Ville Pusa

Changes in Risk Management on Financial Sector After February 2022

Changes and drivers for changes in risk management on financial sector after Russia's full-scale invasion of Ukraine

School of Management
Strategic Business Development
Master of Science in Economics and
Business Administration

Vaasa 2026

UNIVERSITY OF VAASA
School of Management
Author: Ville Pusa
Title of the thesis: Changes in Risk Management on Financial Sector After February 2022: Changes and drivers for changes in risk management on financial sector after Russia's full-scale invasion of Ukraine
Degree: Master of Science in Economics and Business Administration
Degree Programme: Master's Degree Programme in Strategic Business Management
Supervisor: Sniazhana Diduc
Year: 2026 **Pages:** 81

ABSTRACT:

Tämän pro gradu -tutkielman tarkoituksena on tarkastella, miten riskienhallinnan käytännöt ovat muuttuneet Euroopan finanssisektorilla Venäjän helmikuussa 2022 aloittaman täysimittaisen hyökkäyssodan jälkeen. Tutkimus keskittyy erityisesti suomalaisiin finanssialan toimijoihin ja siihen, miten sodan aiheuttama geopoliittinen epävarmuus on vaikuttanut riskienhallinnan painopisteisiin, prosesseihin ja toimintatapoihin. Tutkimuksen tavoitteena on selvittää, millaisia muutoksia finanssialan riskienhallinnassa on havaittu vuoden 2022 jälkeen ja mitä kanavia pitkin merkittävimmät muutokset ovat syntyneet.

Tutkielman teoreettinen viitekehys perustuu yritysten kokonaisvaltaiseen riskienhallintaan, institutionaaliseen teoriaan ja organisaatioiden resilienssiin. Näkökulmien avulla geopoliittista riskiä tarkastellaan sekä ulkoisena toimintaympäristön muutoksena että tekijänä, joka voi välittyä finanssialan organisaatioihin olemassa olevien riskialueiden kautta. Tutkimus toteutettiin laadullisena tutkimuksena, ja empiirinen aineisto kerättiin viidellä anonymisoidulla puolistrukturoidulla asiantuntijahaastattelulla. Haastateltavat työskentelivät suomalaisissa finanssialan organisaatioissa riskienhallintaan liittyvissä tehtävissä. Aineisto analysoitiin temaattisen analyysin avulla.

Tutkimuksen tulokset osoittavat, että riskienhallinta on muuttunut helmikuun 2022 jälkeen, mutta muutos ei ole ollut tasainen kaikilla riskialueilla. Selkeimmät muutokset liittyivät pakotteiden noudattamiseen, talousrikollisuuden torjuntaan, asiakasriskien hallintaan, operatiiviseen resilienssiin, kyberriskeihin, ulkoistamiseen, turvallisuuteen sekä raportointiin. Erityisesti Venäjään ja Valko-Venäjään kohdistuneet pakotteet edellyttivät finanssialan toimijoilta nopeita prosessimuutoksia sekä aikaisempaa tarkempaa seurantaa. Myös operatiivisen riskienhallinnan merkitys kasvoi, sillä geopoliittinen tilanne lisäsi huomiota kyberturvallisuuteen, jatkuvuussuunnitteluun, ulkoisiin palveluntarjoajiin ja kriisivalmiuteen.

Perinteisten finanssiriskien, kuten markkina-, luotto-, likviditeetti- ja pääomariskien, osalta tutkimus ei osoita yhtä merkittävää muutosta riskienhallinnan prosesseissa. Näillä alueilla olemassa olevien työkalujen ja prosessien katsottiin olleen pääosin valmiita muutoksiin, mutta seurannan ja raportoinnin merkitys kasvoi muuttuneessa toimintaympäristössä. Tutkimuksen perusteella sota toimi ennemmin tiettyjä riskienhallinnan osa-alueita kiihdyttäneenä ja vahvistaneena tekijänä, kuin koko finanssisektorin riskienhallinnan uudistajana.

Tutkielma täydentää aiempaa tutkimusta osoittamalla, miten geopoliittinen riski välittyy finanssialan sisäisiin riskienhallinnan käytäntöihin. Käytännön näkökulmasta tulokset korostavat seurannan, raportoinnin, pakotevalvonnan ja operatiivisen resilienssin merkitystä geopoliittisesti epävarmassa toimintaympäristössä. Tutkimuksen tuloksia tulee kuitenkin tulkita laadullisina havaintoina, sillä aineisto perustuu viiteen asiantuntijahaastatteluun.

KEYWORDS: Risk management, Geopolitical risk, Financial sector, Financial institutions, Wartime uncertainty, Operational resilience, Sanctions compliance

Contents

1 Introduction

Armed conflicts have historically caused major disruptions to economic and financial systems (Caldara & Iacoviello, 2022). Unlike normal cyclical downturns or financial crises, wartime conditions introduce abrupt geopolitical uncertainty, political fragmentation and unseen changes in financial systems (European Central Bank, 2022; Caldara & Iacoviello, 2022). Conflicts change expectations, forces policy changes, disrupts financial infrastructure, and reshapes international economic relations, thereby creating a situation that challenge conventional financial risk management frameworks (European Central Bank, 2022). The re-emergence of large-scale conflict in Europe has disrupted the long-standing assumptions of financial integration, financial liberalism and geopolitical stability that have been the major direction since the fall of the Soviet Union and the end of cold war.

Europe's financial sector is especially exposed to conflict era disruptions due to the high level of financial and political integration between European states (European Central bank, 2024). Over the last two decades, the European Union's financial integration has been backed up by EU's regulatory synchronization, monetary union, and while the geopolitical risk was less central in financial sector (European Central bank, 2024). The conditions allowed financial institutions to operate over national borders using risk models characterised by predictable policy and political stability. Wartime conditions in Europe fundamentally changed the nature of business environment and therefore risk conditions from predictable to uncertain (European Central Bank, 2022).

From a financial perspective, the war introduced multiple connected risks not seen in Europe in the last two decades (European Central Bank, 2022). Market risks increased sharply as asset prices reacted to new wartime conditions, sanctions, and shifts in investor and corporate sentiment. Credit risk can increase as corporations and households face higher input costs, disrupted supply chains, and declining economic activity. Liquidity risk may increase due to the changed sentiment of market participants and policy driven market fragmentation. Wartime shifts also intensify less quantifiable risks,

including geopolitical risk, compliance risk, cyber risk, and operational risk associated with critical infrastructure.

Risk management, especially on financial sector, has been characterised by using historical data to create models and stress testing frameworks to capture adverse but plausible scenarios (Basel Committee on Banking Supervision, 2009). While risk management tools have changed along the years due to financial crises such as 2008, the models generally assume geopolitical stability and functioning markets. Wartime however changes these assumptions by introducing non-market variables that are driven by political and security decisions and strategic behaviour of nations. Sanctions, capital controls, and regulatory changes can change financial flows and markets with limited warning time. As large market changes are driven by political decisions during wartime, economic and political risks become more intertwined.

At the institutional level, Europe's financial sector operates with robust regulatory framework shaped by European Central Bank and the European Union, where recent reforms have focused on regulatory harmonizations, ESG risks, ICT risks and anti-money laundering (European Union, 2022; European banking Authority, 2025; Council of the European Union, 2024). However, wartime have caused conditions that differ from normal and stable environment that that the recent reforms are meant for, such as introduction of large-scale sanctions.

Although research on geopolitical risk has expanded in recent years, the existing studies still treat was as a background context rather than a force that actively transforms how financial institutions manage risk and make decisions (Caldara & Iacoviello, 2018). As geopolitical instability becomes a more permanent feature on Europe's landscape (European Central Bank), it is increasingly important to understand how wartime conditions change risk management practices to maintain financial stability.

1.1 Problem area and motivation

Since the end of cold war, the European financial institutions have developed their risk management practises in a relatively stable environment with geopolitical stability and institutional continuity. These practises rely on historical data and assumptions about

market stability, policy predictability, and cross-border financial integration not just in EU but internationally. A large-scale war changes these assumptions. War brings uncertainty and politically driven constrains, such as sanctions, asset freezes, and regulatory interventions and these are changes that European financial institutions have not faced on a large scale.

In this thesis I examine the possible mismatch of existing risk management practises and the realities of wartime conditions. In the last two decades European financial institutions have focused on capital risk practises largely due to the regulatory intervention of the public sector in a response of global financial crisis and European debt crisis. However, these developments have focused on internal vulnerabilities rather than external risks created by geopolitical conflicts. Thus, the existing risk management practices are not well equipped to face the complex external dynamics of wartime changes.

The European regulators have also recognised the need for resilience, with the European Central bank and other EU authorities focusing more on adverse scenarios. However, it remains uncertain how well the current supervisory tools test the resilience that is needed in wartime risk management. Especially considering how the supervision has been on EU member states responsibility with possibly limited resources.

While there is extensive research on financial risk management, the research has been less focused on war as an enduring structural condition influencing financial institutions. Most studies study geopolitical risk at a macroeconomic level, offering little insight to how financial institutions adapt their internal risk practices to meet wartime changes. Understanding this gap is not only vital on a theoretical level, but also for guiding policy and financial institutional decision-making in a time of sustained geopolitical instability.

1.2 Research justification

The academic research of risk management on financial sector has centred on quantitative risk with relatively stable institutional and geopolitical environment. Much of this research focuses on how financial institutions manage market, credit and liquidity risks (Varotto, 2011). Especially after global financial crisis and the following European debt crisis (Basel Committee on Banking Supervision, n.d.). These events prompted far-

reaching reforms in regulation, supervision and governance across Europe and the world. As a result, the research offers a good understanding of how financial institutions handle risks linked to economic volatility and instability.

The academic research on geopolitical risk has also expanded on macroeconomic level (Caldara & Iacoviello, 2018, Hodula et al., 2024). However, the existing research often treats geopolitical changes as broad external shocks rather than examining how financial institutions adapt to these shocks (Hodula et al., 2024, Phan, Tran & Iyke, 2022). While the research offer insight how geopolitical instability shapes economic development and outcomes, it offers only limited insight into financial institutions themselves under war-time conditions.

This has left a clear gap at the intersection of geopolitical risk management and financial risk management. Few studies explore how the wartime changes reshape the internal mechanisms through which financial institutions identify and mitigate risks. In Europe where the financial systems are deeply interconnected within a complex regulatory framework led by European Central bank and other EU institutions but supervised by member states, understanding these changes is especially crucial.

Closing this research gap is important for both theoretical and practical reasons. From a theoretical point of view, examining wartime shifts in risk management provides us a more extensive understanding of how financial institutions respond to politically driven geopolitical uncertainty and to ensuing changes. In practise, understanding these changes can guide regulators, policymakers, and financial institutions in resilience and risk governance decision making processes in an increasingly volatile geopolitical environment. By analysing these wartime shifts within European financial sector, this study aims to bridge the gap between geopolitical risk and institutional risk management practice.

1.3 Research aim questions

The aim of this thesis is to examine how risk management practices and attitudes have changed in European financial institutions after the onset of full-scale Russo-Ukraine War in 2022, and to also assess the main channels through which these changes

occurred. This study considers wartime shifts as structural shifts in the operating environment. The focus will not only be in the traditional financial risk management but also in compliance-driven changes and operational resilience. Also, the thesis aims to differentiate financial sector changes by comparing them with broader risk management changes observed in non- financial sectors. Thus, clarifying whether the observed shifts are specific to financial sector or reflect broader organizational adaptation to geopolitical instability.

To achieve the set research aim, the thesis uses the following objectives:

1. To identify which risk management practices in European financial sector changed in response to the Russo-Ukraine war 2022 and to assess the extent of these changes, if there were any.
2. To identify the primary channels and drivers through which wartime shifts translated into risk management changes, with increased focus on sanctions and compliance, market risk, and operational resilience.
3. To understand risk governance changes and how financial institutions prioritize different risk sectors and decision-making.

This thesis is guided by the following research questions:

1. How risk management changed in European financial institutions after the Ukraine war began, and to what extent?
2. Through which channels (regulatory, internal assessment, or external environment) did the most prominent drive for change occur?

1.4 Scope and limitations

This thesis examines wartime shifts in risk management in Europe's financial sector, Finland acting as the primary empirical setting. Finland offers a particularly relevant setting given its European Union membership, close relationship with Russia, deep financial integration, and direct exposure to wartime spillovers. These include sanctions implementation and growing concerns over cyber and operational risks. This thesis covers the period after the start of Russia's full-scale invasion of Ukraine in February 2022, enabling

the study to capture the immediate aftermath of invasion and the subsequent changes in risk management practices and governance adjustments that followed.

Methodologically, the thesis uses a qualitative interview design and thus focuses on institutional practices as articulated and interpreted by professional experts. The empirical data is reflected to academic research done before February 2022 gathered using thematic literature review. The core empirical material consists of interviews with professional experts involved in risk-related functions in Finland-based financial institutions. "Risk management practices" refers to changes in risk governance and decision processes, control enhancements and changes to analytical and resilience practices. This thesis does not aim to quantify effects of the war on financial outcomes. Wartime conditions are treated as an external shift that reconfigures risk priorities.

A comparison element is included to determine whether observed adjustments are specific to financial institutions or reflect broader organisational risk adaptations. This comparison does not utilize interviews for the broader organisational risk adaptations but focuses on thematic literature review.

The analysis assumes that interviewees provide credible, experience and fact-based accounts of organisational change while recognising that wartime-related practices may involve confidentiality constraints. Accordingly, the thesis views issues such as non-disclosure and selective transparency as inherent limitations of researching sensitive areas of risk management, rather than as shortcomings of the research questions themselves.

1.5 Expected contributions

This thesis contributes to understanding how risk management operates under wartime uncertainty by examining how European financial institutions have adapted their risk practices since February 2022, focusing empirically on Finland. The contributions are three like: theoretical, empirical, and practical. Thus, the thesis reflects both the theoretical and practical natures of research on financial risk management. This thesis also tries to provide a view into Finnish financial institution's' risk management changes and attitudes after the full-scale Ukraine war.

1.6 Structure of the thesis

The structure of this thesis is following. This thesis starts with introduction where basis for the research is set, research gap identified, and research questions established. Following the introduction section this thesis continues with thematic literature review, first focusing on general enterprise risk management practices, followed by financial sector characteristics. Final part of the literature review is geopolitical context of the study. The literature review is then closed by theoretical framework.

After the thematic literature review and theoretical frame have been establish, research methodology section follows where the actual research is explained, empirical data established, and research philosophy set. The next part of the thesis is empirical findings that are analysed in the following discussion section. Finally, the thesis is completed in the conclusion section.

1.7 Definitions of key concepts

This thesis uses several established key concepts to explain risk management in the financial sector. As this study does not focus on credit risk, attention is given to governance, compliance, operational, and geographical risks.

Risk refers to any uncertainty that can threatens an organization's ability to achieve its financial goals, maintain its operations, or ensure long-term sustainability.

Uncertainty refers to unpredictable events or conditions where the exact outcomes cannot be measured.

Risk Governance refers to oversight mechanisms, responsibilities, and structures through which risk management if governed, monitored and controlled within an institution. It includes control functions and leadership to ensure that risks are managed in line with strategy.

Risk appetite refers to the amount of risk the institution is willing to accept when pursuing different goals. Set by the leadership and executed by everyone.

Compliance risk refers to possibility of regulatory actions, financial losses, and reputational harm resulting from a failure to comply with laws, regulations, and internal policies.

In the financial sector highly complex due to the complexity of regulatory environment.

Sanctions risk is a specific part of compliance risk where financial institutions need to follow sanctioned individuals, companies, and transactions. Increased importance after the 2022 attack in Ukraine.

Market risk refers to the possibility of losses caused my movements in the market such as interest rates, exchange rates, and asset and securities prices. With heightened geo-political instability, market risk can change rapidly due to the volatility and uncertainty of the market.

Liquidity risk refers to the probability that an individual, business, or financial institution will be unable to meet short-term financial obligations.

Operational risk refers to the possible loss resulting from inadequate of failed internal processes or policies, human errors, systems, and external events. Operational risk refers to the day-to-day risks in the organisational functions.

Cyber risk is a specific part of organizational risk associated with cyberattacks, data breaches, and other digital disruptions. Lately cyber risk and cyber security have increased in importance in Finland due to the denial-of-service attacks in the banking sector.

Operational resilience refers to an organization's ability to prevent, adapt to, respond to, and recover from disruptive events

Geopolitical risk refers to the risk that is created by political decisions, interstate relations, sanctions, and interstate instability that may affect financial markets and regulations. This thesis geopolitical risk is assumed to create the central driver for changes.

Risk culture refers to the shared attitudes, practices, and behaviours that shape how risk is understood and managed within an organisation.

