what has resulted in lack of advanced business continuity planning when the actual pandemic has happened in 2020.

#### 3.5.4 Reputational risks

Reliability of Reputational risks scales were tested with the Cronbach’s alpha and the result of .862 validated the reliability of obtained results. Obtained results revealed that Reputational risks are considered to have slightly significant criticality by the respondent sample in Survey 1 (average risk criticality score: 2.74 – risk is slightly significant). Average score of control effectiveness for the Reputational risks group is 3.23 – risk is managed to as much extent as possible. This risk group was rated as more significant than IT risks group, but slightly less significant than External and Psychosocial risk groups. Management effectiveness for Reputational risks group was directly opposite: it is managed slightly worse than IT risks group, but better than External and Psychosocial risk groups. Summary of the risk assessment results are presented in Figure 3.13:





**Figure 3.13 Comparison of Criticality of risk and Risk control scores for Reputational risk group (Survey 1)**

▪ In this risk group, the most significant and least managed risk is “Lack of qualified teaching staff”. This risk takes leading position among all risks in all risk groups, taking the third place in top risks with rating of 3.44 – risk is significant. Its management score also is one of lowest in this risk group with average score 2.99 – risk is managed to as much extent as possible, but this could be insufficient. This risk is slightly correlated with “Insufficient level of education quality provided” (Pearson correlation - .480), with “Lack of employee motivation” (Pearson correlation -.431) and “Weak internal risk culture” (Pearson correlation - .384).

▪ Risk of “wrong strategic decisions” in this group rated as second highest with risk criticality score of 3.26 (risk is slightly significant) and risk management score of 3.03 (risk is managed to as much extent as possible). Given that respondents were to large extent managers of educational institutions, the score is quite high, meaning that there is uncertainty and insufficient confidence in effectiveness of strategic decision-making within educational institutions. This risk has quite good correlation with the risk of “Inefficient budget planning” (Pearson correlation - .657), as well to most of other reputational and psychosocial risks (e.g., Pearson correlation of .512 with “Insufficient level of education quality provided”, Pearson correlation of .499 with “Inability to meet employment law requirement, poor work environment”, Pearson correlation of .497 with “Lack of effective planning”,

etc.). Such correlation with other risks proves the validity of the risk and points out to main consequences that arise from manifestation of poor strategic-making risk.

▪ Third risk in this category by criticality is “Lack of effective planning” with risk criticality score of 3.03 (risk is slightly significant) and higher risk management score of 3.04 (risk is managed to as much extent as possible). Effective planning risk is related to the risk of poor strategic making and is one of the triggers for psychosocial risks, such as overloading of employees. It correlates well with “Employee overloading” risk (Pearson correlation .429), “Poor internal risk culture” (Pearson correlation .582), “Insufficient level of education quality provided” (Pearson correlation .546), “Lack of documented internal processes” (Pearson correlation .459), etc. Thus, it is possible to make a conclusion that reputational risks are quite interconnected with other risks.

▪ “Weak internal risk culture” risk is well correlated with the previous three risks, as described above, but it has slightly lower criticality score – 2.95 (risk is slightly significant) and its management effectiveness was rated quite low comparing to other risks in this risk group, 2.86 – risk is managed as much as possible, but insufficiently and in view of some respondents, quite poorly. Strengthening internal risk culture can mitigate most of other risks in reputational and psychosocial risk categories, as it would require order in documentation and processes, clear strategy and good planning. Thus, in order to mitigate most of other more significant risks, it is advisable to focus on mitigating particularly this risk and strengthen internal risk culture and awareness, not only for certain employee group, but for all managers and employees.

▪ “Failure to meet requirements related to innovation and modern technologies” has risk criticality score of 2.79 (risk is slightly significant) and quite balanced risk management score of 3.23 (risk is managed sufficiently to as much extent as possible). Risk is quite well correlated with risk of “Weak internal risk culture” (Pearson correlation .489), “Insufficient level of education quality provided” (Pearson correlation .444), “Lack of effective planning” (Pearson correlation .440), and other. Correlation with “Lack of employee motivation” risk is quite low – Pearson correlation .242. Hence, manifestation of this risk negatively impacts quality of provided education but does not have any significant interconnection with motivation of employees.

▪ “Insufficient level of education quality provided” risk by itself has quite low criticality score – 2.76 (risk is slightly significant) and relatively high-risk management effectiveness score of 3.28 (risk is managed as much as possible to quite a sufficient level). At the same time, this risk mainly is the result of manifestation of other risks, as this risk is most correlated with most of other risks studied in this research as presented in Table 3.8:

**Table 3.8: Correlation of “Insufficient level of education quality provided” risk with other risks**

Risk title	Pearson Correlation coefficient
Educational programs that do not meet regulatory requirements	.604
Confidentiality risk	.566
Inability to meet employment law requirements, poor work environment	.550
Lack of effective planning	.546
Lack of documented internal processes	.531
Inefficient budget planning	.524
Violence and bullying inside the organisation	.514
Risk of wrong strategic decisions	.513

At this point conclusion can be drawn that low quality of education is more of a consequence, rather than stand-alone risk. By mitigating risks related to governance and management of educational institution, quality of education is strengthened naturally.

▪ “Closure of educational institution for any reason” risk is the next one risk by criticality, with criticality score of 2.72 (risk is slightly significant) and risk management effectiveness score of 3.07 (risk is managed to as much extent as possible). This is one of the risks, which is hard to manage due to its unpredictability and dependency on other risk factors. This risk similarly to the previous one is more of a consequence of other risks manifestation, which damage reputation of educational institution and lead to its closure. Respondents, hence, rated it quite low on criticality and quite low on management effectiveness. This risk is well correlated with other risks as presented in Table 3.9:

**Table 3.9: Correlations of “Closure of educational institution for any reason”**

Risk title	Pearson Correlation Coefficient
Risk of catastrophes	.524
Termination of accreditation for educational programmes	.485
Risk of violence and bullying	.482
Risk of educational programmes not being compliant with regulatory requirements	.480
Unethical behaviour of employees	.468
Poor working environment and breaches of employment law	.445
Insufficient level of quality of education	.436
Insufficient number of students	.422

Thus, risk of closure of education institution is tied to other factors such as quality of education, quality of teaching staff, working environment for teaching staff and atmosphere in educational institution. This risk can be managed by addressing the risks which trigger it: attracting more students, working on strong risk culture, developing positive morale among employees, developing compliant educational programmes, documenting internal processes and controls to prevent unethical behaviour and violence, etc.

- “Lack of documented internal processes” should be looked at as the cause for more global risks, such as closure of educational institution, fraud and violence inside the educational institution, lack of qualified teaching staff and insufficient number of students. As a stand-alone risk, respondents rated it as slightly significant with average risk criticality score of 2.49 and risk management effectiveness score of 3.43 (risk is managed quite well). This risk is most correlated with Confidentiality and Privacy risks (Pearson correlation .531 and .473 respectively), which also were rated as well managed low significance risks. However, managing the aspect of documentation is critical to proper functioning of educational institution, as improper or insufficient documentation triggers reputational damages that may result in low level of education quality provided, low morale among employees and subsequent closure of educational institution.

- “Violence and bullying inside the organisation” risk was rated with average criticality score 2.46 (risk is neutral) and risk management effectiveness score of 3.34 (risk is well managed). Violence and bullying risk mitigation strategy is needed to increase risk management effectiveness and decrease the risk.

- “Termination of existing educational programme accreditation” and “Educational programmes that do not meet regulatory requirements” are very similar risks as usually accreditation is terminated for educational programmes that do not meet the requirements set by regulator. Respondents rated the “termination of accreditation” risk with higher average criticality score of 2.37 and risk of “Educational programmes that do not meet regulatory requirements” with 2.18 average criticality score, thus allowing that programmes that do not meet regulatory requirements have lower probability and impact than termination of accreditation. Risk management effectiveness for these two risks is 3.65 and 3.71 (risk is well managed) respectively, meaning that risk of termination of accreditation can be managed slightly less, than risk of non-compliant educational programmes. Pearson correlation between these two risks is .637, which is quite strong correlation. These risks are also well correlated with “low level of education quality provided” (Pearson correlation .453 and .604 respectively), “corruption” (Pearson correlation .487 and .548 respectively), “poor working conditions” (Pearson correlation .496 and .638 respectively) and “unethical behaviour of employees”

(Pearson correlation .518 and .561 respectively). Thus, these risks should also be managed together and in line with other reputational and psychosocial risks, but not as a stand-alone risk.

▪ The lowest criticality score (2.16) and highest risk management effectiveness score (3.35) respondents attributed to “Corruption” risk. Such rating most possibly was selected, as respondents mainly were the managers of educational institutions, deputy managers and teachers. Thus, assessment of this risk creates some sort of conflict of interests given that educational institution managers are the main subjects of corruption risk. This risk demonstrated quite strong correlation with “violence and bullying” risk (Pearson correlation .648), “non-compliance employment practices and poor working environment” (Pearson correlation - .601), “third party supplier risk” (Pearson correlation .518) and “ineffective budget planning” (Pearson correlation .510). Hence, by addressing budget planning, supplier risk, employee morale and working environment it should be possible to further lower the corruption risk.

### 3.6 Responsibility for risk management within the sector of education

One of the open-type questions in the Survey 1 was: “**Who, in your view, should be responsible for the risk management in an educational institution?**”. This question was answered only by 140 respondents out of 235 (60%) as Survey 1 was released in two waves: initial, when this question was not included, and second after half year, when questions were reviewed according to respondent feedback and supplemented to get clearer results. Majority of respondents (90; 64%) answered that the main responsibility lies on the head of institution (e.g., school’s director). Figure 3.14 provides summary of the responses.

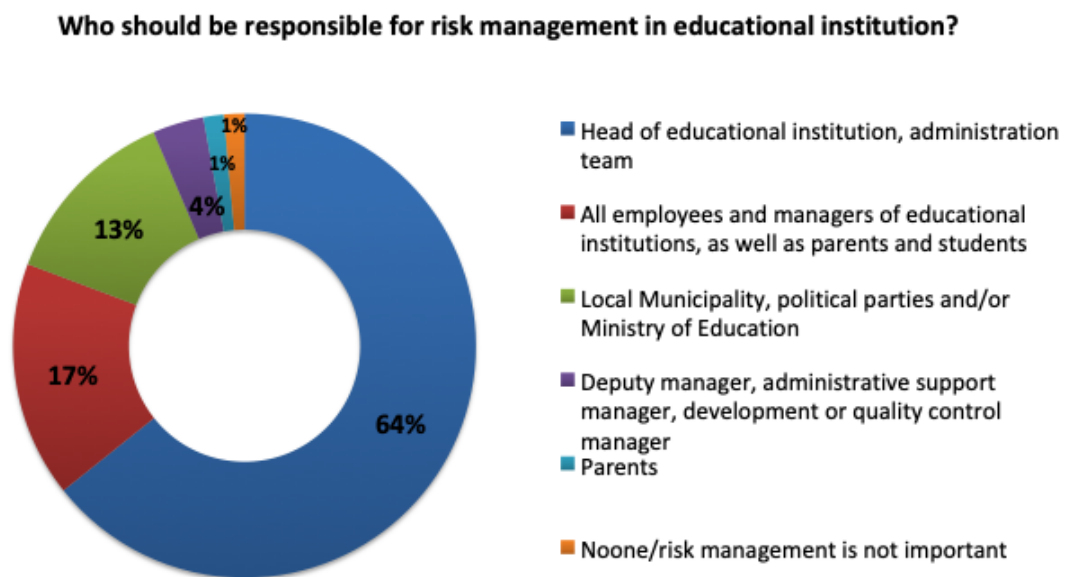


Figure 3.14: **Distribution of respondent answers on question in Survey 1 “Who, in your view, should be responsible for the risk management in an educational institution?” (n=140)**

▪ 64 out of 73 (60%) managers and deputy managers, who answered this question, stated that head of educational institution and school's administrations are responsible for risk management, whereas the same answer was provided by 34 out of 50 (68%) teachers, who answered this question, and 11 out of 12 (92%) employees of educational institution.

▪ As was explained in Section 1.3, the correct answer, that everyone is responsible for risk management, including head of institution, administrative staff, teachers, students, parents, etc., was provided by only 23 or 17% of respondents who answered this question. Analysing the distribution of answers by position or related to institution, 18% of managers (13) and 18% of teachers (9) provided this answer.

▪ 13% of respondents (18 out of 140) consider that for risk management in educational institution should be responsible local Municipality, Ministry of Education or political parties. This could be a valid opportunity for risk management organisation in the sector of education, as it is organised this way in several developed countries. Nevertheless, such responsibility would be very formal and practical daily risk management should stay on managers, employees, students and parents of educational institution. Such practice could be practical for implementation to take the burden off from the educational institutions.

▪ Out of all 140 respondents, who answered this question, only 2 selected answer option that none is responsible as risk management is not important, what demonstrates good level of risk culture and risk management importance for the representatives of educational institutions.

### **3.7 Improving risk management practices in the sector of education**

One of the last questions in Survey 1 was attributed to gathering respondent opinions on what is needed to strengthen and improve risk management in the sector of education. Respondents answered in free form to the question **“What in your opinion is needed to better manage risks in the sector of education?”**.

Answers were read and analysed by the author for similarities and as result were grouped into 10 groups. Summary is provided in Figure 3.15. Some respondents provided very comprehensive answers, which fell simultaneously into several groups, therefore such answers were counted in several groups and total number of answers is higher than the number of respondents. Below in Figure 3.15 is provided a diagram of answers, followed by detailed analysis of each answer group with quotes of the respondents.

### What in your opinion is needed to better manage risks in the sector of education?

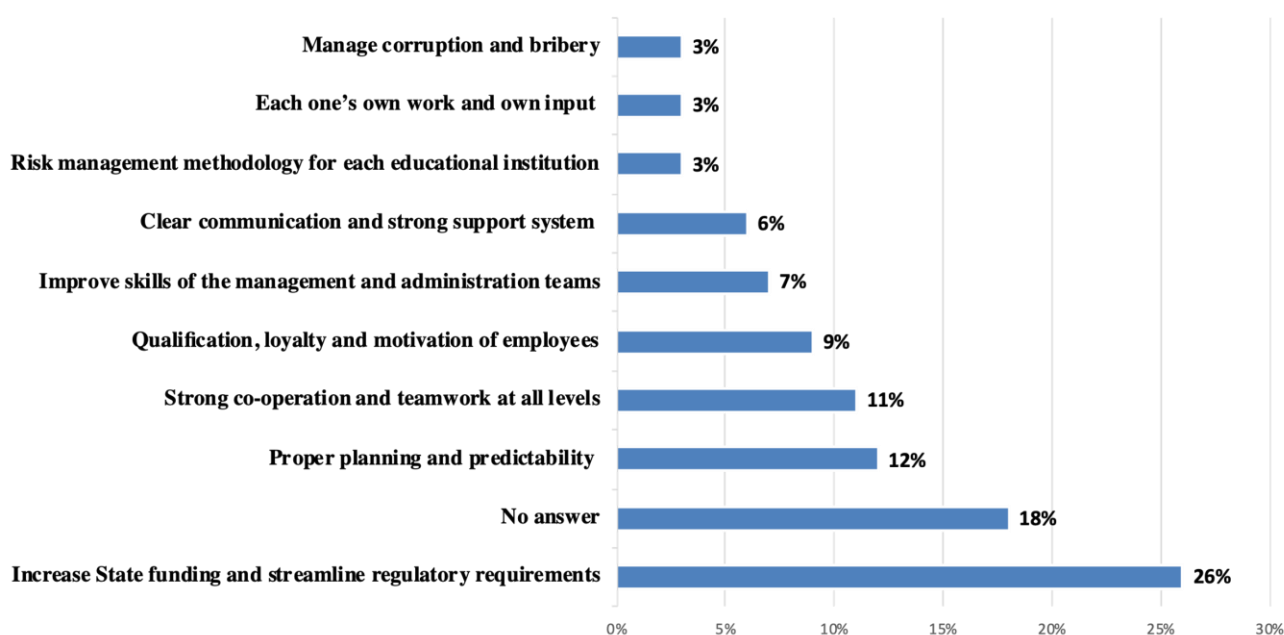


Figure 3.15 Distribution of answers on question “What in your opinion is needed to better manage risks in the sector of education?” (Survey 1)

▪ 63 out of 235 (26%) answers stated that to strengthen and improve risk management in the sector of education as well as to mitigate the key risks, it is important to first of all make an order in the system itself: increase State financing for schools and streamline regulatory requirements, making them more transparent, clear, integrated and relevant. Several quotes from this category that are worth to be mentioned in order to evidence the above conclusion:

- *“Need to end reforming reforms with reform on reform”*
- *“Stable legislation basis, clear municipal policy, known amount of funding in the long run”*
- *“Reduce the number of controlling institutions by transforming them into consultancies who help to streamline and improve all indicators. To create an environment, where there is high personal responsibility for everyone, high motivation for self-growth, creating a culture of cooperation. The school is a model of a mini society where characters, values, accomplishments and goals meet. The way we want to see the society of the future is the model of today's pre-school and school environment. The key words are respectful communication, personal responsibility and cooperation. If everyone takes responsibility for their thoughts, words and actions, then the risks will be reduced in all areas. We have a private school and a collegiate administration. We create an environment where everyone thinks about lifelong self-development and the work environment where one wants to work. Manager coordinates*

*employees and creates an environment where everyone is involved in problem solving. This way risks are identified and mitigated.”*

➤ *“The education system as a whole needs to be put in order”*

➤ *“Stability in the country, clear goals and objectives”*

➤ *“Stable, national, unified understanding of education and long-term management (clear, scientifically based, tested, functional (based on conclusions) education policy, not in 20 years 20 ministers of education and one reform more interesting than another ... unfinished, etc.”*

➤ *“Streamlining legislation, more funding for schools, motivating teachers”*

▪ 43 out of 235 (18%) respondents either did not answer the question (37) or answered «don't know» (3) or replied that risk management is either not important or not possible (3). The fact that so many respondents were either unable or not willing to answer the question or believe that risk management is not important or possible, demonstrates low awareness level about risk management purpose and importance. There is popular silo approach and high level of bureaucracy in the sector of education what makes managers and employees believe that risk management will only complicate life and add up to more useless work. Fact how risk management can be efficient and helpful is not understood almost at all and thus risk management is not very popular among the educational institutions.

▪ 29 out of 235 respondents (12%) stated that proper planning and predictability are very important for efficient risk management. This involves planning for operations continuity, planning for various incidents and situations, planning budget, costs, process of education in different scenarios, etc. Predictability and planning are very important for risk scenarios when work of educational institutions is complicated, such as pandemics, weather disasters (hurricanes, strong frost or high heat, etc.), severe political situation in the country, etc. Few of the most notable quotes of respondents to evidence the above are as follows:

➤ *“Think about possible risks, plan and implement measures to prevent these risks”*

➤ *“Plan the risks and work on preventing them from materialisation”*

➤ *“Identify risks and develop action plans”*

➤ *“Strategic long-term development planning”*

➤ *“Degree of stability, gradual justified changes”*

➤ *“Risk planning. Awareness of employees in risk planning and management processes in the educational institutions should be increased”*

➤ *“Planning the future of the educational system and ensuring stability”*



▪ 25 out of 235 (11%) responses indicated that in order to effectively manage risks it is important to ensure strong co-operation and work as a team. Respondents highlighted that often the key cause of risk manifestation is lack of teamwork and everyone working for personal benefit. If this could be overturned and everyone would work for the common goals as one team on all levels: government, ministry, educational institutions, employees and managers – then the risks could be managed more effectively.

