

**MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY
KARAZIN BANKING INSTITUTE**

Department: **Banking Business and Financial Technologies**

Specialty: **072 Finance, Banking, Insurance and Stock Market**
Educational program: **Financial technologies and banking management**

Group: AF-23M **full-time mode of study**

QUALIFYING MASTER'S THESIS

on the topic:

**ENSURING THE FINANCIAL SECURITY OF THE BANKING SYSTEM:
INTERNATIONAL CONDITIONS**

submitted by the applicant of higher education
LYU DANNIER

The qualifying master's thesis was accepted for
defense by the decision of the Department of
Banking Business and Financial Technologies

Minutes No 4 dated «25» 11 2024

Head of Department

Doctor of Economics, Professor

_____ **Galina AZARENKOVA**

Scientific advisor

Phd of law, As. professor

_____ **Roman GALYCH**

Kharkiv 2024

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
V.N. KARAZIN KHARKIV NATIONAL UNIVERSITY

Faculty EDUCATION AND RESEARCH INSTITUTE
“KARAZIN BANKING UNIVERSITY”
Department Banking Business and Financial Technologies
Level of higher education second (master’s) level
Specialty 072 Finance, Banking, Insurance and Stock Market
Educational program Financial technologies and banking management

APPROVED

Head of department of
Banking Business and Financial Technologies
Doctor of Economics, Professor

Galina AZARENKOVA
(signature) (name and surname)

«25» 09_ 2024.

**ASSIGNMENT
FOR A QUALIFYING MASTER’S THESIS**
assigned to
LYU DANNIER,

1. The topic of the thesis: "ENSURING THE FINANCIAL SECURITY OF THE BANKING SYSTEM: INTERNATIONAL CONDITIONS"

Scientific advisor – PhD of Law, Assoc. Prof. Roman Galych

(last name, first name, patronymic, academic degree, academic title)

approved by the order of the University dated 17 September 2024. No 4601-3к/1025

2. Deadline for submission of thesis by the student 18/11/2024

3. List of questions to be researched:

In section 1: Thoroughly comprehend the financial situation and holistically assess the various financial risks. Conduct a systematic analysis of financial data, promptly identify potential financial risks, and formulate effective risk management measures.

In section 2: Recognize the distinctive characteristics of the bank's asset-liability structure. Carefully analyze the composition and inter-relationships of the bank's assets and liabilities.

In section 3: Comprehensively assess the systemic vulnerability of the Chinese banking system. Analyze the key factors that impact the stability of the banking industry. Establish a risk assessment indicator system that is tailored to the context of China.

4. Plan of qualifying master's thesis

№	Name of work stages
1	Selection of the topic
2	Approval of the plan and tasks of thesis
3	Implementation of thesis
4	Submission of thesis to the department to check for the presence of borrowings from other documents
5	Completion of the admission procedure for the protection of thesis
6	Defence of thesis

5. Date of assignment issuance _25 September 2024

Student _____ LYU DANNIER
Signature

LYU DANNIER
initials, surname

Scientific advisor _____
Signature

Roman Galych
initials, surname

ABSTRACT
ON QUALIFICATION MASTER'S WORK
«ENSURING THE FINANCIAL SECURITY OF THE BANKING
SYSTEM: INTERNATIONAL CONDITIONS» OF
LYU DANNIER

Qualification Master's Work contains 59 pages, 2 tables, 1 figures, 21 references.

Object of research banking system

Subject of research is Ensuring financial security of the banking system: international conditions

Purpose of qualification master's work As a result of the rapid ecological changes in the banking industry, the environment of financial supervision is constantly being adjusted, leading to frequent banking crises. The occurrence of banking crises is not an isolated event, but rather presents a cyclical, frequent, and expanding trend. Every economic or financial crisis is first felt in the banking sector, highlighting the extreme importance of banks in the modern economy and finance.

Tasks of qualification master's work are: From the perspective of the development process of the modern economy, the banking industry was initially cautious and conservative with the innovation of financial instruments and the generalization of financial ecology, more and more of the real economy began to be financialized. Banks not only became the suppliers of credit resources for enterprises and residents, but also increasingly became important supports for fiscal budgets and public debt. The types and development models of banking institutions have become more diverse.

The results obtained can be used to frequent banking crises, highlighting the cyclical and expanding trend of such events. These crises are often the first signs of economic or financial upheaval, underscoring the crucial role of banks in the modern economy. Initially cautious and conservative, banks have evolved to become key providers of credit resources, supporting enterprises, residents, fiscal budgets, and public debt. The diversification of banking institutions and the financialization of the real economy have further shaped the industry, necessitating ongoing adjustments in financial supervision to address the changing landscape and ensure stability.

Keyword: Financial security banking system crisis conditions

CONTENT

INTRODUCTION.....	6
CHAPTER 1 An overview of the international financial security system.....	8
1.1. The composition of the international financial system.....	8
1.2. The role of the banking system in the financial system.....	10
1.3. The impact of international conditions on financial security.....	12
1.4 Typical case analysis.....	14
CHAPTER 2 Cross-border banking supervision and cooperation.....	16
2.1. The challenges of cross-border banking supervision	16
2.2. International regulatory cooperation mechanisms and agreements.....	21
CHAPTER 3 Capital adequacy ratio and liquidity management.....	22
3.1. Capital adequacy ratio requirements and calculation method.....	22
3.2. Liquidity management strategies and practices	23
3.3. Analysis of the relationship between Capital adequacy ratio and liquidity risk.....	24
CONCLUSIONS.....	58
REFERENCES.....	59

INTRODUCTION

In the modern conditions of the development of the economy of Ukraine, ensuring and adequately assessing the financial stability of the bank is a task that both the banks and the state regulators, whose competence is this issue, are trying to solve. That is why many approaches and methods aimed at determining the level of financial stability of banks were developed. These approaches differ in the composition of criteria, variety of indicators, normative values, etc. In addition, the existing methods, although they contribute to the determination and calculation of the appropriate value, are not always suitable for a comprehensive assessment of the level of financial stability of the bank, which determines the problem, relevance and feasibility of further research.

The importance of this question determined the choice of the topic, determined the goal, task, logic and content of the research.

The theoretical basis of the work is the scientific works of domestic and foreign scientists and specialists on ensuring financial stability. The scientific and theoretical basis of the research was the scientific works of the following scientists: Crockett E., Shinazi J., Azarenkova G., Baranovskyi O., Golovko O., Dzyublyuk O., Dovgan Zh., Kovalenko V., Kolobov Yu., Krukhmal O., Maksimova A., Marych M., Mishchenko V., Panasenko G., Petrychenko L., Pogorelenko N., Naumenkova S., Savradim V., Fursova V., Khuthorna M., Sheludko N., Shpika P., Chiyan D., and other scientists. Paying tribute to the contribution of well-known scientists, it should be noted that the volatility of indicators that form the basis of diagnostics of the financial stability of the banking system requires constant and increased attention to it, in order to ensure appropriate adaptive adjustments in the components of macroprudential policy.