2 Literature review

2.1 Risk management foundations

2.1.1 Governance and Strategy

Risk management is not just controls, frameworks, and tools managed by risk managers and analysts, it starts with governance and strategy (Schäffer & Storek, 2022). Governance and strategy work as the core for risk management that directs organization's actions and align organization towards board's and management's goals. Governance structures have been shown to direct risk tolerance, accountability, and decision making (Crawford & Jabbour, 2024). And thus at the end risk governance is a board level responsibility (Viscelli, Beasley & Hermanson, 2016) that directs organization's actions to align with strategy and objectives (Alijoyo & Norimarna, 2021).

Risk governance determines who is responsible for risk related decisions, how oversight is exercised, and how information flows within the organization (Viscelli, Beasley & Hermanson, 2016). In this framework the governing body, the board, carries the final oversight responsibility for risk management, as oversight responsibilities are formally assigned at the board level (Ittner & Keusch, 2015). OECD guides that the Board is responsible for overseeing the risk framework and ensures that responsibility and accountability are clearly defined (OECD, 2014). The board is not however managing the operational risk directly. Instead, it is purely managerial setting where it sets expectations and ensures that risk management is aligned with organization's strategy.

Senior management works on the practical level. Management sets structures, reporting frameworks, and processes for both risk management and operations, while also reporting to the board about planned and actual outcomes (Visvelli, Beasley, & Hermanson, 2016). This places management in a position between operational risk execution and strategic direction (Kumari, 2025; Viscelli, Beasley, & Hermanson, 2016). Therefore, effective risk governance depends not only on the directing set by the board, but also management's ability to set strategic priorities into clear responsibilities and actions (Kumari, 2025).

The risk management and strategy relationship is central in the academic literature (Dhlamini, 2022). The COSO Enterprise Risk Management framework positions risk management as an integral part of strategy and performance, rather than a separate compliance action (COSO, 2017). ISO 31000 argues similarly by stating that risk management should be integrated into governance and strategy and should improve decision making and to help to better allocate organization's resources (ISO, 2018). This suggests that risk management should shape the strategy and not to protect the already selected strategy (Maia & Chaves, 2016). Organizations thus require risk related information when they set strategic objectives, allocate resources, and asses' different courses of action.

Clear role allocation with need-to-know setting forms another part of governance. The IIA three Lines Model defines between first line roles that manage operational risk in day to day operations, second line roles that support and monitor, and the third line roles that provide independent audit (The IIA, 2020). The model however does not release the management of its responsibility, even with oversight functions are in place. The three lines model helps organizations to clarify roles, reduce gaps, and strengthens reporting and governance.

Independent audit also strengthens the risk governance framework (Udoh, 2024). According to the IIA, internal audit provides an independent and objective check on the effectiveness and sufficiency of governance and risk management (The IIA, 2020). This is important as the oversight becomes more weaker when the same agent is responsible for both managing the risks and for evaluating whether that management is effective (Wang, 2025). Therefore, internal audit works as the final line of risk management and supports the governing body by offering independent assessment whether risk management is sufficient.

Risk governance establishes authority, accountability, and oversight, while strategy differs direction and objectives. When these factors are in order, risk management becomes part of the organization, rather than a tool of protection and control (ISO, 2018).

2.1.2 Identification

The starting point for risk management is the identification of the risk. Organizations can not analyse, evaluate, and respond to risks if they have not been recognised (ISO, 2018; COSO, 2017). Hermann (2015) has identified key steps in the risk management process to be the following, risk framing, identification, analysis, evaluation, treatment, monitoring, and communication. The ISO 31000 is also in the support with the risk management framework where risk is also divided into steps (ISO, 2018). However further research has combined some of the steps. Oehmen et al. (2020) defines identification as the first step in the process where sources of uncertainty are systematically searched. This provides a broad insight on risk that may affect the achievement of the objectives. Thus, it is not only limited to obvious or visible uncertainties. Risk identification helps to understand potential events, their sources, and their effects on decisions and outcomes (Glette-Iversen, Flage & Aven, 2023; ISO, 2018).

Identification should begin from objectives and context. ISO 31000 considers risk management as an integrated process across organization's and used to improve decision making (ISO, 2018), while COSO links event identification to the organization's ability to achieve objectives (COSO, 2017). As for this reason, risk identification should not be treated as a checkbox among other steps but as a tool to better the organization's strategy. Risk identification should be connected to the organization's strategy and objectives, what would support those objectives, what could disrupt them (Andersen, 2021). Risk identification should consider both external and internal sources of uncertainty. Internal sources can include process failures, system weaknesses, gaps in governance or controls, and human error (ISO, 2018). External sources can include market shifts, technological disruptions, geopolitical developments, regulatory changes, and stake holder behaviour (COSO, 2017).

Risk identification also depends on the method used to surface the uncertainty. Research shows that different approaches can produce different results, even within the same context. Kontur and Sari (2023) found that a business process approach identified more risks than work breakdown structure approach, suggesting that identification methods shape what risks are identified for decision makers. Di Zio et al. (2024) similarly argue

that in complex situations combining multiple methods is preferable to relying on a single technique or tool. The research suggests that effective risk identification should draw on more than one technique or tools to build a more comprehensive picture of uncertainty.

The academic literature also shows that risk identification becomes more useful when its findings are documented in a structured way. A risk register being a central tool to monitor and reduce identified risks (Whipple & Pitblado, 2010). Leva et al. (2017) in their case study describe the development of a companywide risk register that supported consistent data collection, risk comparison, and communication of key risks. This case study is important because it highlighted that risk identification should produce more than a list of concerns raised. it should create a clear record that supports later assessment, review, follow up (Leva et al., 2017). In practical sense, it improves accountability and provides a broad view of risk environment. In academic sense, it improves the link between risk identification and the rest of the risk management process.

But studies also show caution against formal tools as neutral representations of risk. Risk management frameworks and technologies can shape which uncertainties are translated into accepted risks and which remain outside formal risk treatment (Themsen & Skærbæk, 2018). But it is not only tools and frameworks that can filter different risks. Tekathen and Dechow (2020) reached a conclusion that organisational risk language can narrow over time through communicative path dependency. These studies show that identification is not only a technical process to identify the uncertainties. It is also explanatory process shaped by language, routines, and organisational attention. This means that a well designed framework can support identification, but it can also restrict it if managers start to treat the framework as a perfect picture of uncertainties (Themsen & Skærbæk, 2018; Tekathen & Dechow, 2020).

Risk management should be treated as interactive on-going process rather than a once completed task. New identification and assessment may be needed when decision alternatives change, risk environment changes, or when context and values change (Glette-Iversen et al., 2023). While having no specific research on small signals of risk environment in ERM (enterprise risk management), in a broader picture the identification of

small signals can improve the risk management process by broadening the preparation for uncertainty (Gilmore et al., 2023). Risk identification should be an ongoing process where organisations revisit identifications when early warning signals emerge, risk environment changes, or new information changes the basis on which earlier decisions were made (Hardaway & Flage, 2025; Glette-Iversen et al., 2023).

2.1.3 Assessment & Measurement

The next step after risk identification is to assess their significance, effects, and translate uncertainty into a basis for decision making. In risk management research, this step is generally understood as being part of a broader effort to evaluate how risks affect organisational objectives and how they should be prioritised (Bromiley et al., 2015; Aven, T., 2016). The practical effect of assessment in business setting is provide managers enough information and analysis to base their decisions to best support strategy and objectives, and how resources should be allocated.

Risk assessment in organisations usually blends qualitative judgement with numerical measurement. This is necessary because many business risks cannot be quantified with precision, especially when the uncertainty concern strategic matter, operational disruption, or emerging development (The Risk Coalition, 2023). Research shows that the usefulness of the risk assessment depends not only on the used assessment tool, but also how it is used within the organization (Mikes, 2009). For example, risk workshops are shaped by culture, and that in some settings assessments function less as exact measurements and more of as a structured learning process to support managerial decision making (Bellora-Bienengräber, Harten, & Meyer, 2023). Braumann (2018) in conjuction supports the importance of risk awareness as part of an effective ERM. Thus, the research suggests that assessment should be understood as a process of informed actions rather than purely mechanical calculation.

A common tool in risk management to assess risks in business organisations is through simple tools, such as probability and impact matrices (Dujim, 2015). These tools allow organisations easily to rank risks, compare uncertainties and exposure, and communicate priorities in a visible form, thus remaining popular (Bratvold & Bickel, 2014).

However, it is argued that risk matrices can create misleading impressions of precision and oversimplify complex uncertainties (Dujim, 2015). As such, simple tools are useful as aids for prioritization and communication, rather than as an exact measurement of risks.

When uncertainty is higher or strategic consequences are greater organisations might need more structured and strategic risk assessment (Cordove-Pozo & Roulwette, 2023). Scenario analysis is one important example. Scenario analysis techniques are established tools for dealing with uncertainty by examining possible alternative future developments (Tiberius, Siglow & Sednra-Garcia, 2020). In business risk management this is especially crucial because many uncertainties change overtime so future scenarios are beneficial (Luis et al, 2021). Instead, they develop through different changes and actions. Scenario based assessment allows managers to test assumptions, analyse different path of development, and consider how choices may perform under varying future conditions (Tiberius, Siglow & Sednra-Garcia, 2020).

Research also supports assessment process where risk variables are documented and embedded into organisational processes (ISO 3100, 2018). Leva et al. (2017) highlight that a risk register can support comparison across units, communication to management, and continuous review. However, formal risk management frameworks can not identify every relevant uncertainty due to organisational boundaries (Power, M., 2009). Research shows that organisations need structures in order to compare and monitor risks yet is also shows that structures can narrow risk management's focus and thus limiting the risk assessment (Leva et al, 2017; Power, 2009).

Recent research suggests that assessment creates the most value when it is integrated to be part of management control and performance processes. ERM when integrated into organisations processes have a positive mediator for companies financial performance (Syrova & Spicka, 2022). In support Hiebl (2024) reaches a similar conclusion by highlighting the growing importance of integrating risk into management controls. The mentioned academic literature supports the assumption that assessment, as part of the risk management, should be part of the integrated risk processes and support strategy and help in the possible strategic adjustment.

The academic research presents risk assessment as part of a informed and integrated risk process. It combines decisions, tools, documentation, and where possible, quantification. In business risk management, the assessment's value is created by providing managers data for decision making of present and possible future uncertainties.

2.1.4 Response

The next steps after the initial assessment is for organisations to decide how it will react to the identified and assessed uncertainties. In this part of risk management, the analysis is converted into managerial actions (Bromiley et al., 2015). It is not just about choosing a response option, but also about aligning that choice with the objectives after the consideration of available resources, and the wider control systems of the organisation (Hiebl, 2024). For that reason, risk response should not be treated as a routine administrative step or approval. It is the step in which risk management starts to affect operations, planning, and performance of the organisation (Bromiley, et al., 2015).

Risk response can take several practical forms. Organisations may try to reduce or contain the risk exposure by process redesign, monitoring, controls, stakeholder management, or planning (Dittfeld, Scholten & van Donk, 2021; Harju et al., 2024).

Organisations may also try to share or transfer part of the financial risk through governance arrangements, partnerships, or insurance (Singh & Gaur, 2021; Zhu & Sardana, 2020). Thirdly, organisations may strengthen preparedness and recovery through planning, resource allocation, training, and resilience building measures that help organisations' to continue operations in case of realisation of risks (Ali, Hanafiah, & Mogindol, 2023; Monazzam & Crawford, 2024; Eichholz, Hoffmann & Schwering, 2024). The responses are not mutually exclusive. Organisations may combine them, especially when risks and uncertainties are great (ISO 3100, 2018; Klinke & Renn, 2001).

A key point in recent literature is that there is no one correct response to risk. Suitable responses depend on the nature of the uncertainty, organisational environment and capabilities, and other context (Harju et al., 2024; Singh & Gaur, 2021). Especially in inter-organisational settings, for example, risk mitigation may often extend beyond internal controls. For example, governance choices may help to mitigate risks in multinational

firms in cross border relationships (Singh & Gaur, 2021) while Zhu and Sardana (2020) argue in support, that in emerging markets, risk mitigation might require active cooperation with key stakeholders rather than internal controls. This suggests that risk response can often be relational and not just technical.

Some risk responses do not remove the actual underlying source of uncertainty but instead acknowledges it and works around it. Finance research shows that companies use derivates to hedge on risks (Ji & Wei, 2023). Derivatives such as interest, commodity, and currency usage are widely used in uncertain financial environments. In financial crises derivatives could be used to reduce risks (Lau, 2016). It is common for managers to use derivatives to hedge risk especially in situations where those risks that can rise over relatively short time horizon (Fatemi & Luft, 2002). Hedging however contain additional costs and new risk exposures, known as derivatives risks (Stulz, 2004), while some research shows that some organizations suffer hedging losses from time to time (Adam & Fernando, 2006; Bartram et al., 2011). However, it has been highlighted by Bertram et al. (2009), and Graham and Rogers (2022) that derivates hedging can result in reduction in systematic and total risks. The literature also highlights that highly leveraged organizations prefer operational modifications as hedge strategy (Saharan & Rajendran, 2024). Thus, reaching a conclusion that organizations might do financial or operational hedging depending on the risks and organization's structure.

Business literature also increasingly highlights risk response as capability building. Ali, Hanafiah and Mogindol (2023) describe business continuity management as a strategic practice that allows businesses to respond effectively to crises and mitigate the impact of unexpected events. Monazzam and Crawford (2024) highlighted that risk management practices can help organizations' to develop risk resilience resources and capabilities over time. Eichholz, Hoffmann, and Schwering (2024) concurred that risk management orientation and the planning function are positively associated with organizational resilience and competitive advantage in times of crisis. Ma and Zhang (2022) also adds that that resilience capacity supports both proactive and reactive crisis management strategies and improves crisis management performance. The literature shows that risk response should not only be understood as a short-term reaction, but that it can help

organizations to build structures and capabilities that improve organizations' ability to absorb shocks, adapt to different situations and to continue operations.

The risk response in business management is best understood as selection and implementation of actions and processes that modify exposure, allocate consequences, or strengthen resilience. Different responses are context dependent and often combine several different actions, such as operational mitigation, contractual or financial transfers, and continuity or resilience measures. Organizations can also choose to accept risk without taking any proactive measures to avoid, mitigate, or to transfer it (ISO 3100, 2018).

2.1.5 Monitoring and Reporting

Monitoring and reporting are the next part of business risk management where earlier risk assessments are checked against current conditions, and risk information is used to support oversight and decision-making (Elshandidy et al., 2018). This step is different from identifying, assessing, or responding to risks. It does not focus on what the risks are or how to respond to them. Instead, it focuses on whether the organization's understanding of risk is still accurate, whether controls and actions are working as planned, and whether changes in the internal or external environment require new management action (Elshandidy et al., 2018; Posch, 2020). In a business setting, monitoring and reporting are important because risk conditions rarely remain stable. Risk conditions can change over time, and a risk that once seemed acceptable may become unacceptable if the environment changes, if controls weaken, or if planned responses do not work as intended (Elshandidy et al., 2018; Posch, 2020). Monitoring thus focuses on tracking the changes in risk conditions, while reporting focuses on communicating those changes to management.

The recent literature on the subject suggests that successful monitoring depends on structured indicators and on integration within the organization's wider control system (Posch, 2020). Posch highlights that risk focused controls and risk focused information sharing work as complementary practices, especially when organizations operate with higher risk appetite (Posch, 2020). Posch's finding is important due to the fact that it

shows that monitoring is not only a matter of collecting data. It also depends on whether risk information moves across units and reaches those responsible for planning and decision making. Huber, Kraus, and Meidell (2025) also argue that enterprise risk management becomes more useful when it is linked with established performance management tools, such as balanced scorecard. Pehlivanlı, Aykaç Alp, and Katanalp (2024) shows that key risk indicators and broader performance measures can be combined into an early warning system that can help organizations detect deteriorating risk conditions in time. These studies show that monitoring is most effective when it is indicator based, continuous, and integrated into ordinary management routines rather than treated as a separate task.

Reporting is a closely related but a distinct role. Once the information on risk has been monitored and collected, it must be transformed into a form that managers, boards, and stakeholders can understand and use as a basis for decisions (Hassanein, 2022; Posch, 2020). Bryce et al. (2019) highlights the importance of internal reporting, and the potential risks if organizations fails to do so. It has been also highlighted that outside risk reporting can have positive effect on the cost of capital (Heinle & Smith, 2017) and increase corporate value (Campbell et al., 2017). However outside risk reporting can also introduce costs and inform the markets or organization’s risks and thus harm their competitive position (Hassanein, 2022).

On the governance aspect Crovini et al. (2026) shows that value of risk reporting is influenced by how well it is connected to the business model. This suggests that reporting is more beneficial when risks are presented in relation to the organization’s value creation instead of presented as isolated threats (Crovini et al., 2026).