Some of the most notable quotes to evidence the above:

- *“Meaningful cooperation between different institutions”*
- *“Cohesive teamwork. Preferably - the teamwork of the administration team”*
- *“I think that there must be risk assessment and management in every professional field so that it complies with the international laws and requirements of the employers towards this specialty. This means working in a team, assessing the interests and needs of all stakeholders”*

▪ 20 out of 235 (9%) respondents indicated that in order to better manage risks in the sector of education the most important aspects are the qualification, loyalty and motivation of employees. The main idea is to constantly develop employees and invest in them, fostering loyalty and professionalism, at the same time not overloading them and performing constant controls over the quality of their work. Some of the most notable quotes to be mentioned to provide evidence for the above:

- *“If smart, knowledgeable people would work in the sector”*
- *“Raising the qualification of employees, providing additional courses in the specialty”*
- *“Potential teacher overload (and burnout) needs to be reduced to manage risks more effectively”*
- *“Teachers of any seniority level should hold at least one open lesson per academic year”*

▪ 16 out of 235 (7%) replied that in order to manage the risks more proficiently it is needed to improve skills of the management and administration teams, especially in risk management as such. The key cause for risk manifestation these respondents indicated was weak management skills of the administration staff and as a result weak risk management in the institution. Hence in order to improve, it is needed to strengthen the management teams in educational institutions. Some of the most notable quotes that form the above statements are as follows:

- *“Good leadership of educational institutions willing to accept and manage risks; who keep pace with changing times and can solve institution problems indicating possible risks”*
- *“Heads of educational institutions are not trained as business managers. They do not understand budget planning (it comes from the school board), do not plan the development opportunities for their educational institution (it is decided by the municipality of the city).”*

*Their powers are very limited, educational institutions are managed by the municipality and the school board”*

- *“Training of managers in risk management topic”*
- *“A more knowledgeable manager with knowledgeable management team members”*
- *“More professional work of managers”*

▪ 14 out of 235 (6%) replied that clear communication and strong support system are crucial for successful and strong risk management. Under this statement it is meant that better information exchange is needed between institutions and parents, between managers and employees, between regulatory institutions and educational institutions, etc. Without clear and transparent communication there is higher inclination for incidents and poor handling of incidents related to miscommunication and insufficient information sharing. In addition, stronger support system in form of better salaries for teachers, motivational package, support of the senior management instead of reprimands, more sufficient human resources, etc. The most notable quotes in this group are as follows:

- *“Timely exchange of information at all levels”*
- *“Better information flow”*
- *“Increase awareness of employees about risk planning and management processes in the educational institution”*

▪ 8 out of 235 (3%) responses stated that in order to manage risks effectively it is important to have proper risk management methodology in place for each educational institution. It was noted that having risk registry, analysing and fixing each incident, as well as development of risk management handbook would help to manage risks more effectively. Some of the quotes are as follows:

- *“Unified risk management methodology. Preferably according to the type of educational institution: primary, secondary, professional education...”*
- *“System, methodology, guidelines.”*
- *“Explain the most effective risk management solutions, create a risk handbook”*

▪ 8 out of 235 respondents (3%) believe that it is each one’s own work and own input are the key pre-requisite for successful risk management within the educational institutions. It is important to raise awareness of employees and understanding of the risk management. Some of the quotes from this category:

- *“Be aware of as many potential risks as possible.”*
- *“Ability to identify the risks”*
- *“Understanding the risks and own work”*

▪ 7 out of 235 (3%) responses indicated that the most important is to manage corruption and bribery risks in the sector of education to achieve effective risk management. For example, some of respondents said the following:

- *“An anti-corruption action plan is needed in every educational institution.”*
- *“As often as possible to control how appropriately the educational institution spends and allocates salary rates to teachers and administration.”*
- *“Eliminate the «blat» system in the educational institution.”*

### 3.8 Insurance

Only 83 out of 236 respondents (35%) stated that their educational institution has some kind of an insurance policy. 75 out of 236 respondents (32%) stated that their educational institution most probably does not have an insurance policy. 73 out of 236 respondents (31%) stated that they do not know whether their institution has an insurance policy at all. 5 out of 236 respondents (2%) left this question without an answer. Figure 3.16 visually summarises the results of this question. Hence, respondents split mainly into 3 equal parts, where 1/3 of respondents does not know at all whether their educational institution uses insurance and 1/3 knows that their educational institution does not use insurance. This is another evidence of weak risk management in the educational institutions, as insurance is a great tool to minimise impact of rare but plausible high loss events, such as explosion, fire, floods, etc.

#### DOES YOUR INSTITUTION MAKE USE OF INSURANCE TO MITIGATE RISKS?

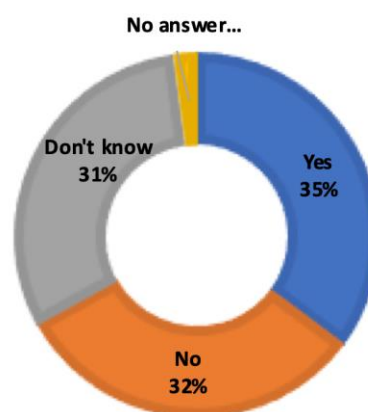


Figure 3.16 **Distribution of respondent answers whether their institution makes use of insurance (Survey 1)**

Out of 1/3 of respondents, who replied “yes” to this question, stated the following insurance types used by their educational institutions:

- Health insurance for employees
- Building insurance
- Travel insurance for students and teachers while going out on excursions
- Valuable assets inside the building
- Traumas during competitions for sport schools

Many respondents also indicated that their insurance is sponsored by the local municipality and in private schools it is sponsored by the founders of the school.

### **3.9 Summary on Survey 1 results**

➤ In rating on the scale from 1 to 5 how well are risks managed in the sector of education (1 – “poor”, 6 – “strong” risk management), respondents had a tendency to choose middle number, between 3 and 4. This result provides evidence about uncertainty of respondents on how risks are managed in the organisation they belong to and possible cognitive bias choosing the numbers in the middle being unsure which is the correct answer. Such result indirectly supports the initial hypothesis, that there is low awareness about risk management in the sector of education, what could trigger such a result.

➤ Managers of educational institutions tend to evaluate risk management in their educational institutions more positively with the mean ( $\mu$ ) score 3.21 (n=117).

➤ Teachers and employees rated risk management with lower mean ( $\mu$ ) score 2.79 (n=94).

➤ Survey 1 results demonstrated low awareness of respondents about incident reporting and low usage of this management tool in the educational institutions of Latvia. The conclusion can be made that the risk management awareness and risk culture may not be at the sufficiently high level in the educational institutions of Latvia and require focused training and raising of awareness.

➤ Survey 1 revealed an observation, that when the risk was assessed as more critical, management of effectiveness for the same risk was assessed as very low and vice versa, thus creating “scissors” effect between risk criticality and level of its management.

➤ According to results of the Survey 1, the most critical and topical risks in the education sector in Latvia are overloading of employees (average 4 points out of 5), insufficient funding (average 3.8 points out of 5), lack of employee motivation (average 3.5 points out of 5), lack of qualified staff (average 3.5 points out of 5), wrong strategic decision making on the management

level (average 3.5 points out of 5), changes in the political environment and legislation (average 3.4 points out of 5).

➤ The top risk is considered by the respondents is “overloading of employees”. This risk is caused by other defined risks, such as issues with funding, motivation and inadequate strategic decisions. This risk is strongly correlated with “lack of effective planning” and “weak internal risk culture”, hence, all these risks need to be addressed simultaneously for greater effect.

➤ Overloading of employees (top risk) usually results in exhaustion, over-burning, problems with health and decrease in autonomous motivation. Average score of existing controls for this risk is 2.76 (educational institutions manage it as much as possible, but there are no strong controls or there is no possibility to implement strong controls). Such score provides a clear lack of risk management and of well-established risk controls. This serves as evidence, that introduction of risk management practices in the educational institutions should be relevant to strengthen the controls to improve risk management effectiveness.

➤ The second top risk was “insufficient funding” and there is weak or no understanding how this risk could be managed on the level of educational institutions. Risk is highly correlated with the risk of increasing cost of education; however, it might be irrelevant to some educational institutions. There is missing dialogue between the regulator, State management and educational institutions on this topic. Fostering such dialogue and clear communication would enable better understanding, and thus management, of this risk.

➤ The third top risk and second highest rated risk by respondents among psychosocial risk group risks was “lack of staff motivation”, which is tightly correlated with “weak internal risk culture” and “lack of qualified teaching staff”. This risk is supposed to be also interrelated with the “overloading of employees” risk.

➤ The fourth top risk and also top risk in the “reputational risks” group, was “lack of qualified teaching staff”. Similarly, as previous top risks, this risk correlates with “weak internal risk culture” and “lack of staff motivation” risk. Hence, the internal culture aspect needs to be given more attention and strong risk culture needs to be cultivated in order to address the majority of the top risks.

➤ The fifth top risk was the risk of “wrong strategic decisions”, which was mostly rated as critical by managers of educational institutions and this risk was very well correlated with the risk of “inefficient budget planning”. Thus, materialisation of this risk may increase such risks like corruption and third-party (supplier) failures. As the strategic decisions are taken on various levels (State level, individual institution level), it can bring material financial and reputational losses.

➤ Survey 1 revealed that IT and Information security risks are considered by the respondents as not significant (average risk criticality score: 2.46 – risk is neutral), which is well managed

(average score of control effectiveness for the IT and Information Security risk group is 3.31 – “risk is managed to as much extent as possible”). In this risk group, the most topical risk according to the respondents of Survey 1 is “Dependency on IT” risk with average criticality score 2.6 – “risk is slightly significant”.

➤ In the External risks category, the most critical risk is considered to be “Insufficient funding risk” with average score of 3.6 – “risk is very significant” and risk management effectiveness score of 2.68 – “risk is managed to as much extent as possible”. This may mean that it is not well understood how to manage this risk and respondents subjectively provided the rating that everything what is known as possible is done but accept that not to the full extent.

➤ The educational institutions hardly can manage political risk, hence risk management score for this risk is the lowest among all 32 risks in all risk groups, meaning that this risk has weakest controls and has weakest risk management. At the same time, this risk is one of the most impactful on the sector of education - changing political environments often are connected to educational reforms, causing the most significant changes in the sector of education, which constitutes the core of this risk.

➤ Educational institutions cannot influence the market economy and the external environment, however changes in it may have significant impact on the educational institutions: from changes in funding to changes in number of applicants and students, to changes in compensation of employees and in internal culture.

➤ Within the Reputational risk group, the most significant and least managed risk is “Lack of qualified teaching staff”. Risk of “wrong strategic decisions” in this group rated as second highest. Given that respondents were to large extent managers of educational institutions, there seems to be an uncertainty and insufficient confidence in effectiveness of strategic decision-making within educational institutions.

➤ Low quality of education is more of a consequence, rather than stand-alone risk. By mitigating risks related to governance and management of educational institution, quality of education shall be strengthened naturally.

➤ Risk of closure of educational institution is tied to other factors such as quality of education, quality of teaching staff, working environment for teaching staff and atmosphere in educational institution. It can be managed by addressing the triggers: attracting more students, working on strong risk culture, developing positive morale among employees, developing compliant educational programmes, documenting internal processes and controls to prevent unethical behaviour and violence, etc.

➤ Corruption risk was rated by respondents in Survey 1 as the least significant and most well managed risk. By further addressing budget planning, supplier risk, employee morale and working environment it should be possible to lower the corruption risk more.

➤ Although risk of “weak internal risk culture” was not rated by the respondents as one of the top risks and its overall criticality score was quite low (2.95 – risk is slightly significant), it came up as the one, which is correlated to almost all of the top risks and majority of the risks in the provided risk list. Thus, the conclusion can be made, this risk should be taken and addressed as the top risk, because through mitigating this risk it is possible to achieve downgrading of other significant risks.

➤ Only 17% of respondents in Survey 1 indicated correctly that risk management responsibility lies on all stakeholders. This proves the hypothesis and one of the theses that there is low understanding of risk management in the sector of education.

➤ According to Survey 1 results, in order to better manage the risks in educational sector, the following is needed:

- Increased State funding and streamlined regulatory requirements;
- Proper planning and predictability;
- Strong co-operation and teamwork at all levels;
- Qualification, loyalty and motivation of employees;
- Improved skills of management and administration staff in educational institutions;
- Clear communication and strong support system;
- Risk management methodology for each educational institution;
- Each stakeholder’s input;
- Stronger controls over corruption and bribery.

➤ In Survey 1, 1/3 of respondents does not know at all whether their educational institution uses insurance and 1/3 knows that their educational institution does not use insurance. This is another evidence of weak risk management in the educational institutions, as insurance is a great tool to minimise impact of rare but plausible high loss events, such as explosion, fire, floods, etc.

### **3.10 Survey 2 results**

The second survey, as mentioned earlier, was developed in order to clarify the results of the first survey, to confirm the top risks for the educational sector and brainstorm on the possible risk mitigation actions. There were 40 respondents in the second survey, who also participated in the first survey. Number of respondents was lower in the second survey due to its scope: there were less questions, but all of them required an open answer and justification.

The first question asked to the respondents was whether risk management is important at all in their view and whether educational institutions would benefit from investing time into developing tailored risk management programmes for themselves. The question did not have a choice of pre-defined answers – respondents had to write an open free style answer and majority of the respondents also provided explanation to their answer.

90% of respondents (36 out of 40) replied that risk management is definitely important and it is worth spending time on the risk management programme development for the educational institutions and 10% of respondents (4 out of 40) replied that risk management is not important. Below are some of notable answer quotes provided for this question by respondents that provide evidence of importance of risk management for stakeholders in sector of education:

- *“Yes, it is definitely important to manage risks. It would be difficult to say whether a developed program would help, but the availability of specialist consultations on this issue would definitely help.”*
- *“Yes, it is definitely important, because it can have a significant impact on the future operation of the educational institution.”*
- *“Yes, risk management is important for stable operations”*
- *“Yes, it is important, but first it would be important to explain to the heads of the institutions what it gives to the institutions they run. Let it not be a formal event, but a system with meaning to the organization.”*
- *“Risk management is important, and it is necessary to do so, but another regulatory document - I do not know how much is needed. School leadership is already drowning in the mountains of guidelines and strategies.”*
- *“It is important to manage risks and to develop risk prevention programs”*
- *“Yes, it is definitely one of the most important tasks for the management team.”*

Those respondents, who answered that risk management is not important, justified it as follows:

- *“Not important, because everything is determined by political forces.”*
- *“It would be important if these risks could be affected or at least mitigated. If these conditions do not exist, then it is formalism.”*
- *“This is a secondary issue. The educational institution has to deal with more topical issues.”*

It can be concluded from the explanations provided that what frightens representatives of educational institutions most are another bureaucratic document and new regulatory requirements for implementation of formal activities, which may not bring real value to the institution, but instead will swallow already scarce resources. Therefore, in order to avoid such result, it is important to think and plan beforehand, how to realise risk management programmes. For example, it could be that each



educational institution could receive funding for additional full-time employees, who would be responsible for risk management implementation, on the other hand, it could be also centrally located risk management teams within each municipality, who would develop, implement and oversee risk management programmes in all schools located in the municipality, as well as educate teachers and school management about risk management and risk management plans. This is a high-level question that should be decided by high-level decision maker (e.g., Ministry of Education) and the decision cascaded to municipalities and schools. The most important is to take into account that the main purpose of educational institutions is to provide education rather than to implement formal requirements, therefore it should be well thought through beforehand to avoid placing extra burden on educational institutions.

The second question was also open style aimed to clarify what consequences of the top risks developed through the Survey 1 and was defined as follows:

**“According to the survey, the most critical risks in the education sector in Latvia are:**

- 1. Employee overload (average 4 points out of 5)**
- 2. Insufficient funding (average 3.8 points out of 5)**
- 3. Lack of employee motivation (average 3.5 points out of 5)**
- 4. Lack of qualified staff (average 3.5 points out of 5)**
- 5. Wrong strategic decision making (average 3.5 points out of 5)**
- 6. Changes in the political environment/legislation (average 3.4 points out of 5)**

**In your opinion, what are the consequences of each of these risks or can they cause? (e.g., financial terms, reputation, etc.)”**

There were provided the answers by all 40 respondents, which were processed by author for the key words highlighted in bold in the quotes below, as well as trigger words or secondary consequences highlighted in italic, in order to map consequences to risks and to build structure of risks vs. risk consequences in Table 3.10 (only detailed enough answers are listed below for analysis and structuring in the Table 3.10):

➤ *“Poor funding leads to low wages and poor motivation. As a result, there is lack of motivation and insufficient human resources, with time there is less and less competent professionals working in educational institutions, what further leads to **deteriorating quality of education.**”*

➤ *“Motivation to work as a teacher is decreasing due to constant *fight for funding, low wages and high level of responsibility.* Overload leads to health problems, but low wages do not allow education sector's employees to care well for own's health. This *decreases the prestige and attractiveness of teacher's profession* and, as a result, **students, who study pedagogy in university, end up choosing to work in other sectors,** where it is possible to earn more, e.g., banking sector. This*

leads to *waste of State funding* for students, who study pedagogy and choose not to work in educational sector and leads to decreased demand for pedagogy related programmes in universities.”

➤ “*Salary level for teacher's profession is as low as minimum salary and similar to salary level of any profession, which does not require any higher education, which is not the case for teacher's profession. Hence the **prestige of this profession is so low due to low financing**, that there is **no motivation for younger people to get into teacher's profession**. Teachers have to work in different schools simultaneously to survive, what results in **overload**. *Insufficient funding is mainly caused by **incorrect and failed strategic decision making** and all of top risks listed are interconnected and each one of them is a driver for the next one.*”*

➤ “The first four risks are *interconnected* and cause each other, but the *most significant consequences they cause* is **lack of qualified staff**.”

➤ “The first four risks cause **deteriorating quality of education** and *decreasing number of employees in educational sector*. Fifth risk cause *decreasing number of students and teachers due to insufficient funding*. The sixth risk results in **inability to adopt to new system and programmes, inadequacy of equipment, need for existing strategy to be redesigned again**.”

➤ “Overload of employees results in **decreased quality of work and motivation of employees**. Insufficient funding results in *decreased motivation, lowers **prestige of profession** and causes overload of employees*, because employees try to take on more work in order to earn more, as a result **quality of educational services is deteriorating**. Insufficient funding and overload also result in *insufficient number of qualified employees*. Nobody wants to work overtime for very small salary and take away time from their own interests, friends and family. Changes in legislation may cause **lowered quality of work and motivation** as well, because not usually the norms defined in new legislation are explained with good quality and are open for interpretation and not always are acceptable by educational sector employees.”

➤ “All of the risks result in **degradation of teachers profession** *what further leads to degradation of the society*.”

➤ “The risks result in *insufficient human resources* and **inability to achieve set goals** for educational institutions.”

➤ “The first risk results in *loss of ability to work for employees*. The second one results in *outflow of skilled labour to better paid jobs*. Third and fourth risks in most direct way **affect the quality of education**. As for fifth and sixth risks - result in **lack of stability**, *which affects everything mentioned above*.”

➤ “Overload is caused by *continuous changes in the education system*, which creates *lack of motivation among teachers*. Public attitudes and the incompetence of politicians in topic of education have led to that *students no longer take responsibility for their own learning* but blame funding.”

➤ “Overload of employees often is connected to inability of employees to comply with the job agreement rules. Lack of motivation is caused by **low salaries**. Working according to work agreement saves from low funding.”

➤ “*Loss of employees, deterioration of students' performance, decrease of prestige of schools* in society.”

➤ “Overload of employees results in *burnout, neurological and somatic diseases for employees - long-term incapacity for work*. Overload and lack of motivation results in *depression, vegetative dystonia - long-term incapacity for work, occupational diseases*. Lack of skilled and qualified employees are *damaging the reputation* of educational institutions and sector as a whole. Wrong strategic decisions are made at the State level, because the administrative apparatus is not reduced, but instead schools are being liquidated - this can lead to the *demise of the State!* Changes in the political environment have plunged the school system into a *state of endless reform*.”

➤ “Overload *prevents the implementation of academic programme and facilitation of fascinating lessons for children*. Underfunding in the sector of education creates **inferiority feeling** in employees, which is associated with the **lack of motivation**.”

➤ “Any of these risks can have **financial consequences** for the organization - in the short or long term. Risks 1 and 3 will additionally cause problems within the organization - *worsening psychological climate and deteriorating relationships*; risks 2 and 4 may already have a greater **impact on reputation**, as *information about underpaid or incompetent employees may be made public*. Risk 5 and 6, in addition to financial losses, threatens with *bankruptcy, liquidation of the organization or unproductive 'vegetation' of an institution*.”

➤ The first risk results in **decreasing quality of work**. Second risk leads to *insufficient human resources in educational institutions*. Third risk results in **deteriorating quality of education** and *schools being forced to employ as teachers the employees without life purpose for teaching*. As a result of the fourth risk the **students will suffer**. Fifth risk will lead to **general decrease of education level in Latvia**. Fifth risk may have a positive or negative effect on education in general.”