The object of the study is the banking system of Ukraine.

The subject of the research is modern approaches and methods of diagnosing the stability of the banking system based on macroeconomic and prudential indicators.

Research methods: theoretical generalization - to study and systematize existing

theoretical approaches to determining the content and structural components of the stability of the banking system and the basics of monitoring and interpreting system stability based on indicators of financial stability; a systematic approach to the study of organizational and economic support, a graphic method for the purpose of summarizing statistical data and their analysis; mathematical modeling - to calculate the main indicators for the purpose of their further evaluation and interpretation.

The scientific novelty of the qualifying master's thesis consists in the generalization of existing theoretical provisions regarding the definition of the concepts of "financial stability of the banking system" and "financial stability of the bank", as well as in the application of mathematical modeling tools and methods for assessing the financial stability of Ukrainian banks.

1. AN OVER VIEW OF THE INTERNATIONAL FINANCIAL SECURITY SYSTEM

1.1 The composition of the international financial system

The international financial system is a complex and extensive system, it covers the rules, practices, policies, mechanisms and organizations that regulate the international payment, settlement, exchange and transfer of national currencies. Its composition can be analyzed from several angles, and the following is a detailed description from both broad and narrow perspectives:

In a broad sense, the international financial system consists mainly of three parts: the International Monetary System: the International Monetary System is the core part of the international financial system; It regulates the relations between national currencies and international payment rules. In the current international environment, the international monetary system such as Jamaica system, the international reserve currency diversification, exchange rate arrangements are also diversified, providing countries with more options, at the same time, the stability and predictability of the international monetary system put forward higher requirements. International Financial Organization System: THE INTERNATIONAL FINANCIAL ORGANIZATION SYSTEM includes International Monetary Fund (IMF) , World Bank and other international financial institutions. These institutions play an important role in the international financial system, such as providing financial assistance, promoting international cooperation and coordinating international monetary policy. The IMF plays a key role in maintaining the stability of the international monetary system and promoting global economic growth, while the World Bank focuses on poverty reduction and development. International Financial Supervision System: with the development of international financial market, financial supervision becomes more and more important. The international financial supervision system aims to ensure the stability, transparency and effective operation of the financial market and prevent the

occurrence of systemic financial risks. The system includes the cooperation and coordination mechanism among financial supervision institutions, and the formulation and implementation of international financial supervision standards.

In a narrow sense, the international financial system mainly refers to the international monetary arrangements, specifically including the following aspects:

International Exchange Rate System: the international exchange rate system refers to the exchange rate relationship between national currencies and its decision mechanism. Under the Jamaican system, fixed exchange rate and floating exchange rates coexist, and each country has the right to choose the appropriate exchange rate system according to its own economic situation and development needs.

Balance of payments and international reserve system: Balance of payments refers to the record of economic transactions between a country and other countries over a period of time. The International Reserve System refers to the foreign exchange reserve, Gold Reserve and other assets that countries hold in order to meet the demand of international payments. In the modern international financial system, the adjustment of balance of payments and the management of international reserves have become an important part of monetary policy and macroeconomic management.

Coordination of national and international economic policies: countries need to take into account changes in the international economic environment and policy responses of other countries when formulating and implementing economic policies. Therefore, the coordination of national economic policy and international economic policy has become an important part of the international financial system. Such coordination will help reduce trade frictions and promote global economic cooperation and development.

Challenges to International Financial Security, The international financial security system faces numerous challenges, including:

Financial Crises : Events such as the 2008 global financial crisis highlight the vulnerabilities of the system and the need for improved risk management and crisis prevention mechanisms.

Geopolitical Risks : Tensions and conflicts between countries can disrupt financial markets, disrupt trade flows, and lead to capital outflows, affecting financial stability.

Cybersecurity Threats : The increasing digitization of financial services makes them vulnerable to

cyberattacks, which can disrupt operations, steal sensitive information, and cause financial losses. Climate Change : Physical risks from extreme weather events and transition risks from the shift to a low-carbon economy can impact the financial sector, including through asset stranding and valuation changes.

Measures to Safeguard International Financial Security to address these challenges, various measures have been implemented: Strengthening Regulation and Supervision : Enhancing prudential standards for financial institutions, improving transparency and disclosure requirements, and strengthening cross-border cooperation and information sharing among regulators. Developing Crisis Prevention and Resolution Mechanisms : Establishing early warning systems, contingency planning, and resolution frameworks to manage and mitigate the impact of financial crises. Promoting Financial Inclusion and Stability : Expanding access to financial services for underserved populations, while ensuring that these services are provided in a stable and sustainable manner. Addressing Geopolitical Risks : Engaging in dialogue and cooperation among countries to manage geopolitical tensions and reduce their impact on financial markets. Enhancing Cybersecurity : Implementing robust cybersecurity measures, including encryption, multi-factor authentication, and regular security assessments, to protect financial systems and data. Addressing Climate-Related Risks : Integrating climate considerations into financial decision-making, developing green financial products, and promoting sustainable finance practices.

1. 2. The role of the banking system in the financial system

Banking system plays an important role in the financial system, is the core component of the financial market, for economic stability, growth and development has a far-reaching impact. The following are the main roles and functions of the banking system in the financial system:

Credit Intermediation: Banks act as a bridge between the supply and demand of funds by taking deposits and making loans, the idle, small, short-term monetary funds in society will be concentrated and converted into large, long-term funds to support

social and economic development. This kind of credit intermediary function is the most basic and important function of the bank.

Payment intermediary: Banks provide efficient and convenient means of payment for customers through account management, transfer and settlement, which greatly reduces transaction costs and speeds up the circulation of money and the turnover of funds, it promotes the smooth production and exchange of commodities.

Credit creation: on the basis of the function of credit intermediary and payment intermediary, the bank can create the derivative deposit which exceeds the original deposit by means of loans, investments, etc., play an important role in promoting economic development. But this also requires banks in the process of credit creation must follow certain principles to avoid excessive expansion of financial risks.

Financial services: with the continuous development and improvement of the financial market, banks have also provided diversified financial services, including deposit and loan, settlement, exchange, agency, information consulting, investment and financing, etc. , the utility model meets the diversified financial needs of customers and improves the efficiency and convenience of the financial market. The central bank, the core of the banking system, regulates the Macroeconomic regulation and control of money supply and credit through reserve requirement, rediscount rates and open market operations, thus affecting economic growth, price stability, balance of payments and other macroeconomic objectives. The banking system is therefore also an important tool for national Macroeconomic regulation and control.