Monitoring and reporting should be understood as continuing mechanism that keep risk management relevant over time. Monitoring tracks whether exposures, indicators, and controls are changing, while reporting transforms the information into usable form that can support managerial action, board oversight, and external evaluation. The value of risk monitoring and reporting lies the ability to provide visibility after the initial assessments have been made and in ensuring that changes in risk conditions are noticed early enough to support decision making process.

2.1.6 Culture and Continuous Improvement

Risk culture refers to the shared assumptions, norms, and patterns of behaviour that shape how people in an organization perceive, discuss, react, and handle risk (Bockius & Gatzert, 2024; Braumann, 2018). In recent scientific literature, it is treated as a central part of organization risk management rather than as an informal background condition (Bockius & Gatzert, 2024). Formal policies and controls do not alone determine behaviour on their own. Employees still interpret rules, make trade-offs, decide whether to raise issues, and judge how much uncertainty and risks are acceptable in everyday work (Bockius & Gatzert, 2024; Braumann, 2018). Braumann (2018) argues that risk awareness is a key mechanism in this process, due to the fact that risk management becomes more effective when employees understand how their actions are related to the potential causes and outcomes of the risks. Thus, risk culture matters because it affects everyday decisions across organization, and not specific risk management practices.

A strong risk culture is not a culture that avoids all risks. In organizations, it is more useful to understand it as a culture that aligns risk taking with objectives, responsibilities, and risk acceptance (Bockius & Gatzert, 2024; Braumann, Grabner & Posch, 2020; Ghafoori et al., 2023). Scientific research shows that leadership has a central role in creating such a culture. Braumann, Grabner & Posch (2020) highlights that tone from the top leadership influences risk awareness through two channels: management communicates expectations from the top, and it also encourages bottom-up communication and escalation of risk issues. Ghafoori et al. (2023) also shows that management's commitment directs risk, risk capability and training, risk communication, risk strategy, and risk support. These studies show that risk culture us built through signals, communication, incentives, training, and example by top leadership.

The literature also shows that organizations can also influence risk culture with management controls and everyday practices. Posch (2020) highlights that risk-focused result controls and risk-focused information sharing support each other in helping employees include risk in their decision-making. Effect is stronger in companies with a higher risk appetite. Research also shows that organizations use risk culture controls, which

indicates that risk culture does not just develop on its own and can be influences by management (Grieser & Pedell, 2022). Marc, Arena, and Peljhan (2023) argues that risk management systems become more effective when managers use them interactively rather than only as technical structures. Risk culture is not static setting; it is continuously improving. Risk culture does not develop with formal statements alone. It develops when managers connect risk information with normal organizational routines.

Bockius and Gatzert (2024) argues that organizational risk culture should be assessed regularly and improved along targeted areas. Ghafoori et al. (2023) showed a way to measure risk culture across several areas, which helps organizations to evaluate it more clearly and track changes over time. It has also been shown that these types of assessments can also reveal gaps between formal risk governance frameworks and how employees actually behave in practice (Dürst, & Kunz, 2025a). This shows that continuous improvement needs to be based on measurements and evidence, not only on managerial intuition. recent research also suggest that improvement is strongest when organizations treat is as interactive process. Dürst and Kunz (2025b) conducted an one year study in which risk culture was developed through survey results, targeted interventions, governance mechanisms, and formal revies process. The underlying result is broad. Risk culture improves when organizations combine participation, assessment, and follow up, rather than rely in awareness messaging alone. Continuous improvement requires repeated review of how people understand risk, how they respond to uncertainty, and whether actual behaviour aligns with the organization's expectations and strategy (Dürst, & Kunz, 2025b; Dürst & Kunz, 2025b).

Risk culture should be viewed as a factor that shapes strategic behaviour as well as control. Research shows that organizations with more pronounced high-risk culture invest more in innovation and generate stronger innovation outcomes (Ho et al., 2024). Thus, risk culture is not only about caution and loss prevention. It also influences how organizations pursue opportunities under uncertainty (Ho et al., 2024). The aim of risk culture is to support informed, deliberate, and accountable risk taking that aligns with organizational strategy and managerial oversight.

2.2 Financial sector characteristics

The financial sector is different from other sectors because its core function is directly connected to the allocation and circulation of money, credit, and associated risks in the wider economy. Financial institutions mediate between savers, borrowers, investors, households, companies, and public authorities by providing lending, payment services, investments and savings. Thus, failure can have effects that go beyond the organization itself (Basel Committee on Banking Supervision, 2024). While the bankruptcy of a non-financial sector company can be significant for its stakeholders, hardship or bankruptcy in the financial sector can also affect credit availability, payments processing, assets, wider market confidence and overall financial stability (IMF, 2009; Bernanke, 1983).

A key feature of financial mediation is maturity transformation. Banking sector in particular finance long-term and less liquid assets, such as mortgages, with liabilities that are short-term and more liquid, such as deposits (Diamond & Dubvig, 1983). This practice is economically important due to the fact that it allows customers to have liquid claims while enabling long-term financing for companies, households, and public sector. However, if depositors or investors lose confidence in the organization, they may seek to divest or reduce their associated risks (Diamond & Dubvig, 1983; Bank of Finland, 2023). In situations like these, organizations may face liquidity pressure if it can not convert those assets into cash quickly enough without losses.

This confidence between financial sector and their customers and investors is one of the key defining features of the financial sector. Contracts are often dependent on trust that future obligations will be honoured, payments will go through and deposits will remain available for customers (Bank of Finland, 2023). Thus, mutual confidence is not only reputational issue but also a condition for the operation of financial institutions. The loss of confidence can spread quickly due to the fact that many financial claims are liquid, transferable, and highly sensitive to new information (Diamond & Dubvig, 1983; Bank of Finland, 2023). Thus, financial institutions are subject to regulatory safety-net and stability requirements, such as capital and liquidity requirements, recovery planning, resolution frameworks, and deposit guarantee schemes (Basel Committee on Banking Supervision, 2024; European Banking Authority). In the European Union the deposits are guaranteed

to an extent, highlighting that depositor confidence is also a public-policy concern and not only as a private contractual issue.

Financial sector is also largely interconnected. Financial institutions are connected through lending relationships, securities holding, payment systems, common asset exposures, and shared service providers (Tobias & Brunnermeier, 2016; IMF, 2009). These can help financial institutions with diversifications, but they also transmit stress from one institution or market situation to another. For example, losses in one institution can affect stakeholders directly, while broader fall in asset prices can affect institutions indirectly if they hold similar exposure. Thus, financial-sector risk is not only institutional, but systemic. Financial institution may be systemically important due to it's size (IMF, 2009). Systemic risk may also rise from the collective behaviour of many institutions that react similarly under stress, for example by reducing lending or selling assets (Tobias & Brunnermeier, 2016).

Financial sector has a systemic role in the economy. Banks and other financial institutions provide payment services, credit, investment channels, insurance, and other services that households, companies and the public sector rely in their everyday economic activity (Bank of Finland). Scientific literature has highlighted that if financial sector is disrupted for a reason or another, the effects may extend to consumption, investments, employment, and economic growth (Bernanke, 1983), thus affecting real economy. This connection causes risk management in financial sector to be broader than ordinary enterprise risk management. In the following subsections this thesis will go into more detail characteristics of financial sector risk management.

2.2.1 Governance and risk appetite

Governance is a central characteristic of risk management in the financial sector. The governance framework must do more than just support management. It must ensure that business decisions, risk-taking, internal controls, and regulatory obligations are aligned with the institution's financial capacity, strategy, and role in wider financial system. The Basel Committee (2015) highlights that effective corporate governance is critical to the proper functioning of banking sector and the economy, and that it supports

robust risk management, decision-making, public confidence, and the safety and solvency of banks.

In financial institutions the management body, usually the board, has the final responsibility for the governance arrangements (Directive, 2013, Art. 88). It is the managements responsibility to define the institution's strategy, approving its risk appetite, overseeing senior management, and ensuring that risk management and internal controls are effective (European Banking Authority, 2021). The responsibility of the board is important, especially because under favorable economic situations financial risks may accumulate before they become visible but materializes quickly when economic conditions worsens. Thus, governance in financial institutions must be forward-looking and need to account for current profitability but also the sustainability of the business model and the institution's ability to absorb negative developments (The Basel Committee, 2015; European Central bank, 2016).

A key feature of governance framework is the risk appetite and risk appetite framework. in the financial sector risk appetite is especially important because risk-taking is part of the business model and excessive or poorly controlled risk-taking can threaten solvency, liquidity, and confidence in the institution. The Financial Stability Board (2013) describes an risk appetite framework to include risk appetite statement, risk limits, and clear roles and responsibilities for the board, senior management, internal audit and business lines. The risk appetite framework should connect strategic objectives with risks such as credit, market, liquidity, operational, conduct, and capital adequacy. Risk appetite framework should also be integrated in planning, budgeting, capital management, and recovery planning, rather than just being a directive document (European Central bank, 2016; The Financial Stability Board, 2013).

However, risk appetite framework is not useful if employee behavior does not support it. The risk appetite framework is limited in its value if financial institution's internal culture rewards short-term profitability or risk-taking that is inconsistent with approved limits. Thus, the management body and the senior management need to communicate expectations, ensure accountability, and create conditions where risk concerns are

escalated without being ignored or suppressed (European Banking Authority, 2021; European Central bank, 2016; Financial Stability Board, 2013).

In governance internal control functions form another central part. The EBA Guidelines on Internal Governance (2021) state that internal controls should include risk management function, a compliance function, and internal audit function. These functions are intended to provide independent oversight for institutions in relation to risks. The risk management function supports the identification, measurement, monitoring, and reporting of risks. The compliance function monitors compliance with legal, regulatory, and internal requirements. And the internal audit provides independent assurance on the effectives of governance, risk management, and internal controls (European Banking Authority, 2021). The independence and authority of these functions are important due to financial institutions possible desire to prioritize growth. Aebi, Sabato, and Schmid (2012) found that banks where chief risk officers reported directly to the board rather than chief executive officer performed better during the 2007-2008 financial crisis highlighting the fact that risk governance is not just a formal compliance requirement in financial sector but may also improve institutional resilience. However, risk governance should not be understood as a guarantee against losses. Even well-designed governance structures can be ineffective if the information flow are insufficient, risk limits are not enforced, or if control functions do not have practical independence (European banking Authority, 2021; Stulz, 2014)).

2.2.2 Capital, liquidity and supervisory review

Capital and liquidity are central for financial sector risk management, especially banking sector. Because banks and some other financial institutions operate with leverage, maturity transformation and confidence sensitive funding, the institutions must be able to absorb losses and meet obligations also under adverse conditions (Basel Committee on Banking Supervision, 2008; Financial Stability Institute, 2019). Capital and liquidity are not just only internal management concerns, but also regulatory and supervisory

requirements implemented to support financial stability (Basel Committee on Banking Supervision, 2024; Finnish Financial Supervisory Authority, n.d.).

Capital regulation focuses on the institution's ability to absorb losses. In banking, own capital requirements are intended to ensure that institutions hold sufficient capital in relation to the risks they take (Finnish Financial Supervisory Authority, n.d.). However, capital sustainability is not only a matter of complying with minimum capital rations. Institutions also must understand their risk profile (Basel Committee on Banking Supervision, 2024; European Central bank, 2018). Liquidity regulations address a related vulnerability. A financial institution may be solvent but still fail if it can not obtain cash or other liquid assets when obligations fall due. Thus, liquidity risk management focuses on the ability to meet payment obligations in normal and stressed conditions (European Central Bank, 2018). The liquidity Coverage ratio supports short-term resilience by requiring banks to hold liquid assets for stress situations, while Net Stable Funding Ratio promotes a more stable funding structure over a longer period of time (Basel Committee on banking Supervision, 2013; Basel Committee on banking Supervision, 2014).

In the European banking sector, capital and liquidity adequacy are also assessed through internal processes. The Internal Capital Adequacy Assessment Process, or ICAAP, requires institutions to assess if their own capital is sufficient in relation to their risk profile and strategy (European Central bank, 2018). Also, the Internal Liquidity Adequacy Assessment Process, or ILAAP, requires institutions to assess if their liquidity resources and liquidity risk management are adequate (European Central bank, 2018). These requirements are important due do them placing direct responsibility on the institutions themselves, not only on the supervisor. A bank must be able to demonstrate that it identifies material risks, measures them appropriately, plans capital and liquidity over longer period of time and considers adverse scenarios in its decision-making (European Central bank, 2018; European Central bank, 2018).

These assessments are connected to external supervision by supervisory review. In the European Union the Supervisory Review and Evaluation Process, or SREP, is used to assess how institutions manage risks that can affect their capital, liquidity, governance and overall viability (European Central bank, 2025; European banking Authority, 2022). The

SREP assesses the institution's business model, internal governance, risk controls, capital and liquidity adequacy, and supervisors may impose additional requirements or qualitative measures based on the assessment (European Central bank, 2025; European Banking Authority, 2022). Financial institutions also face stress testing. Stress testing is central for supervision, as it evaluates whether institutions can remain resilient under adverse economic, market, or institution-specific scenarios (European Banking Authority, 2022; European Central bank, 2018; European Central bank, 2018).

Capital, liquidity, and supervisory review shape the environment within financial institutions can pursue profitability and growth. A strategy that may appear profitable in the short term can be unsustainable if it creates excessive leverage, unstable funding, weak liquidity or capital needs that cannot be met under stress (Basel Committee on Banking Supervision, 2024; European Central bank, 2025; European Central bank, 2018). This illustrates how financial-sector risk management differs from general enterprise risk management, institutions must consider not only profitability but also solvency, liquidity, confidence and potential effects of distress.

2.2.3 Risk data, reporting, and model risk

Financial-sector risk management rely heavily on information systems, quantitative methods, and timely reporting, thus making risk data, reporting, and model risk a central features. Decisions on credit risk, market risk, liquidity, capital adequacy, and business strategy require data that is accurate, complete, and available when needed (Basel Committee on Banking Supervision, 2013). If risk data is fragmented, inconsistent or delayed, management may receive an incomplete picture of the institution's actual risk position. The Basel Committee's BCBS 239 (2013) was developed after the global financial crisis partly due to many banks had difficulties aggregating exposures and identifying concentrations across business lines.

Risk data aggregation and reporting are thus not only technical issues but also governance and control issues. Effective reporting should support the management body and senior management in monitoring risks, risk appetite, and changes in the institution's risk profile (Basel Committee on banking Supervision, 2013; European Central Bank,

2024). This requires clear data ownership, consistent definitions, reliable IT architecture, and controls over data quality. The European Central Bank has highlighted that weaknesses in risk data aggregation and reporting can reduce the effectiveness of risk management and decision-making (European Central Bank, 2024). This is important due to risk positions in financial sector may change quickly and delayed reporting may weaken the ability to respond (European Central Bank, 2018; Basel Committee on Banking Supervision, 2013).

One part of risk data is model risk. Financial institutions use models for credit decisions, pricing, risk measurements, capital calculations, stress testing, and fraud detection (Cosma, Rimo, & Torluccio, 2013). Models can improve consistency and analytical capacity, but they may also create risk if they rely on weak assumptions, poor data, unsuitable methodology or incorrect implementation (European Central Bank, 2025; Federal Reserve, 2025). This is also supported by literature where is has been highlighted that risk models have limitations, especially when they are used mechanically or when market conditions differ from the assumptions built into the model (Danielsson, 2022; Cont, 2006).

Internal models however can be particularly important in banking because they can be used for regulatory purposes. The European Central bank's (2013) Guide to Internal Models sets out supervisory expectations for how institutions apply internal model requirements under the European Union framework, highlighting the fact that internal models are not just internal matter, but also a supervisory concern. Institutions have to be able to justify model design, assumptions, and use. They must also ensure that model changes are controlled and that models remain appropriate when conditions change (European Central bank, 2013). A good model risk frame should include independent validation, documentation, and escalation procedures (Federal Reserve, 2025). Validation provides independent challenge to the model, but validation cannot remove all uncertainty. Models simplify reality and may perform poorly when risks interact in unexpected ways and thus models should support decision making, not replace governance or critical review (European Central Bank, 2007).

Financial institutions in addition to internal reporting requirements are subject to extensive external disclosure requirements. Under the Basel framework, Pillar 3 reports are intended to promote banks' reporting discipline (European Central Bank, 17.11.2022). banks are required to publish information on their risk profile, risk management, and exposures. These disclosures allow external stakeholders such as investors and other market participants to assess the institution's financial and risk position. External reporting improves transparency and confidence on the markets (Roychowdhury, Shroff, & Verdi, 2019)

Risk data, reporting, and model risk management is essential because they affect how institutions measure, monitor, and control risk. It is also part of the supervisory process which is crucial for financial sector.