➤ “The first risk leads to *burnout of employees* and **decline in quality of education**. The second risk **threatens sustainable development** and results on *decline in quality of education, staff overload* and **loss of reputation**. Third risk results in *loss of reputation* and *threatens sustainable development of educational sector*. Fourth risk results in *deterioration of quality of education* and *threat to sustainable development of educational sector*. Also, fifth risk *threatens sustainable*

*development and may result in closure of an institution. Sixth risk also threatens sustainable development, prevents attraction of employees and affects reputation.”*

➤ “Risks 1-4 cause a sharp **decline in quality of education** and pose a **threat of school's liquidation**; second, third and fourth risks **weaken or even destroy corporate culture inside educational institutions**. Fifth and sixth risks may result in *liquidation a school, school's diminishing role in the society, shift from sustainable institution to unstable and unconvincing.*”

➤ “All risks lead to **worsened quality of work** and **inability to achieve set goals.**”

➤ “Overloading of employees creates a *negative work environment*, **poor quality of work** and *frequent absence of employees due to illness*. Insufficient funding results in **insufficient remuneration**, which forces the *hiring of unskilled workers*, which in turn result in **low-quality work**. Lack of motivation of employees leads to schools being forced to hire employees, who come to work in the educational sector for such a low salary, often they are people who come to work for reasons other than what they want to do. There is **no healthy competition in this sector**, which *lowers the quality of work*. The **victims are children** and, consequently, *the whole future of Latvia*. *Disordered educational system creates chaos at all levels of education* and therefore **pedagogy is often studied by those who do not like it at all**, so that *we get a teacher who has somehow graduated from university/high school only because they are not onboarded elsewhere*. In addition, *working with children in our country is not properly valued, both in terms of attitudes and finances*, **prestige of profession is very low**. As for *political decisions*, it is unfortunate that they are *more often detrimental to the education system.*”

➤ “The main problem is that after a few years, the Latvian education system may face a *catastrophic lack of well-trained and motivated teachers.*”

➤ “First risk causes *health problems for employees* and, consequently, *financial problems*. Second and fourth risks result in **decline in quality of education** and *failure to offer a modern teaching environment and programs*. Third risk leads to *decrease in quality of education* and **falling student engagement**. Fifth and sixth risks **affects total trust in the education system** and its *reputation.*”

➤ “Each of the above risks contributes to the **decline in the quality of education.**”

➤ “1-4 risks affect the **quality of education** and result in *lack of learning resources*, **lowering the level of education in the country.**”

One of the key observations resulting from the Survey 2 is that all top risks are interrelated between themselves and trigger each other. For example, overload and insufficient funding drive decreasing motivation and risk of lacking competent employees in the educational sector, what may lead also to incorrect strategic decision-making. On the other hand, changes in political environment

also decrease motivation of employees and may result in overload. Strategic decision making and insufficient funding are also interconnected.

The consequences listed by the respondents of Survey 2 for all of the top risks identified can be summarised as presented in Table 3.10:

**Table 3.10: Key consequences caused by the top risks as per Survey 2 (mapping made by author from the above quotes)**

<b>Risk name</b>	<b>Consequences</b>
1. Overloading of employees	<ul style="list-style-type: none"> <li>- deteriorating quality of education</li> <li>- health problems, lost ability to work, burnout</li> <li>- decreases the prestige and attractiveness of teacher's profession</li> <li>- leads to lack of qualified staff</li> <li>- worsening psychological climate and deteriorating relationships</li> <li>- decreases motivation of employees</li> <li>- prevents the implementation of an academic programme and facilitation of fascinating lessons for children</li> </ul>
2. Insufficient funding	<ul style="list-style-type: none"> <li>- outflow of skilled labour to other sectors, lack of qualified human resources</li> <li>- low wages, decreasing motivation, less competent professionals</li> <li>- deteriorating quality of education</li> <li>- inability to achieve institutions' set goals</li> <li>- damage of reputation</li> <li>- decreases the prestige and attractiveness of teacher's profession</li> <li>- failure to offer a modern teaching environment and programs</li> <li>- overload</li> <li>- worsening psychological climate and deteriorating relationships</li> </ul>
3. Lack of motivation of employees	<ul style="list-style-type: none"> <li>- deteriorating quality of education</li> <li>- damaging reputation of educational institutions and sector as a whole</li> <li>- worsening psychological climate and deteriorating relationships</li> <li>- decreases the prestige and attractiveness of teacher's profession</li> <li>- inability to achieve institutions' set goals</li> </ul>

Table 3.10: **continuation**

<p>4. Insufficiency/lack of qualified staff</p>	<ul style="list-style-type: none"> <li>- deteriorating quality of education</li> <li>- failure to offer a modern teaching environment and programs</li> <li>- inability to achieve institutions' set goals</li> <li>- decreases the prestige and attractiveness of teacher's profession</li> <li>- damage of reputation</li> <li>- worsening psychological climate and deteriorating relationships</li> </ul>
<p>5. Incorrect strategic decision making</p>	<ul style="list-style-type: none"> <li>- bankruptcy, liquidation of the organization or unproductive 'vegetation' of institution</li> <li>- deteriorating quality of education</li> <li>- decreases the prestige and attractiveness of teacher's profession, school's role in the society</li> <li>- inability to achieve institutions' set goals</li> <li>- lack of stability</li> <li>- insufficient funding</li> <li>- decreasing number of students</li> </ul>
<p>6. Changes in political environment</p>	<ul style="list-style-type: none"> <li>- lowered quality of work and motivation, deteriorating quality of education</li> <li>- decreases the prestige and attractiveness of teacher's profession, school's role in the society</li> <li>- damage of reputation</li> <li>- inability to adapt and inadequacy of equipment</li> <li>- inability to achieve institutions' set goals</li> <li>- lack of stability</li> <li>- endless reforms</li> <li>- bankruptcy, liquidation of the organization or unproductive 'vegetation' of institution</li> </ul>

From the Table 3.10 above a conclusion can be made that the top risks are interrelated and cause one another. Graphical representation in Figure 3.17 provides summary how the top risks cause each other according to results of respondent responses in Survey 2:

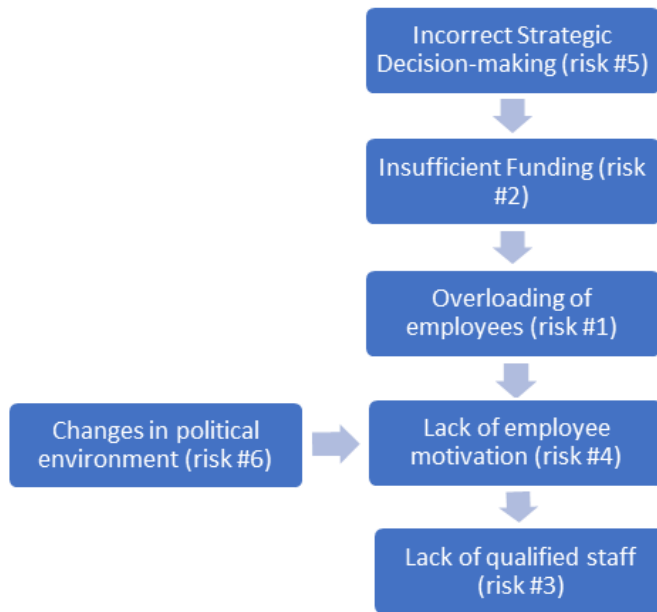


Figure 3.17 **Interrelation of the top 6 risks as per Survey 2 results**

All of the above-mentioned top risks lead to the following consequences on overall presented in Figure 3.18 (sorted by % of respondent enforcement), where deteriorating quality of education takes the 1<sup>st</sup> place (30% of respondents marked it as a consequence to materialisation of all of the top risks):

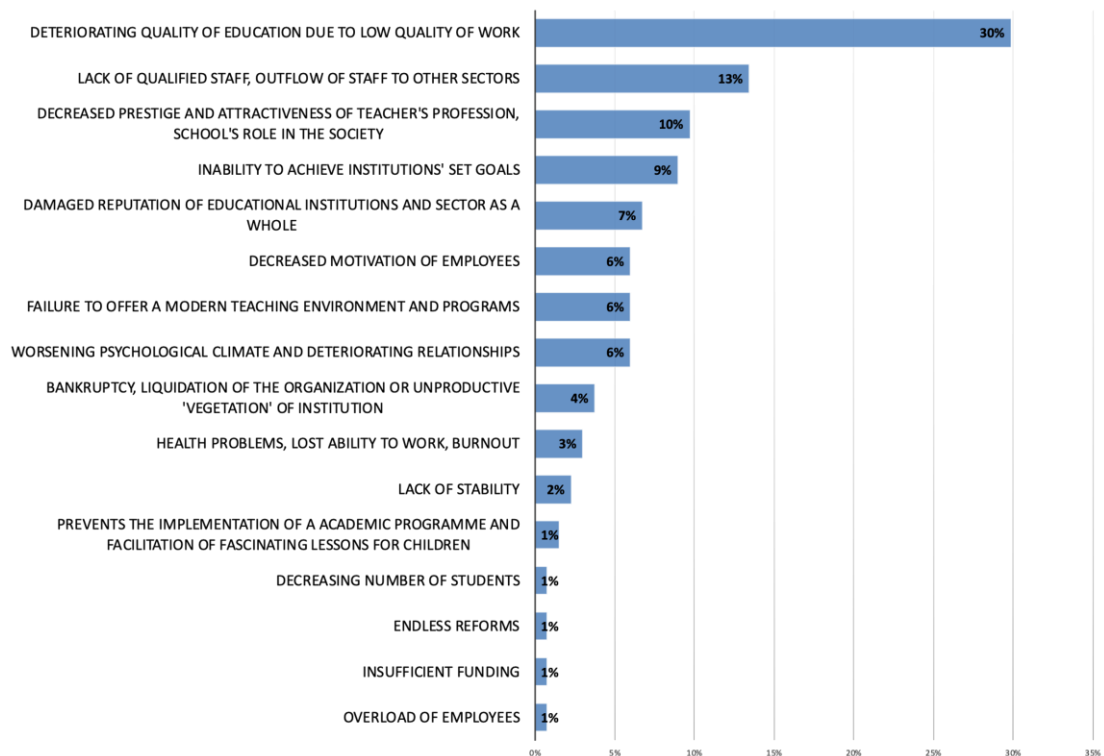


Figure 3.18 **Key consequences caused by the top risks Survey 2**

The third question was also open style aimed to clarify what can be done to mitigate the top risks developed through the Survey 1 and the question was defined as follows:

**“How the above-mentioned consequences of the most topical risks could be reduced or eliminated, in your opinion? How the above risks can be most effectively managed?”**

Respondents provided mostly detailed answers with number of different mitigation actions for different risks, only three respondents out of forty were unable to answer the question. Some mitigation actions were repeatedly proposed by different respondents, thus it was possible to draw out most topical mitigation actions. Table 3.11 provides detailed summary of the answers provided by respondents to the third question in Survey 2 together with the frequency of repeated answers. Each answer will be discussed in detail in further text.

**Table 3.11 Mitigation actions suggested by respondents of Survey 2 to manage the top risks (sorted by frequency of answers)**

Mitigation actions proposed	As % of all mitigation actions proposed
Increase salaries to raise the prestige of profession and motivation, offer additional benefits	27%
Strategic and budget planning with professional opinion and advice	14%
Support and protect teachers from the top	8%
Long-term stable educational policy on State level	8%
Increase funding for educational institutions	6%
High level of competence of the manager and internal cooperation in the organization	6%
To improve the emotional state of employees in the workplace. Mutual support (cohesion) events should be promoted in collectives.	4%
Decrease workload	4%
Honesty and professionalism at all levels	4%
Good internal communication, information exchange	2%
Implement strict logging of worked hours	2%
To allow for each school to act individually, set priorities, salaries, rates, improve the school environment	2%
Switch responsibility for student achievements from teacher to student	2%
Precise organization of processes and clear division of responsibilities	2%
Develop feedback culture	2%
Provide all teachers with assistant teachers	2%
Active involvement of the trade union	2%
Programme for preparation of teachers	2%



➤ Increase salaries to increase the prestige of profession and motivation, offer additional benefits: mitigation action was proposed 13 times by the respondents (around one third (27%) of all proposed mitigation actions). This mitigation action was mentioned for the risks related to lack of motivation, overloading of employees and insufficient qualified human resources in the educational sector. By raising salaries for teachers and teaching assistants and introducing valuable social benefits (e.g. free healthcare, partially paid homes, discounts in shops, etc.) it would be possible to raise the prestige of teacher's profession, raise motivation for teachers to keep and value their jobs, attract more qualified personnel to join schools as teachers, what would resolve the problem of lacking motivated and qualified employees in schools and would improve the overall quality of education in the country.

➤ Strategic and budget planning with professional opinion and advice: was mentioned a mitigation action seven times (14% of all mitigation actions) for risks related to incorrect strategic decision-making, insufficient funding and overloading of employees. Respondents highlighted that it is important to listen to the opinions of experts when planning the strategy and budget. It was highlighted by several respondents that strategic and budget decisions are taken behind closed doors without involvement of subject matter specialists and without holding discussions with stakeholders, what escalates the risk of incorrect decisions detrimental for the educational sector and quality of education.

➤ Support and protect teachers from the top: four times respondents mentioned that in the current set-up teachers are placed under pressure and criticism from the side of top management, Ministry and regulators, as well as from parents' and students' side. By protecting teachers from the level of Ministry and regulatory authorities, it would be possible to raise the motivation of teachers, to raise the prestige of the job and to increase number of qualified staff working in educational sector. In current set-up working in educational sector as a teacher is perceived as masochism to certain extent due to constant criticism from all sides and lack of support. Providing motivation, inspiration and backing up the teachers by their management would provide the needed protection for the teachers to improve their level of motivation, what can be perceived even better, than raised salary.

➤ Long-term stable educational policy on the State level: four times the respondents indicated that a good solution to mitigate all risks would be a stable long-term educational policy in place of constant reforms, which are happening during the last three decades. Majority of respondents in previous questions were referring to the reforms as the key cause for decreasing quality of education, diminishing motivation of employees and destroyed prestige of teachers' profession.

➤ Increase funding for educational institutions: mitigation action was proposed three times (6% of all mitigation actions) and the rationale of respondents for this mitigation action for that by

increasing the funding it would be possible to raise salaries, buy better equipment and create better environment for teaching, what would be very motivational for employees and would raise the prestige of profession and career in the educational sector. With more funding educational institutions would be able to achieve set goals, motivate employees, improve the psychological climate in the teams.

➤ High level of competence of the manager and internal cooperation in the organization: three times respondents proposed as the mitigation action raising the competence of managers and administrators in the educational sector, who are responsible for leadership and decision-making. With the good leadership it would be possible to solve risk of overloading, underfunding, low salaries and lack of motivation, what deteriorates quality of education and result in insufficient number of qualified employees in educational institutions. By investing into the knowledge, competence and skills of the managers it would be possible to resolve most of the problems with minimal costs. In addition, internal communication, transparency, positive attitude and open information flow are important elements for successful leadership, which would make employees more motivated, satisfied and happy.

➤ To improve the emotional state of employees in the workplace. Mutual support (cohesion) events should be promoted in collectives: this mitigation action was mentioned two times by the respondents. The key idea is that it is not always all about the salary, but also very much about the attitude. Many respondents mentioned that positive attitude is very important, but the accent here is placed on teamworking and developing positive co-operative environment in the workplace, positive culture and relationship among employees. This can be achieved through strong leadership, as mentioned above, but also through teamworking (cohesion) events specially organised for employees' interaction outside of working environment.

➤ Decrease workload – two times respondents mentioned that decreasing the workload while keeping the salary level would help to mitigate risk of overloading and lack of motivation among employees.

➤ Honesty and professionalism at all levels: two times respondents indicated that playing an honest game, ensuring transparency and professionalism would help to eliminate incorrect strategic decision-making, raise level of motivation for employees and remove the threatening effect of the political environment, which affects the educational sector with endless reforms and uncertainty.

➤ Good internal communication, information exchange: one respondent specifically highlighted that proper internal communication and open information exchange would help in raising levels of motivation as well as take correct strategic decisions. There is a problem that due to problems

in communication top-down, often school managers are confused about future plans and are not able to communicate correct strategy and action plan to the employees.

➤ Implement strict logging of worked hours: one respondent proposed as a measure to avoid overloading of employees to strictly log worked hours. This mitigation action can be very tricky as often teachers work from home and working hours include not only time in the school, but also administrative tasks often performed at home and outside of normal working hours. So, this could be biased by time estimations and trigger risk of internal fraud. Implementing automated logging of working hours would require certain investment in IT systems as in such case all employees would need to be supplied with working computers, where such time logging software would be installed.

➤ To allow for each school to act individually, set priorities, salaries, rates, improve the school environment: one respondent considered letting schools a freedom to do own set-up to mitigate risk of overloading, lack of motivation, insufficiency of qualified labour and incorrect strategic decision. In author's view, this mitigation action is not feasible, as decentralising controls could lead to inequality among schools, where some schools would perform better than others due to different leadership, corruption, fraud and loss of control from the regulatory side.

➤ Switch responsibility for student achievements from teacher to student: one respondent indicated that current set up is built in a way where teachers are responsible for students' achievements what makes students feel irresponsible and not caring for their own achievements, all pressure being placed on the shoulders of teachers. On one side the statement is correct to certain extent, on the other side, in author's view, removing responsibility of teachers for students' progress could raise a risk of increasing number of students underachieving due to missing responsibility on both sides of the teaching-learning process. In author's view the responsibility should be shared equally among teachers, students and student parents/guardians.

➤ Precise organization of processes and clear division of responsibilities: one respondent brought up very popular in risk management topic of sorting out processes and responsibilities first. Often due to lack of properly defined responsibilities and incorrectly built processes, number of different risks are created. Precise organisation of processes and clear division of responsibilities are a great way to mitigate risk of overloading, risk of lacking motivation and risk of incorrect strategic decision-making. Though, this risk mitigation is much dependent on the leadership style of each educational institution's management.

➤ Develop feedback culture: one respondent indicated that feedback culture should be developed to deal with decreasing motivation of employees. In current set up it is very often practiced criticising and showing negative attitude to each other in teaching teams, what worsens the internal climate. To improve on this part, it would be beneficial for all stakeholders to provide feedback

correctly and build teams with correct feedback culture. This is often practiced by larger companies and corporations in other sectors, e.g., in finance and commercial sectors.

➤ *Provide all teachers with assistant teachers*: one respondent proposed mitigation of risk of overloading and decreasing motivation by providing each teacher with an assistant. However, this risk mitigation could prove complicated due to shortage of qualified labour in the educational sector.

➤ *Active involvement of the trade union*: one respondent stated that risk of overloading can be mitigated by more active involvement of the trade union, which should fight for the rights of teachers and other employees in educational sector.

➤ *Programme for preparation of teachers*: one respondent highlighted that new teachers onboarded in the schools are not ready to face the harsh environment that goes with the profession and are not well prepared to teach students. As a result, quality of education is deteriorating, new teachers often choose to escape to other sectors or lose motivation. Therefore, a good programme of teacher preparation for working in educational institutions should be developed, to prepare their expectations and skills for real job.

### **3.11 Summary on Survey 2 results**

3.11.1 Survey 2 results indicated that despite risk management is perceived as important, representatives of educational institutions are mainly frightened of new regulatory requirements for implementation of formal activities related to risk management, which may not bring real value to the institution, but instead will swallow already scarce resources.

3.11.2 Risk management must be organised in a way that will not put additional burden on educational institutions, as in such case it will be done very formally and will not bring much value. For organising it in a value-adding way it should be well thought through on the regulatory level.

3.11.3 Survey 2 results led to conclusion that all of the top risks identified in Survey 1 are interrelated between themselves and trigger each other.

3.11.4 Majority of respondents in Survey 2 indicated, that not managing identified in Survey 1 top risks may mainly lead to deteriorating quality of education, outflow of qualified staff to other sectors, decreased prestige of teacher's profession and deteriorating role of school in the society.

3.11.5 The most topical mitigation action for top risks suggested by respondents in Survey 2 was to increase salaries in the sector of education in order to raise the prestige of profession and motivation of teachers and to offer additional benefits, as well as involve into strategic and budget planning professional experts. Salaries would have to be increased significantly to compete with other sectors, to where majority of employees are leaving, according to some of the respondent answers.

### 3.12 Interviews with risk management experts

In year 2022 several interviews were conducted with risk experts in order to validate findings, assumptions, conclusions and recommendations for this research. The criteria for selection of risk experts was as follows: at least 15 years professional experience in different areas of risk management. Due to the fact that it is quite challenging to find such experts in general in Latvia and no availability of risk management experts in the sector of education, the interviews were conducted with the following two experts meeting the criteria, who are working in risk management in Finance sector for 15 years or more in different areas of risk management and one respondent has direct experience of teaching risk management in higher education institution. Following several interviews with risk experts the author decided to leave only results of the two interviews, because there was no variation in opinions among the experts observed, hence there was no added value to publish all interviews and the most detailed and bright interviews are reproduced below, that contain the views of all interviewed experts.

SK: 20 years of risk management experience in Finance sector in areas of operational, compliance, anti-money laundering and credit risks, out of which 15 years in risk leadership positions in the biggest Latvian banks, which include such positions as Head of Operational risk, Head of Compliance and AML risks, Head of Risk Management, Risk Director and 5 years of risk consulting experience to banks, payment institutions, regulatory authorities, etc. Visiting lecturer in one of higher education institutions in Riga focusing on risk management tutoring. Education: Master's degree in Finance from University of Latvia, Certified Anti-Money Laundering Specialist (ACAMS). Member of The Professional Risk Managers' International Association and Association of Certified Anti-Money Laundering Specialists.

NS: 15 years of risk management practical experience in Finance sector, of which 5 years in credit risk management with focus on financial institutions in one of Latvia's largest banks, 10 years in counterparty credit risk and market risk areas in Latvia's largest banks. Indirect experience with operational risk and compliance risk through professional exposure. Education: Master's degree in Economics from the University of Latvia.

Tables 3.12 - 3.15 provide details of the interviews in a comparable format, each table is followed by author's analysis. Author highlighted in bold those phrases and sentences, where the answers of both risk experts are similar.