The cornerstone of stabilizing the financial market: the banking system can absorb and disperse financial risks and maintain the stability of the financial market through its huge asset scale and extensive business network. At the same time, the banking system also undertakes the social responsibility of protecting the safety of customer funds and preventing financial crimes, which provides strong guarantee for the healthy development of the financial market.

1.3.The impact of international conditions on financial security

The impact of international conditions on financial security is multifaceted and complex. Various global factors can significantly influence the stability and resilience of financial systems, both domestically and internationally. Here are some key considerations:

Geopolitical Risks

Geopolitical tensions and conflicts, such as trade wars, sanctions, and military conflicts, can disrupt global supply chains, affect capital flows, and create market volatility. These events can lead to uncertainty and risk aversion in financial markets, impacting asset prices, credit availability, and overall financial stability.

Economic Conditions

The global economic environment, including growth rates, inflation levels, and interest rate movements, has a direct impact on financial security. For instance, a global economic downturn can lead to increased defaults on loans, reduced consumer spending, and weakened corporate profits, all of which can affect the health of financial institutions.

Financial Globalization

Financial globalization has increased the interconnectedness of financial markets, making it easier for risks to spread across borders. This means that financial instability in one country can quickly spread to others, creating a domino effect that can affect global financial security.

Regulatory Changes

Changes in international financial regulations can also impact financial security. New rules and standards, such as those related to capital requirements, liquidity management, and risk management, can affect the operations and profitability of financial institutions. Additionally, cross-border regulatory cooperation and enforcement actions can help mitigate risks but also present challenges in terms of coordination and compliance.

Technological Advancements

The rapid development of financial technology (fintech) and digital currencies has brought new opportunities but also new risks to financial security. Cybersecurity threats, data breaches, and fraud are becoming increasingly sophisticated and can have a significant impact on financial institutions and their customers.

Climate Change

Climate change is another emerging risk that can affect financial security. Extreme weather events, sea-level rise, and other climate-related phenomena can damage infrastructure, disrupt supply chains, and affect the profitability of businesses. These impacts can have a ripple effect on financial institutions, particularly those with significant exposures to affected sectors.

Mitigating the Impact of International Conditions on Financial Security

To mitigate the impact of international conditions on financial security, several strategies can be employed:

Diversification : Diversifying investments and exposures across different geographic regions, asset classes, and sectors can help reduce the risk of concentrated exposures.

Risk Management : Implementing robust risk management frameworks and monitoring systems can help identify and mitigate potential risks before they become critical.

Regulatory Cooperation : Enhancing cross-border regulatory cooperation and information sharing can help address emerging risks and ensure a more consistent and effective regulatory environment.

Technology Adoption : Leveraging technology, such as advanced analytics and artificial intelligence, can improve risk detection and response capabilities.

Climate Resilience : Building resilience to climate-related risks through adaptive strategies and sustainable practices can help protect financial institutions and their customers from the adverse impacts of climate change.

The global economic situation is one of the important factors affecting financial security. When the global economy is growing steadily, international trade and investment activities are active and financial markets are booming, contributing to the

stability and security of the financial system. However, if the global economy falls into a recession or growth slows, corporate profits fall, investor confidence suffers, financial market volatility increases and financial security is challenged.

Geopolitical tensions or conflicts often lead to increased volatility in financial markets and pose a threat to financial security. For example, regional conflicts, terrorist activities, trade disputes between countries can trigger market panic, leading to capital outflows, exchange rate fluctuations, stock market falls and other adverse consequences. In addition, geopolitical risks may also affect the operations and investment decisions of multinational enterprises, further exacerbating the uncertainty in financial markets.

The change of international trade environment has an important impact on financial security. The rise of trade protectionism, the increase of trade barriers and the frequent occurrence of trade disputes may lead to the deterioration of international trade environment and affect the profitability and market competitiveness of multinational enterprises. At the same time, a trade war could trigger currency volatility and financial market turmoil, posing a challenge to financial security.

International capital flows are another key factor affecting financial security. The freedom and scale of capital flow directly affect the stability and security of financial market. When there is a large inflow of international capital into a country, it may contribute to a boom in the country's financial markets and a rise in asset prices; however, if the outflow accelerates, it may lead to turmoil in the country's financial markets and a fall in asset prices. In addition, cross-border financial activities may bring the risk of cross-border contagion of financial risks, posing a threat to global financial security.

The adjustment and change of international financial policy have important influence on financial security. The adjustment of monetary policy, fiscal policy and financial regulatory policy in major economies may lead to volatility and uncertainty in financial markets. For example, monetary policy adjustments by central banks in advanced economies such as the Fed could lead to increased global capital flows and exchange rate volatility; The loose fiscal policies adopted by some countries in

response to the economic recession may increase the government debt burden and financial risks

1.4 Typical case analysis

Global financial crisis, also known as the world financial crisis, sub-prime crisis, credit crisis, refers to the global financial assets or financial institutions or financial market crisis. It manifests itself in a sharp fall in global financial asset prices or in the collapse or near-collapse of financial institutions, or in the collapse of a financial market such as the stock market or the bond market. The global financial crisis began to appear in the 19th century, among which the most famous ones were the financial crisis that caused the Great Depression in 1930 and the global financial crisis that broke out in 2008. The following is a detailed analysis of the global financial crisis: definitions and characteristics: a global financial crisis is a sharp deterioration of all or most of the financial sector's financial indicators, to affect the relevant countries or regions and even the world's economic stability and development. Features: the Stock Market Plunge, the international financial crisis is one of the main signs. Capital flight is one of the main signs of the international financial crisis. Normal Bank credit relationship is destroyed, and accompanied by bank runs, money shortage and financial institutions, such as a large number of bankruptcies and failures. Official reserves have fallen sharply, the currency has depreciated sharply and inflation is high. Difficulties in repaying debts.

2. CROSS-BORDER BANKING SUPERVISION AND COOPERATION

2.1 The challenges of cross-border banking supervision

Cross-border banking supervision faces a multitude of challenges, stemming from various aspects such as regulatory differences, information sharing barriers, and the complexity of cross-border financial activities. Here are some key challenges:

Regulatory Differences

Different countries have varying levels of financial market development, legal systems, and cultural backgrounds, which lead to significant differences in financial regulatory standards and requirements. These differences pose significant challenges for cross-border banks that must comply with different regulatory rules when operating in multiple countries. This increases compliance costs and complexity, and may lead to regulatory arbitrage or non-compliance risks.

Information Sharing Barriers

Effective cross-border banking supervision requires timely and accurate information sharing among regulators in different countries. However, due to legal, technical, and privacy protection constraints, cross-border information sharing often faces numerous obstacles. This lack of information sharing can hinder the timely detection and resolution of potential risks, thereby affecting the timeliness and effectiveness of supervision.