2.2.4 Operational resilience, ICT, and third-party dependency

One key characteristic on financial sector risk management is operational resilience due to the systematic role of the sector and heavy dependence on digital systems (Regulation (EU) 2022/2554, 2022). Disruptions can cause internal inefficiency but also external effects in customer access, payment flows, and confidence. Thus, operational risk is increasingly understood through resilience, the ability to prevent, withstand, respond, and recover from disruptive events (Regulation (EU) 2022/2554, 2022; Basel Committee on banking Supervision, 2021).

ICT risk is increasing in importance every year. Banks and other financial institutions rely on information systems for core processes such as payments, trading and lending. Cyberattacks, system failures, or long service outages can thus create financial loses, legal consequences, and reputational damage. Cyber incidents also may have broader implications when they affect critical services or interconnected institutions (Aldasoro et al., 2023).

Operational resilience is also regulated. In the European Union, the Digital Operational Resilience Act, DORA, strengthens the regulatory framework for ICT risk management (Regulation (EU) 2022/2554, 2022). DORA's purpose is to ensure that financial entities

can withstand, respond to, and recover from ICT-related disruptions, including cyberattacks and systems failures (Regulation (EU) 2022/2554, 2022). With financial sector's systematic role in the wider society, financial sector's ICT-problems are not just internal risk but a systemic risk with regulatory oversight and demands.

One part of the operational resilience is third-party dependency. Financial institutions rely heavily on external providers for software, payments, and other critical or important functions (Regulation (EU) 2022/2554, 2022). Outsourcing may improve efficiency and access to specialized expertise but it can also create dependency, risk concentration, and reduced control over critical operations (European Banking Authority, 2019; Financial Stability Board, 2023). Thus, financial institutions have to assess outsourcing arrangements before entering them, monitor providers during the contract, and maintain exit strategies for critical services (European Banking Authority, 2019). With many institutions relying on the same service provider, the risk is especially significant, because disruption at the provider may affect several financial institutions at the same time (Financial Stability Board, 2023).

ICT risk and third-party dependency are important because they directly affect the continuity of financial services. Thus, operational resilience complements risk management by focusing on the institution's ability to continue delivering critical services during disruptions.

2.2.5 Recovery, Resolution, deposit protection and capital stack

Recovery and resolution arrangements are unique in financial sector risk management due to the failure of the institutions may affect depositors and wider financial stability. Unlike in ordinary corporate solvency, financial sector failure may require specific crisis management tools to preserve critical functions. An effective resolution should allow authorities to resolve failing institutions without severe systematic disruption or reliance on taxpayer support (Financial Stability Board, 2024).

Recovery planning means actions that an institution can take before failure is unavoidable. Credit institutions and investment firms are expected to identify recovery options, indicators, and governance arrangements to responding to severe financial stress

(European Banking Authority, 2021). These measures should be based on qualitative and quantitative indicators and institutions should also meet minimum list of categories set by regulators. Recovery planning is crucial due to it requires institutions to consider stress situations in advance rather than reacting only after problems have escalated to preserve the restore their financial and business viability (European Banking Authority, 2021).

However, if recovery planning is insufficient a resolution planning becomes relevant. In the European Union authorities are provided with means and tools to resolve failing and likely to fail banks (Single Resolution Boad, n.d.; Directive 2014/29/EU). Resolution aims to maintain critical functions and reduce wider disruptions, not to protect shareholders or creditors from losses. Tools such as bail-in can support market discipline by making shareholders and creditors absorb losses, but literature notes practical and systemic challenges especially in broader crises (Avgouleas & Goodhart , 2015; Tröger, 2025; Cutura, 2021) highlighting the fact financial sector while being highly regulated is complex sector with possibilities for failures in the end.

Capital stack determines how losses are absorbed in stress or resolution situations. Shareholders are bearing the losses first, followed by creditors in accordance with the priority of their claims (Financial Stability Board, 2024). The minimum requirement for own funds, MREL, (Single Resolution Board, 2024) ensures that banks maintain sufficient loss-absorbing capacity to support effective resolution. This shows direct link between liability structure to resolvability.

With banks having systemic role in societies regulators have set deposit protection schemes to support depositor confidence complementing recovery and resolution. In the European Union deposits are guaranteed at EUR 100 000 per depositor (European Banking Authority, n.d.). These schemes do not remove the risk from the financial institutions failure but reduces the risk of destabilizing withdrawals. On the whole, financial sector risk management extends beyond normal continuity planning. Regulators set directives and have tools in disposal that other sectors do not have.

2.2.6 AML/CFT, sanctions and conduct risk

AML/CFT, sanctions, and conduct risk are unique financial sector risk characteristics because financial institutions act as gatekeepers of the financial system. By opening accounts, payment processing, providing financing, they may be used for money laundering, terrorist financing, sanctions evasion, or other illegal activities. Financial crime risk management is thus not only a compliance matter but also part of the maintaining market trust (Regulation 2024/1620; Financial Action Task Force, 2014; Levi & Reuter, 2006). The Financial Action Task Force framework directs a risk-based approach, meaning that institutions and authorities should identify, asses, and understand money laundering and terrorist financing risks and apply proportionate controls (Financial Action Task Force, 2014). Financial service providers are also mandated by law to know their customers to achieve this (Finanssivalvonta, n.d.). In practice this requires customer due diligence, transaction monitoring, and suspicious activity reporting. Regulators have also provided risk factor guidelines to help identify factors related to customers, products, and geographic areas (European Banking Authority, 2024). However, academic literature has shown that risk assessments involve judgement and that may be affected by bias or overconfidence (Ogbeide, H. et al, 2023)

In the European Union the framework is becoming more centralized with newly established Anti-Money Laundering Authority, AMLA, with regulatory, supervisory, and enforcement powers (Regulation 2024/1620) moving a part of authorities' responsibility from nation states to intranational level highlighting the importance of AML/CFT risk. AMLA is to directly supervise high-risk cross-border financial entities, reflecting concern that fragmented national supervisory may be insufficient in a cross-border financial system (Regulation 2024/1620).

Another key financial crime characteristic is sanctions compliance. Financial institutions must screen customers, transactions, and counterparties against applicable sanctions and consider the possible circumvention risks. Weak sanctions controls can lead to legal, financial, and reputational consequences and may result in allowing sanctioned parties to access the financial system (European Banking Authority, 2024).

Conduct risk expands the perspective from financial crime to the treatment of customers and market participants. Conduct risks can arise from unsuitable products, misleading information, poor advice, or weak product governance (European Banking Authority, 2025; OECD, 2022; Daly & Sullivan, 2020). Regulations and guidelines direct financial institutions on product responsibility, consumer protection, disclosure, and responsibility thus highlighting financial sectors importance in the wider economy.

AML/CFT, sanctions and conduct risks show that financial institutions do not just have responsibilities on profit and prudential soundness but that they also must prevent the misuse of the financial system and ensure fair treatment.

2.2.7 Climate & ESG Risk

Climate, environmental and broader ESG risks are ever more important in financial sector risk management. Although ESG is not unique to financial institutions, ESG risk takes a specific from due to they are often transmitted through borrowers, investment portfolios, and other external stakeholders and not through their own operations. Thus supervisors treat ESG risks as drivers of existing financial risk categories, such as credit, market, and business-model risk (European Central Bank, 2020).

The regulatory framework is increasingly requiring ESG risks to be integrated into ordinary risk management. The European Banking Authority (2025) requires institutions to identify, measure, and monitor ESG risks and to prepare resilience plans over different time horizons. The Basel committee (2022) also highlights governance, risk assessment and management, and reporting of climate-related financial risks. Thus, ESG is being increasingly part of risk management on financial sector through different risk management tools, rather than only sustainability reporting. However, it has also been shown by stress test that banks do not integrate climate risks sufficiently into their internal models and frameworks (European Central bank, 2022).

2.3 Geopolitical context

European Central Bank defines geopolitical risk as “threat, realisation and escalation of adverse events associated with wars, terrorism and any tensions among states and political actors that affect the peaceful course of international relations” (European Central Bank). In financial sector academic literature, the concept is strongly associated with Caldara and Iacoviello’s (2018; 2022) framework, which measured geopolitical risk through newspaper coverage of geopolitical tensions and distinguishes between geopolitical threats and realised events. Distinction is importance due to geopolitical risk can affect financial institutions even before a conflict materialises by influencing market expectations, investment decisions, and market confidence (Caldara & Iacoviello, 2018; Baker, Bloom & Davis, 2016).

Geopolitical risk is related to political risk and policy uncertainty, but it focuses more specifically on international tensions, terrorism, and conflict-related event (Caldara & Iacoviello, 2018). Academic research has shown that policy uncertainty and political instability can increase market volatility and reduce investment and economic activity (Baker, Bloom & Davis, 2016; Bekaert et al, 2016). For financial institutions, geopolitical shocks are particularly significant because they can simultaneously affect several risk categories, such as market, credit, operational, and compliance risks (Caldara & Iacoviello, 2018), and financial institutions should consider severe adverse conditions (Basel Committee on banking Supervision, 2018).

One key challenge in managing of geopolitical risk is that it is often external to the financial institution and difficult to estimate using historical data or conventional probability-based models (Caldara & Iacoviello, 2018; Knight, 1921). Knight’s distinction between measurable risk and uncertainty is relevant in this context, since geopolitical events are often characterised by uncertain timing, escalation paths, and different economic consequences (Knight, 1921). As a result, geopolitical risk is different from other financial sector risks that can be modelled using historical data and established statistical methods (Knight, 1921; Basel Committee on banking Supervision, 2018).

The interconnected nature of financial institutions increases the importance of geopolitical risk (European Banking Authority, 2025). Geopolitical shocks can affect asset prices,

funding conditions, borrowers, payment systems, sanctions compliance, and operational continuity (Caldara, D. & Iacoviello, M., 2018; Basel Committee on banking Supervision, 2018). Thus, geopolitical risk should not only be considered as a separate risk category, but also as a factor that can influence existing financial and non-financial risks (Caldara & Iacoviello, 2018).

2.3.1 Transmission channels from geopolitical risk to financial institutions

Geopolitical risk can affect financial institutions through many interconnected channels simultaneously (Caldara & Iacoviello, 2022; Phan, Tran & Iyke, 2022; Basel Committee on banking Supervision, 2018; European Central Bank, n.d.). Unlike risks limited to one business area, geopolitical shocks and uncertainty can influence many different products and business areas at the same time (Caldara, D. & Iacoviello, M., 2022; Phan, Tran & Iyke, 2022). Financial institutions are thus exposed not only to direct losses from affected countries or counterparties, but also indirect effects through markets, customers, regulation, and confidence (Phan, Tran & Iyke, 2022; Basel Committee on banking Supervision, 2021).

One of the transmission channels is market risk (European Central bank). Caldara and Iacoviello (2022) show that higher geopolitical risk is associates with lower stock prices. For financial institutions rapid changes in market valuations may affect for example investment and trading portfolios, collateral values, and internal risk measures (Caldara & Iacoviello, 2022; Basel Committee on banking Supervision, 2018; European Central Bank). Credit risk is also a channel (European Central Bank, n.d.). Geopolitical shocks can weaken firms and households through lower investment, trade disruptions, inflation, and reduced economic activity, thus affecting repayment capacity (Caldara, D. & Iacoviello, M., 2022; Baker, Bloo & Davis, 2016). Phan, Tran and Iyke (2022) highlights that higher geopolitical risk is associated with lower and stability, suggesting that geopolitical events can affect banks even without direct exposure to conflict areas.

Liquidity and funding risks are also key channels during geopolitical uncertainty (European Central Bank, n.d.). Increased risk aversion and inflation may raise funding costs,

reduce market liquidity, and increase the importance of liquidity buffers (Caldara & Iacoviello, 2022; European Central Bank; Basel Committee on banking Supervision, 2018). Another significant channel is operational and compliance risks (European Central Bank). Military conflict, sanctions, cyber threats, and disruptions in payment systems or service providers can threaten operational continuity (Council of the European Union, 2014; European Banking Authority, 2019; Basel Committee on banking Supervision, 2021). Sanction regulations require financial institutions to improve customer due diligence, transaction screening, and reporting processes (Council of the European Union, 2014).

2.3.2 Pre-2022 risk management approaches under geopolitical uncertainty

Before the Russia's full-scale invasion of Ukraine in 2022, geopolitical risk was not treated as a separate risk category in banking regulation. Instead, its effects were managed through existing frameworks such as country-risk assessment (Basel Committee on banking Supervision, 1982), stress-testing (Basel Committee on banking Supervision, 2018; European Banking Authority, 2018), ICAAP (European Central Bank, 2018), operational resilience and ICT security (European Banking Authority, 2019; Basel Committee on banking Supervision, 2021), and sanctions compliance (Council of the European Union, 2014). This shows that geopolitical shocks can affect several risk categories simultaneously, as well as broader geopolitical uncertainty affecting financial institutions (Phan, Tran & Iyke, 2022).

Country-risk management is one traditional approach. Guidance defined country-risk as the possibility that sovereign or other borrowers may be unable or unwilling to meet payment obligations because of official actions, political developments, or external shocks (Basel Committee on banking Supervision, 1982). Banking institutions were thus required to identify and control exposures linked to other countries and cross-border borrowers (Basel Committee on banking Supervision, 1982). However, geopolitical event are not just cross-border risk, as they can also affect domestic borrowers and funding conditions through broader macroeconomic channels (Basel Committee on banking Supervision, 2018; Caldara & Iacoviello, 2018). In addition, operational continuity and market functioning could be disrupted directly through cyber-attacks (Doerr et al, 2022).

Stress testing and scenario analysis were the central tools for assessing geopolitical uncertainty and risks before 2022. The Basel Committee (2018) describes stress testing as a key management and supervisory tool for assessing adverse outcomes across multiple risks. ICAAP guidelines require banking institutions to consider changes in the operational environment when doing assessment (European Central Bank, 2018). Overall geopolitical risks were already contained in different risk management tools, but more of a background actor, rather than a driving force for risks.

2.3.3 European financial sector exposure to Russia-related geopolitical risk

Europe's Russia-related geopolitical risk was already relevant before the full-scale invasion of Ukraine in 2022. After Russia's annexation of Crimean Peninsula and destabilisation of eastern Ukraine in 2014, the European union introduced restrictive measures through sanction regulation (Council of the European union, 2014). This sanctions package created a direct link between geopolitical developments and financial-sector compliance, because banking institutions had to consider sanctions and exposure to Russian entities in their control frameworks (Council of the European union, 2014).

Financial sectors exposure was also indirect. Before 2022, the European Union was highly dependent on Russian fossil fuels. In 2021 Russia supplied more than 40% of EU's gas consumption, 27% of oil imports, and 46% of coal imports (European Commission, 2022). This exposure could transfer to financial institutions through indirect means via firms and households who could face higher energy prices, inflation, weaker economic activity, and reduced borrower repayment capacity (European Commission, 2022; European banking Authority, 2021). Thus, even institutions with no direct exposure to Russia could still be affected through customers and macroeconomic conditions.

European supervision priorities also indicated that geopolitical risk was mainly addressed through existing risk categories rather than as its own risk category. The ECB's 2022 – 2024 supervisory priorities focused on areas such as climate-related risk, counterparty credit risk, and operational and IT resilience (European Central bank, 2021). Thus,

the European financial sector's context was characterised by identified Russia-related vulnerabilities, but these were managed through tradition broader frameworks. The European Central Bank (European Central Bank, n.d.) has identified the need for increased supervisory action due to heighted geopolitical risks.

2.3.4 Finnish financial context and exposure

For Finland, Russia related geopolitical risk was relevant because of geography and economic exposure. Finland and Russia share a border of more than 1300 kilometres, which makes Russia's security environment a direct factor for Finland (Ministry of the Interior (2025). This does not however directly link Finnish financial institutions to have a large exposure to Russia. The bank of Finland's 2022 Financial Stability Review (2022) stated that direct Russia exposures accounted for only less than 0,1% of the Finnish banking sector's assets and 0,3% of insurance companies' total assets. Thus, Finnish financial institutions exposure is better understood through indirect transmission channels. Of Finland's exports around 5% went to Russia, while Russia's share of imports were about 12% (Simola, 2024).

Before the full-scale invasion, Finland's official financial stability discussion focused strongly on domestic vulnerabilities, especially household indebtedness and climate change mitigation (Bank of Finland, 2021). This shows that Russia related geopolitical risk was not the dominant pre-2022 theme in Finland, even though the regional context made it relevant. After the invasion, risks to financial stability increased because Russia's war in Ukraine triggered an energy crisis, increased inflation, and weakened the economic outlook (Bank of Finland, 2022). Thus, the Finnish context highlights how geopolitical shock with limited direct financial exposure can still require attention from risk management through different risk channels.