Table 3.12 Interview results with experts in risk management: part 1

SK - Risk Management Expert and Advisor	NS, Financial Risk Management Specialist
<p><b>1. Could you please provide your opinion on risk management methodologies and their practical application in different industries, organizations? Are there any common models and methodologies that could be adapted by the sector of education? Can you recommend any specific risk models and risk management methodologies?</b></p>	
<p>There are <b>many common risk management principles and elements</b> that shall be adhered to by risk management practitioners. This ensures that risk management discipline applies well tested and validated standards and follows best practices, e.g., ISO 31 000. However, all institutions are different due to their objectives, strategies and tactics they deploy. Therefore <b>application of one fit for all model or methodology would not take into account specifics of the organizations and therefore would negatively affect the quality of decisions that are made based on the risk analysis and conclusions.</b> Risk doesn't exist without objectives; <b>primarily objectives drive the risk</b> not vice versa. Naturally companies apply different approaches for setting strategy and their goals, the same applies to risk management.</p> <p>In practice risk management generates a value when the senior management does see and can explain the link between risk management and profit generation (or main activity of an institution). Hence the <b>development of a risk management framework starts with understanding the goals of an organization (even if it is a public institutions like schools are).</b> This is a key step required to design a risk appetite. Even in similar organizations risk appetite statements could be different. This is supported by different goals, different risk perception, resources and skills available, etc. Based on the risk appetite it is a risk manager's call then to organize and apply different risk management tools like incident data collection, risk assessments, <b>key risk indicator monitoring,</b> internal controls, planning for business continuity, risk reporting, etc.</p>	<p>There are <b>different models and methodologies in risk management, which are based on key principles or pillars.</b> There can be qualitative and quantitative risk management models, but each <b>methodology and model shall be specifically designed for specific organisational needs depending on its acceptable risk appetite limits and strategic goals. To manage the risks it is important to develop relevant risk scenarios and access them according to internally developed risk assessment methodology.</b> Although the key principles for risk assessment are the same (you need to define relevant scenarios for your organisation, assess probability and impact of this scenario happening), but how it will be done in practice depends on each individual institution as they should develop internally individual methodologies based on their specifics. Scenarios also will differ in different institutions mostly as all <b>depends how much risk is acceptable for an organisation. There does not exist such thing that one can open a book and copy the methodology out from there. It is possible to adopt the key principles, but not the entire methodology.</b></p> <p>It is important to develop individual <b>key risk indicators</b> for each individual institution, but also in centralised way in order to be able to compare different institutions in one sector. Thus, if the purpose is to understand risks on a high level in the sector as a whole, then it would be possible to develop centralised methodology on the sectoral level, but <b>it would not address risk management of each individual institution and would not be a fit for all.</b></p> <p>In overall, it would be great if educational sector would introduce KRI metrics and risk assessments.</p>

All risk experts confirmed that there is no such common risk management methodology, which would be fit for all needs and which one could take from a book and apply directly in practice. As experts have confirmed, risk management methodology is based on common principles, which were in detail described in sections 1 and 2 of this dissertation, however risk management shall take into account specific objectives, strategies, size, characteristics of individual institutions, which define its acceptable level of risk and relevant risk scenarios for assessment. It was confirmed through the interviews that risk management starts with goal and strategy setting, as was mentioned in section 2.8. All risk experts mention the importance of monitoring key risk indicators (theoretical details in section 1.4.12) and the risk assessments (described in 1.4.4, 1.4.7, 1.4.16). Also all risk experts highlight the importance of defining the risk appetite or the acceptable level of risk (described in 1.4.6).

Thus, it can be summed up, that research results in theoretical part of this dissertation led to correct conclusion that there is no one fit for all methodology and recommendations on the risk management cycle as was described above.

Table 3.13 **Interview results with experts in risk management: part 2**

<b>2. Who is responsible for risk management in an organization?</b>	
<p><b>SK:</b> Risk management is all about decision making that is supported by well aggregated and analysed information, understood risk cause and potential impact on organizations objectives. Often the job title of “risk manager” gives misleading message to the company as others believe that risk manager is ultimately responsible for the management of risk, when in <b>reality risk manager takes the responsibility for creating the framework and methodology for risk management</b> that would support timely and qualitative decision making.</p> <p>It is obvious, that <b>everyone in an organisation contributes to and has its specific role in risk management</b>. For instance, teachers are responsible for risk management on day-to-day level, whereas school director is responsible for taking risk management decisions on more strategic level. Those roles who are responsible for setting the objectives are simultaneously responsible for risk management. Management and risk management are interlinked. Students and their parents in this case are customers of the educational service providers and are affected by the risk management effectiveness of an institution. They are responsible for adhering to specific standards and rules at schools that are in fact a product of risk management.</p>	<p><b>NS:</b> Everyone in an organisation should be risk aware, what means that <b>everyone must understand the risks connected to their actions</b>. There should be <b>someone responsible for creating risk culture and risk framework</b>, but in overall it is everyone’s responsibility to be risk aware and to prevent risks from materialising. In every organisation there should be risk function who shall train everyone in organisation, stress the importance of risk awareness, facilitate risk culture and blueprint acceptable level of risk and principles.</p>

All of the experts had the same opinion that risk awareness is the responsibility of all stakeholders, where everyone has specific role in risk management: students and parents comply with the rules and understand risks connected to their actions, whereas teachers are responsible on operational level to manage and report the risks, but the decision-makers and specialised risk function focus on creating the risk management framework and requirements. The answers of experts correspond to findings and conclusions made in sections 1.2 and 3.6. Thus, it can be concluded, that it is important to ensure proper communication across the stakeholders of the sector of education about their risk management responsibilities, clearly stating the practical details of such responsibility, and to provide comprehensive training on how every stakeholder's actions contribute to overall risk management of an institution and educational sector as a whole.

Table 3.14 **Interview results with experts in risk management: part 3**

<b>3. Is risk management coordinator required for successful risk management?</b>	
<p><b>SK:</b> A key challenge to the efficiency of risk management is the flow of timely and complete information about emerging risks, occurred risk incidents, etc. Therefore, <b>a network of well-trained risk coordinators</b> definitely helps to deal with this challenge. <b>At least one competent risk management coordinator for each organisation is critical</b> for successful risk management. IRM (2012) summarise on page 35 that specific risk expertise and skills are needed for risk management. As summarised in this IRM guidance paper, risk ‘champions’ and risk manager are required. For sure, risk ‘champions’ or risk management coordinators are needed to manage risk, however they also <b>shall be taught and trained</b>. This would support the establishment of so called sound risk culture very much. <b>Each school shall have their own risk coordinator</b>, who communicates across all stakeholders at the school, collects data about incidents and risks and co-ordinates mitigation of risks. Stakeholders would be motivated to collaborate with coordinators, as this is not a blaming role. Once the role is set and communicated within the institution colleagues will come to this person to discuss identified risks and incidents. This is how then the risk management would be achieving its goal. Moreover, on a broader level (State school system) risk coordinators would have an opportunity for networking and would be able to share their experience and come to a better proposals of risk mitigation actions. This definitely contributes to a better and safer school system.</p>	<p><b>NS:</b> Definitely in each and every educational institution there <b>should be at least one risk coordinator, who knows specifics of this particular organisation, is involved in everyday processes and also has competencies in risk management</b>. It would also be useful to have <b>centralised risk coordinator of the borough level who would collect data from every institution’s risk coordinators</b> and form global risk picture for the entire sector.</p>



As it was already mentioned in chapter 1.4.11 and throughout the text, risk coordinator is an important role for educational institutions, as this person could perform risk management tasks and build risk management framework seamlessly. All of the experts also stated that appointing a risk coordinator or ‘risk champion’ is of critical importance and the experts stressed that every institution should have their own risk coordinator. In addition, what was not mentioned specifically anywhere on the dissertation, the experts pointed out at “network of well-trained risk coordinators” and “centralised risk coordinator in the borough who would collect data from every institution’s risk coordinators” – here the experts are talking about centralised risk management function on the State level, which would ensure that risk coordinators of every institution communicate and network, and which collects risk data from all coordinators to form a global high-level view on risk picture from the State level. This is an interesting idea, which could be developed further in practice, however author did not find confirmation for this type of approach during the research.

To sum up, the results of the research and risk experts have confirmed the importance of appointing a competent risk management coordinator in every institution to ensure seamless and professional integration of risk management in the sector of education.

Table 3.15 **Interview results with experts in risk management: part 4**

<b>4. Would you recommend using risk matrix as visualization tool in risk management (Figure 1.1)?</b>	
<p>Risk matrix – is a tool. However, we tend to use different tools for different purposes. Once again risk matrix as a <b>visualization tool</b> can be <b>adopted for every institution up to their needs</b>. If we use a metaphor here, then the development of a risk matrix could be compared with a thermometer – we use one for measuring temperature of the body and absolutely different by its construction for measuring the temperature of air of surfaces. It is therefore crucial to make recipients of this visualization able to read and interpret the information that is provided by the tool. If management understands how risk matrix works, what are the conclusion there, how risk appetite is reflected on this matrix, what are the options for risks that are within ‘red’ risk zone, etc., then it will be very valuable for taking informed risk decisions. Therefore I would support the idea that <b>risk matrix is designed by each institution individually</b>.</p>	<p>This is the only type of matrix that could be used for risks in educational sector. It is <b>great tool</b> for overview, prioritisation and sharing of risk information. <b>Every organisation though should develop their own threshold and scales</b>, but some methodology could exist for common overview of the sectoral level for the purpose of comparison and global view.</p>

Risk matrix was described in section 1.4.7 and it was important to confirm with the risk experts that such visualisation tool used in risk management can be recommended to the sector of education, as it does not contain the essence of risk management, such as other tools and approaches described and discussion throughout the dissertation, and at the same time there are many different types of risk matrices that could be developed, therefore a confirmation from the risk experts was needed that this tool should be recommended. All experts confirmed that risk matrix is a great tool for visualisation and for better understanding of risk profile of an institution, as it serves a function of thermometer to certain extent and visualises the risk profile. However, as risk experts correctly put it and as was confirmed by research results, risk matrix is a product of individual institutions and shall be developed according to specific institution's needs with scales developed according to internally approved acceptable level of risk. Thus, the matrix can be used in the way as described in section 1.4.7 or amended as needed for more convenient use.

Table 3.16 Interview results with experts in risk management: part 5

<p><b>5. According to the survey conducted in the sector of education within the research, the most critical risks in the education sector in Latvia are:</b></p> <ol style="list-style-type: none"> <li><b>1. Employee overload</b></li> <li><b>2. Insufficient funding</b></li> <li><b>3. Lack of employee motivation</b></li> <li><b>4. Lack of qualified staff</b></li> <li><b>5. Wrong strategic decision making</b></li> <li><b>6. Changes in the political environment/legislation</b></li> </ol> <p><b>Can you please locate using this risk matrix these top six risks for the educational sector?</b></p>																																																			
<table border="1"> <tr> <td>4 Catastrophic</td> <td></td> <td>●#5</td> <td></td> <td></td> </tr> <tr> <td>3 Major</td> <td></td> <td>●#4</td> <td>●#1</td> <td></td> </tr> <tr> <td>2 Moderate</td> <td></td> <td></td> <td>●#6</td> <td>●#3 ●#2</td> </tr> <tr> <td>1 Minor</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>1 Unlikely</td> <td>2 Possible</td> <td>3 Probable</td> <td>4 Highly probable</td> </tr> </table>	4 Catastrophic		●#5			3 Major		●#4	●#1		2 Moderate			●#6	●#3 ●#2	1 Minor						1 Unlikely	2 Possible	3 Probable	4 Highly probable	<table border="1"> <tr> <td>4 Catastrophic</td> <td></td> <td></td> <td></td> <td>●#1 ●#2</td> </tr> <tr> <td>3 Major</td> <td></td> <td></td> <td>●#3 ●#6</td> <td>●#4</td> </tr> <tr> <td>2 Moderate</td> <td></td> <td>●#5</td> <td></td> <td></td> </tr> <tr> <td>1 Minor</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>1 Unlikely</td> <td>2 Possible</td> <td>3 Probable</td> <td>4 Highly probable</td> </tr> </table>	4 Catastrophic				●#1 ●#2	3 Major			●#3 ●#6	●#4	2 Moderate		●#5			1 Minor						1 Unlikely	2 Possible	3 Probable	4 Highly probable
4 Catastrophic		●#5																																																	
3 Major		●#4	●#1																																																
2 Moderate			●#6	●#3 ●#2																																															
1 Minor																																																			
	1 Unlikely	2 Possible	3 Probable	4 Highly probable																																															
4 Catastrophic				●#1 ●#2																																															
3 Major			●#3 ●#6	●#4																																															
2 Moderate		●#5																																																	
1 Minor																																																			
	1 Unlikely	2 Possible	3 Probable	4 Highly probable																																															

The final question was asked to seek opinion of risk experts from other areas on criticality of risks, which rated as top risk in surveying educational sector stakeholders. During rating, all experts commented on the reasons for selecting a certain quadrant for the risk, however, it can be observed, that final results are quite different and this may be explained by that risk experts do not have direct exposure to the sector of education and do not have experience with risks in the sector of education.

Risk nr. 1 “Overloading of employees” to SK seemed as quite probable with major impact, whereas for NS this risk seemed as highly probable and catastrophic due to recent teacher’s streak – risk nearly materialised and it would have destructive effect if it happens.

Risk nr. 2 “Insufficient funding” seemed highly probable to both experts, but the impact assessment differs. SK believe that the impact is moderate, whereas NS believes that it is catastrophic and recent preparation and near realisation for teachers’ streak proves it – no teachers at schools due to their dissatisfaction about funding would lead to closing majority of schools for uncertain period of time.

Risk nr. 3 “Lack of employee motivation” seemed highly probable to SK as it already is seen as materialising, whereas NS commented that this risk is caused the first two risks and therefore on its own is less probable.

Risk nr. 4 “Lack of qualified staff“ was rated by both experts with the same impact score – that it would have major impact, however, SK believes in probability of this risk materialising as possible, but NS believes that it is highly possible as it seems already close to realisation, when schools openly communicate about inability to find needed teachers.

Risk nr. 5 “Wrong strategic decision making” was rated by both experts with the same probability score “Possible”, but the impact score is different. SK believes that impact would be catastrophic, because strategic decisions create significant risks, whereas NS does not see it as critical because the managers of educational institutions are strong and intelligent enough to make efficient strategic decisions, which would not bring significant negative impact.

Risk nr. 6 “Changes in the political environment/legislation” was rated as “probable” by both risk experts, however SK commented that this risk causes the other risks, but on its own has moderate impact, but NS commented that as it leads to other risks it has major impact.

In overall, risk experts placed all risks mainly in “yellow” and “red” zones, what confirmed that these risks are significant and can be called as top risks.

### **3.13 Summary of interviews with experts**

The interviews with experts have confirmed the following statements set out in this dissertation:

- There is no common risk management methodology that is fit for all. Every institution shall develop their own risk management framework basing it on key principles and tools used in risk management;
- All stakeholders are responsible for risk awareness and understanding what consequences their actions would bring, this is multi-linear risk management at different levels: educational managers are responsible for framework and decision-making, teachers are responsible for day-to-

day operational risk management, students and their parents are responsible for adhering to rules and standards and for preventing risks from materialising by their actions;

- Risk management coordinators are central figures towards achieving successful risk management in the sector of education;

- Risk matrix is very useful visualisation and “risk temperature measurement” tool for the sector of education;

- The top 6 risks identified as most important for the sector of education were also assessed as important and significant by the risk experts.

## CONCLUSION

Risk management can be integrated into the sector of education in Latvia with aid of key concepts and tools of risk management, such as incident reporting tool, risk identification and assessment framework, root cause analysis, risk mitigation planning, business continuity planning, establishment and monitoring of KRIs, transparent governance, development of internal risk culture, careful data management, comprehensive process management and responsible third-party risk management. In order to integrate risk management into the sector of education seamlessly, the approach shall not put additional burden on educational institution with request just to comply with requirements with existing resources trying to adopt difficult to understand methodologies, but focus need to be placed on value of risk management with the help of risk specialists. In order to achieve successful integration of risk management, educational institutions shall receive additional funding for hiring risk co-ordinators with solid expertise in risk management, who need in turn to continuously train stakeholders in their educational institution, develop risk management framework specific for their institution and apply the tools and approaches listed above, be open and available for consultations for internal stakeholders. Such risk co-ordinators shall stay in contact with other risk co-ordinators in different educational institutions to understand wider picture and to share knowledge, and report to the regulatory authorities on the risk level and risk profile of their institution.

The most relevant risks to the sector of education proved to be psychosocial and reputational risks, such as insufficient funding, overloading of employees, lacking motivation among employees, insufficiency of qualified staff, incorrect decision-making and changes in political and regulatory environments. These risks appeared to be interconnected and may cause one another. For example, employee overload and insufficiency of qualified staff are mainly caused by lack or insufficient funding and incorrect strategic planning, lacking motivation of employees is caused by unstable political environment and continuous regulatory changes. Thus, in order to successfully manage risks in the sector of education, those risks that cause other risks shall be treated first.

Survey 1 revealed an observation, that when the risk was assessed as more critical, management of effectiveness for the same risk was assessed as very low and vice versa, thus creating “scissors” effect between risk criticality and level of its management. Throughout the analysis it was made apparent that respondents considered risks less critical where risk controls seemed to be clear and risk can be managed by a single educational institution, as well as where risk itself was not experienced directly by the respondents in the past. Those risks which are harder to control and which are dependent on State level decisions, as well which are understandable through past experience, seemed the most critical for the respondents and the least controlled. Thus, the importance of risk management

on the State level by regulatory institutions shall not be underestimated and shall start from there, before implementing it across the sector. For example, before implementing any changes, State authorities shall perform the risk assessment of planned changes and develop risk mitigation action plan prior to proceeding with deployment of planned reforms or new requirements.

The study has proved the hypothesis: majority of respondents in Survey 2 indicated, that not managing the top risks identified in Survey 1 mainly leads to deteriorating quality of education, outflow of qualified staff to other sectors, decreased prestige of teacher's profession and deteriorating role of school in the society. Survey 1 and Survey 2 proved that there is low awareness and understanding about the risk management in the sector of education, as well as demonstrated low maturity of risk management in the educational institutions of Latvia and highlighted lack of capability and capacity to employ risk management tools. Apart from the answers and comments provided by respondents directly indicating that there are no resources to employ risk management methodologies and that risks are not managed sufficiently, there were also indirect indicators such as trend in selecting middle numbers to rate risks and controls, avoidance to answer certain questions, concerns of respondents that additional requirements for risk management could trigger additional formal work activities with already scarce resources.

The top risks identified through the risk assessment survey carried for this research commonly lead to such consequences as: deteriorating quality of education, outflow of qualified staff to other better paid sectors and thus lack of qualified staff in the educational sector, decreased prestige of teacher's profession and declining role of schools in the society. By not addressing the top risks systemically in a centralised way, these consequences, which already started to materialise, will take bigger resonance with time and may result in losses on national level.

Risk management usually starts from defining objectives and strategic goals, as described in the theoretical part of this study, and based on strategy, mission and goals, material and most relevant risks are identified, assessed and afterwards monitored and reported. Material risks should be reviewed and re-assessed following changes in strategic objectives. In order to perform this correctly, experience and competence of the responsible person is a key. Results of this study have proved that these concepts are not well known and understood in the educational sector in Latvia as of now, coupled with scarce resources, it leads to poor planning, lack of risk management and inability to meet strategic objectives. Therefore, appointing a risk coordinator, who possesses relevant competencies and experiences, would result in smoother integration of risk management and ability to grab all the benefits risk management brings. In addition, to manage risks successfully it is important to measure and report them, what cannot be achieved without adequate resources,

motivation and competence, which could be resolved by appointing risk coordinators in each educational institution.

Theses for defence were proved in full and analysed from different angles, thus the aim of the research was achieved and fulfilled:

➤ *Risk management is an essential element of the future management of education, but its importance is underestimated at present moment in the sector of education due to poor understanding of the topic* - the research results confirmed that risk management is not well understood in Latvia and its benefits are underestimated. 140 out of 235 respondents (60%) in Survey 1 in their answers were inclined to that risk management in their educational institution is rather weak than strong, and only 95 respondents (40%) were inclined to that their institution is rather strong than weak in risk management. In Survey 2 risk importance was enforced by 90% of respondents. Answers of respondents and trends in Survey 1 provided evidence of poor understanding of the topic, for example, only 17% of respondents (23 out of 140) answered correctly to question “Who should be responsible for risk management in an educational institution?” that every stakeholder is responsible to certain extent, whereas incident reporting was not known to 2/3 of respondents in Survey 1 and majority of respondents indicated that incidents can only be reported by the managers, which is contradicting risk management core principles. 69 respondents out of 235 (29%) assured that there is no incident reporting process established in their educational institutions, whereas 79 respondents out of 235 (34%) were unsure whether such process exists in their educational institutions. Hence, it can be concluded that there is modest understanding of the risk management topic in the educational sector, risk management is not applied holistically and only several individual institutions voluntarily implement risk management programmes basing it on their own knowledge, initiative and expertise.