Complexity of Cross-border Financial Activities

Cross-border financial activities involve multiple countries and regions, and require the participation and cooperation of multiple regulatory agencies. The differences in responsibilities, resource allocations, and risk management strategies among regulatory agencies in different countries further complicate the coordination of cross-border supervision. Moreover, different countries may have differing attitudes and strategies towards financial risks, which further increases the difficulty of cross-border regulatory coordination.

Technological Challenges

With the rapid development of financial technology, cross-border banks are increasingly relying on digital and automated systems for their operations. However, this also brings new technological challenges to supervision, such as cybersecurity threats, data breaches, and fraud. Regulators need to keep pace with technological advancements to ensure that cross-border banks are operating securely and in compliance with regulations.

Language and Cultural Barriers

Language and cultural differences can also pose challenges to cross-border banking supervision. Regulators may struggle to communicate effectively with banks operating in different languages or cultural contexts, which can hinder the effectiveness of supervision and cooperation.

Mitigating the Challenges of Cross-border Banking Supervision

To address these challenges, several strategies can be employed:

Strengthening International Cooperation : Regulators should strengthen cooperation and coordination with their international counterparts to develop common standards and practices for cross-border banking supervision. This can help reduce regulatory differences and facilitate information sharing.

Improving Information Sharing Mechanisms : Efforts should be made to establish efficient cross-border information sharing mechanisms, overcoming legal, technical, and privacy protection barriers. This will enable regulators to obtain timely and accurate information about the operations and risks of cross-border banks.

Enhancing Technological Capabilities : Regulators should invest in technological upgrades to keep pace with the rapid development of financial technology. This includes enhancing cybersecurity measures, improving data analysis capabilities, and developing automated supervision tools.

Promoting Cultural and Language Understanding : Regulators should strive to understand the language and cultural context of cross-border banks they supervise. This can be achieved through training programs, language courses, and cultural exchange activities

cross-border risk contagion. Cross-border banks operate globally and have

complex business networks, the risk of any one branch can quickly spread to other branches around the world, forming a systemic risk. Especially when a country has financial crisis, transnational banks may become an important channel of risk transmission, aggravating the turbulence of global financial markets. For example, in the 2008 global financial crisis, a number of international banks were hit hard by their large holdings of risky assets, which led to a global credit crunch and market panic. Inconsistency in regulatory standards there are significant differences in financial regulatory systems, laws and regulations and regulatory standards between different countries, which pose significant challenges to cross-border banking regulation. On the one hand, the need for cross-border banks to comply with the regulatory requirements of multiple countries at the same time increases compliance costs and operational complexity; on the other hand, inconsistencies in regulatory standards may lead to regulatory arbitrage, that is, international banks choose to operate in less regulated countries or regions to escape the more stringent regulatory requirements.

The global activities of multinational banks are so complex that it is difficult for regulators to fully understand their risk profile and operations. The Information asymmetry problem is so severe that it is difficult for regulators to identify and respond to potential risks in a timely manner. In addition, the disclosure of information by multinational banks is often inadequate, especially in cross-border operations, where the transparency and comparability of information is low, further adding to the difficulty of regulation. Cross-border banking supervision needs close cooperation and coordination among national supervisors. In practice, however, cross-border regulatory co-operation often faces obstacles due to differences in regulatory systems, interests and cultural backgrounds. For example, the cooperation mechanism of national regulators in information sharing, joint inspection and crisis management is not perfect, so it is difficult to deal with the cross-border risk effectively.

The monetary policy of our country adheres to the main keynote of “Give priority to me” and matches the economic cycle of our country. It is expected that the monetary policy of our country will remain on the loose side in the future, but the structural monetary policy will take the lead. This policy orientation has a profound

impact on the operation and supervision of multinational banks in China. On the one hand, loose monetary policy helps lower market interest rates and provides a more favorable financing environment for multinational banks. At the same time, structural monetary policy tools, such as targeted RRR cuts and re-lending, can guide multinational banks to increase financial support for key areas and weak links, and promote economic restructuring and upgrading. On the other hand, the prudent and loose monetary policy also puts forward higher requirements for the risk management of transnational banks. Against the background of lower interest rates and intensified market competition, multinational banks need to pay more attention to risk management and internal control to ensure the sound operation of business. At the same time, regulators also need to strengthen the supervision of transnational banks to prevent and defuse financial risks.

Establishing and perfecting the cooperation mechanism of cross-border supervision is the key to deal with the challenges of cross-border banking supervision. National regulators should strengthen cooperation in information-sharing, joint inspections and crisis management to jointly develop cross-border regulatory standards and rules. At the same time, strengthen communication and coordination with international financial organizations and regional financial regulatory agencies to promote the formation of a global unified cross-border banking regulatory system. It is an effective way to reduce regulatory arbitrage to promote the unification or compatibility of supervisory standards of transnational banks. On the basis of respecting their respective regulatory systems, national regulatory bodies should strengthen the coordination and convergence of regulatory standards, and form regulatory standards that are both in line with national conditions and internationally comparable. At the same time, international banks are encouraged to proactively adapt to and comply with higher regulatory standards to enhance the overall stability and security of the global financial system.

Strengthening information disclosure and transparency construction of transnational banks is an important means to enhance the effectiveness of supervision. Regulators should require multinational banks to disclose information on their

operations, financial position and risk profile in accordance with uniform standards and formats to ensure that information is comprehensive, accurate and timely. At the same time, we should strengthen the exchange and sharing of information among transnational banks, improve the comparability and usability of information, and provide more sufficient basis for the supervisory authorities. It is the key to ensure the sound operation of transnational banks to clarify the responsibilities and obligations of home and host countries in the supervision of transnational banks. Home country regulators should strengthen their supervision and coordination of the global operations of transnational banks to ensure that they comply with international regulatory standards and requirements. For their part, host country regulators should conduct stringent supervision and inspection of the domestic branches of transnational banks to ensure that they comply with local laws and regulations and regulatory requirements. At the same time, we should strengthen the supervision cooperation and coordination between the home country and the host country to deal with the cross-border risks brought by transnational banks.

Macro-prudential regulatory framework is an important tool to deal with systemic financial risks. National Supervisors should learn from international advanced experience, establish and improve macro-prudential supervision system, and strengthen the monitoring and evaluation of cross-border banking systemic risk. Through the implementation of counter-cyclical capital buffer, leverage limits, liquidity management and other measures to enhance the ability of transnational banks to resist systemic risk. At the same time, we will strengthen coordination and coordination between Macro and micro prudential regulation to form regulatory synergy and enhance overall regulatory effectiveness. With the development of financial technology, regulators should actively explore the use of technology to enhance the efficiency and accuracy of cross-border banking supervision. For example, the use of big data, artificial intelligence and other technologies to conduct in-depth mining and analysis of business data of transnational banks to identify potential risk points in a timely manner; and the use of blockchain technology to enhance the transparency and traceability of cross-border transactions, to prevent money laundering

and other illegal activities; to build an intelligent regulatory platform, realize the automatic collection, processing and analysis of regulatory information, and enhance the real-time and accuracy of regulation.