2.3.5 Literature gap and relevance for present study

The thematic literature review shows that geopolitical risk was mainly recognised as a risk that materialises through other risk channels. However, Caldara and Iacoviello (2018;

2022) showed that geopolitical risk affects financial markets and expectations, and geopolitical risk is associated with lower bank stability (Phan, Tran & Iyke, 2022). This present a clear gap in research where geopolitical risk is considered its own risk channel, even though European Central bank has identified the importance and is working with banks to develop good practices to manage geopolitical risks (European Central Bank).

Thus, this thesis adds to the literature by examining how financial institutions adapted to changes in geopolitical risks, if adaptation was needed. This thesis also tries to examine geopolitical risk as its own risk channel, not only a factor in other traditional risk channels.

3 Theoretical framework

This thesis uses an institutionally embedded risk management adaptation framework to examine how European financial institutions change their risk management practices after Russia's full-scale invasion of Ukraine in February 2022. The framework combines enterprise risk management, institutional theory and organisational resilience. Together these perspectives explain what risk management practices may change, why financial institutions face pressure to change, and how the adapt under geopolitical uncertainty.

Enterprise risk management (ERM) provides the main structure for change. ERM understands risk management as an integrated process that is connected to governance, strategy, identification, assessment, response, monitoring, reporting, and finally risk culture (Bromiley et al, 2015; COSO, 2017). Thus, geopolitical risk is not only understood as only one separate risk channel. Instead, it examines how geopolitical risk may reshape existing risk management practices across several areas.

Institutional theory explains why financial institutions adapt. Financial sector is highly regulated environment where risk management is shaped by laws, supervision, and existing norms (Cavey, 2020). After the war started, regulatory and supervisory attention increased especially around sanctions, operational continuity, and cyber resilience. As the sector is highly regulated, even when institutions have limited direct exposure to Russia, they face changes.

Organisational resilience helps to explain the purpose of adaptation. Geopolitical risk is difficult to manage only through historical data because its timing, escalation and consequences are uncertain (Caldara & Iacoviello, 2022). Resilience thus highlights institutions' ability to anticipate disruption, resist and recover from it (Xiao & Cao, 2017).

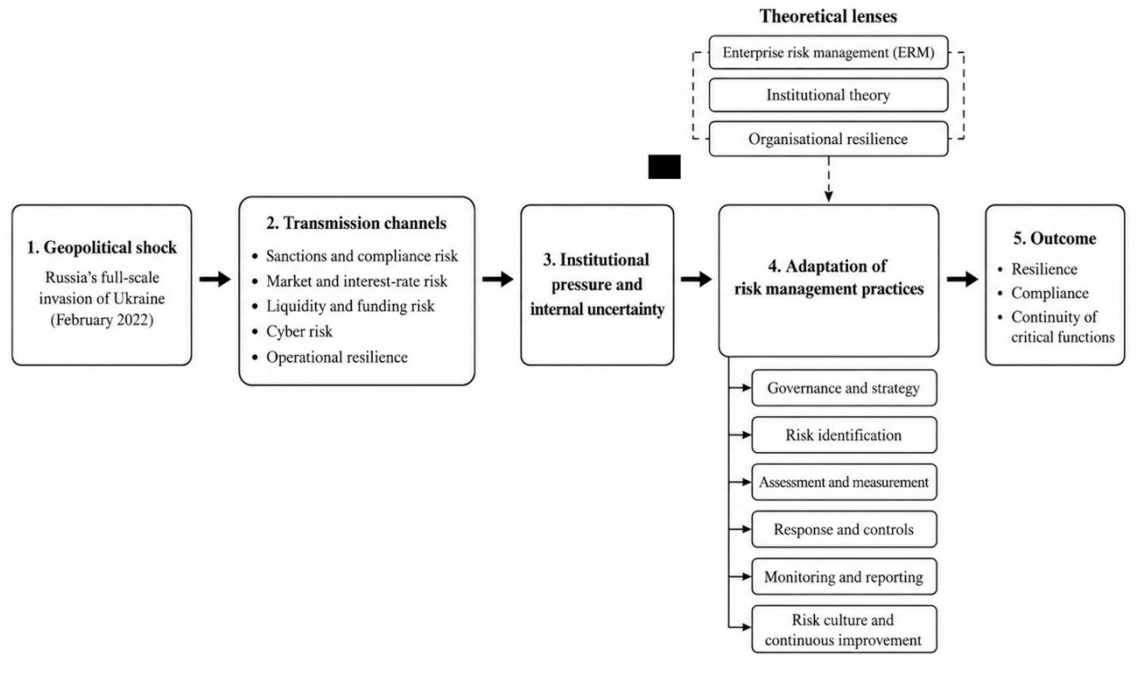

Figure 1. Theoretical framework. Figure created using artificial intelligence. Prompt: "Create a figure of the theoretical framework that was given to in the last message" (ChatGPT, 2026).

The theoretical framework assumes that the geopolitical shock affects financial institutions through several transmission channels. These effects may lead to changes in multiple different practices. the framework addresses the literature gap that geopolitical risk is often studied at the macro level, while less attention has been given to internal risk management adaptations (Caldara & Iacoviello, 2022; Phan, Tran & Iyke, 2022)

4 Methodology

This thesis follows a qualitative and exploratory design. The study examines how risk management attitudes and practices in the financial sector changed after Russia's full-scale invasion of Ukraine in February 2022. A qualitative approach is suitable as the research focuses on organisational practices, professional interpretations, and changes in risk management processes and attitudes, rather than measurable financial outcomes.
The methodological orientation is primarily interpretivist as the study aims to understand how risk management professionals describe and interpret changes in areas such as governance, compliance, and monitoring (Saunders, Lewis, & Thorhill, 2003). This study is also exploratory due to the fact that previous research has focused more on risk management as theory, and not on how financial institutions internally adapt their risk management practices during geopolitical crises.
The research approach is thematic and theory informed. Existing theories on enterprise risk management, institutional theory, and organisational resilience guide the analysis, the interview data allows new findings to emerge. This supports the aim of understanding how geopolitical uncertainty has influenced risk management practices.

4.1 Research design and empirical context

This thesis uses a qualitative interview-based research design. The empirical purpose is to examine how risk management practices have changed after February 2022 and how these changes are explained by professionals working with risk related responsibilities. The research design is good because the study focuses on internal practices and attitudes, organisational interpretation, and professional judgement.
The empirical context is an anonymised Finnish banks and professionals working there. The Finnish context is relevant because Finland is geographically close to the geopolitical shocks caused by Russia's war in Ukraine.
This study should be understood as a qualitative organisational expert study. Thus, the aim is not statistical generalisation to the whole European financial sector, but analytical insight how risk management is understood and described.

4.2 Data collection: semi-structured expert interviews

The empirical data was collected through semi-structured expert interviews. The method was suitable because the study examines professional interpretations of risk management changes rather than externally measurable outcomes. Semi-structured interviews allowed the same core topics to be discusses with each interviewee while also giving interviewees the possibility to emphasise issues most relevant to their own area of expertise. Interviewees were also given follow-up question based on their answers.

The interviews focused on changes in risk management after the February 2022, the drivers of those changes, the risk areas affected, changes in reporting, and the permanence of crisis related changes. The interviews focused on changes caused by geopolitical developments, rather than general risk management changes caused by other reasons. Semi-structured interviews supported comparison across interviewees while still allowing detailed expert level responses.

All interviews were conducted in Finnish. Interviews were recorded with the consent of the participants and later transcribed for analysis. Most interviews lasted between 12-18 minutes with one additional interview was longer. Because the subject of the thesis concerns financial sector risk management and potential sensitive organisational data, the interview material was handled confidentially and anonymised before being used in the thesis.

4.3 Sampling and participants

The interviewees were selected by purposive expert sampling and were approached by email about their wiliness to participate. The study required participants with direct knowledge of risk management on the financial sector.

The sample consisted of five interviewees from Finland based financial institutions. To protect confidentiality, the interviewees are referred to as interviewees. Their job names, job-titles, and organisational units are not disclosed. However, the sample included expertise from several relevant risk areas. General risk and compliance management,

quantitative risk control, financial crime and sanctions related risk management, operational risk, and first-line business risk management. The sample included experts from every level of corporate structure.

Interviewee 1	Chief Operational Risk Officer	Full picture in business risk
Interviewee 2	Chief Risk Officer	Full picture in risk monitoring and compliance
Interviewee 3	Head of Risk Monitoring	Expertise in second line risk monitoring
Interviewee 4	Head Risk Manager	Expertise in second line operational risks
Interviewee 5	Head of Financial Crime	Expertise in financial crime and customer relation management

Figure 2. Interviewee profile table

The sample covers both financial and non-financial risk perspective. It also includes both control-function and business-side perspectives, which is beneficial due to risk management practices are not limited to one function inside a financial institution. The sample had organisational background from three different Finnish financial institution. The interviewees were thus able to provide insight into varied risk areas.

4.4 Data preparation

After the interviews were conducted, the recordings were transcribed into written form for analysis. Since all interviews were conducted in Finnish, the original empirical material was also in Finnish. The analysis was conducted using the original Finnish transcripts to preserve the original meanings of the interviewees' answers. Interview transcripts were systematically read and key answers for questions were categorised into themes and then analysis was made to spot commonalities and differences between different interviewees. Answers were not codified as direct quotes were not used in this study.

4.5 Data analysis: thematic analysis

The interview data was analysed using thematic analysis. Thematic analysis was used because the study aims to identify repeated patterns in how interviewees describe changes in risk management. Thematic analysis allows the researcher to organise qualitative interview material into themes that are relevant to the research questions, while remaining open to new findings from the data (Braun, V., & Clarke, V., 2006).

The data analysis started with repeated reading of the transcripts to become familiar with the material. Relevant data was then divided into themes based on the issues discussed by the interviewees. These themes were then compared across the five interviews, and highlighting answers were presented in the final findings.

The analysis was based on theory and theoretical framework but not limited by them. the theoretical framework guided attention to existing theory, while interviews were used to identify how data appeared in practise.

4.6 Research quality and trustworthiness

The research quality is assessed through the trustworthiness of the qualitative research process rather than through statistical validity or reliability. Credibility is kept by interviewing professionals whose work is directly connected to different risk management channels and areas.

Transparency is based on the disclosed research design, sampling logic, data collection, and thematic analysis process. The analysis was conducted systematically by reading the transcripts and grouping them into themes connected to the research aim. Consistency in the study was achieved by using same core interview questions, while still allowing participants to discuss issues specific to their own expertise.

Study's transferability is limited because the study is based on five expert interviews from anonymised financial institutions. Thus, the findings should not be interpreted as representative of the whole financial sector. The study however provides analytical insight into how risk management professionals understand and describe risk changes under geopolitical uncertainty.

4.7 Methodological limitations

The main limitation of the study is the size of the empirical sample. Another limitation is that the interviews reflect the participants' professional interpretations of change. This study does not independently measure risk changes or the effectiveness of specific risk management actions. Answers are also be limited by the interviewees' current roles and confidentiality constraints of the financial sector risk management. The major limitation was the constraint of not being able to use direct quotes of the interviewees, as the transcripts were treated as notes, rather than definite data to present. This was due to confidentiality. Interviewees are also referred to only as interviewees due to possible cross referencing of public statements made by official organisational representatives versus as private person as in for this study. Due to senior leadership being public information, no organisational links were presented due to possible identification based on time in current position.

5 Findings

This chapter presents findings from five anonymised expert interviews with data organised by themes according to the methodology. The interviews examined how risk management changed after 2022, and how the changes appeared in practice.

The interviewees indicated that risk management changed after February 2022, although unevenly across risk areas. Interviewees linked these changes not only to the war through sanctions, regulations, but also through market conditions, technological development, and internal organisational development.

The clearest changes concerned sanctions, financial crime prevention, and customer-risk management. Russia and Belarus sanctions were highlighted along with sanctions circumvention and country-risk assessment. Operational risk was also highlighted. Especially operational resilience, cyber and information security, outsourcing, and broader security-related risks.

However, the interviewees did not mention changes in quantitative financial-risk management. Existing tools and frameworks were already in place or modified before February 2022, but the changed environment increased the importance of monitoring.

The interviewees also suggested that some changes remained temporary crisis responses, while others become more permanent capabilities and have been refined since the crisis implementation. The interviewees differed on how the institutions were prepared to the crisis. Some indicated that changes were made before the February 2022, while others claimed that existing controls were enough and no changes were needed.

5.1 Overall perception of the risk management change after February 2022

The interviews clearly showed that risk management changed after February 2022. Although the extent and nature of the change depended on the interviewee's are of responsibility. As sanctions, compliance, operational risk, and resilience was highlighted as areas with the clearest change. However, the interview with expertise in risk monitoring presented more moderate view by suggesting that tools and processes for monitoring

already existed before the war and no major changes have happened since, although need for monitoring and preparedness increased. Interviewee did not however directly link the increase to the changes in the geopolitical situation.

One central finding is that Russia's invasion of Ukraine in February 2022 was not described as the only source of change. Interviewees linked developments to several overlapping factors including internal risk assessment, technological change, and organisational growth. One interviewee highlighted that financial institutions already needed to assess in a forward-looking manner, and thus being prepared for environmental changes, while another interviewee highlighted that post 2022 environment as increasingly complex and multidimensional.

The interviews thus suggest that the war acted less as a single isolated cause for change, and more as an obstacle that accelerated existing developments. Immediately after the Russian invasion, institutions increased monitoring and assessed possible effects on current processes, risks, and operation practices. Especially in areas such as sanctions and customer-related compliance, this led to concrete process changes to meet wide ranging regulatory changes. However, in quantitative risk management, the effects appeared mainly through market volatility, economic uncertainty, and caused risk managers to verify that the current frameworks and scenarios remained sufficient.

The findings indicate that geopolitical changes affected several interconnected risk categories simultaneously. Most common categories that were raised were sanctions, technology risk, and operational continuity. In the end risk management became more active and more sensitive to external development. However, the interviews did not suggest that all risk management practices were changed after February 2022.

5.2 Drivers of change

The interviews highlighted drivers of risk management change as multiple instead of as one single cause, Russia's invasion. When asked whether changes came from as a result of an internal assessment, market conditions or regulatory demands, several interviews stated that all the drivers had played a role.

One highlighted driver for change for change was internal assessment. An interviewee explained that financial institutions are expected to assess the risk environment continuously and take possible future scenarios into account. Thus, being part of the normal risk management processes rather than new developments. Another interviewee similarly described normal risk management development where possible risks are assessed whether they can threaten the organisation's strategy and whether risk management needs to be adjusted to support strategic objectives.

Regulation and supervisory requirements were also repeatedly mentioned by multiple interviewees. One interviewee described sanctions regulation after the beginning of the war as a concrete source of process changes, especially in relation to Russia and Belarus. Another interviewee stated that regulation had created the largest amount of work in their risk area. Interviewees also referred to the increased supervisory expectations, digital operational resilience requirements, and increased attention to outsourcing and operational risk management.

Market and macroeconomic conditions formed a final identified driver. Interviewees described the post-2022 period as involving market volatility, interest-rate changes, and wider economic uncertainty. These changed required increased monitoring of risks. However, in the interview with expertise in risk monitoring, these changes did not bring new developments in risk management, but rather a small increase in pre-2022 risk monitoring.

Finally, one interviewee raised technological developments as a broader driver for change. Artificial intelligence and cyber threats were raised as concerns for operational resilience.

5.3 Sanctions, financial crime, and customer risk management

Three interviewees raised sanctions, financial crime prevention, and customer-risk management among the most concrete areas of change. One interviewee highlighted that in their area of responsibility, sanctions had clearly been the largest change after February 2022. The interviewee described Russia- and Belarus-related sanctions as requiring fast reactions and changes to processes to meet the regulatory demands. In the early stage

of the war, this included restrictions connected to payment traffic and later the work focused more on sanctions monitoring and the identification of sanctions circumvention. The interviews showed hat sanctions related work was not only operational checking whether customer or counterparty appears on a sanctions list. One interviewee highlighted that the post 2022 sanctions environment included more detailed requirements than previous sanctions. This required the organisation to develop capabilities for identifying affected customers, monitoring relevant customer activity, and reaction processes when sanctions-related conditions were met. The same interviewee also described sanctions circumvention as a separate and continuing area of attention, especially where customer activity indicates a high-risk country links.

When asked about country-risk the interviewees highlighted customer-risk management. Interviewees described country-risk as a relevant factor in customer assessment, transaction monitoring, sanctions screening, and financial crime risk assessment. One interviewee answered that proactive assessment of country risk carried out, especially from the perspective of customer backgrounds and customer related risks. Another interviewee highlighted country-risk is significant and that sanctions regulation strongly guides assessment.

The interviews also showed that customer-risk decisions are not just simple exclusion decisions. The need to assess customers individually rather than end customer relationship only because customer seemed riskier was raised by one interviewee. Interviews indicated that sanctions and financial crime-related work involve stronger control expectations and case-specific assessments.