➤ *Risks that need to be assessed and prioritized in terms of likelihood and seriousness, are not managed well in the sector of education in Latvia* - the results of the study lead to conclusion, that employees and managers working in the educational sector to large extent are not ready to face the “unknown unknowns” and even most of “known unknowns”, such as terrorist attacks, bomb explosions, war situation, extreme weather conditions, etc., due to lack of planning for such extreme situations and missing risk management competencies. As the results of the study have revealed, universities and high schools have the poorest safety controls as compared to schools and pre-school educational institutions, because for smaller children the risk is taken on more seriously on the State level of management, whereas for universities and high schools it is left for autonomous decision-making in regard to security measures and usually the barrier to increasing security is underfunding.

Assessment of risk criticality and risk control effectiveness by the respondents in Survey 1 showed that when risks are well managed and kept under control, there is a perception that risks are

not critical. On the other hand, when respondents had perception that a risk is not well handled and that there are no strong controls, was observed tendiness to rate the risk as more critical. For example, although the empirical research did not confirm that cyber security related risk is of high importance to educational institutions, the theoretical and desktop research demonstrated high resonance of this risk and high impact. With the new tendency of online lessons, keeping all documents in clouds and on computers, this risk is not taken seriously enough as it should be. This leads to conclusion that cyber security risk should be rated as one of the top risks given that it is one of the top risks worldwide and that educational institutions are not aware of its importance and there are lack of clear and communicated action plans for situations if such risk would materialise.

➤ All large educational institutions and education governing bodies shall appoint a risk coordinators, who will be responsible for building and maintaining risk management framework and setting the acceptable level of risk, reporting to the management of educational institutions or governing bodies, where the strategic decisions take place - from the Survey 2 results it can be concluded that educational institutions are exhausted of constant reforms and changes in regulatory requirements. Hence, it is important for the State and regulatory bodies to focus on maintaining consistency, focus on adding value and keep constant requirements and approaches, creating long-term development strategy and objectives, which would not require new changes in the short-term. More active communication and discussion with educational institutions is required in order to prevent the effect of unexpected in short-term changes and risk assessment prior to implementing any changes is needed with involvement of internal and external stakeholders. Results of empirical study demonstrated that what frightens representatives of educational institutions most is new regulatory burden and new regulatory requirements for implementation of formal activities, which may not bring real value to the institution, but instead can swallow already scarce resources. Therefore, when implementing risk management programmes, it is important first to communicate the value risk management brings, perform risk assessment and mitigate all material risks, organise the requirement enforcement in a simple manner and, ideally, have the risk coordinator doing most of the job for risk management documentation.

Risk coordinator would be an employee with specifically risk management background and education, who could be able to utilise a number of tools developed for employers for management of risks, such as incident reporting, an important tool for learning from own failures and for effective management. In the sector of education, incident reporting can help to identify gaps, strengthen security and safety, improve the quality of education and provide holistic risk picture for each individual institution and for groups of institutions, addressing their current problems. Having an incident register in every educational institution would assist managers and officials to address the



correct problems faced by concrete institutions and to analyse regional problems and correlation of incidents with other factors that would help to realise required developments. But all of the above can only be achieved with enough resources and strong level of competence in this area, therefore full-time dedicated risk coordinator would be the best solution to achieve it with the smallest struggle.

Risk identification and risk assessment tools used on a regular basis can significantly strengthen the risk management of each educational institution by preparing them for facing all risks identified and assessed through the risk assessment. Combined with scenario analysis and resiliency planning, institutions can prepare themselves to manage the threats called “known unknowns” as well as “unknown unknowns”. Resiliency plans for different high impact situations should be developed and regularly reviewed by each educational institution.

Having in place a risk coordinator, who would be responsible to running and implementing the above-mentioned tools, educational institutions would be in position to mitigate existing risks, improve the quality of education by addressing risk causes, risks and problems, attract competitive staff and increase funding through transparent addressing of the fund spending, effective reporting and implementing efficiency measures where inefficiencies are discovered.

## RECOMMENDATIONS

Recommendations for educational institutions:

➤ Educational institution management needs to provide more attention to the internal corporate culture, foster positive internal culture, educate employees on risk management and communicate value from the risk management activities, raising the internal risk culture and overall positive environment.

➤ Planning and risk culture need to be addressed in order to mitigate the risk of employee overload, as confirmed by the correlation analysis in the research.

➤ Attention needs to be paid to the cyber risks. In co-operation with Cert.lv educational institutions should develop and work out action plan for cyber-attacks, as well as train staff to keep safe from phishing attacks, ransomware attacks, etc. There should be good co-operation established between educational institutions and Cert.lv.

➤ Dedicated trainings should be performed for all employees of educational institutions as well as students on regular basis about actions in emergency, for example in case of terrorist attacks, fires, bombings, mass shooting, etc. Roles and responsibilities should be divided to avoid panic when sharp and fast reaction is needed. “War games” should be played on regular basis by all educational institutions as a mandatory requirement, during which a situation of real threat is played.

➤ Risk management plan provided in Appendix 1 to this study and can be utilised for effective risk management in the educational institution. Main risk management tool examples are provided in Appendices 2-5 and taxonomy of risks specially developed for risk sector is provided in Appendix 4.

➤ Risk coordinator shall be appointed for developing and implementing risk management framework and culture.

Recommendations for State authorities and municipalities:

➤ Health and psychological well-being of teachers should be of foremost importance in management of education, as it has direct impact on the quality of education and the main affected stakeholders are students. Specific policies addressing workload of teachers should be designed in a centralised way, implemented and regularly checked by independent professional. Perception of teaching job and social status should be raised and promoted, to attract more students to pursue teaching job with intrinsic motives.

➤ One of the steps to tackle cyber risks is to follow and develop the Cyber Security Strategy and to ensure that education in ICT cyber security is integrated it into the curriculum. Systematic continuing education sessions should be organised for teachers on tackling security, privacy and cyber

security issues, as well as trainings on actions that need to be taken in the events of unexpected disaster situations caused by the external factors (pandemics, wars, terrorist attacks, etc.).

➤ To manage the lack of motivation risk and to address the prestige of the teacher's profession, teacher and managerial professional development programmes shall be developed with interesting professional development training courses that are of interest to teachers and educational sector management (collection of their wishes and consultations would be a plus), which raise the competence levels, professional skills and abilities and help to understand changing environments and risks. These training courses should be provided free of charge to the employees of the sector of education and development programmes and course options should be carefully designed for different job holders, i.e., teacher programmes, manager programmes, teaching support staff programmes, etc.

➤ Managers should have continuous professional development mandatory trainings on leadership, budget planning, risk management, strategic planning, etc. The results of the survey provided evidence that majority of current managers of educational institution have weak planning skills, are overwhelmed by changes and responsibilities, and do not have the capacity to ensure strategically correct resource allocation, staff motivation, attracting of funding and qualified staff. However, the other side of the coin is such, that managers are often blocked by higher standing controlling institutions and regulatory requirements, lack of proper communication and two-way dialogue. This should be improved as a matter of urgency in the sector of education in order to ensure its further positive development.

➤ To raise the risk awareness and facilitate risk management to enjoy its benefits to full extent, it is important to create publicly available common risk management methodology for the sector of education, which can be adapted by every institution to meet their specific goals. The risk registry and guidelines developed for this study in Appendix 1-5 could be utilised by all educational institutions for their risk identification and risk assessment exercises, the incident reporting form and incident register in the way as provided by this study could be utilised for analysing and fixing of incidents, risk management handbook on the basis of this study could be developed for different types of educational institutions to manage risks more effectively.

➤ Comprehensive training and awareness raising about risk management topic is needed in the sector of education for managers, teachers and employees. Special training programmes can be designed to address different parts of risk management, such as resiliency and business continuity, risk assessments, incident management, monitoring of KRIs. Provide funding for risk coordinators in every educational institution and on the State level for centralised collection of risk reports and statistical analysis for sectoral risk management.

➤ On the State level think and plan beforehand, how to realise risk management programmes in the educational sector of Latvia, prepare the strategy and action plan. For example, it could be that each educational institution could receive funding for additional full-time qualified employee, who would be responsible for risk management implementation, on the other hand, it could be also centrally located risk management teams within each municipality, who would develop, implement and oversee risk management programmes in all schools located in the municipality, as well as educate teachers and school management about risk management and risk management plans. Training programmes need to be developed and implemented for risk coordinators, as well as for managers and employees of educational institutions.

➤ The controlling institutions overseeing the educational institutions should work as partners of educational institutions, provide trainings and consultations, advise on implementation of regulatory requirements and collect opinions from the educational institutions' representatives about certain regulations. Co-operative approach may prove more effective rather than directive approach and may mitigate such risks as lack of motivation, lack of qualified employees, poor internal risk culture, etc. There should be strong teamwork between educational institutions' managers, teachers and regulatory bodies, State governing authorities, parents, students, etc. – i.e., among all the stakeholders.

➤ Regulators should communicate requirements in clear and concise way and ensure provision of all necessary resources to enable educational institutions to realise them, provide training and vision how certain requirements should be implemented.

## REFERENCES

1. Abraham, J.M. (2013) *Risk Management: An Accountability Guide for University and College Boards*. Association of Governing Boards of Universities and Colleges, Washington, DC.
2. Abraham, J. M., Baird, R., Neugebauer, F. (2013) Leveraging Enterprise Risk Management: Opportunity for Greater Relevance. *EDUCAUSE Review*, v.48, n.6, p.28-40, Nov-Dec 2013. ISSN-1527-6619. ERIC database. <https://er.educause.edu/-/media/files/article-downloads/erm1363.pdf> [Accessed on 02.08.2018]
3. Achampong, F. K. (2010) Integrating Risk Management and Strategic Planning. *Planning for Higher Education*, v.38, n.2, p.22-27, January -March 2010. ISSN-0736-0983. ERIC database.
4. Adams, J. F. (1973) The Governing Board's Role in Risk Management and Insurance for Higher Education. *Journal NACUBO Professional File*, Mar 1973, v.4, n. 1. ERIC database.
5. Asian Development Bank [ADB] (2010) *Education Sector Risk Assessment Guidance Note*. July 2010, ADB: Philippines. <https://www.adb.org/sites/default/files/institutional-document/31318/guidance-note-education-sector-risk-assessment.pdf> [Accessed on 15.05.2017]
6. Asian Development Bank [ADB] (2016) *A Wake-up Call: Enterprise Risk Management at Colleges and Universities Today*. A Survey. A Survey by the Association of Governing Boards of Universities and Colleges and United Educators. <https://www.mass.edu/foradmin/trustees/documents/2019-03-28%20RiskSurvey2014.pdf> [Accessed on 15.05.2021]
7. Alberts, C.J., Dorofee, A.J. (2009) A Framework for Categorizing Key Drivers of Risk. *Technical Report*. Carnegie Mellon University: Software Engineering Institute, U.S. Department of Defence.
8. Alliance of Schools for Cooperative Insurance Programs [ASCIP] (2016) *Risk Management Primer for School Districts*. ASCIP, 17 June 2016. <https://ascip.org/wp-content/uploads/2016/06/ASCIP-Risk-Management-Primer-for-School-Districts-SIXTH-DRAFT-2016-06-20.pdf> [Accessed on 06.05.2018]
9. APPA (2018) *The Landscape, Framework, and Strategies for Managing & Mitigating Risk*. APPA Thought Leaders Series 2018. Association of Higher Education Facilities Officers. ISBN: 978-0-913359-20-4. <https://files.eric.ed.gov/fulltext/ED592253.pdf> [Accessed on 17.07.2021]
10. Ariff, M.S.B.M., Zakuan, N, Tujadin, M.N.M., Ahmads, A., Ishak, N., Ismail, K. (2014) A Framework for Risk Management Practices and Organizational Performance in Higher Education. *Review of Integrative Business & Economics Research*, 3(2), pp. 422–432.

- [http://sibresearch.org/uploads/2/7/9/9/2799227/riber\\_b14-179\\_422-432.pdf](http://sibresearch.org/uploads/2/7/9/9/2799227/riber_b14-179_422-432.pdf) [Accessed on 30.08.2020]
11. Aven, T. (2015) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research* 253 (2016) 1–13. <https://core.ac.uk/download/pdf/82320116.pdf> [Accessed on 06.05.2018]
  12. Barnett, J. (2014). Efficient and Effective Management in Higher Education: An Insider Action Research Perspective. (Doctoral Dissertation, Cardiff University, UK). <https://repository.cardiffmet.ac.uk/bitstream/handle/10369/7944/J%20Barnett%20Efficient%20and%20Effective%20Management%20in%20Higher%20Education%20Final.pdf?sequence=1&isAllowed=y> [Accessed on 19.09.2019]
  13. Basel Committee of Banking Supervision [BCBS] (2001) *QIS 2 - Operational Risk Loss Data*, 4 May 2001. <https://www.bis.org/bcbs/qisoprisknote.pdf> [Accessed on 8.02.2020]
  14. Basel Committee of Banking Supervision [BCBS] (2011) *Principles for the Sound Management of Operational Risk*, Bank for International Settlements, June 2011. <https://www.bis.org/publ/bcbs195.pdf>. [Accessed on 02.08.2018]
  15. Basel Committee of Banking Supervision [BCBS] (2011) *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches (BCBS196)*, Bank for International Settlements, Basel: Switzerland. ISBN: 92-9197-856-6. <https://www.bis.org/publ/bcbs196.pdf> [Accessed on 7.05.2020]
  16. Basel Committee of Banking Supervision [BCBS] (2018) *Cyber-resilience: range of practices*. 18 December 2018. Bank for International Settlements, Basel: Switzerland. ISBN 978-92-9259-228-8. <https://www.bis.org/bcbs/publ/d454.pdf> [Accessed on 14.05.2020]
  17. Basel Committee of Banking Supervision [BCBS] (2021) *Principles for Operational Resilience*. March 2021. Bank for International Settlements. ISBN 978-92-9259-467-1 <https://www.bis.org/bcbs/publ/d516.pdf> [Accessed on 05.12.2021]
  18. Beals, S., Fox, C. & Minsky, S. (2015) *Why a mature ERM effort is worth the investment*. Risk Management and Insurance Society (RIMS) Executive Report. [http://glossary.rims.org/Documents/MatureERM\\_whitepaper.pdf](http://glossary.rims.org/Documents/MatureERM_whitepaper.pdf) [Accessed on 29.05.2021]
  19. Beasley, M.S. (2013) *Enterprise Risk Management Can Be a Strategic Opportunity*. National Association of College and University Business Officers. <https://files.eric.ed.gov/fulltext/ED560753.pdf> [Accessed on 13.05.2021]
  20. Beasley, M.S., Clune, R., Hermanson, D.R. (2005) Enterprise Risk Management: An Empirical Analysis of Factors associated with the Extent of Implementation. *Journal of Accounting and*

- Public Policy*, 24:521–531. DOI: <https://doi.org/10.1016/j.jaccpubpol.2005.10.001> [Accessed on 30.08.2020]
21. Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: SAGE.
  22. Beck, U. (2000) *Risk Society Revisited: Theory, Politics and Research Programmes*. In *The Risk Society and Beyond: Critical Issues for Social Theory*. Edited by Adam, B. Beck, U. and Van Loon, J. London: SAGE
  23. Blass, R. (2021) “*Visi nervozi, bērniem panika!*” *Attālinātās mācības daudziem noiet greizi uzreiz pēc brīvlaika* (“*Everyone nervous, kids panic!*” *For many, distance learning goes wrong right after their free time*). *Bez Tabu*. <https://skaties.lv/beztabu/nejedzibas/visi-nervozi-berniem-panika-attalinatas-macibas-daudziem-noiet-greizi-uzreiz-pec-brivlaika/> [Accessed on 06.01.2022]
  24. Borcan, O., Lindahl, M., Mitrut, A. (2017) Fighting corruption in education: What works and who benefits? *American Economic Journal: Economic Policy* Vol. 9 (1), pp. 180–209. DOI: <https://doi.org/10.1257/pol.20150074> [Accessed on 14.05.2019]
  25. Bruemmer, K.N. (2016) *Risk Perceptions in the Management of Student Organizations*. ProQuest LLC, Ph.D. Dissertation, North Dakota State University. <https://www.proquest.com/docview/1794656034> [Accessed on 05.05.2018]
  26. Brynin, M. (2014) Individual Choice and Risk: The Case of Higher Education. *Sociology*, Vol. 47, Issue 2, pp. 284–300. DOI: 10.1177/0038038512444814 [Accessed on 05.05.2018]
  27. Business Continuity Institute (2016) *BCM Legislations, Regulations, Standards and Good Practice*. February 2016. <https://www.thebci.org/static/uploaded/aa17d414-03ac-4ddb-a43657dd6297312d.pdf>. [Accessed on 02.08.2018]
  28. Cameron, C. (2017) The Strategic and Legal Risks of Work-Integrated Learning: An Enterprise Risk Management Perspective. *Asia-Pacific Journal of Cooperative Education*, v.18, n.3, p.243-256. DOI: <https://files.eric.ed.gov/fulltext/EJ1159152.pdf> [Accessed on 12.07.2020]
  29. Cameron, C., Klopper, C. (2015) University Lawyers: A Study of Legal Risk, Risk Management and Role in Work Integrated Learning Programmes. *Journal of Higher Education Policy and Management*, v.37, n.3, p.344-360. DOI: <http://dx.doi.org/10.1080/1360080X.2015.1034423> [Accessed on 14.07.2020]
  30. Canham, A., Jun G. T., Waterson, P., Khalid, S. (2018) Integrating systemic accident analysis into patient safety incident investigation practices, *Applied Ergonomics*, V. 72 (2018), pp. 1–9, Web of Science scientific database.
  31. Centko, J.D (2013) *A Report Card for Risk Management in Higher Education for Two-Year Colleges in Minnesota, Wisconsin, and Michigan: A Study to Assess Gaps Regarding Risk*

- Management in Higher Education*. ProQuest LLC, Ph.D. Dissertation, North Dakota State University. Accessed at <https://www.proquest.com/docview/1960621259> [Accessed on 05.09.2018]
32. CERT.LV (2018) Publiskais pārskats par CERT.LV uzdevumu izpildi 2017. gadā (Public report on fulfillment of CERT.LV tasks), published 23.03.2018 online on CERT.lv. [https://cert.lv/uploads/CERT-LV\\_gada\\_2017\\_publ\\_galaversija.pdf](https://cert.lv/uploads/CERT-LV_gada_2017_publ_galaversija.pdf) [Accessed on 16.05.2018]
  33. Chapelle, A. (2019) *Operational Risk Management*, UK: John Wiley & Sons, Ltd.
  34. Chassang G. (2017) The impact of the EU general data protection regulation on scientific research, *Ecancermedicalsecience online journal*, 11: 709. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/> [Accessed on 03.01.2017]
  35. Chr. Michelsen Institute (2006) Corruption in the Education Sector, U4 Anti-Corruption Resource Center, Issue 4:2006, Bergen, Norway: Chr. Michelsen Institute. <https://www.cmi.no/publications/file/2563-corruption-in-the-education-sector.pdf> [Accessed on 05.08.2018]
  36. Clark, S. B., DeCato, K. D.; George, D., Henderson, D.; Henry, A. A.Jr., Hoch, Ch. (2016) *Enterprise Risk Management in the Great City Schools, Spring 2016*. Council of the Great City Schools, Washington, DC. <https://files.eric.ed.gov/fulltext/ED569197.pdf> [Accessed on 26.08.2018]
  37. Clyde-Smith, J. (2014) Utilising Enterprise Risk Management Strategies to Develop a Governance and Operations Framework for a New Research Complex: A Case Study. *Journal of Higher Education Policy and Management*, v.36, n.3, p.327-337. DOI: <http://dx.doi.org/10.1080/01587919.2014.899051> [Accessed at 24.11.2018]
  38. Collins, L., Collins, D. (2013) Decision Making and Risk Management in Adventure Sports Coaching. *Quest Journal*, v.65, n.1, p.72-82. DOI: <http://dx.doi.org/10.1080/00336297.2012.727373> [Accessed at 05.05.2018]
  39. Colquitt L.L., Hoyt R.E., Lee R.B. (1999) Integrated risk management and the role of the risk manager. *Risk Management and Insurance Review*. V. 2, Issue 3, September 1999, pp. 43-61. DOI: <https://doi.org/10.1111/j.1540-6296.1999.tb00003.x> [Accessed on 30.08.2020]
  40. Committee of Sponsoring Organizations [COSO] (2004) *Enterprise Risk Management—Integrated Framework*. <https://www.coso.org/pages/erm-integratedframework.aspx> [Accessed on 30.08.2020]
  41. Curwood, B., Kaake, K. (2016) *Risk Management: A Canadian Case Study*. 2017 Investment Management Consultants Associations Inc.