2.2 International regulatory cooperation mechanisms and agreements

The Basel Accord is a set of key global bank capital and risk regulatory standards developed by the Bussell Commission. The Basel Committee is one of the four standing committees of the Bank for International Settlements, comprising national banking regulators. The agreement is aimed at improving the stability and resilience of the global banking sector by imposing Capital adequacy ratio, risk management and disclosure requirements on banks, to ensure that banks have enough capital to cover potential losses and risks.

3.CAPITAL ADEQUACY RATIO AND LIQUIDITY MANAGEMENT

3.1 Capital adequacy ratio requirements and calculation method

The Capital adequacy ratio is an important measure of the capital adequacy of banking institutions, reflecting the extent to which banks are able to absorb losses with their own capital in the face of risk. The following is a detailed explanation of the Capital adequacy ratio requirements and the calculation method:

The requirements of the Capital adequacy ratio are in accordance with the requirements of the capital management measures for commercial banks (on a trial basis)(Order No. 1 of 2012 of the CBRC) , commercial banks are required to meet the following minimum Capital adequacy ratio: core Capital adequacy ratio: not less than 5% . Core tier one capital is the most important part of bank capital, including paid-in capital or common stock, capital reserve, Surplus Reserve, General Risk Reserve, undistributed profit and minority shareholder capital.

Grade I Capital adequacy ratio: not less than 6% . Tier one capital includes not only core tier one capital, but also other tier one capital, such as preferred stock and its premium, minority shareholder capital can be included in part.

Capital adequacy ratio: not less than 8% . Total capital includes core tier one capital, other tier one capital and tier two capital.

The Capital adequacy ratio $\text{Capital adequacy ratio} = (\text{total capital} - \text{corresponding capital deduction}) / \text{risk-weighted assets} \times 100\%$ tier one Capital adequacy ratio = $(\text{tier one capital} - \text{corresponding capital deduction}) / \text{risk-weighted assets} \times 100\%$ core tier one Capital adequacy ratio = $(\text{core tier one capital} - \text{corresponding capital deduction}) / \text{risk-weighted assets} \times 100\%$ of which, total capital includes core tier one capital, other tier one capital and tier two capital; risk-weighted assets include credit risk-weighted assets, market risk-weighted assets and operational risk-weighted assets. These assets are given different risk weights based on different levels of risk, and then calculate the total risk-weighted assets.

3.2 Liquidity management strategies and practices

Corporate liquidity management strategies and practices 1. Short-term strategy to determine liquidity needs: the enterprise needs to assess the daily cash flow and expected short-term liabilities to determine the minimum amount of liquidity reserves required. This involves detailed analysis of the financial position and operations to ensure that sufficient funds are available to cover both day-to-day operations and short-term liabilities. Optimize cash management: improve the efficiency of cash receipts and expenditures, reduce cash flow fluctuations. Enterprises can achieve the effective management of cash flow by reasonably arranging the collection of accounts receivable and the payment time of accounts payable, as well as by means of centralized collection and payment. Strengthen the management of accounts receivable: make a reasonable account period, strengthen communication and cooperation with customers, ensure that accounts receivable can be collected in time, reduce the risk of bad debts. At the same time, enterprises can also use credit insurance and other means to further protect the safety of accounts receivable. Control the level of inventory: to ensure that the inventory turnover rate is reasonable, to avoid excessive inventory of the capital occupation and waste. Enterprises can improve the efficiency of inventory management by implementing lean inventory management and optimizing supply chain. Short-term financing strategy: according to the financing needs and conditions of enterprises, choose appropriate financing instruments, such as bank loans, commercial paper, short-term bonds. At the same time, we should pay attention to the financing cost and risk to ensure the rationality and effectiveness of financing strategy.

Long-term strategy to determine long-term funding needs: assess the size and timing of long-term funding based on business development planning, investment plans, and capital structure considerations. This helps the enterprise to make the reasonable fund raising and the use plan. Drawing up fund raising plan: including long-term debt financing, equity financing, internal financing and other ways. Enterprises should choose appropriate financing methods according to their own conditions and market environment to ensure the stability and sustainability of long-term funds.

Capital Investment: Adopt diversified investment strategy, diversify risk, and cooperate with liquidity management strategy. Through reasonable investment arrangement, improve the rate of return of long-term capital, while ensuring the safety of capital.

The practice suggests setting up a liquidity management system, including setting up a special liquidity management team, setting up a liquidity prediction model, setting up a monitoring and reporting mechanism to ensure the effectiveness and timeliness of liquidity management. Strengthen risk management: regularly assess and adjust liquidity management strategy, pay attention to the market environment and industry trends, timely response to potential risks and challenges. Improve the use of funds: through optimizing the allocation of funds, strengthen the internal management, improve the use of funds, create more value for the enterprise.

3.3 Analysis of the relationship between Capital adequacy ratio and liquidity risk

The relationship between the capital adequacy ratio (CAR) and liquidity risk in the banking sector is a crucial aspect of financial stability and risk management. Below is an analysis of this relationship:

Definition and Importance

Capital Adequacy Ratio (CAR) : This is a measure of a bank's capital relative to its risk-weighted assets. It reflects the bank's ability to absorb potential losses and maintain solvency.

Liquidity Risk : This refers to the risk that a bank may not be able to meet its short-term obligations as they come due. It arises when a bank lacks sufficient liquid assets to cover its immediate financial needs.

Positive Correlation

A higher CAR generally indicates a lower liquidity risk for a bank. This is because:

Enhanced Risk Absorption : A higher CAR means that the bank has more capital to absorb losses, including those arising from liquidity shortfalls. This increases the

bank's resilience and ability to withstand unexpected shocks.

Improved Credit Quality : Banks with higher CARs tend to have better credit quality, as they are more likely to adhere to prudent lending practices. This reduces the likelihood of default and, consequently, the need for the bank to sell assets quickly to meet liquidity needs.

Enhanced Market Confidence : A higher CAR can boost market confidence in the bank, making it easier for the bank to raise funds and manage liquidity during times of stress.

Negative Correlation (Indirect)

While a higher CAR directly reduces liquidity risk, there can be indirect effects that may complicate this relationship:

Risk-Taking Behavior : In some cases, banks with high CARs may take on more risk in pursuit of higher profits. This can include investing in less liquid assets, which may increase liquidity risk in the long run. However, this is generally mitigated by prudent risk management practices.