5.4 Operational resilience, cyber, security, and third-party dependencies

Operational risk and operational resilience were repeatedly highlighted as being more important areas since February 2022. One interviewee highlighted that operational risk has become more important, especially cyber risk, continuity, resilience, and information security. The same interviewee also stated that the have faced increased cooperation with authorities, new expectations and reporting requirements related to continuity planning, crisis processes and preparedness.

Operational risk environment being affected by several simultaneous developments were also highlighted by another interviewee. These included tighter regulation, technological changes, and changes in the geopolitical environment. In this interview, digital operational resilience regulation was also described as having increased requirements especially for outsourcing and ICT-related risk management. Outsourcing process was described as having developed significantly, including stronger attention to risk management steps, auditability, exit-planning, and testing.

Closely related cyber and information-security risks were also connected to the changed geopolitical environment. One interviewee described how cyber threats had grown in importance and linked this to hostile actors, criminal groups, and attempts to create distrust and uncertainty. The same interviewee described banks as visible targets because disruptions in banking services can create wider uncertainty and weaken public trust. Technology dependencies were also discussed through the example of cloud and large service providers. The interviewee noted that concentration risk in third-party technology services as an important concern due to disruption affecting one major third-party service provider could affect several financial institutions at the same time.

One important raised aspect was security. One interviewee stated that physical security at bank branches and workplace safety had become more prominent than before. The interviewee connected these developments both to wider societal development, but also to the changed security environment. In the same interview employee screening and national security related procedures were highlighted as increasingly important.

5.5 Financial risks

The financial risks were also affected but not on the same level as operational risks according to interviewees. In the quantitative financial risks focused interviews it was a theme that organisation already had the necessary tools and procedures for monitoring financial risks such as credit, liquidity, market risks, and capital adequacy before the war. According to the interviewees there were no large changes in the risk management processes. Instead, the changes in risk environment were transferred trough

macroeconomic factors such as market volatility, interest-rate movements and the need to monitor whether the situation remained within existing stress scenarios.

The interviewees with broad knowledge of quantitative risks described financial risk management as mainly forward-looking and based on preparedness. According to one interviewee the organisation had already prepared with buffers, hedging plans, and had monitoring practices in place. However, one interviewee noted that monitoring and reporting had increased after 2022, especially on risks related to strong interest-rate movements and market changes.

One interviewee described the assessment of macroeconomic effects after February 2022, including possible effects on expected credit losses. This interview also supported the fact that financial risk framework remaining largely unchanged, even when overall risk situation was assessed.

The interviews showed that some development occurred in the financial risk monitoring. One interviewee noted that monthly balance-sheet-level indicators may have been too slow in the volatile conditions. As a result, monitoring was divided into smaller parts so that more volatile parts can be followed more frequently. The answer however shows differences. One interviewee highlighted that changes were already made before the full-scale war started in February 2022.

The interviewees noticed changes in the risk environment but highlighted that risk frameworks stayed the same. Instead, the changes were mainly in intensified monitoring and reporting.

5.6 Reporting

The interviews shoed that reporting and escalation practices changed but in common distinct way. When asked about lower reporting threshold, some interviewees did not identify this change. One interviewee stated that the reporting threshold had not been decreased, due to the risk framework being same and risk appetite had not changed. However, the interviewee stated that more issues had crosses the existing threshold, meaning that more matters required reporting than before.

Another interviewee described reporting in quantitative financial risk through intensified monitoring. Accord to the interviewee, when identified risk levels rise, intensified monitoring can be introduced for a defined period. After February 2022, strong interest-rate movements and market changes led to more frequent monitoring and reporting. The same interviewee also noted that the ability to move to increased monitoring had improved due to earlier manual solutions had later been developed into more automated processes.

The interviews also showed that the reporting content became more responsible to the external environment. One interviewee stated that the world situation needs to visible in risk reporting that reporting topics can not be fixed permanently in advance.

The risk information governance was also described as becoming more structured. One interviewee highlighted that risk information must move quickly from lower organisational levels to the management when needed. In the same interview a formalised escalation procedure was described where certain situations are first escalated to the next level but can be escalated directly to higher lever if the situation requires so.

One interviewee gave a different perspective. With the amount of reportable information having grown so much that more filtering and reporting layers were needed. The issue was not a simply lower or higher reporting threshold, but the need to ensure that senior management receives the most critical information.

5.7 From reactive crisis response to permanent capabilities

The interviews showed that changes after February 2022 included both temporary crisis responses and more permanent changes in working practices. Several interviewees described the first phase after the full-scale war as requiring reaction, intensified monitoring, or immediate process adjustments. One interviewee described daily monitoring in the early phase, where the possible effects of the war on risks, processes, and operating practices were assessed. Another interviewee stated that some early sanctions related actions were short-term reactions but that these were later replaced or developed into more precise and longer-term capabilities.

Other interviewees described crisis related changes as becoming part of more permanent preparedness. One interviewee stated that some changes were temporary but that the overall development direction had remained the same. According to this interviewee, the permanent change was less about continuous intensified monitoring and more about the ability to quickly return to intensified monitoring when situation required so. The same interviewee also stated that that stronger emphasis on forward-looking assessment and scenario thinking had remained.

In one interview it was described that both temporary and permanent elements had been used in operational risk. The interviewee stated that new processes or monitoring should not simply remain forever after each crisis because this would permanently increase the amount of work. Instead, crisis responses should be actively increased and later actively reduced. Overall, the interviews described crisis response as a process where immediate measures may later be reduced, improved, or developed into more stable capabilities.

5.8 Summary of key findings

The interviewees answered positively to the question that did risk management change after February 2022, but the amount varied strongly. Interviewees recognised that the risk environment had become more demanding. They also connected changes to several overlapping risk areas and channels.

The clearest changes were described in sanctions, financial crime prevention, and customer-risk management. Interviewees highlighted that Russia and Belarus related sanctions required fast crisis reactions, more detailed monitoring and attention to sanctions circumvention. Interviewees also identified changes in customer-risk management, especially where country-risk related factors and customer background were relevant to risk assessment.

Operational risk was also highlighted as more important. Interviewees mentioned increased importance in operational resilience, cyber security, outsourcing, and broader security related risks. Some interviewees also noted that authority cooperation had

increased and authorities had new expectations and stronger requirements connected to operational and digital resilience.

Financial risk management did not face similar identified changes. In the risk reporting focused interview, it was highlighted that sufficient tools and processes were already in place while another interviewee with broad knowledge of risk reporting highlighted that changes were made already before the full-scale invasion. However, the interviewees described intensified monitoring and developed capabilities in reporting.

Interviewees also stated that reporting had changed. One interviewee described that no reporting thresholds were decreased, but more information crosses the threshold than previously. Other interviewees described more structured reporting and changes in the reporting process.

Interviews showed that some crisis changes were temporary, while others became more permanent capabilities. Many early actions were later reduced, improved, or developed into more stable processes. Interviewees also highlighted that while some changes were reduced, the capability stayed and these changes could be implemented quickly if situation requires.

6 Discussion

6.1 Uneven nature of post-2022 risk management change

The findings indicate that risk management changed after February 2022, but the change was not consistent between risk channels and areas. The clearest changes were identified in sanctions, financial crime prevention, customer-risk management, operational resilience, cyber risk, and reporting. By contrast the interviews did not show a similar transformation in quantitative financial risk management. In the interview that focused on risk reporting, it was stated that frameworks and tools had not changed and were already in place before the full-scale war began. The change in financial risks was thus mainly visible as intensified monitoring rather than as a fundamental change in risk management frameworks. However, another interviewee with different level of seniority and organisational background highlighted that changes were already made beforehand due to the requirement of forward-looking risk management, thus highlighting that not all financial institutions were similarly prepared for changes.

This suggests that geopolitical shocks and risks do not affect all parts of risk management equally in the same way. In the thematic literature review it was found that risk can be transferred through several channels, including market, credit, operational, and compliance risk (Caldara & Iacoviello, 2022; Phan, Tran & Iyke, 2022). The empirical findings support this view. In the interviews geopolitical risk was not always described as a separate risk. Instead, it was understood as through existing risk areas, especially sanctions and operational resilience. This supports the claim that geopolitical risks are understood as underlying risk, rather than a risk area of its own.

The findings showed that Russia's full-scale invasion of Ukraine in February 2022 was not the only understood source of change. Interviewees referred to regulation, internal assessment, technological development as sources for changes. However, as it was previously identified geopolitical risk is underlying risk that affects through different risk areas, and thus possibility of geopolitical risk being the underlying source for changes remains unclear. According to the interviews a more accurate thinking would be that the post 2022 environment intensified selected risk areas and increased existing development.

However, no post 2022 literature was found on these existing developments, highlighting a clear gap in literature.

This is consistent with the enterprise risk management perspective, where changes in the external environment should be reflecting in the risk management process. The findings show that the main post-2022 changes were selective strengthening of those areas most directly exposed to geopolitical risk.

6.2 Drivers of change and institutional pressure

The findings show that the drivers of risk management change were interconnected rather than clearly separate. Interviewees noted regulation, internal assessment, technological development, and broader changes in the operating environment as the main drivers for change. Thus, Russia's full-scale invasion of Ukraine should not be treated as the only direct driver of all observed changes. However, the literature and findings shows that geopolitical shocks and risks can create pressure through several existing risks channels and areas.

Regulation and supervisory actions were among the clearest drivers identified in the interviews. This was especially noticeable in sanctions related are, where interviewees described fast process changes after the introduction of Russia and Belarus related sanctions. Recently regulation has addressed operational resilience, outsourcing, ICT risks, and reporting requirements. This supports the institutional theory used in the theoretical framework. Financial institutions operate in a highly regulated sector where regulations, supervisory expectations direct risk management practices (European Banking Authority, 2021; European Central Bank, 2016; Financial Stability Board, 2013).

Several interviewees also described internal assessment as an important driver of change. However, this should not be interpreted as fully separate from regulation. In the financial sector internal assessment is party shaped by regulatory and supervisory requirements (European Central Bank, 2018; Basel Committee on Banking Supervision, 2018). Macroeconomic factors resulted from geopolitical shocks were also identified as a driver for change. However, this mainly had changes in increase of monitoring and

reporting. Overall, the findings indicate that post-2022 risk management change resulted from combined geopolitical, regulatory, internal, and market-related pressures.

6.3 Sanctions and Operational resilience as main adaptation areas

The clearest direct changes after February 2022 were identified in sanctions, financial crime prevention, and operational resilience. These findings suggest that geopolitical risk affected financial institutions mainly through compliance and operational channels, rather than through more traditional country-risk. This is in support of literature reviews argument that geopolitical risk often affects existing risk categories instead of being as a separate risk type.

Sanctions were the most direct example of change. Interviewees described Russia and Belarus related sanctions as requiring fast reaction and concrete process changes. Highlighting the fact that financial institutions were not ready for far reaching sanctions, even though sanctions are not a new concept. The findings the sanctions development expanded beyond sanctions-list screening to include sanctions circumvention processes. This shows a move from crisis reaction change to towards more developed financial crime risk management capabilities. The continuing focus on sanctions circumvention development also indicates that the post-2022 environment revealed a need to refine existing controls and analytical capabilities.

Operational resilience was noted as a second major change area. One surprising finding was the rise of physical security in operation risks. This indicates that operational risk is increasingly linked to societal stability and the continuity of critical financial services rather than only to internal process failures. Interviewee also highlighted the issue of concentration risk in large technology and service providers. This is significant because disruption at a major provider could affect several financial institutions simultaneously. Thus, the findings support the view that operational resilience is not only an institution-specific issue, but also a systemic concern in an interconnected financial sector.

6.4 Reporting, monitoring, and scalable crisis response

The findings shows that reporting and monitoring changed after February 2022 but not necessarily through formal changes in reporting thresholds. One interviewee stated that the reporting threshold had not been lowered, due to the risk framework and risk appetite had remained the same. However, risk reporting increased as the total number of issues that crossed the threshold increased as a result in changed risk environment. This shows, and as the interview noted, that the existing risk framework as sufficient. However, other interviewee noted that reporting had to be filtered and layered due do the amount of information. Thus indicating that the reporting system was insufficient for the increase in reporting. Interviewee also described how indicators were divided into smaller parts so that more volatile areas could be followed more frequently. This supports the view that risk management adapted through increased sensitivity and more detailed monitoring rather than through a complete change in framework.

the development of automation in risk reporting can be interpreted as making intensified monitoring more manageable. As the increase in monitoring and reporting as a direct effect of Russia's full-scale war, it could be argued that the geopolitical shock caused the automation process development. However, the interviewee does not directly claim this.

A broader implication is that crisis response became more scalable. Interviewees described how some immediate crisis measures were later reduced, improved, or developed into more stable capabilities. This suggests that the permanent change was not necessarily the continuation of all crisis measures, but the ability to activate intensified monitoring, reporting, and response processes more quickly when needed.

6.5 Theoretical implications and research contribution

The findings support the theoretical framework but also refine it. From the enterprise risk management perspective, the findings show that geopolitical risk affected several parts of risk management, especially risk identification, response, monitoring, reporting, and operational resilience. However, the effect was not equal across all areas. Financial

risk frameworks remained stable, while compliance, customer-risk management, operational resilience, cyber risk, and reporting become more active. This suggests that geopolitical risk does not necessarily require a complete redesign of risk management frameworks, but it can change how existing frameworks are used and prioritised.

The findings also support the institutional theory perspective. The interviews showed that regulation, sanctions, supervisory expectations, and formal requirements were central drivers of change. Even internal assessment cannot be fully separated from the institutional environment, because financial institutions are required to assess risks continuously and adjust their controls when the operating environment changes. Thus, the findings imply that the financial sector risk management adaptation was shaped both by organisational assessment and institutional pressure.

The organisational resilience perspective is supported by the findings on crisis response, operational continuity, monitoring, and preparedness. The findings suggest that the permanent change was not necessarily the continuation of all temporary crisis measures. Instead, the more important change was the ability to increase monitoring, reporting, and response processes quickly when the situation required it.

This thesis contributed to the literature gap by showing how geopolitical risk translated into internal risk management practices on the financial sector. The findings support the existing literature of geopolitical risk being an underlying factor to other risk channels and areas and that it materialised through those channels. This supports the argument that geopolitical risk affects financial institutions through existing risk channels, while also showing that these channels may become more important under wartime conditions.

7 Conclusion

The purpose of this thesis was to examine how risk management practices in the European financial sector changed after Russia's full-scale invasion of Ukraine in February 2022. The study focused especially on financial institutions operating in the Finnish context and analysed how wartime geopolitical uncertainty and shocks affected risk management practices and attitudes. The research was guided by two research questions: how risk management changed after the beginning of the war, and through which channels the did the most important drivers of change occurred.

The thesis approached the topic through a qualitative research design based on five anonymised expert interviews. The empirical findings were analysed in relation to the theoretical framework, which combined enterprise risk management, institutional theory, and organisational resilience. This made it possible to examine risk management change both as an internal organisational process, and as a response to external institutional and geopolitical pressure.

Overall, the study shows that the post-2022 risk management change was not uniform across all risk areas. The clearest changes were found in sanctions, financial crime prevention, customer-risk management, operational resilience, cyber risk, and reporting. In contrast, traditional financial risk management frameworks appeared more stable, although monitoring and preparedness became more important.

7.1 Main conclusions on risk management change

The first research question asked how risk management changed in European financial institutions after the beginning of the war in Ukraine, and to what extent. Based on the empirical findings, risk management did change after February 2022, but the change was uneven across different risk areas and financial institutions were not similarly prepared. The findings do not support the conclusion that the war caused a complete transformation of financial-sector risk management. Instead, the change was more selective. Some risk areas became significantly more active and visible, while others remained largely based on existing frameworks and practices.

The identified changes were in sanctions, financial crime prevention, operational resilience, cyber risk, security, outsourcing, and reporting. In these risk areas, the post 2022 risk environment required faster reactions, more detailed monitoring and reporting, and stronger attention to external developments. Sanctions were the area with highest impact of change. Implemented Russia and Belarus related sanctions required financial institutions quickly to adjust processes. Sanctions were not new concept, but the scale and impact of the implemented sanctions were too much for existing sanctions processes.

Operational risk and resilience also became more important after February 2022. The findings showed increased attention to cyber threats, information security, continuity planning, third-party dependencies, outsourcing, and even physical security. These changes shows that operational risk is increasingly understood in relation to the wider security and geopolitical environment.

Reporting and monitoring also increased in importance. New systematic processes were created for information to move more freely, but at the same time filtering and layering was introduced in to the reporting process so that only the essential information goes to the management. In financial risk management reporting saw an increase in numbers even though reporting thresholds remained unchanged, thus highlighting the fact that external environment had become more demanding. One key finding was the created abilities to quickly respond to geopolitical shocks with developed heightened monitoring and reporting.