- <https://investmentsandwealth.org/getattachment/90bb74dd-e521-4104-a92c-8298ff710cca/IWM17MarApr-RiskMgmtCanadianCaseStudy.pdf> [Accessed on 05.09.2018]
42. Datu Valsts Inspekcija (2018) Videokonferences par personas datu aizsardzības jautājumiem. Latvijas Pašvaldību Savienība, Rīga. [Videoconference series]. <http://www.lps.lv/lv/zinas/lps/3970-videokonferences-par-personas-datu-aizsardzibas-jautajumiem> [Accessed on 18.04.2018]
43. De Balle, P., Faye, I. (2021) *Financial institutions are showing resilience and will be central to the recovery*. Worldbank Private Sector Development Blog, 17 May 2021. <https://blogs.worldbank.org/psd/financial-institutions-are-showing-resilience-and-will-be-central-recovery> [Accessed on 06.09.2021]
44. Dekker, H.C., Sakaguchi J., Kawaid T. (2013) Beyond the contract: Managing risk in supply chain relations. *Management Accounting Research*, Vol. 24, Issue 2, June 2013, pp. 122-139. DOI: <https://doi.org/10.1016/j.mar.2013.04.010> [Accessed on 18.09.2018]
45. Demmel A., Kuschewsky M. (2017) GDPR – The Data Protection Officer ("DPO") Requirement, Role and Implementation. *Squire Patton Boggs*. Berlin, Brussels. [https://www.squirepattonboggs.com/~media/files/insights/events/2017/01/need-to-know-gdpr-the-data-protection-officer-requirement-role-and-implementation/gdpr\\_data\\_protection\\_officer\\_role\\_requirement\\_and\\_implementation\\_jan17.pdf](https://www.squirepattonboggs.com/~media/files/insights/events/2017/01/need-to-know-gdpr-the-data-protection-officer-requirement-role-and-implementation/gdpr_data_protection_officer_role_requirement_and_implementation_jan17.pdf) [Accessed on 15.04.2018]
46. Dimitrijevic L., Dakic J. (2014) The risk management in higher education institutions. *Online Journal of Applied Knowledge Management*, Vol. 2(1), pp. 137 – 152. [http://www.iiakm.org/ojakm/articles/2014/volume2\\_1/OJAKM\\_Volume2\\_1pp137-152.pdf](http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp137-152.pdf) [Accessed on 02.02.2018]
47. Ding R., Dekker H.C., Groot T. (2013) Risk, partner selection and contractual control in interfirm relationships. *Management Accounting Research*, Vol. 24, Issue 2, June 2013, Pages 140-155. DOI: <https://doi.org/10.1016/j.mar.2013.04.007> [Accessed on 18.09.2018]
48. Dionne, G. (2013) *Risk Management : History, Definition and Critique*. Working Paper 13-02. CIRPEE, Canada. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.687.3037&rep=rep1&type=pdf> [Accessed on 19.08.2018]
49. Dombrovskis, V., Guseva, S., Murasovs, V. (2011) Motivation to Work and the Syndrome of Professional Burnout among Teachers in Latvia. *Procedia - Social and Behavioral Sciences*, 29, pp. 98 – 106. [https://ac.els-cdn.com/S1877042811026735/1-s2.0-S1877042811026735-main.pdf?\\_tid=fa6174b9-c14f-43a9-9c99-](https://ac.els-cdn.com/S1877042811026735/1-s2.0-S1877042811026735-main.pdf?_tid=fa6174b9-c14f-43a9-9c99-)

- [ab93f2c70459&acdnat=1547549152\\_ee55f2d95681d4cf5c12df71c7d7a6eb](https://doi.org/10.1111/j.1539-6975.2012.01506.x) [Accessed on 02.08.2018]
50. Douglas, M., Wildavsky, A. (1982) *Risk and culture: an essay on the selection of technical and environmental dangers*. Berkeley: University of California Press. ISBN: 9780520050631.
  51. Dunklee, D.R., Shoop, R. J. (1993) *A Primer for School Risk Management: Creating and Maintaining District and Site-Based Liability Prevention Programs*, U.S.A.: Allyn and Bacon
  52. Dutta, K. & Babble, D. F. (2014) Scenario Analysis in the Measurement of Operational Risk Capital: A Change of Measure Approach. *Journal of Risk and Insurance*, 81 (2), 303-334. <https://doi.org/10.1111/j.1539-6975.2012.01506.x> [Accessed on 23.04.2021]
  53. Dzanuškāns J. (2011) Personālu datu drošības aspekti izglītības jomā. *Latvijas Pašvaldību savienības izdevums „Logs”*, Nr. 10 (196), 20.-21.lpp. [http://www.jdz.lv/lv/wp-content/uploads/publikacijas/janis-dzanuskans/10.2011\\_Logs.pdf](http://www.jdz.lv/lv/wp-content/uploads/publikacijas/janis-dzanuskans/10.2011_Logs.pdf) [Accessed on 30.03.2018]
  54. Eger, L., Egerová, D. (2016) Project Risk Management in Educational Organizations: A Case from the Czech Republic. *Educational Management Administration & Leadership*, v.44, n.4, p.578-598, July 2016. DOI: <http://dx.doi.org/10.1177/1741143214558573> [Accessed on 20.03.2019]
  55. Elson, R.J., O’Callaghan, S., Walker, J.P. (2015) Integrating Corporate Governance Concepts in the classroom with the Risk Assessment Project. *Journal of Instructional Pedagogies Volume 17, November, 2015*. ERIC database.
  56. Employer Confederation of Latvia (2010) *Darba dēvēja rokasgrāmata / Employer’s Handbook*. Latvijas Darba devēju konfederācija: 2010. <http://osha.lv/lv/publications/files/darba-deveja-rokasgramata.pdf> [Accessed on 31.01.2018]
  57. European Association for Quality Assurance in Higher Education (2015) *Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG)*. Brussels, Belgium. [https://www.enqa.eu/wp-content/uploads/2015/11/ESG\\_2015.pdf](https://www.enqa.eu/wp-content/uploads/2015/11/ESG_2015.pdf) [Accessed on 12.05.2021]
  58. European Parliament, European Council (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal*. <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf> [Accessed on 14.01.2018]
  59. Ferguson, M.E., Drake M.J. (2021) Teaching Supply Chain Risk Management in the COVID-19 Age: A Review and Classroom Exercise. *Decision Sciences Journal of Innovative Education*,

- v.19, n.1, p.5-14, January 2021. DOI: <http://dx.doi.org/10.1111/dsji.12230> [Accessed on 17.07.2021]
60. Fernet, C., Trépanier, S.G., Austin, S., Levesque-Côté, J. (2016) Committed, inspiring, and healthy teachers: How do school environment and motivational factors facilitate optimal functioning at career start? *Teaching and Teacher Education*, 59 (2016), pp. 481-491. DOI: <http://dx.doi.org/10.1016/j.tate.2016.07.019> [Accessed on 02.08.2018]
  61. Filtness, A.J., Goode, N., Cook, R. (2015) Incident reporting culture in recreational hot air ballooning, *Procedia Manufacturing*, V.3 (2015) pp. 1165 – 1172, Web of Science scientific database.
  62. Forlin, P. (1995) Risk management in Australian science education: A model for practice. *Australian Science Teachers Journal*, June 1995, Vol. 41, I. 2, p. 22-28. ISSN-0045-0855.
  63. Frigo, M.L., Anderson, R.J. (2011) *Embracing Enterprise Risk Management*. Committee of Sponsoring Organisations of the Treadway Commission (COSO), January 2011. <http://www.markfrigo.com/Embracing Enterprise Risk Management-GettingStarted - COSO-Frigo and Anderson-January 2011.pdf> [Accessed on 02.08.2018]
  64. FSB (2013) *Principles for and Effective Risk Appetite Framework*. Financial Stability Board. [https://www.fsb.org/wp-content/uploads/r\\_131118.pdf](https://www.fsb.org/wp-content/uploads/r_131118.pdf) [Accessed on 14.05.2021]
  65. Garnett, J. (2019) Academic Libraries -- Changing the Approach: Resilience Building against Disruptive Events and the Contribution to Disaster Risk Reduction Frameworks. *New Review of Academic Librarianship*, v.27, n.1, p.113-129. DOI: <http://dx.doi.org/10.1080/13614533.2019.1703767> [Accessed at 14.05.2021]
  66. Gillespie, S. J. (2014) *Correlational Study of Risk Management and Information Technology Project Success*. ProQuest LLC, Ph.D. Dissertation, Capella University. [http://gateway.proquest.com/openurl?url\\_ver=Z39.88-2004&rft\\_val\\_fmt=info:ofi/fmt:kev:mtx:dissertation&res\\_dat=xri:pqm&rft\\_dat=xri:pqdiss:3610813](http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqm&rft_dat=xri:pqdiss:3610813) [Accessed on 05.05.2018]
  67. Gines K. (2018) Getting Up to Speed With GDPR. *Successful Meetings Magazine*, 67(3), 72-78. [http://successfulmeetings.texterity.com/successfulmeetings/march\\_2018?pg=86#pg86](http://successfulmeetings.texterity.com/successfulmeetings/march_2018?pg=86#pg86) [Accessed on 02.05.2018]
  68. Glaser A. (2018) The Cambridge Analytica Scandal Is What Facebook-Powered Election Cheating Looks Like. *Online Journal*. The Slate Group. <https://slate.com/technology/2018/03/the-cambridge-analytica-scandal-is-what-facebook-powered-election-cheating-looks-like.html> [Accessed on 17.04.2018]

69. Guadix, J., Carrillo-Castrillo, J., Onieva, L., Lucena, D. (2015) Strategies for psychosocial risk management in manufacturing. *Journal of Business Research*, 68, pp. 1475–1480. DOI: <http://dx.doi.org/10.1016/j.jbusres.2015.01.037> [Accessed on 02.08.2018]
70. Gushchina, O., Ochepovsky, A. (2019) Data Mining for the E-Learning Risk Management. *Turkish Online Journal of Distance Education*, v.20, n.3, Article 13, p.181-196, July 2019. <https://files.eric.ed.gov/fulltext/EJ1221479.pdf> [Accessed on 17.07.2021]
71. Hačatrjana, L. (2021) *Attālinātā mācīšanās COVID-19 pandēmijas laikā: kas skolēniem ir palīdzējis un traucējis tikt ar to galā? (Remote studying during Covid-19 pandemic: what has helped students and what disturbed them?)*. Report of the first pilot study of the postdoctoral research project no. 1.1.1.2/VIAA/4/20/697. [https://www.lu.lv/fileadmin/user\\_upload/LU.LV/Post\\_doc\\_projekti/Pecdoktorantura\\_4\\_karta/Pilotpetijuma-zinojums-Hacatrjana-Liena.pdf](https://www.lu.lv/fileadmin/user_upload/LU.LV/Post_doc_projekti/Pecdoktorantura_4_karta/Pilotpetijuma-zinojums-Hacatrjana-Liena.pdf) [Accessed on 06.01.2022]
72. Hadden, L.B., Hermanson, D.R., DeZoort F.T. (2003) Audit Committees Oversight Of Information Technology Risk. *Review of Business Information Systems (RBIS)*, Vol. 7, Issue 4, pp. 1-12. DOI: <https://doi.org/10.19030/rbis.v7i4.4509> [Accessed on 30.08.2020]
73. Hakanen, J. J., Bakker, A. B., Schaufeli, W. B. (2006). Burnout and work engagement among teachers. *Journal of School Psychology*, 43(6), pp. 495-513. DOI: <https://doi.org/10.1016/j.jsp.2005.11.001>
74. Hall, J.C. (2013) Perspectives: Intellectual Risk Management. *Change: The Magazine of Higher Learning*, v.45, n.2, p.25-27. DOI: <http://dx.doi.org/10.1080/00091383.2013.764260> [Accessed at 24.11.2018]
75. Hallak, J., Muriel P. (2007) *Corrupt Schools, Corrupt Universities: What Can be Done?* Paris: International Institute for Educational Planning. [www.unesco.org/iiep](http://www.unesco.org/iiep) [Accessed on 15.05.2017]
76. HM Treasury (2004) *The Orange Book: Management of Risk – Principles and Concepts*, London: HMSO. [www.hm-treasury.gov.uk/d/orange\\_book.pdf](http://www.hm-treasury.gov.uk/d/orange_book.pdf) [Accessed on 02.08.2018]
77. Hoffman A. (2018) What is the Cambridge Analytica controversy regarding Facebook data? *Quora*. <https://www.quora.com/What-is-the-Cambridge-Analytica-controversy-regarding-Facebook-data> [Accessed on 17.04.2018]
78. Huber M., Rothstein H. (2013) The risk organisation: Or how organisations reconcile themselves to failure. *Journal of Risk Research*, 16 (6) (2013), pp. 651-675. DOI: <http://dx.doi.org/10.1080/13669877.2012.761276> [Accessed on 09.05.2018]
79. Huber, C., Scheytt, T. (2013) The dispositif of risk management: Reconstructing risk management after the financial crisis. *Management Accounting Research*, Vol. 24, Issue 2, June 2013, pp. 88-99. DOI: <https://doi.org/10.1016/j.mar.2013.04.006> [Accessed on 17.09.2018]

80. Hustoles, C. L. J. (2012) *Through the Eyes of Higher Education Attorneys: How Department Chairs Are Navigating the Waters of Legal Issues and Risk Management*. ProQuest LLC, Ph.D. Dissertation, Western Michigan University. <https://www.proquest.com/docview/1037994257> [Accessed on 24.11.2018]
81. ISO (2018) *31000:2009 Risk management*. International Organization for Standards, Geneva, Switzerland. <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf> [Accessed on 18.09.2019]
82. Ivancevich, D.M., Hermanson, D.R., Smith, L.M. (1998) The association of perceived disaster recovery plan strength with organizational characteristics. *Journal of Information Systems*, 12.1 (1998): 31-43.
83. Izglītības kvalitātes valsts dienests [IKVD] (2021) *Laba skola – kāda tā ir? Priekšstati, mīti un pārmaiņas! (A good school - what is it like? Concepts, myths and change!)*. Skola 2030 publication. <https://www.skola2030.lv/lv/jaunumi/blogs/laba-skola-kada-ta-ir-prieksstati-miti-un-parmainas> [Accessed on 06.01.2022]
84. Jacobus, D. (2015) *New Paradigm of Managing Risks: Risk and Control Self-Assessment*. The 2014 International Conference on Agro-industry (ICoA): Competitive and sustainable Agroindustry for Human Welfare. Agriculture and Agricultural Science Procedia 3 (2015) 32 – 34. DOI: <https://doi.org/10.1016/j.aaspro.2015.01.008> [Accessed on 18.11.2019]
85. Johnson, J. (2015) *The basics of corruption risk management A framework for decision making and integration into the project cycles*. U4 Issue 2015: 18. <https://www.u4.no/publications/the-basics-of-corruption-risk-management-a-framework-for-decision-making-and-integration-into-the-project-cycles.pdf> [Accessed on 14.05.2021]
86. Kaļķis, V. (2008) *Darba vides risku novērtēšanas metodes*. Rīga: Latvijas Izglītības Fonds.
87. Karadsheh, L. A. (2010) *A Framework for Integrating Knowledge Management with Risk Management for Information Technology Projects*. ProQuest LLC, D.M.I.T. Dissertation, Lawrence Technological University. ISBN: ISBN-978-1-1097-2246-8. <https://www.proquest.com/docview/275941047> [Accessed on 02.02.2017]
88. Kelliher P.O.J., Acharyya M., Couper A., Grant K., Maguire E., Nicholas P., Smerald C., Stevenson D., Thirlwell J., Cattle N. (2016) *Good practice guide to setting inputs for operational risk models*, British Actuarial Journal, Vol. 22, part 1, pp. 68–108, published on 21 March 2016. Institute and Faculty of Actuaries. DOI: [10.1017/S1357321716000179](https://doi.org/10.1017/S1357321716000179) [Accessed on 24.10.2019]
89. Kelliher P.O.J., Wilmot D., Vij J., Klumpes P.J.M. (2013) *A common risk classification system for the Actuarial Profession*. British Actuarial Journal 18(01). DOI:

- 10.1017/S1357321712000293. <https://www.researchgate.net/publication/259433133> [Accessed on 01.03.2020]
90. Khan, M., Andreoni, A., and Roy, P. (2016) *Anti-corruption in adverse contexts: A strategic approach*. Working Paper. London: School of Oriental and African Studies (SOAS). Available at: [https://eprints.soas.ac.uk/23495/1/Anti-Corruption%20in%20Adverse%20Contexts%20\(1\).pdf](https://eprints.soas.ac.uk/23495/1/Anti-Corruption%20in%20Adverse%20Contexts%20(1).pdf) [Accessed on 14.05.2018]
91. Kingdon, G. G., Little, A., Aslam, M., Rawal, S., Moe, T., Patrinos, H., Beteille, T., Banerji, R., Parton, B., Sharma, S. K. (2014) *A rigorous review of the political economy of education systems in developing countries*. Final Report. Education Rigorous Literature Review. UK Department for International Development. <https://eppi.ioe.ac.uk/cms/Portals/0/PDF%20reviews%20and%20summaries/Political%20economy%202014Kingdon.pdf?ver=2014-04-24-141259-443> [Accessed on 14.02.2018]
92. Kirya, M. (2019) *Education sector corruption: How to assess it and ways to address it*. U4 Issue 2019:5. U4 Anti-Corruption Resource Centre. Available at <https://www.u4.no/publications/education-sector-corruption-how-to-assess-it-and-ways-to-address-it.pdf> [Accessed on 14.05.2021]
93. Kitagawa, K. (2021) Conceptualising 'Disaster Education'. *Education Sciences*, v. 11, Article 233. <https://files.eric.ed.gov/fulltext/EJ1297303.pdf> [Accessed on 17.07.2021]
94. Kleffner A. et al. (2003) The effect of corporate governance on the use of enterprise risk management: evidence from Canada. *Risk Management and Insurance Review*. V.6, Issue 3, pp. 53-73. DOI: <https://doi.org/10.1111/1098-1616.00020> [Accessed at 17.07.2019]
95. Kurens, M. (2020) *Bankas spēs pārciest Covid-19 krīzi arī tad, ja tā ievilksies / Banks will be able to survive the Covid-19 crisis even if it drags on*; TVNET interview, 2.04.2020. <https://www.tvnet.lv/6939267/bankas-spes-parciest-covid-19-krizi-ari-tad-ja-ta-ievilksies>. [Accessed on 06.01.2022]
96. Kuriyan, R., Bailur, S., Gigler, B., Park, K. (2011) *Technologies for transparency and accountability: Implications for ICT policy and implementation*. World Bank, Open Development Technology Alliance. DOI: 10.13140/RG.2.2.19320.24320 [Accessed on 05.05.2018]
97. Laiveniece, D. (2014) *Zinātniskās rakstīšanas skola*. Liepāja : LiePA.
98. Latvijas Banka (2013) *Business Continuity Provision for the Payment and Securities Settlement Systems in Latvia*. Bank of Latvia website, 01.01.2013. <https://www.bank.lv/en/your-profile/media/559-payment-and-settlement-systems/2724-business-continuity-provision-for-the-payment-and-securities-settlement-systems-in-latvia> [Accessed on 02.08.2018]

99. Lehtonen, J., Silina, R., Abelniece, B. (2011) *Riska un Krīzes komunikācija (Risk and Crisis Communication)*, Latvia: Biznesa Augstskola Turība (Turība Business School)
100. Leitch, M. (2010) ISO 31000:2009 – The New International Standard on Risk Management. *Risk Analysis*, Vol.30 (6) pp. 887–892. DOI: <https://doi.org/10.1111/j.1539-6924.2010.01397.x> [Accessed at 09.05.2018]
101. Leitch, M. (2016) *Intelligent internal control and risk management: Designing high-performance risk control systems*. Routledge. ISBN 9780566087998.
102. LETA (2019) *Another four children from Sigulda hospitalized for suspected food poisoning*. Published as news article on 15.09.2019 on [www.leta.lv](http://www.leta.lv). <https://www.leta.lv/eng/home/important/BA3FECBD-4DCA-45D5-8068-22464E9B2262/> [Accessed on 02.10.2020]
103. Liebenberg A., Hoyt, R. (2003) The determinants of enterprise risk management: evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, V. 6, Issue 1, February 2003, pp. 37-52. DOI: <https://doi.org/10.1111/1098-1616.00019> [Accessed at 17.07.2019]
104. Līmane, E., Voronova, I. (2013) Uz riskiem balstītas pieejas pielietošana revīzijā un iekšējās kontroles sistēmā / Applicability of the risk-based approach in revision and internal control system. *Economics and Business*, Vol.24, 2013. DOI: DOI: 10.7250/eb.2013.008 [Accessed on 26.08.2018]
105. Lundquist A. E. (2015) *Enterprise Risk Management (ERM) at U.S. Colleges and Universities: Administration Processes Regarding the Adoption, Implementation, and Integration of ERM*. Doctoral Dissertation, Western Michigan University, U.S. <https://scholarworks.wmich.edu/dissertations/1181/> [Accessed on 18.09.2019]
106. Lundquist, A., Shackelford, A. (2011) Responding to and Supporting Students with Disabilities: Risk Management Considerations. *New Directions for Higher Education*, n.154, p.65-75, Summer 2011. ISSN: ISSN-0271-0560. DOI: <http://dx.doi.org/10.1002/he.435> [Accessed on 05.05.2018]
107. Margaryan, A., Littlejohn, A., Stanton, N. (2016) Research and development agenda for Learning from Incidents, *Safety Science Journal*, V. 99 (2017), p. 5–13, Web of Science scientific database.
108. Martinez-Martinez D.F. (2018) Unification of personal data protection in the EU: Challenges and implications. *Journal El Profesional de la Información*, 27(1), 185-194. eISSN: 1699-2407. <http://www.elprofesionaldelainformacion.com/contenidos/2018/ene/17.pdf> [Accessed on 02.05.2018]