Regulatory Requirements : Regulatory requirements for CARs can vary across countries and regions. In some cases, these requirements may lead to banks focusing more on meeting regulatory thresholds rather than managing liquidity risk effectively.

Empirical Evidence

Empirical studies have generally supported the positive correlation between CAR and reduced liquidity risk. For example:

Studies have shown that banks with higher CARs are less likely to experience liquidity crises.

During financial crises, banks with higher CARs have been able to maintain stable funding and continue lending to the economy.

There is a close relationship between Capital adequacy ratio and liquidity risk, two crucial aspects of banking management. The following is an analysis of Capital adequacy ratio and liquidity risk: I. Capital adequacy ratio definition: a Capital adequacy ratio is the ratio of capital held by a bank to its risk-weighted assets, it reflects the extent to which banks are able to absorb losses with their own capital when exposed

to risk. The higher the Capital adequacy ratio, the more solvent the banks are and the better able to withstand risk. Market Environment: changes in the market environment, such as business cycles and financial policies, have an impact on the Capital adequacy ratio of banks. Regulatory Requirements: regulators have clear Capital adequacy ratio requirements that banks need to meet in order to maintain sound operations. The profitability, asset quality and risk management of a bank will affect its Capital adequacy ratio. What it does: Improve Risk Resilience: Capital adequacy ratio banks are more resilient to risks and better able to protect depositors and other creditors. To promote the sound operation of banks: the Capital adequacy ratio requirements of banks to strengthen risk management, improve asset quality, and thus achieve sound operation.

Definition of liquidity risk: liquidity risk is the risk that a bank can not meet the needs of creditors or debtors in time when it is faced with capital flow. This could damage the creditworthiness of banks and even create systemic risk. Influence Factor: balance sheet structure: the banks balance sheet structure directly affects its liquidity level. If the maturity mismatch between assets and liabilities is serious, or the structure of liabilities is too single, it may increase liquidity risk. Market Environment: changes in the market environment, such as market interest rate fluctuations, financial market turbulence, etc. , may have an impact on bank liquidity. Customer Behavior: customer deposits and withdrawals also have uncertainty, which may have an impact on bank liquidity. Relationship to Capital adequacy ratio: Interaction: there is an interaction between Capital adequacy ratio and liquidity risk. Banks that are Capital adequacy ratio tend to be more risk-resilient, which helps reduce liquidity risk. At the same time, good liquidity conditions also helped banks to maintain high Capital adequacy ratio. Co-management: Banks need to take comprehensive measures to manage Capital adequacy ratio and liquidity risks. For example, by optimizing the structure of assets and liabilities, strengthening liquidity forecasting and monitoring, improving the level of risk management to reduce liquidity risk; Increase Capital adequacy ratio by increasing the channels through which capital is replenished and used more efficiently.

In the case of our listed commercial banks, Capital adequacy ratio has an

important impact on their profitability and liquidity risk. On the one hand, moderate Capital adequacy ratio can improve the banks risk resistance, reduce the loss reserve, reduce the cost of financing, enhance market credibility, and is conducive to the promotion of profitability. On the other hand, excessive Capital adequacy ratio may also lead to excessive idling of bank funds, reducing the efficiency of capital utilization, thus negatively affecting profitability. At the same time, the level of Capital adequacy ratio is also directly related to the level of liquidity risk of banks. Capital adequacy ratio banks tend to have better liquidity risk management capabilities and are better able to manage liquidity risks.

Financial market stability and risk prevention

1. Financial market stability assessment methods

Framework and principles of Financial Market Stability Assessment Framework

financial market stability assessment usually includes risk identification, risk assessment, risk monitoring and early warning, risk response and disposal. Risk identification is the basis for a comprehensive inventory of the various types of risks that may exist in financial markets; risk assessment is the core, and quantitative analysis is used to assess the probability and impact of risks; risk monitoring and early warning is the guarantee, establish a real-time monitoring system to capture risk signals and give early warning; risk response and disposal is the key to develop and implement effective risk management and disposal strategies.

principle of comprehensiveness of assessment: the assessment should cover all important areas and key links in financial markets to ensure that there are no blind spots. Forward-looking principle: pay attention to the future potential risk prediction, advance the development of response measures. The principle of dynamism: the financial market environment is changing and the assessment methodology needs to be flexible to adapt to new circumstances. Scientific principle: Based on rigorous data analysis and model prediction, to ensure the objectivity and accuracy of the assessment results。

The common systemic risk assessment models include network model, Financial Stability Index (FSI) , stress test and scenario analysis. The network model analyzes the transmission path and speed of risk in the network by constructing the related

network among financial institutions, and the financial stability index by integrating several macroeconomic and financial market indicators, while assessing the overall stability of the financial system, stress tests and scenario analysis combine extreme changes in macroeconomic variables to simulate the response of the financial system under different scenarios.

Risk prevention measures and practice cases

Risk identification and evaluation definition: risk identification is the process that economic units and individuals judge, classify and sort the faced and potential risks, and identify the nature of risks. On the basis of risk identification, risk assessment is to estimate and forecast the probability and degree of loss by using probability theory and mathematical statistics. Case in point: in financial institutions, conduct regular security vulnerability scans and network penetration tests to identify and assess possible security risks to systems, including hacking, customer information leakage, and so on.

The definition of risk avoidance: risk avoidance is the investment subject consciously give up risk behavior, completely avoid specific loss risk. Case Study: An Enterprise, considering investing in a new technology, finds that the technology has high technical risk and market uncertainty, so it decides to abandon the investment plan in order to avoid potential losses.

Loss control definition: loss control is not to abandon the risk, but to plan and take measures to reduce the possibility of loss or reduce the actual loss. Practice case: in the supply chain management, manufacturing enterprise through the establishment of supplier evaluation mechanism, signed long-term cooperation agreement, the establishment of supply chain risk-sharing mechanism and other measures, reduce losses due to supply disruptions or quality issues.

Definition of risk transfer: risk transfer refers to the transfer of the risk of the assignor to the transferee by contract.

The main forms are contracts and insurance. Practice case: the enterprise purchases the property insurance or the liability insurance, will because of the natural disaster, the accident and so on causes the property loss or the legal indemnity responsibility transfers to the insurance company to assume.

Definition of risk retention: risk retention is the assumption of risk, which means that if the loss occurs, the economic main body will pay with any funds available at that time.

Case study: after fully evaluating its risk tolerance, the enterprise decides to keep some low or controllable risks for itself, such as setting up risk reserves to deal with possible losses. Second, practice case detailed financial institutions risk prevention case background: a financial institution faced with the risk of hacking, which may lead to customer information leakage and financial losses.