Overall, the findings suggest that the war acted more as an accelerator and intensifier than as the only source of risk management change. The most important change was the increased ability to react, monitor, and adjust existing practices under geopolitical uncertainty.

7.2 Main conclusions on drivers and transmission channels

The second research question asked through which channels the most prominent drivers of risk management change occurred. The findings show that the drivers of change were interconnected rather than separate. Russia's full-scale invasion of Ukraine was an important background factor, the the findings did not support the conclusion that all

observed changes were caused directly and only by the war and heightened geopolitical risk. Instead the main drivers included regulation, internal risk assessment, and wider market and macroeconomic conditions.

Regulation was identified as one of the clearest drivers for change. This was especially highlighted in sanctions related risk management, where Russia and Belarus related sanctions required fast process changes and more in-depth monitoring. Sanctions are based on regulatory demands and laws, and this shows a clear direct line with driver for change and a process change in financial institution. I this sense, sanctions formed the most direct link between the geopolitical shock and risk management practices.

Internal assessment was also highlighted as a driver for change. Interviewees described that financial institutions are required to assess changes in the external environment and adjust practices when needed. However, internal assessment can not be fully separated from regulation in the financial sector due to heavy regulation setting and supervisory expectations. Thus, even the driver for internal assessment has background in regulation.

Wider market and macroeconomic conditions were also identified to cause increase in monitoring and reporting rather than changes in risk management frameworks. These drivers however created permanent capabilities in the risk reporting process.

Overall, the findings suggest that geopolitical risk materialised mainly through existing risk categories. The most important channels were regulation and internal assessment, while financial risks were affected more indirectly through market and macroeconomic developments.

7.3 Contributions of the study

7.3.1 Theoretical contributions

This thesis contributes to the literature by linking geopolitical risk with internal risk management adaption in the financial sector. While previous research often examines geopolitical risk at the macro level, this study focuses on how it affects financial institutions through different risk channels. The findings suggest that geopolitical risk functions

mainly as an underlying driver for existing risk categories rather than creating entirely new one. Thus, this study failed to establish geopolitical risk as its own risk category.
This study also shows that the political shocks cause changed. on many different levels. On one hand in sanctions compliance a totally new processes had to be implemented quickly, while in the traditional financial risk, the existing tools and frameworks were adequate and only caused a rise in monitoring and reporting.

7.3.2 Empirical contributions

The empirical contribution of this thesis is based on the interviews with Finnish financial sector professionals. The findings provide insight into how experts experienced post 2022 changes in risk management practices. the clearest change was in sanction compliance, but operational resilience was also noted.
The study also demonstrates that risk management change was uneven across different risk areas. Traditional financial risk frameworks changed less significantly, with the main adjustment being intensified monitoring and reporting.

7.3.3 Practical contributions

The practical contribution of this thesis is that it highlights the importance os scalable and adaptive risk management capabilities. Financial institutions need the ability to strengthen monitoring and reporting processes quickly when the external environment requires.
The findings further suggest that sanctions compliance, cyber preparedness, operational resilience, and third-party risk management are particularly important under geopolitical uncertainty. Overall, the thesis shows that geopolitical risk should be understood as a factor that can simultaneously intensify multiple existing risk areas

7.4 Limitations

This thesis has several limitations that should be considered when interpreting the findings. The first limitation is the size of the empirical sample. This study is based on five

expert professional interviews. The sample delivers a comprehensive insight in to the financial sectors risk management practices, but however due to the size of the sample no generalisation could be made to the whole Finnish or European financial sector. Findings should therefore be understood as analytical insights into risk management adaptation.

A second limitation is connected to the nature of the interview data. The findings are based on the professional interpretations and experiences of the interviewees. The study does not independently measure whether the described risk management changes occurred. Therefore, the thesis can identify perceived and described changes, but it can not evaluate their effectiveness.

Third limiting factor concerns confidentiality. Since the topic concerned financial sector risk management, the interviewees were unable to discuss all organisational practices in detail. Thus, limiting the depth of the empirical data.

Finally, the thesis focuses mainly on Finnish financial institutions. Even though European financial sector in interconnected, conclusions about other countries or institutions should be made carefully.

7.5 Future research

Future research could expand this study in several ways. First, a larger empirical sample would allow a better understanding of how financial institutions have adapted to geopolitical uncertainty after February 2022. This could include interviews with several types of financial institutions and supervisory authorities.

Second, a future study could compare financial institutions across different European countries. This would help to examine whether the Finnish context differs from the other European markets, especially with countries with different levels of geopolitical exposure to Russia.

Third, future research could compare financial and non-financial sectors. This would make it possible to assess whether the changes identified in this thesis are specific to financial institutions or part of a broader organisational adaptation to geopolitical risk.

Lastly, future research could examine whether the risk management changes described in this thesis have improved actual resilience. This would require research that goes beyond interview based evidence and evaluates whether strengthened processes have improved institutions' ability to manage future geopolitical risks.

7.6 Final remarks

Overall, this thesis shows that Russia's full-scale invasion of Ukraine did not transform all areas of financial sector risk management equally. Instead, the post 2022 environment intensified selected risk areas and increased the need for more scalable abilities and more forward looking risk management practices. The most significant changes were in sanctions compliance, operational resilience, ICT risks and reporting. Traditional financial risk frameworks remained stable, although monitoring and preparedness became more important.

The findings suggest that geopolitical risk should not be understood only as an external background conditions. Geopolitical risk can affect several existing risk categories at the same time and create pressure for both longer-term capability and immediate crisis response development. Thus, effective risk management during geopolitical uncertainty requires the ability to quickly adjust the established frameworks when environment changes.

References

Adam, T. R., & Fernando, C. S. (2006). Hedging, speculation, and shareholder value. Journal of financial economics, 81(2), 283-309. https://doi.org/10.1016/j.jfineco.2005.03.014

Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. Journal of Banking & Finance, 36(12), 3213-3226. https://doi.org/10.1016/j.jbankfin.2011.10.020

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). Operational and cyber risks in the financial sector.

Alijoyo, A., & Norimarna, S. (2021, March). The role of enterprise risk management (ERM) using ISO 31000 for the competitiveness of a company that adopts the value chain (VC) model and life cycle cost (LCC) approach. In *3rd International Conference on Business, Management and Finance. Oxford, United Kingdom* (pp. 11-14).

Ali, Q. S. A., Hanafiah, M. H., & Mogindol, S. H. (2023). Systematic literature review of Business Continuity Management (BCM) practices: Integrating organisational resilience and performance in Small and medium enterprises (SMEs) BCM framework. International Journal of Disaster Risk Reduction, 99, 104135. https://doi.org/10.1016/j.ijdrr.2023.104135

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European journal of operational research, 253(1), 1-13. https://doi.org/10.1016/j.ejor.2015.12.023

Avgouleas, E., & Goodhart, C. (2015). Critical reflections on bank bail-ins. Journal of Financial Regulation, 1(1), 3-29. https://doi.org/10.1093/jfr/fju009

Baker, S. R., Bloom, N., & Davis, S. J. (2016). Measuring economic policy uncertainty. The quarterly journal of economics, 131(4), 1593-1636. https://doi.org/10.1093/qje/qjw024

Bank of Finland. Financial stability. Bank of Finland. Retrieved 2.3.2026 from https://www.suomenpankki.fi/en/financial-stability/

Bank of Finland. (2021). Financial stability. Annual Report 2021. Bank of Finland.

Bank of Finland. (2022). Financial stability. Annual Report 2022. Bank of Finland.

Bank of Finland. (2023). “Confidence in the financial system is created through persistent action.”

Bartram, S. M., Brown, G. W., & Conrad, J. (2011). The effects of derivatives on firm risk and value. Journal of financial and quantitative analysis, 46(4), 967-999. https://doi.org/10.1017/S0022109011000275

Basel Committee on Banking Supervision. Basel III: international regulatory framework for banks. Bank for International Settlements.

Basel Committee on Banking Supervision. (1982). Management of Banks’ International Lending: Country Risk Analysis and Country Exposure Measurement and Control. Bank for International Settlements.

Basel Committee on Banking Supervision. (2008). Principles for Sound Liquidity Risk Management and Supervision. Bank for International Settlement.

Basel Committee on Banking Supervision. (2009). Principles for sound stress testing practices and supervision.

Basel Committee on Banking Supervision. (2013). Basel III: The Liquidity Coverage Ratio and liquidity risk monitoring tools. Bank for International Settlements.

Basel Committee on Banking Supervision. (2022). Principles for the effective management and supervision of climate-related financial risks. Bank for International Settlements.

Basel Committee on Banking Supervision. (2014). Basel III: The Net Stable Funding Ratio. Bank for International Settlements.

Basel Committee on Banking Supervision. (2015). Corporate Governance Principles for Banks. Bank for International Settlements.

Basel Committee on Banking Supervision. (2018). Stress Testing Principles. Bank for International Settlements.

Basel Committee on Banking Supervision. (2024). Core Principles for Effective Banking Supervision. Bank for International Settlements.

Basel Committee on Banking Supervision. (2013). Principles for effective risk data aggregation and risk reporting. Bank for International Settlements.

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.

Bekaert, G., Harvey, C. R., Lundblad, C. T., & Siegel, S. (2016). Political risk and international valuation. Journal of Corporate Finance, 37, 1-23. https://doi.org/10.1016/j.jcorpfin.2015.12.007

Bellora-Bienengräber, L., Harten, C., & Meyer, M. (2023). The effectiveness of risk assessments in risk workshops: the role of calculative cultures. Journal of risk research, 26(2), 163-183. https://doi.org/10.1080/13669877.2022.2108120

Bernanke, B. S. (1983). “Non-Monetary Effects of the Financial Crisis in the Propagation of the Great Depression.” American Economic Review, 73(3), 257–276. https://doi.org/10.3386/w1054

Board of Governors of the Federal Reserve System, FDIC & OCC. (2026). Supervisory Guidance on Model Risk Management.

Bockius, H., & Gatzert, N. (2024). Organizational risk culture: A literature review on dimensions, assessment, value relevance, and improvement levers. European Management Journal, 42(4), 539-564. https://doi.org/10.1016/j.emj.2023.02.002

Braumann, E. C. (2018). Analyzing the role of risk awareness in enterprise risk management. Journal of management accounting research, 30(2), 241-268. https://doi.org/10.2308/jmar-52084

Braumann, E. C., Grabner, I., & Posch, A. (2020). Tone from the top in risk management: A complementarity perspective on how control systems influence risk awareness. Accounting, organizations and society, 84, 101128. https://doi.org/10.1016/j.aos.2020.101128

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long range planning, 48(4), 265-276. https://doi.org/10.1016/j.lrp.2014.07.005

Bryce, C., Chmura, T., Webb, R., Stiebale, J., & Cheevers, C. (2019). Internally reporting risk in financial services: an empirical analysis. Journal of Business Ethics, 156(2), 493-512. https://doi.org/10.1007/s10551-017-3530-6

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., & Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. Review of Accounting Studies, 19(1), 396-455. https://doi.org/10.1007/s11142-013-9258-3

Caldara, D., & Iacoviello, M. (2018). Measuring Geopolitical Risk. International Finance Discussion Papers 1222. https://doi.org/10.17016/IFDP.2018.1222

Caldara, D., & Iacoviello, M. (2022). Measuring geopolitical risk. American economic review, 112(4), 1194-1225.

Cavey, S. (2020, November 25). Financial Institutions Are Among the Most Regulated: Six Global Compliance Standards You Should Know. PaymentsJournal. Retrieved 2.4.2026 from https://www.paymentsjournal.com/financial-institutions-are-among-the-most-regulated-six-global-compliance-standards-you-should-know/

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management – Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/guidance-erm

Cont, R. (2006). Model uncertainty and its impact on the pricing of derivative instruments. Mathematical finance, 16(3), 519-547. https://doi.org/10.1111/j.1467-9965.2006.00281.x

Cordova-Pozo, K., & Rouwette, E. A. (2023). Types of scenario planning and their effectiveness: A review of reviews. Futures, 149, 103153. https://doi.org/10.1016/j.futures.2023.103153

Cosma, S., Rimo, G., & Torluccio, G. (2023). Knowledge mapping of model risk in banking. International Review of Financial Analysis, 89, 102800. https://doi.org/10.1016/j.irfa.2023.102800

Crawford, J., & Jabbour, M. (2024). The relationship between enterprise risk management and managerial judgement in decision-making: A systematic literature review. *International Journal of Management Reviews*, *26*(1), 110-136. https://doi.org/10.1111/ijmr.12337

Crovini, C., Giunta, F., Nielsen, C., & Simoni, L. (2026). Market valuation of risk reporting: the role of business model disclosure. Abacus, 62(1), 1-49. https://doi.org/10.1111/abac.12342

Council of the European Union. (2014). Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. Official Journal of the European Union, L 229, 31 July 2014.

Cutura, J. A. (2021). Debt holder monitoring and implicit guarantees: did the BRRD improve market discipline?. Journal of Financial Stability, 54, 100879. https://doi.org/10.1016/j.jfs.2021.100879

Dadoukis, A., Fusi, G., & Sakkas, A. (2025). Geopolitical risk premia in the European banking sector. Available at SSRN. https://dx.doi.org/10.2139/ssrn.5198995

Daly, M., & O Sullivan, P. (2020). Conduct risk within the United States financial sector. Journal of Decision Systems, 29(sup1), 4-17. https://doi.org/10.1080/12460125.2021.1882364

Danıelsson, J. (2002). The emperor has no clothes: Limits to risk modelling. Journal of Banking & Finance, 26(7), 1273-1296. https://doi.org/10.1016/S0378-4266(02)00263-7

Dhlamini, J. (2022). Strategic risk management: A systematic review from 2001 to 2020. Journal of Contemporary Management, 19(2), 212-237. https://doi.org/10.35683/jcm22008.165

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. Journal of political economy, 91(3), 401-419. https://doi.org/10.1086/261155

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms. Official Journal of the European Union, L 176, 338–436.

Directive (EU) 2014/59/EU Of The European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council.

Dittfeld, H., Scholten, K., & Van Donk, D. P. (2021). Proactively and reactively managing risks through sales & operations planning. International Journal of Physical Distribution & Logistics Management, 51(6), 566-584. https://doi.org/10.1108/IJPDLM-07-2019-0215

Di Zio, S., Bolzan, M., Marozzi, M., & Scioni, M. (2024). Delphi-based scenarios and risk management: A parallelism between paths destined to meet. Socio-economic planning sciences, 92, 101832. https://doi.org/10.1016/j.seps.2024.101832

Doerr, S., Gambacorta, L., Leach, T., Legros, B., & Whyte, D. (2022). Cyber risk in central banking. Bank for International Settlements, Monetary and Economic Department.

Duijm, N. J. (2015). Recommendations on the use and design of risk matrices. Safety science, 76, 21-31. https://doi.org/10.1016/j.ssci.2015.02.014

Dürst, N., & Kunz, J. (2025a). How to conduct effective risk culture assessments. Journal of Management Control, 1-46. https://doi.org/10.1007/s00187-025-00402-y

Dürst, N., & Kunz, J. (2025b). Embedding risk culture in a financial institution: an action research perspective. Review of Managerial Science, 1-36. https://doi.org/10.1007/s11846-025-00946-2

Eichholz, J., Hoffmann, N., & Schwering, A. (2024). The role of risk management orientation and the planning function of budgeting in enhancing organizational resilience and its effect on competitive advantages during times of crises. Journal of management control, 35(1), 17-58. https://doi.org/10.1007/s00187-024-00371-8

Elshandidy, T., Shrives, P. J., Bamber, M., & Abraham, S. (2018). Risk reporting: A review of the literature and implications for future research☆. Journal of Accounting Literature, 40(1), 54-82. https://doi.org/10.1016/j.acclit.2017.12.001

European Banking Authority. Deposit Guarantee Schemes data.

European Banking Authority. (2015). Guidelines on product oversight and governance arrangements for retail banking products.

European Banking Authority. (2018). Guidelines on Institutions' Stress Testing, EBA/GL/2018/04.

European Banking Authority. (2019). EBA Guidelines on ICT and Security Risk Management EBA/GL/2019/04.

European Banking Authority. (2019). Guidelines on outsourcing arrangements, EBA/GL/2019/02.

European Banking Authority. (2021). Guidelines on Internal Governance under Directive 2013/36/EU.

European Banking Authority. (2021). Guidelines on recovery plan indicators under Article 9 of Directive 2014/59/EU.

European Banking Authority. (2021). Risk Assessment of the European Banking System. December 2021.

European Banking Authority. (2022). Guidelines on common procedures and methodologies for the supervisory review and evaluation process and supervisory stress testing, EBA/GL/2022/03.

European banking Authority. (2024). Guidelines amending Guidelines EBA/2021/02 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/849

European Banking Authority. (2024). Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures.

European Banking Authority. (2025). Guidelines on the management of environmental, social and governance (ESG) risks.