109. Martoglu, M. (2015) The Role of School Management in the Prevention of School Violence, *Procedia - Social and Behavioral Sciences*, 182 (2015) 695 – 702, Elsevier Ltd.; Retrieved from: <https://doi.org/10.1016/j.sbspro.2015.04.815> [Accessed on 02.05.2018]
110. Mazaheri, A., Montewka, J., Nisula, J., Kujala, P. (2015) Usability of accident and incident reports for evidence-based risk modeling – A case study on ship grounding reports, *Safety Science*, V. 76 (2015), pp. 202–214, Web of Science scientific database.
111. McDonald T.J., O’Byrne D., O’Leary P., O’Riordan, C. (2020) Development of an Academic Risk Model to support Higher Education Quality Assurance. *6th International Conference on Higher Education Advances (HEAd’20)*, Universitat Politècnica de València, València, 2020. DOI: <http://dx.doi.org/10.4995/HEAd20.2020.11261> [Accessed on 06.08.2018]
112. McNeil, A.J. (2013) Enterprise Risk Management. *Annals of Actuarial Science*, Vol. 7, Issue 1, March 2013, pp 1-2. Cambridge University Press 14 Jan 2013. DOI: 10.1017/S1748499512000334 [Accessed on 09.05.2018]
113. McShane, M. (2018) Enterprise risk management: history and a design science proposal. *The Journal of Risk Finance*, Vol. 19(2), pp. 137-153. DOI: <https://doi.org/10.1108/JRF-03-2017-0048> [Accessed on 18.09.2019]
114. McWilliam, E. L. and Taylor, P.G., Singh, P. (2002) Doctoral Education, Danger and Risk Management. *Higher Education Research and Development*, Vol. 21 (2), pp. 119- 129. DOI: [10.1080/07294360220144042](https://doi.org/10.1080/07294360220144042) [Accessed on 14.04.2018]
115. Meerts-Brandsma, L., Furman, N., Sibthorp, J. (2017) Benchmarking Outdoor Expeditionary Program Risk Management Strategies. *Journal of Outdoor Recreation, Education, and Leadership*, v. 9, n. 2, p. 262-266. ERIC database.
116. Mertoglu, M. (2015) The Role of School Management in the Prevention of School Violence. *Procedia - Social and Behavioral Sciences* 182 (2015), 695–702. DOI: 10.1016/j.sbspro.2015.04.815 [Accessed on 11.02.2018]
117. Meyer T. (2012) How About Safety and Risk Management in Research and Education? *Procedia Engineering*, Vol. 42, pp. 854-864. DOI: <https://doi.org/10.1016/j.proeng.2012.07.478> [Accessed on 20.09.2018]
118. Miķeļsone, I. (2021) *Profesionālās un emocionālās izdegšanas samazināšanas riska cēloņu analīze un to samazināšanas iespējas skolotāju profesionālajā darbībā (Analysis of the Risks and Causes of Professional and Emotional Burnout and Professional Burnout Prevention Strategies)*. Master Thesis. University of Latvia. <https://dspace.lu.lv/dspace/handle/7/54032> [Accessed on 26.09.2021]



119. Ministries of Defence and Education (2011) *Civīlā Aizsardzība / Civil Protection Procedure*. Methodological material for general and professional education institutions. Valsts izglītības satura centrs: 2011.  
[https://registri.visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/civila\\_aizsardziba.pdf](https://registri.visc.gov.lv/vispizglitiba/saturs/dokumenti/metmat/civila_aizsardziba.pdf)  
[Accessed on 31.01.2018]
120. Ministry of Defence of Latvia (2014) *Latvijas kiberdrošības stratēģija 2014 –2018 (Cyber Security Strategy of Latvia 2014-2018)*. [https://ccdcoe.org/uploads/2018/10/Latvia\\_Cyber-Security-Strategy-2014-2018\\_original.pdf](https://ccdcoe.org/uploads/2018/10/Latvia_Cyber-Security-Strategy-2014-2018_original.pdf) [Accessed on 02.08.2018]
121. Ministry of Defence of Latvia (2019) *Latvijas kiberdrošības stratēģija 2019–2022 (Cyber Security Strategy of Latvia 2019-2022)*.  
<https://www.mod.gov.lv/sites/mod/files/document/kiberstrategija.pdf> [Accessed on 26.08.2020]
122. Ministry of Education and Science of Latvia (2018) *Pārskats par Latvijas augstāko izglītību 2017.gadā, Galvenie statistikas dati (Overview of Latvian Higher Education in 2017, Key Statistics)*. [http://www.izm.gov.lv/images/izglitiba\\_augst/Parskats-par-Latvijas-augstako-izglitibu-2017gada.pdf](http://www.izm.gov.lv/images/izglitiba_augst/Parskats-par-Latvijas-augstako-izglitibu-2017gada.pdf) [Accessed on 27.04.2018]
123. Ministry of Education and Science of Latvia (2019) *Studiju programmas 2019 (Study Programmes 2019)*. <https://www.izm.gov.lv/lv/media/2128/download> [Accessed on 11.05.2021]
124. Moldovan L. (2012) Integration of Strategic Management and Quality Assurance in the Romanian Higher Education. *Procedia - Social and Behavioral Sciences, Vol. 58 (2012), pp. 1458-1465*. DOI: <http://doi.org/10.1016/j.sbspro.2012.09.1132> [Accessed on 08.05.2018]
125. Morris, V.E. (2007) *URMIA White Paper: ERM in Higher Education*. Bloomington, IN: University Risk Management and Insurance Association.  
<https://www.odu.edu/content/dam/odu/offices/risk-management/DOCS/erm-urmia-white-paper.pdf> [Accessed on 09.05.2018]
126. Morrison T. (2018) GDPR: Impact on the education sector. *UK Association of Colleges* [Series of Workshops] Rollits LLP: UK.  
<https://www.aoc.co.uk/sites/default/files/Rollits%20GDPR%20Session%20080218.pdf>  
[Accessed on 21.04.2018]
127. Murphy, K.L. (2015) Assessing Risk Management: How Effective Is Your Program? *Journal of Physical Education, Recreation & Dance, v.86, n.3, p.32-36*. DOI: <http://dx.doi.org/10.1080/07303084.2014.998392> [Accessed on 14.07.2020]

128. Murphy, K. L., Donovan, J. B., Berg, D. A. (2016) Analysis of Risk Management in Adapted Physical Education Textbooks. *Physical Educator, Spring 2016*, Vol. 73, Issue 2, p. 388-414; ISSN-0031-8981. <http://dx.doi.org/10.18666/TPE-2017-V74-I1-6441> [Accessed on 12.07.2020]
129. National Association of College and University Business Officers [NACUBO] and the Association of Governing Boards of Universities and Colleges [AGB] (2007) Meeting the Challenges of Enterprise Risk Management in Higher Education. Washington, DC: summit on Enterprise Risk Management.
130. Patrinos, H. A., Kagia, R (2007) Maximizing the Performance of Education Systems. *Series: In: "Campos, J. Edgardo; Pradhan, Sanjay (Ed.). The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level"*, pp. 63-86 Washington, DC: The World Bank. Accessed at <https://etico.iiep.unesco.org/en/resource/maximizing-performance-education-systems-case-teacher-absenteeism> [Accessed on 15.05.2017]
131. Pattanajureepan, P., Sirisuthi, C., Ieamvijarn, S. (2014) Development of Risk Management System in Private School General Education. *Asian Social Science; Vol. 10, No. 1*; Published by Canadian Center of Science and Education. DOI: 10.5539/ass.v10n1p276 [Accessed on 02.08.2018]
132. Pelletier, S. (2012) New Strategies for Managing Risks: A Balancing Act for Boards, *Trusteeship, v.20, n.1, p.14-19, January -Febryary 2012*. ERIC database.
133. Perera, A.A.S., Rahmat A.K., Khatibi A., Azam, S.M.F. (2020) Review of Literature: Implementation of Enterprise Risk Management into Higher Education. *International Journal of Education and Research, Vol. 8, No. 10, October 2020*. <https://www.ijern.com/journal/2020/October-2020/14.pdf> [Accessed on 14.05.2021]
134. Petroni, A. (1999) Mapping the Diffusion of Advanced Risk Management Practices Among Italian Small- and Medium-Sized Firms. *Risk Management and Insurance Review. V. 2, Issue 3, September 1999, pp. 125-140*. DOI: <https://doi.org/10.1111/j.1540-6296.1999.tb00007.x> [Accessed on 30.08.2020]
135. Pettere, G., Voronova, I. (2004) *Riski uzņēmējdarbībā un to vadība*, Mācību līdzeklis. Rīga: Banku augstskola.
136. Pierce, D. (2019) Risk and Reward. *Community College Journal, v.89, n.4, p.16-21, February - March 2019*. [https://www.ccjournal-digital.com/ccjournal/june\\_july\\_2021/MobilePagedReplica.action?pm=2&folio=Cover#pg1](https://www.ccjournal-digital.com/ccjournal/june_july_2021/MobilePagedReplica.action?pm=2&folio=Cover#pg1) [Accessed on 14.07.2021]
137. PKF UK LLP (2011) *A Good Practice Guide to Risk Management Within the Further Education Sector*, London: PKF (UK) LLP;

- [https://www.aoc.co.uk/sites/default/files/CFDG\\_Risk\\_Management\\_Guide\\_0.pdf](https://www.aoc.co.uk/sites/default/files/CFDG_Risk_Management_Guide_0.pdf) [Accessed on 15.05.2018]
138. Porthin, M. (2004) *Advanced Case Studies in Risk Management*. Helsinki University of Technology. Master's degree thesis, Espoo, 4 August 2004. [https://www.academia.edu/27667499/Markus\\_Porthin\\_Advanced\\_Case\\_Studies\\_in\\_Risk\\_Management](https://www.academia.edu/27667499/Markus_Porthin_Advanced_Case_Studies_in_Risk_Management) [Accessed on 05.09.2018]
139. Pouls, C., Jeandarme, I. (2015) Risk Assessment and Risk Management in Offenders with Intellectual Disabilities: Are We There Yet? *Journal of Mental Health Research in Intellectual Disabilities*, v.8, n.3-4, p.213-236. DOI: <http://dx.doi.org/10.1080/19315864.2015.1070221> [Accessed at 24.11.2018]
140. Puntervold, H. A. (2017) *Reputation Management in Higher Education Institutions: A Comparative Analysis of Public and Private, Norwegian and American Higher Education Institutions* (Master Dissertation, University of Oslo). <https://www.duo.uio.no/bitstream/handle/10852/57614/Masteroppgave-av-Hanne-A--Puntervold.pdf?sequence=1> [Accessed on 14.05.2021]
141. Purdy, G. (2010) ISO 31000:2009 – Setting a New Standard for Risk Management. *Risk Analysis*, V. 30 (6), pp. 881–886. DOI: <https://doi.org/10.1111/j.1539-6924.2010.01442.x> [Accessed on 05.05.2018]
142. PwC (2021) *Managing risk in higher education*. <https://www.pwc.co.uk/government-public-sector/education/documents/higher-education-sector-risk-profile-2021.pdf> [Accessed on 4.07.2021]
143. Raban, C., Turner L.C. (2006) Quality risk management. *Modernising the architecture of quality assurance, Perspectives: Policy and Practice in Higher Education, Vol. 10 (2)*, pp. 39-44. DOI: <http://dx.doi.org/10.1080/13603100600644522> [Accessed on 05.05.2018]
144. Ravelo, J. L. (2012) *30% of aid lost to corruption – Ban Ki Moon*. Devex News, 10 July. <https://www.devex.com/news/30-percent-of-aid-lost-to-corruption-ban-ki-moon-78643> [Accessed on 10.04.2017]
145. Reamer, F. G. (2013) Social Work in a Digital Age: Ethical and Risk Management Challenges. *Social Work*, v.58, n.2, p. 163-172, April 2013. DOI: <http://dx.doi.org/10.1093/sw/swt003> [Accessed at 25.11.2018]
146. Rhodes, G. (2014) Risk Management for Study Abroad Programs: Issues and Resources to Inform Program Development, Administration, and Training. *New Directions for Student Services*, n.146, p. 41-50, Summer 2014. ISSN: ISSN-0164-7970. DOI: <http://dx.doi.org/10.1002/ss.20089> [Accessed on 05.05.2018]

147. Riskrecon (2018) *Third-Party SecurityRisk Management Playbook*. Q1 2018  
[www.thirdpartyplaybook.com](http://www.thirdpartyplaybook.com). <https://22dyr93oemmu1f89w73y1wlh-wpengine.netdna-ssl.com/wp-content/uploads/2020/04/RR-Playbook-Detail-2018-q1.pdf> [Accessed on 14.05.2021]
148. Ross., K., Levacic, R. (1999) *Needs-based resource allocation in education via formula funding of schools*. UNESCO International Institute for Educational Planning.  
<http://www.iiep.unesco.org/en/publication/needs-based-resource-allocation-education-formula-funding-schools> [Accessed on 18.05.2017]
149. Rubino, M. (2018) Comparison of the Main ERM Frameworks: How Limitations and Weaknesses can be Overcome Implementing IT Governance. *International Journal of Business and Management*, Vol. 13, No. 12, pp. 203-214. DOI:10.5539/ijbm.v13n12p203 [Accessed on 19.09.2020]
150. Scheer, D., Benighaus, C., Benighaus, L., Renn, O., Gold, S., Röder, B., Böhl, G-F. (2014) The Distinction Between Risk and Hazard: Understanding and Use in Stakeholder Communication. *Risk Analysis*, Vol. 34 (7), pp. 1270–1285.  
[https://www.academia.edu/17796848/The\\_Distinction\\_Between\\_Risk\\_and\\_Hazard\\_Understanding\\_and\\_Use\\_in\\_Stakeholder\\_Communication](https://www.academia.edu/17796848/The_Distinction_Between_Risk_and_Hazard_Understanding_and_Use_in_Stakeholder_Communication) [Accessed on 04.05.2018]
151. Scherz, P. (2018) Risk, Prudence and Moral Formation in the Laboratory. *Journal of Moral Education*, v.47, n.3, p. 304–315. DOI: <https://doi.org/10.1080/03057240.2017.1406345>. [Accessed on 30.09.2019]
152. Singh, A. (2009) *Improving Information Security Risk Management*. ProQuest LLC, Ph.D. Dissertation, University of Minnesota. ISBN: ISBN-978-1-1095-5859-3.  
<https://www.proquest.com/docview/304941066> [Accessed on 02.02.2017]
153. Slovic, P. (1987) The Perception of Risk, *Science*, Vol. 236, pp. 280-285. DOI:[10.1126/science.3563507](https://doi.org/10.1126/science.3563507) [Accessed on 04.09.2020]
154. Soin K., Collier P. (2013) Risk and risk management in management accounting and control. *Management Accounting Research*, Vol. 24, Issue 2, June 2013, Pages 82-87. DOI: <https://doi.org/10.1016/j.mar.2013.04.003> [Accessed on 17.09.2018]
155. Souto, I., Pereira, A., Brito, E., Sancho, L., Jardim, J. (2018). Psychosocial Risk Factors and Distress in Higher Education Teachers. *The European Proceedings of Social & Behavioural Sciences*, ISSN: 2357-1330.  
[https://www.researchgate.net/publication/325713292\\_Psychosocial\\_Risk\\_Factors\\_and\\_Distress\\_in\\_Higher\\_Education\\_Teachers](https://www.researchgate.net/publication/325713292_Psychosocial_Risk_Factors_and_Distress_in_Higher_Education_Teachers) [Accessed on 02.05.2018]

156. Staender, S. (2011) Incident reporting in anaesthesiology, *Best Practice & Research Clinical Anaesthesiology*, V. 25 (2011), pp. 207–214; Web of Science scientific database.
157. Starr K. (2012) Problematizing ‘Risk’ and the Principals: The Risky Business of Managing Risk in Schools. *Educational Management Administration & Leadership* 40 (4) 464–479. DOI: 10.1177/1741143212438221. [Assessed on 11 May 2018]
158. Stemm, E., Bofinger, C., Cliff, D., Hassall, M.E. (2018) Failure to learn from safety incidents: Status, challenges and opportunities, *Safety Science*, V. 101 (2018), pp. 313–325, Web of Science scientific database.
159. Syreyshchikova N.V., Pimenov D. Yu., Mikolajczyk T., Moldovanc L. (2020) Development of a Risk Management Technique in Strategic Planning of Universities. Case study of a Polytechnical Institute. *Procedia Manufacturing*, Vol. 46, pp. 256-262. DOI: <https://doi.org/10.1016/j.promfg.2020.03.038> [Accessed on 14.05.2021]
160. Taleb, N.N. (2020) *The Black Swan, 2nd Edition*. Колибри: Азбука-Артикус; Черный лебедь. Под знаком непредсказуемости (2-е изд., дополненное) | Талеб Нассим Николас; ISBN 978-5-389-09894-7
161. Tedesco, L., Ing, C. (2021) *Basel Committee issues principles for operational resilience and risk*. Article published in 14th April 2021. <https://www.mccarthy.ca/en/insights/articles/basel-committee-issues-principles-operational-resilience-and-risk> [Accessed on 06.01.2022]
162. Tekathen, M., Dechow, N. (2013) Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case. *Management Accounting Research*, Vol. 24, Issue 2, pp. 100-121. DOI: <https://doi.org/10.1016/j.mar.2013.04.005> [Accessed on 18.09.2018]
163. The Institute of Operational Risk (2010) *Key Risk Indicators*. Operational Risk Sound Practice Guidance. November 2010. <https://www.ior-institute.org/public/IORKRIGuidanceNov2010.pdf>
164. The Institute of Risk Management [IRM] (2002) *The Risk Management Standard*, London: IRM; Retrieved from: [https://www.theirm.org/media/886059/ARMS\\_2002\\_IRM.pdf](https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf) [Accessed on 02.04.2017]
165. The Institute of Risk Management [IRM] (2010) *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO31000*. AIRMIC, Alarm, IRM: 2010. <https://www.ferma.eu/app/uploads/2011/10/a-structured-approach-to-erm.pdf> [Accessed on 06.04.2017]
166. The Institute of Risk Management [IRM] (2012) *Risk Culture: resources for practitioners*. Institute of Risk Management, London. [https://www.treasurers.org/ACTmedia/IRM\\_riskculture\\_full\\_Oct12.pdf](https://www.treasurers.org/ACTmedia/IRM_riskculture_full_Oct12.pdf) [Assessed on 28.10.2022]