Preventive measures: strengthen network security protection, including the installation of firewall, intrusion detection system. Conduct regular security vulnerability scanning and network penetration testing. Store and transfer customer information in encrypted form. Establish an emergency response mechanism to take immediate action if unusual activity or attack is detected. Train the staff to improve the awareness of network security and the ability to prevent. Results: through the implementation of the above measures, financial institutions successfully reduce the risk of hacking, to ensure the security of customer information and funds.

Financial market stability and risk prevention

Financial market stability and risk prevention are closely intertwined concepts that are crucial for the health and sustainability of financial systems. Below is a detailed analysis of these topics:

Financial Market Stability, Financial market stability typically refers to market prices remaining relatively stable over a certain period of time, with fluctuations within an acceptable range. This stability is the foundation for the effective operation of the market, ensuring the rational allocation of resources and the long-term confidence of investors. A stable market can provide investors with peace of mind to invest funds, and businesses can more easily obtain financing, thereby driving sustained economic growth. Factors influencing the stability of financial markets

The intrinsic mechanism of the market: The liquidity, transparency, and efficiency of the financial market are all key factors. A highly liquid market can ensure that the buying and selling of assets are not affected by significant fluctuations in

trading volume, thereby maintaining price stability. Transparency helps reduce information asymmetry and lower the likelihood of market manipulation. Efficient financial markets can quickly respond to market changes and reduce the magnitude of price fluctuations.

Macroeconomic policies: The rational use of monetary and fiscal policies can effectively regulate the economic cycle and reduce the impact of economic fluctuations on the market. For example, when the economy is overheated, excessive investment can be suppressed by raising interest rates or reducing government spending to prevent the formation of market foam; During an economic recession, stimulating the economy by lowering interest rates or increasing government spending can help stabilize market sentiment.

Regulatory measures: Strong regulation can prevent market manipulation, insider trading, and other improper behaviors, protecting the interests of investors. At the same time, regulatory agencies also need to continuously improve market rules, adapt to the development of financial innovation, and ensure the healthy development of the market.

Market participant behavior: Rational investor behavior can promote the smooth operation of the market, while irrational speculative behavior may lead to increased market volatility. Therefore, improving the education level of investors and enhancing their risk awareness are crucial for maintaining market stability.

Establish a sound regulatory system: Strengthen financial supervision, ensure the stable operation of financial institutions, and prevent the generation and spread of financial risks. Regulatory agencies should strengthen the supervision of capital adequacy, risk management, and internal control of financial institutions.

Implementing macroeconomic policies: formulating and implementing appropriate monetary policies, fiscal policies, and structural reforms to promote stable economic growth. Economic policies should focus on preventing and resolving financial risks, while avoiding excessive expansion and relaxation.

Enhancing the risk resistance capability of financial institutions: Financial institutions should strictly comply with risk management regulations, establish

effective risk monitoring and evaluation systems, and improve their own risk resistance capabilities. In addition, financial institutions should strengthen internal controls to prevent the occurrence of operational and credit risks.

Strengthening financial market supervision: ensuring the fair, transparent, and orderly operation of financial markets. Regulatory agencies should strengthen their supervision of financial market transactions, information disclosure, and market manipulation to prevent abnormal fluctuations and vicious competition in the financial market.

Establish and improve the financial risk management system: Establish and perfect the financial risk management system, strengthen early warning and monitoring of systemic and cross-border risks. Financial institutions should actively assess and manage various risks to ensure asset liability balance and financial stability.

Promoting the diversified development of financial markets: By introducing more diversified investors and financing channels, the impact of a single market or product on market stability can be reduced. For example, encouraging more companies to raise funds through channels such as the stock market and bond market; At the same time, promote the development of financial innovation products, such as futures and other derivative instruments, to meet the needs of different investors.

Strengthen international cooperation: Strengthen cooperation with financial regulatory agencies in other countries and regions, share experiences and information, and jointly address global financial risks.

Evaluating the stability of financial markets typically involves multiple aspects, including but not limited to:

Credit rating: Evaluating the credit status of financial institutions or products through rating agencies to understand their default risk and stability.

Market indicator analysis: The volatility of market indicators such as stock price indices, bond yields, and exchange rates can reflect the stability of the financial market.

Stress testing: Simulating extreme market conditions to evaluate the risk resistance and stability of financial institutions or markets.

Macro prudential policy assessment: Evaluating the impact of macroeconomic

policies on financial market stability, as well as the necessity and effectiveness of policy adjustments.

Financial market stability refers to the condition where financial markets operate smoothly, with prices reflecting fundamental values and market participants able to fulfill their obligations. Stability is essential for maintaining investor confidence, fostering economic growth, and preventing financial crises.

However, achieving and maintaining financial market stability can be challenging due to various factors, including market volatility, interconnectedness among financial institutions, and external shocks such as natural disasters or geopolitical events. These factors can disrupt market functioning, leading to instability and potential losses for investors.

Risk Prevention, Risk prevention is a systematic approach aimed at identifying, assessing, controlling, and reducing the potential negative impacts that potential risks may have on organizations or individuals. It involves multiple stages, including risk identification, risk assessment, risk control, and risk monitoring.

The Importance of Risk Prevention

Protecting asset security: Through risk prevention, potential threats to asset security can be identified and addressed in a timely manner, ensuring that assets are not damaged.

Maintaining reputation: Effective risk prevention measures can reduce reputation damage caused by risk events and maintain a good image for the organization or individual.

Promoting sustainable development: Risk prevention helps organizations or individuals make wise decisions in the face of uncertainty, thereby promoting their sustainable development.

Methods for risk prevention

Risk identification: By collecting and analyzing relevant information, potential risks are identified. This includes both internal and external risks, such as market risk, credit risk, operational risk, etc.

Risk assessment: Evaluate the identified risks to determine their likelihood and degree of impact. This helps identify which risks need to be prioritized and what measures should be taken to mitigate them.

Risk control: Based on the results of risk assessment, develop and implement corresponding risk control measures. This may include strategies such as risk avoidance, risk reduction, risk transfer, and risk acceptance.

Risk avoidance: Avoiding risks by giving up or changing certain activities. For example, avoiding entering high-risk markets or industries, or changing business processes to reduce potential risks.

Risk reduction: taking measures to reduce the likelihood or impact of risk occurrence. For example, strengthening internal controls, enhancing employee safety awareness, adopting new technologies, etc.

Risk transfer: transferring risks to third parties through purchasing insurance, signing contracts, and other means. For example, purchasing property insurance to transfer the risk of asset loss caused by natural disasters.

Risk acceptance: After assessing the likelihood and impact of the risk, it is decided to accept the risk and take corresponding response measures. This is usually a strategy adopted in situations where the risk is low or cannot be effectively transferred.