European Banking Authority. (2025, April 3). Enhancing Europe's resilience against rising geopolitical risks. EBA.

European Central Bank. Addressing the impact of geopolitical risk. European Central Bank. Retrieved 5.5.2026 from https://www.bankingsupervision.europa.eu/framework/priorities/html/geopolitical-risk.en.html

European Central Bank. (2007). "Model risk: An overview of the issues." Financial Stability Review.

European Central Bank. (2016). SSM Supervisory Statement on Governance and Risk Appetite.

European Central Bank. (2018). ECB Guide to the internal capital adequacy assessment process (ICAAP).

European Central Bank. (2018). Report on the thematic review on effective risk data aggregation and risk reporting. ECB Banking Supervision.

European Central Bank. (2020). Guide on climate-related and environmental risks.

European Central Bank. (2021). Supervisory priorities for 2022–2024. ECB Banking Supervision.

European Central bank. (2022). 2022 climate risk stress test. European Central Bank - Banking Supervision.

European Central Bank. (2022.11.17). Pillar 3 reconciliation: improving banks' reporting discipline. European Central Bank. Retrieved 3.5.2026 from https://www.bankingsupervision.europa.eu/press/supervisory-newsletters/newsletter/2022/html/ssm.nl221117_2.en.html

European Central Bank. (2025). ECB Guide to Internal Models.

European Central Bank. (2024). Guide on effective risk data aggregation and risk reporting.

European Central Bank. (2025). Supervisory methodology 2025: Supervisory Review and Evaluation Process. https://www.bankingsupervision.europa.eu/activities/srep/2025/html/ssm.srep202511_supervisorymethodology2025.en.html

European Commission. (2022). In focus: Reducing the EU's dependence on imported fossil fuels. European Commission. Retrieved 3.4.2026 from https://commission.europa.eu/news-and-media/news/focus-reducing-eus-dependence-imported-fossil-fuels-2022-04-20_en

Fatemi, A., & Luft, C. (2002). Corporate risk management: costs and benefits. Global Finance Journal, 13(1), 29-38. https://doi.org/10.1016/S1044-0283(02)00037-6

Financial Action Task Force. (2014). Guidance for a Risk-Based Approach: The Banking Sector.

Financial Stability Institute. (2019). Definition of capital in Basel III — Executive Summary. Bank for International Settlements.

Financial Stability Board. (2013). Principles for an Effective Risk Appetite Framework.

Financial Stability Board, International Monetary Fund & Bank for International Settlements. (2009). Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments. https://www.imf.org/external/np/g20/pdf/100109.pdf

Financial Stability Board. (2023). Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities.

Financial Stability Board. (2024). Key Attributes of Effective Resolution Regimes for Financial Institutions, revised version 2024.

Finanssivalvonta. Customer due diligence and customer identification. Finanssivalvonta. Retrieved from https://www.finanssivalvonta.fi/en/consumers/customer-due-diligence-and-customer-identification/ on 4.5.2026.

Finnish Financial Supervisory Authority. Capital adequacy and liquidity regulation (CRR/CRD). https://www.finanssivalvonta.fi/en/regulation/regulatory-framework/crrcrd/

Ghafoori, E., Mata, F., Lauren, N., Faulkner, N., & Tear, M. J. (2023). Measuring risk culture in finance: Development of a comprehensive measure. Journal of Banking & Finance, 148, 106720. https://doi.org/10.1016/j.jbankfin.2022.106720

Gilmore, N., Koskinen, I., Burr, P., Obbard, E., Sproul, A., Konstantinou, G., ... & Bruce, A. (2023). Identifying weak signals to prepare for uncertainty in the energy sector. Heliyon, 9(11).

Glette-Iversen, I., Flage, R., & Aven, T. (2023). Extending and improving current frameworks for risk management and decision-making: A new approach for incorporating dynamic aspects of risk and uncertainty. Safety science, 168, 106317. https://doi.org/10.1016/j.ssci.2023.106317

Graham, J. R., & Rogers, D. A. (2002). Do firms hedge in response to tax incentives?. The Journal of finance, 57(2), 815-839. https://doi.org/10.1111/1540-6261.00443

Grieser, F., & Pedell, B. (2022). Exploring risk culture controls: to what extent can the development of organizational risk culture be controlled and how?. Journal of Accounting & Organizational Change, 18(5), 752-788. https://doi.org/10.1108/JAOC-11-2020-0189

Hardaway, K., & Flage, R. (2025). A framework for evolving assumptions in risk analysis. Risk Analysis, 45(8), 2232-2242. https://doi.org/10.1111/risa.70009

Harju, A., Schaefer, K., Hallikas, J., & Kähkönen, A. K. (2024). The role of risk management practices in IT service procurement: A case study from the financial services industry. Journal of Purchasing and Supply Management, 30(2), 100899.

Herrmann, J. W. (2015). Engineering decision making and risk management. John Wiley & Sons.

Hodula, M., Janků, J., Malovaná, S., & Ngo, N. A. (2024). Geopolitical risks and their impact on global macro-financial stability: Literature and measurements (No. 9/2024). BOFIT Discussion Papers.

Ittner, C. D., & Keusch, T. (2015, March). The influence of board of directors' risk oversight on risk management maturity and firm risk-taking. AAA. https://dx.doi.org/10.2139/ssrn.2482791

Hassanein, A. (2022). Risk reporting and stock return in the UK: does market competition matter?. The North American Journal of Economics and Finance, 59, 101574. https://doi.org/10.1016/j.najef.2021.101574

Heinle, M. S., & Smith, K. C. (2017). A theory of risk disclosure. Review of Accounting Studies, 22(4), 1459-1491. https://doi.org/10.1007/s11142-017-9414-2

Hiebl, M. R. (2024). The integration of risk into management control systems: towards a deeper understanding across multiple levels of analysis. Journal of Management Control, 35(1), 1-16. https://doi.org/10.1007/s00187-024-00373-6

Ho, P. H., Huang, C. W., Lin, C. Y., & Yen, J. F. (2024). Risk culture in corporate innovation. International Review of Financial Analysis, 91, 102999. https://doi.org/10.1016/j.irfa.2023.102999

Huber, C., Kraus, K., & Meidell, A. (2025). Integrating the balanced scorecard and enterprise risk management: Exploring the dynamics between management control anchor practices and subsidiary practices. Management Accounting Research, 66, 100924.

International Organization for Standardization [ISO]. (2018). ISO 31000:2018 Risk management — Guidelines. ISO

Institute of Internal Auditors (IIA). (2020). The Three Lines Model: The IIA's Framework for Governance, Risk Management, and Control. Institute of Internal Auditors.

Ji, P., & Wei, L. (2023). Hedging with derivatives to increase firm value. Finance Research Letters, 55, 103981. https://doi.org/10.1016/j.frl.2023.103981

Klinke, A., & Renn, O. (2001). Precautionary principle and discursive strategies: classifying and managing risks. Journal of Risk Research, 4(2), 159-173. https://doi.org/10.1080/136698701750128105

Knight, F. H. (1921). Risk, uncertainty and profit (Vol. 31). Houghton Mifflin.

Kountur, R., & Sari, M. R. (2023). Risk identification approaches and the number of risks identified: the use of work breakdown structure and business process. Humanities and Social Sciences Communications, 10(1), 588. https://doi.org/10.1057/s41599-023-02028-8

Kumari, S. (2025). Investigating the Role of Middle Management in Bridging the Gap Between Strategic Planning and Operational Execution in Large-Scale Enterprises. Journal of Informatics Education and Research, 5(4). https://doi.org/10.52783/jier.v5i4.3992

Lau, C. K. (2016). How corporate derivatives use impact firm performance?. Pacific-Basin Finance Journal, 40, 102-114. https://doi.org/10.1016/j.pacfin.2016.10.001

Leva, M. C., Balfe, N., McAleer, B., & Rocke, M. (2017). Risk registers: Structuring data collection to develop risk intelligence. Safety science, 100, 143-156. https://doi.org/10.1016/j.ssci.2017.05.009

Levi, M., & Reuter, P. (2006). Money laundering. Crime and justice, 34(1), 289-375. https://doi.org/10.1086/501508

Luís, A., Garnett, K., Pollard, S. J., Lickorish, F., Jude, S., & Leinster, P. (2021). Fusing strategic risk and futures methods to inform long-term strategic planning: Case of water utilities. Environment Systems and Decisions, 41(4), 523-540. https://doi.org/10.1007/s10669-021-09815-1

Maia, I. R. D., & Chaves, G. M. M. (2016). Integration of risk management into strategic planning: a new comprehensive approach. Society of Actuaries and Casualty Actuarial Society.

Marc, M., Arena, M., & Peljhan, D. (2023). The role of interactive style of use in improving risk management effectiveness. Risk Management, 25(2), 9. https://doi.org/10.1057/s41283-023-00114-4

Ministry of the Interior (2025, September 15). Minister Rantanen and Commissioner Brunner: Finland's strong eastern border secures all of Europe. Finnish Government.

Mikes, A. (2009). Risk management and calculative cultures. Management accounting research, 20(1), 18-40. https://doi.org/10.1016/j.mar.2008.10.005

Monazzam, A., & Crawford, J. (2024). The role of enterprise risk management in enabling organisational resilience: a case study of the Swedish mining industry. Journal of Management Control, 35(1), 59-108. https://doi.org/10.1007/s00187-024-00370-9

OECD. (2022). G20/OECD High-Level Principles on Financial Consumer Protection. OECD.

Oehmen, J., Günther, A., Herrmann, J. W., Schulte, J., & Willumsen, P. (2020). Risk management in product development: risk identification, assessment, and mitigation–a literature review. In Proceedings of the Design Society: DESIGN Conference (Vol. 1, pp. 657-666). Cambridge University Press. https://doi.org/10.1017/dsd.2020.27

Ogbeide, H., Thomson, M. E., Gonul, M. S., Pollock, A. C., Bhowmick, S., & Bello, A. U. (2023). The anti-money laundering risk assessment: A probabilistic approach. Journal of Business Research, 162, 113820. https://doi.org/10.1016/j.jbusres.2023.113820

Organisation for Economic Co-operation and Development (OECD). (2014). Risk management and corporate governance. OECD Publishing. https://www.oecd.org/en/publications/risk-management-and-corporate-governance_9789264208636-en.html

Pehlivanlı, D., Alp, E. A., & Katanalp, B. (2024). Introducing the overall risk scoring as an early warning system. Expert Systems with Applications, 246, 123232. https://doi.org/10.1016/j.eswa.2024.123232

Phan, D. H. B., Tran, V. T., & Iyke, B. N. (2022). Geopolitical risk and bank stability. Finance Research Letters, 46, 102453. https://doi.org/10.1016/j.frl.2021.102453

Posch, A. (2020). Integrating risk into control system design: The complementarity between risk-focused results controls and risk-focused information sharing. Accounting, organizations and society, 86, 101126. https://doi.org/10.1016/j.aos.2020.101126

Power, M. (2009). The risk management of nothing. Accounting, organizations and society, 34(6-7), 849-855. https://doi.org/10.1016/j.aos.2009.06.001

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (2022, December 27). Official Journal of the European Union, L 333/1, europa.eu

Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism. (2024, June 19). Official Journal of the European Union,

Roychowdhury, S., Shroff, N., & Verdi, R. S. (2019). The effects of financial reporting and disclosure on corporate investment: A review. Journal of accounting and economics, 68(2-3), 101246. https://doi.org/10.1016/j.jacceco.2019.101246

Saharan, A., & Rajendran, M. (2024). Do corporate hedge theories explain the natural hedge strategies of firms? A meta-analytic review. International Review of Economics & Finance, 94, 103361. https://doi.org/10.1016/j.iref.2024.05.040

Saunders, M., Lewis, P., & Thornhill, A. (2003). Research methods forbusiness students. Essex: Prentice Hall: Financial Times.

Schäffer, U., & Storek, F. (2022). Transforming risk management: Transforming risk management. Controlling & Management Review, 66(1), 30-35. https://doi.org/10.1007/s12176-021-0435-0

Simola, H. (2024, July 4). The collapse of trade with Russia has had a limited effect on Finnish manufacturing. Bank of Finland Bulletin. https://urn.fi/URN:NBN:fi-fe2024070560698

Singh, D., & Gaur, A. S. (2021). Risk mitigation strategies in international B2B relationships: Role of institutions and governance. Journal of Business Research, 136, 1-9. https://doi.org/10.1016/j.jbusres.2021.07.026

Single Resolution Board. Resolution tools.

Single Resolution Board. (2024). Minimum Requirement for Own Funds and Eligible Liabilities.

Stulz, R. M. (2004). Should we fear derivatives?. Journal of Economic perspectives, 18(3), 173-192.

Stulz, R. M. (2014). Governance, risk management, and risk-taking in banks (No. w20274). National Bureau of Economic Research. https://doi.org/10.3386/w20274.

Syrová, L., & Špička, J. (2022). Exploring the indirect links between enterprise risk management and the financial performance of SMEs. Risk management, 25(1), 1. https://doi.org/10.1057/s41283-022-00107-9

Tekathen, M., & Dechow, N. (2020). Semantic narrowing in risk talk: The prevalence of communicative path dependency. Management Accounting Research, 48, 100692. https://doi.org/10.1016/j.mar.2020.100692

The Risk Caolition. (2023, May 26). Navigating Not easily Quantifiable risks: the role of the board Risk Committee. The Risk Coalition. Retrieved 2.4.2026 from https://www.riskcoalition.org.uk/blog-posts/navigating-not-easily-quantifiable-risks-the-role-of-the-board-risk-committee

Themsen, T. N., & Skærbæk, P. (2018). The performativity of risk management frameworks and technologies: The translation of uncertainties into pure and impure risks. Accounting, Organizations and Society, 67, 20-33. https://doi.org/10.1016/j.aos.2018.01.001

Thomas, P., Bratvold, R. B., & Eric Bickel, J. (2014). The risk of using risk matrices. SPE Economics & Management, 6(02), 56-66. https://doi.org/10.2118/166269-PA

Tiberius, V., Siglow, C., & Sendra-García, J. (2020). Scenarios in business and management: The current stock and research opportunities. Journal of business research, 121, 235-242. https://doi.org/10.1016/j.jbusres.2020.08.037

Tobias, A., & Brunnermeier, M. K. (2016). CoVaR. The American Economic Review, 106(7), 1705.

Tröger, T. H. (2018). Too complex to work: a critical assessment of the bail-in tool under the European bank recovery and resolution regime. Journal of Financial Regulation, 4(1), 35-72. https://doi.org/10.1093/jfr/fjy002

Udoh, O. R. (2024). Enhancing internal audit efficiency for effective risk management and corporate governance frameworks. International Journal of Research Publication and Reviews, 5(12), 3646-3659.

Varotto, S. (2011). Liquidity risk, credit risk, market risk and bank capital. International Journal of Managerial Finance, 7(2), 134-152. https://doi.org/10.1108/17439131111122139

Viscelli, T. R., Beasley, M. S., & Hermanson, D. R. (2016). Research insights about risk governance: Implications from a review of ERM research. *Sage Open*, *6*(4), 2158244016680230. https://doi.org/10.1177/2158244016680230

Wang, P., & Liang, S. (2025). Internal audit independence, legal person governance structure, and financial reporting quality. International Review of Economics & Finance, 101, 104142. https://doi.org/10.1016/j.iref.2025.104142

Whipple, T., & Pitblado, R. (2010). Applied risk‐based process safety: A consolidated risk register and focus on risk communication. Process Safety Progress, 29(1), 39-46. https://doi.org/10.1002/prs.10320

Zhu, Y., & Sardana, D. (2020). Multinational enterprises' risk mitigation strategies in emerging markets: A political coalition perspective. Journal of World Business, 55(2), 101044. https://doi.org/10.1016/j.jwb.2019.101044

Xiao, L., & Cao, H. (2017). Organizational resilience: The theoretical model and research implication. In ITM Web of Conferences (Vol. 12, p. 04021). EDP Sciences. https://doi.org/10.1051/itmconf/20171204021

Appendices

Appendix 1. Core interview questions

1. Could you briefly describe your role and responsibilities in the organization?
2. Have you noticed any changes in risk management after February 2022?
3. If yes, through which channel have the changes occurred? In other words, were the changes initiated internally, forced by the market situation, or required by regulation?
4. In which business lines have the changes taken place? For example, operational resilience, market risk, sanctions/compliance, or liquidity risk. Has any area become particularly emphasized?
5. Could you describe some processes that have changed, been added, or been removed? Has the focus shifted toward certain processes?
6. Has the threshold for reporting decreased within the organization?
7. Are the possible changes only temporary, or has there been a permanent change in operating practices?
8. Considering that the geopolitical situation is ongoing, is proactive assessment of risk processes being conducted in relation to possible country risk?
9. Were there any warning signs before 2022 that the risk management framework should have detected?