167. The Institute of Risk Management [IRM] (2018) *From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks*. Institute of Risk Management, London. <https://www.theirm.org/media/3512521/IRM-Report-Review-of-the-COSO-ERM-frameworks-v2.pdf> [Accessed on 08.05.2019]
168. Toma, S-V., Alexa I.V., Sarpe, D.A. (2014) Identifying the Risk in Higher Education Institutions. *Procedia Economics and Finance*, Vol. 15, pp. 342-349. DOI: [https://doi.org/10.1016/S2212-5671\(14\)00520-6](https://doi.org/10.1016/S2212-5671(14)00520-6) [Accessed on 14.05.2021]
169. Transparency International (2013) *Global corruption report: Education*. Available at: [https://images.transparencycdn.org/images/2013\\_GCR\\_Education\\_EN.pdf](https://images.transparencycdn.org/images/2013_GCR_Education_EN.pdf) [Accessed on 18.05.2017]
170. Trinite, B. (2016). Epidemiology of Voice Disorders in Latvian School Teachers. *Journal of Voice*, Vol. 31, No. 4, pp. 508.e1–508.e9. DOI: <http://dx.doi.org/10.1016/j.jvoice.2016.10.014>
171. Tufano, P. (2011) *Managing Risk in Higher Education*. Forum for the Future of Higher Education, 2011. <http://forum.mit.edu/wp-content/uploads/2017/05/FF11ManagRisk.pdf> [Accessed on 23.03.2020]
172. TVNET/LETA (2020) *Neveiksmīgu attālināto mācību gadījumā tiks pagarināts brīvlaiks un mācību gads (In case of unsuccessful distance learning, the free time and the academic year will be extended)*. News of Latvia, 13.03.2020. <https://www.tvnet.lv/6922402/neveiksmigu-attalinato-macibu-gadijuma-tiks-pagarinats-brivlaiks-un-macibu-gads> [Accessed on 06.01.2022]
173. U4 Anti-Corruption Resource Center (2006) *Corruption in the Education Sector*. U4: Bergen. [www.U4.no/themes/education](http://www.U4.no/themes/education) [Accessed on 05.05.2017]
174. UNESCO (2017) *Accountability in education: Meeting our commitments*. Global Education Monitoring Report 2017/2018. <https://gem-report-2017.unesco.org/wp-content/uploads/2017/10/2017-GEM-Report-Statistical-Tables.pdf> [Accessed on 18.03.2019]
175. UNICEF (2021) *Education under attack. The safe schools declaration*. Available at: <https://www.unicef.org/education-under-attack> [Accessed on 06.01.2022]
176. Vaduguns (2021) *Esmu negatīvs! (I am negative!)* Northern Latgale Newspaper, Media Support Fund project, 24.09.2021. [http://vaduguns.lv/index.php?option=com\\_content&view=article&id=6844:esmu-negativs-24-09-2021&catid=171&Itemid=844](http://vaduguns.lv/index.php?option=com_content&view=article&id=6844:esmu-negativs-24-09-2021&catid=171&Itemid=844) [Accessed on 06.01.2022]
177. Valsts Izglītības Centrs (2021) *Mācību procesa pilnveides atbalsts. Metodiskie ieteikumi pārmaiņu vadītājiem un īstenotājiem skolā (Support for the improvement of the learning process. Methodological recommendations for change managers and implementers at schools)*. ESF

- Skola 2030 Project. ISBN 978-9934-24-034-8. <https://mape.skola2030.lv/resources/5949>  
[Accessed on 06.01.2022]
178. Vollmer, S. (2015) *6 steps to manage risks and drive performance*. CGMA Magazine. <https://www.fm-magazine.com/news/2015/oct/manage-risks-drive-performance-201513224.html> [Accessed on 02.02.2018]
179. Waite, D., Allen, D. (2003) Corruption and abuse of power in educational administration. *Urban Review Vol. 35 (4) pp. 281–96*. DOI: [10.1023/B:URRE.0000017531.73129.4F](https://doi.org/10.1023/B:URRE.0000017531.73129.4F) [Accessed at 08.10.2018]
180. Waithe, E. (2016) *An Analysis of Enterprise Risk Management and IT Effectiveness Constructs*. ProQuest Dissertations Publishing, 2016. <https://www.proquest.com/docview/1868415505>  
[Accessed on 17.07.2021]
181. Wales, J., Magee, A., Nicolai, S. (2016) *How does political context shape education reforms and their success? Lessons from the Development Progress project*. Dimension Paper 6. London: Overseas Development Institute. <https://cdn.odi.org/media/documents/10808.pdf> [Accessed on 18.03.2019]
182. Walker, R. (2013) *Winning with Risk Management, Chapters 1-5*, World Scientific Publishing Co. Pte. Ltd.: Singapore
183. Wandee, M., Sirisuthi, C., Leamvijarn, S. (2017) The Study Elements and Indicators of Risk Management System for Secondary Schools in Thailand. *International Education Studies; Vol. 10, No. 3; 2017*. ISSN 1913-9020 E-ISSN 1913-9039. DOI: <https://doi.org/10.5539/ies.v10n3p154> [Accessed on 05.05.2018]
184. Washburn J. (2005) *University Inc: The Corporate Corruption of Higher Education*. New York: Basic Books. ISBN: 978-0465090518.
185. Wessels, J.S., Sadler, E. (2015) Risk management in higher education: An open distance learning perspective. *Southern African Business Review Special Edition Accounting Research* 2015, pp. 74-98. DOI: <https://doi.org/10.25159/1998-8125/5807> [Accessed on 30.08.2020]
186. Westhuizen, J., Stanz, K. (2017) Critical incident reporting systems: A necessary multilevel understanding, *Safety Science, V. 96* (2017), pp. 198–208, Web of Science scientific database.
187. Wheeler B. (2017) GDPR: Do you really need a Data Protection Officer (DPO)? *Ascentor Online Journal*. Gloucester: UK. <http://www.ascentor.co.uk/2017/06/gdpr-data-protection-officer-dpo/> [Accessed on 14.01.2018]
188. Whitney, S.N. (2016) Institutional Review Boards: A Flawed System of Risk Management. *Research Ethics, v.12, n.4, p.182-200, October 2016*. DOI: <http://dx.doi.org/10.1177/1747016116649993> [Accessed on 12.07.2020]

189. World Bank (2019) *The Changing Nature of Work*. World Development Report 2019. International Bank for Reconstruction and Development: Washington. ISBN: 978-1-4648-1328-3. <https://documents1.worldbank.org/curated/en/816281518818814423/pdf/2019-WDR-Report.pdf> [Accessed on 25.10.2022]
190. Yokoyama, K. (2018) The Rise of Risk Management in the Universities: A New Way to Understand Quality in University Management. *Quality in Higher Education*, v. 24, n.1, p.3-18. DOI: <http://dx.doi.org/10.1080/13600869.2018.1425080> [Accessed at 12.07.2020]
191. Zeinab A. (2016) Quantification of Operational Risk: A Scenario-Based Approach, *North American Actuarial Journal*, DOI: <https://doi.org/10.1080/10920277.2016.1176581> [Accessed on 07.05.2021]
192. Захаров Н. Ю., Ильина Т. С. (2016) *Количественный анализ рисков образовательных учреждений высшего образования*. Российская научно-техническая конференция, приуроченная ко Дню радио «Обработка информации и математическое моделирование». Новосибирск: СибГУТИ, 2016. <https://docplayer.ru/46037893-Kolichestvennyy-analiz-riskov-obrazovatelnyh-uchrezhdeniy-vysshego-obrazovaniya.html> [Accessed on 12.09.2018]
193. Захаров Н. Ю., Ильина Т. С. (2016) *Управление образовательными рисками / Educational risks management*. Вестник ВГУИТ/Proceedings of VSUET, No 4, 2016. DOI: <http://doi.org/10.20914/2310-1202-2016-4-290-295> [Accessed on 12.09.2018]
194. Корнейчук, В. И. (2011) *Организация управления операционным риском, связанным с деятельностью персонала, в кредитной организации / Organisation of operational risk management related to personnel activity in a credit institution*. Журнал Финансы и Кредит/Journal Finance and Credit, 12 (444) - 2011. <https://cyberleninka.ru/article/n/organizatsiya-upravleniya-operatsionnym-riskom-svyazannym-s-deyatelnostyu-personala-v-kreditnoy-organizatsii> [Accessed on 02.07.2020]



## APPENDIX 1: RISK MANAGEMENT PLAN

**Table 4.1 Risk management plan for educational institutions (developed by author according to theoretical research results, details described in Sections 1 and 2)**

<b>Activity</b>	<b>Frequency</b>
Strategy planning and material risk identification, setting of acceptable level of risk	Annual
Risks and controls self-assessment	Annual
Scenario analysis and mitigation action planning	Annual
Crisis and Business Continuity Planning	Annual
Incident reporting, analysis, incident data collection	Continuous, daily
Risk assessments related to changes (regulatory, political, internal)	On ad-hoc basis
Setting and reviewing of Key Risk Indicators	Annual
Monitoring Key Risk Indicators	Continuous (daily, weekly, monthly, quarterly, year-on-year)
External loss data collection	Monthly
Risk reporting	Monthly, quarterly
Review of internal documentation	Annual
Third-party risk assessment	Annual

## APPENDIX 2: RISK ASSESSMENT REGISTER

Table 5.1 Risk assessment register's example (developed by author according to theoretical research detailed in Section 1)

Risk scenario detailed description	Root cause	Probability assessment	Impact assessment	Risk importance (probability *impact)	Risk response	Mitigation action, responsible and deadline	Status of risk and mitigation actions
<i>Due to overload teachers will take a lot of sick leave simultaneously and as a result there will be not enough personnel to ensure continuity of all lessons for pupils.</i>	<i>External: insufficient funding</i>	<i>Highly probable (4)</i>	<i>Major (3)</i>	<i>Very high (12)</i>	<i>Mitigate</i>	<i>Develop motivation plan, review spending and allocate budget for well-being of teachers, develop well-being plan with minimum financial investments needed. Responsible: headteacher's deputy Deadline: 30 September 2021</i>	<i>Not started/ In progress / Done</i>
<i>Due to flu epidemic school will be closed for quarantine in the mid of the academic year</i>	<i>External: flu epidemic</i>	<i>Low (2)</i>	<i>Moderate (2)</i>	<i>Low (4)</i>	<i>Accept</i>	<i>N/A</i>	<i>N/A</i>

### APPENDIX 3: INCIDENT REGISTER

Table 6.1 Incident register's example (developed by author according to theoretical research detailed in Section 1)

Incident ID	Registration Date	Discovery date	Description	Root cause	How it was discovered	Consequences, losses	Mitigation actions	Status (open/closed)
<i>Unique incident ID number</i>	<i>When incident was reported</i>	<i>When incident was discovered</i>	<i>What, how and why happened</i>	<i>What caused the incident</i>	<i>How it was found out</i>	<i>Losses in EUR or other consequences</i>	<i>What can be done to prevent this in future?</i>	<i>Close when all details are clear about consequences</i>

## APPENDIX 4: RISK TAXONOMY

**Table 7.1 Registry of risks, causes and examples of mitigation actions for educational sector (developed by author according to theoretical and empirical research results)**

<b>Risk category</b>	<b>Risk type</b>	<b>Risk sub-type</b>	<b>Cause</b>	<b>Examples of risk mitigation</b>
Environmental	Terrorist attack	Mass shooting	External	Crisis management planning
		Bombing		
		Kidnapping		
		Mass capturing		
	Disasters	Fire	Human neglect / External factors	Crisis management and business continuity planning
		Flood		
		Nature disaster		
	Pandemic, epidemic, etc.	Pandemic	External	Crisis management and business continuity planning
		Epidemic		
	School internal environment	Poor air quality	Inadequate processes / Personnel neglect / Corruption	Internal procedures and controls, emergency action plans, safety rules, appropriate equipment, inventories of equipment and facilities, activities conducted away from hazardous areas, supervision of students, communication and posting of guidelines for emergency actions plans and emergency exit procedures, certification of responsible employees.
		Danger to health and life due to unstable constructions		
		Drugs on site		
		Classroom safety issues		
Poor organisational design of work				
Problematic evacuation from the building				

**Table 7.1:** continuation

	Food provision	Poor food quality	Inadequate processes / Personnel neglect / Corruption / External	Internal procedures and controls, regular food quality checks, risk assessment and due diligence of food suppliers and/or employees responsible for food supplies.
		Food not available at school		
Psychosocial	Staff burn-out	Lack of resources caused overload	Funding / Inadequate processes / External requirements	Planning of resource usage, lesson plans, curriculum guidelines, lesson objectives, appropriate equipment, activities conducted away from hazardous areas, certification of teachers, constant communication and supervision of processes, internal procedures and controls, monitoring of key risk indicators.
		Losing of key employee		
		Implementation of reform in education		
		Change of methodologies in teaching		
		Underperformance		
	Lack of employee motivation	Inadequate salaries	Funding / Inadequate internal processes / External requirements / Managerial neglect	
		Inadequate internal environment		
		Agressive internal culture and attitudes		
		Problems with parents		
		Overload, increasing job demands		
		Underperformance		
		Insufficient information exchange		
		Unfavourable working conditions and organisational design of work		
	Employees' health problems due to stress	Long-term sick leave		
		Compensation for health problems		
Physical disorders				

**Table 7.1:** continuation

		Psychological disorders		
	Human errors	Documentation mistakes	Personnel	Four eyes principle, documented procedures and instructions, monitoring of key risk indicators.
		Missed documentation		
		Not achieving planned objectives		
Technological	Information Security	Confidential data leak	Personnel neglect / Inadequate internal procedures / External fraud	Documented guidelines and rules, controls, four eyes principle, constant training and communication of requirements, auditing, anti-virus software, cyber protection systems, crisis management and business continuity planning.
		Personal data breach		
		Breach of information security requirements		
		Cyberattack		
	Telecommunications and utilities	Electricity power failure	External / Systems	Crisis management and business continuity planning
		Internet unavailable		
		Telephone connection not working		
	Information Systems	Disruptions in IT systems	Systems	Crisis management and business continuity planning
		IT systems's downtime		
	Ethical	Corruption	Bribery and extortion	Personnel
Lobbying				
Violent behaviours		Bullying		
		Mobbing		
		Damage to physical assets		
		Damage to health of employee		
Internal fraud		Damage to health of student		
		Theft		
	Fraud			
Legal	Third-party risks	Failure in supply management	External	

**Table 7.1:** continuation

		Vendor exits contract		Internal procedures and controls, regular checks, risk assessment and due diligence of suppliers, monitoring of key risk indicators.
	Employment practices	Sudden death of employee	Inadequate processes / Personnel neglect / Corruption	Documented internal procedures and controls, emergency action plans, crisis planning, safety rules, appropriate equipment and work design, activities conducted away from hazardous areas, supervision of students, communication and posting of guidelines for emergency actions plans and emergency exit procedures, certification of responsible employees, planning continuous training for staff, monitoring of regulatory requirements, co-operation with regulatory authorities, due diligence of suppliers, independent auditing of internal procedures.
		Injury		
		Inadequate employment practices		
		Inadequate recruitment practices		
	Regulatory	Non-compliance with regulatory requirements		
		Accreditation failure		
	Lack of competence	Incompetent employee		
		New educational programme introduction failure		
		Inadequate strategic decision-making		
		Lack of qualified teaching staff		
	Students' health and safety	Sudden death of student		
		Injury		
		Poisoning		
Problematic evacuation from the building				
Political	Educational reforms	Educational reforms	External	Crisis and business continuity planning, risk assessment
Economic	Funding	Insufficient funding	External	Crisis and business continuity planning
	Budget allocation	Inadequate budget allocation	Personnel / Processes	Training of responsible employees, consultations with experts
Social	Powerty	Missing school	External	

**Table 7.1:** continuation

		Inability to buy school necessities		
		Hygiene problems		
		Problems with learning		
	Discrimination	Social justice issues	Inadequate internal processes	
		Gender inequality		
	Teen pregnancy and parenting	Student pregnancy	External	Documented internal rules and guidelines, co-operation and constant communication with parents, social services and police, crisis and business continuity planning, special arrangements for students with problems.
		Student who is a parent		
	Achievement demotivation	Drop-Outs		
		Repeating school year		
		Failure to pass academic year		
	Domestic violence	Psychological disorders		
		Physical injuries and disorders		
		Violent behaviour		
		Missing school and dropouts		
	Serious illnesses and health issues	Missing school and dropouts		
	Suicide	Student suicide		
		Employee suicide		
		Suicide on school's premises		
	Behaviour of parents	Violent behaviour of parents		
		Unsupportive behaviour of parents		
Cultural	Cultural differences	Culture specific traditions	External	Documented internal procedures and controls, internal behaviour and safety rules, supervision of students, communication and posting of guidelines for students and employees.
		Misbehaviour due to culture		
		Bullying and mobbing		



## APPENDIX 5: BUSINESS CONTINUITY PLAN

**Table 8.1 Example of Business Continuity and Resiliency Plan (developed by author based on theoretical research results)**

Scenario	Actions	Key contact people	Phone numbers
<i>Extreme risk scenario</i>	<i>Description of relevant actions</i>	<i>List of names of the main decision-makers and responsible people for each scenario and their phone numbers</i>	
1. Fire			
2. Floods			
3. Terrorist attack			
4. Extreme weather			
5. Cyber attack			
6. Cyber attack, IT downtimes			
7. War			
8. Pandemic/epidemic			
9. Civil strikes			
10. Lack of communication channels due to national threat or military attack			

## APPENDIX 6: EMPIRICAL RESEARCH SURVEY 1

### Risk Management in the Sector of Education

#### Scientific Research Survey 1

*Terms used in the survey:*

**Risk** - the probability of suffering a loss from an adverse event.

**Risk management** - a set of technical, organizational, legal methods and measures aimed at reducing the probability and consequences of adverse events.

**Incident** - an event that can cause losses, system or process outages, disruptions, emergencies, crises or disasters.

---

1. What is your connection with the sector of education?
  - a. Head or deputy head of an educational institution
  - b. Teacher / lecturer in an educational institution
  - c. Nanny, teacher's assistant or learning support function
  - d. Employee of an educational institution
  - e. The child's parent
  - f. Other (please specify) \_\_\_\_\_
  
2. To which type of educational institution do you have a relation?
  - a. Pre-school educational institution (kindergarten)
  - b. School (Primary or Secondary school from 1st grade)
  - c. College, gymnasium or high school (7th or 10th grade)
  - d. University, Technical school, Vocational education
  - e. University

f. Other (please specify) \_\_\_\_\_

3. On the scale from 0 to 6 please rate the effectiveness of risk management in your educational institution? (0 – very poor, 6– very strong, e.g., risk management tools are commonly used, such as risk assessments, incident reporting, etc.)

---

4. Who do you think is responsible for risks and risk management in educational institutions?

---

---

5. Is it common in the educational institution, to which you belong to, to register incidents in the internal register?

a. Yes

b. No

c. I do not know

d. Other: \_\_\_\_\_

6. Please rate the risks below by significance for your organisation using the following scale:

Risk importance

- 1 Risk is not at all significant
- 2 Risks is neutral
- 3 Risk is slightly significant
- 4 Risk is very significant
- 5 Risk is critical

Risk management effectiveness

- 1 Risk is not managed at all
- 2 Risk is very poorly managed
- 3 Risk is managed as much as possible
- 4 Risk is well managed
- 5 Risk is managed to the highest standards

Nr.	Risk description	Importance	Management effectiveness
1	Lack of qualified teaching staff		
2	Lack of staff motivation		
3	Weak internal risk culture		
4	Overloading of employees		
5	Lack of effective planning causing losses in terms of time and money		
6	Insufficient pool of applicants		
7	Inadequate level of quality of education provided		
8	Lack of documented internal processes		
9	Inability to meet modern requirements in teaching and application of technologies		
10	Information Security risk for limited accessibility information		
11	Privacy risk		
12	Cyber security risk		
13	Lack of sufficient funding		
14	Insufficient information exchange and accessibility		
15	Changes in the market and external environment		
16	Increase of cost for educational services		
17	Inadequate strategic decision making		
18	Ineffective budget allocation		
19	Dependency of external vendors; vendor unethical behaviour; vendor delivery failure		
20	Corruption		
21	Violence and bullying inside the organisation		
22	Parent unethical/incompliant behaviour		
23	Poor internal health and safety management		
24	Inability to meet employment law requirements, poor work environment		
25	Dependency on technology		
26	Inappropriate educational programmes not meeting regulatory requirements		
27	Termination of accreditation for existing education programmes in the nearest future		
28	Closure of educational institution for any reason		
29	Catastrophe risk (fire, explosion, building structure damages and collapses, floods, etc.)		
30	Unethical behaviour, incl. theft, of employees, incl. teaching staff		
31	Change of legislation		
32	Changes of political governance		

Other risks (please list):

---

7. What in your opinion is needed to better manage risks in the sector of education?

---

8. Does your educational institution use insurance services? (If known)

If yes, what does it include? In percentage terms, how much budget share is allocated to insurance? (If known)

---

## APPENDIX 7: EMPIRICAL RESEARCH SURVEY 2

### Risk Management in the Sector of Education

#### Scientific Research Survey 2

Additional questions about risk management in the educational institutions.

1. Do you think it is important to manage risks and develop risk management programmes for educational institutions?

---

2. “According to the survey, the most critical risks in the education sector in Latvia are:

*1. Employee overload (average 4 points out of 5)*

*2. Insufficient funding (average 3.8 points out of 5)*

*3. Lack of employee motivation (average 3.5 points out of 5)*

*4. Lack of qualified staff (average 3.5 points out of 5)*

*5. Wrong strategic decision making (average 3.5 points out of 5)*

*6. Changes in the political environment/legislation (average 3.4 points out of 5)*

In your opinion, what are the consequences of each of these risks or can they cause? (e.g., financial terms, reputation, etc.)”

---

3. How the above-mentioned consequences of the most topical risks could be reduced or eliminated, in your opinion? How the above risks can be most effectively managed?

---

4. Please indicate what is your connection with the education sector?

- a. Head or deputy head of an educational institution
- b. Teacher / lecturer in an educational institution
- c. Nanny or learning support function performing employee
- d. Employee of an educational institution
- e. Parent of the child
- f. Interest education
- g. Other

5. Please indicate which type of educational institution you represent?

- a. Preschool educational institution (kindergarten)
- b. School (Primary, Primary or Secondary School from 1st grade)
- c. College, gymnasium or high school (7th or 10th grade)
- d. University, Technical school, Vocational education
- e. Education of interests
- f. University
- g. Other