Risk monitoring: Continuously monitor the effectiveness of risk control measures and make adjustments and optimizations based on actual situations. This helps ensure the effectiveness of risk prevention measures and timely detection of new risks.

Practical cases of risk prevention

Enterprise risk management: Many enterprises have established a comprehensive risk management system, including setting up risk management committees, formulating risk management policies, conducting risk assessments and monitoring, etc. These measures help companies identify and respond to potential risks in a timely manner, ensuring their stable development.

Risk management of financial institutions: Financial institutions play an important role in risk prevention. They reduce financial risks by implementing strict

risk management systems, strengthening internal controls, and providing risk management training. In addition, financial institutions actively participate in international financial regulatory cooperation to jointly address global financial risks.

Personal risk management: Individuals can also protect their interests through risk prevention. For example, purchasing health insurance to cope with disease risks, purchasing property insurance to cope with natural disaster risks, and reducing investment risks through diversified investments.

Challenges and Responses to Risk Prevention

Although risk prevention plays an important role in protecting asset security, maintaining reputation, and promoting sustainable development, it still faces some challenges in practice. For example, risk identification may be affected by information asymmetry, risk assessment may be influenced by subjective judgments, and risk control measures may be affected by resource constraints. To address these challenges, the following measures need to be taken:

Strengthening information collection and analysis: By enhancing information collection and analysis capabilities, potential risks can be more accurately identified.

Improving the accuracy of risk assessment: Adopting more scientific and objective risk assessment methods can reduce the impact of subjective judgments on risk assessment results.

Optimize resource allocation: Ensure the implementation of key risk control measures by optimizing resource allocation under limited resource conditions.

Strengthening international cooperation and communication: By enhancing international cooperation and communication, we can jointly address cross-border risks and challenges.

Risk prevention is a proactive approach to managing potential risks that could threaten financial market stability. It involves identifying, assessing, and mitigating risks before they can cause significant harm. Effective risk prevention requires a comprehensive understanding of the risks facing financial markets and the tools and techniques available to manage them.

Types of Risks

Credit Risk : The potential loss arising from a borrower's inability to repay a loan or meet its contractual obligations. Financial institutions use credit risk management techniques, such as credit scoring models and credit derivatives, to assess and mitigate this risk.

Market Risk : The potential loss due to fluctuating market prices of financial instruments, including risks associated with interest rates, currencies, equities, commodities, and derivatives. Market risk management involves using techniques like portfolio diversification, hedging, and stress testing to mitigate potential losses.

Liquidity Risk : Arises when an institution is unable to fulfill its financial obligations due to an insufficient availability of liquid assets. Effective liquidity risk management involves maintaining adequate liquidity buffers, developing contingency funding plans, and regularly monitoring and stress testing liquidity positions.

Operational Risk : The risk of financial loss due to inadequate or failed internal processes, systems, or human error. It includes risks associated with technology failures, fraud, legal and regulatory compliance, and vendor management. Operational risk management involves implementing robust internal controls, conducting regular audits, and training staff on risk awareness.

Systemic Risk : The risk of widespread disruptions or failures in the financial system that could have a significant impact on the overall economy. It arises from interconnectedness and interdependencies among financial institutions. Systemic risk management involves regulatory oversight, stress testing, and contingency planning at both the institutional and systemic levels.

Risk Assessment and Mitigation

Risk assessment is the process of identifying and analyzing potential risks and their potential negative impacts on organizations or individuals. It usually includes the following steps:

Risk identification:

Identify potential risks that may have a negative impact on the project, organization, or individual.

It can be identified through various methods, such as brainstorming, expert

interviews, historical data analysis, etc.

Risk analysis:

Conduct in-depth analysis of identified risks to determine their likelihood of occurrence, degree of impact, and potential causes.

Qualitative and quantitative methods can be used for analysis, such as risk matrix, Monte Carlo simulation, etc.

Risk assessment:

Based on the comprehensive analysis of risk analysis results, determine which risks need to be prioritized and what measures should be taken to reduce them.

Risk assessment typically involves weighing the likelihood and impact of risks to determine their level and priority.

2、 Risk mitigation

Risk mitigation is the process of taking measures to reduce or mitigate potential risks based on risk assessment. Risk mitigation measures can include the following:

Risk avoidance:

Avoiding risks by changing plans, strategies, or behaviors.

For example, avoiding entering high-risk markets and choosing low-risk investment portfolios.

Risk reduction:

Take measures to reduce the likelihood or impact of risk occurrence.

For example, strengthening internal controls, enhancing employee safety awareness, adopting new technologies.

Risk transfer:

Transfer risks to third parties through purchasing insurance, signing contracts, and other means.

For example, purchasing property insurance to transfer asset loss risks caused by natural disasters, or transferring supply chain risks through signing risk sharing agreements with suppliers.

Risk acceptance:

After assessing the likelihood and degree of impact of the risk, it is decided to

accept the risk and take corresponding response measures.

This is usually a strategy adopted in situations where the risk is low or cannot be effectively transferred.

Practical cases of risk assessment and mitigation

Enterprise risk management:

Enterprises can reduce the impact of potential risks on their businesses by establishing a comprehensive risk management system, including setting up a risk management committee, developing risk management policies, conducting risk assessments and monitoring.

For example, a certain enterprise successfully reduced financial and operational risks by strengthening internal control and risk management training.

Risk management of financial institutions:

Financial institutions play an important role in risk prevention by implementing strict risk management systems, strengthening internal controls, and providing risk management training to reduce financial risks.

For example, banks reduce credit risk by implementing strict credit approval processes and strengthening post loan management.

Personal risk management:

Individuals can also protect their interests through risk assessment and mitigation.

For example, purchasing health insurance to cope with disease risks, purchasing property insurance to cope with natural disaster risks, and reducing investment risks through diversified investments.

Challenges and responses to risk assessment and mitigation

Although risk assessment and mitigation play an important role in protecting the interests of organizations and individuals, there are still some challenges in practice:

Asymmetric information:

During the risk assessment process, there may be an issue of information asymmetry, which makes it difficult to accurately identify all potential risks.

The response methods include strengthening information collection and analysis

capabilities, as well as utilizing the opinions of professional institutions and experts.

Resource limitations:

Risk mitigation measures may require significant resource investment, including funds, manpower, and time.

The response methods include optimizing resource allocation, ensuring the implementation of key risk control measures, and considering cost-benefit analysis.

Risk management culture:

There may be a lack of risk management culture within the organization, resulting in employees lacking attention and enthusiasm for risk management.

The response methods include strengthening risk management training and education, increasing employees' awareness and importance of risk management.

Information security technology prevention and data protection are crucial aspects of ensuring the confidentiality, integrity, and availability of information and information systems. Below is a detailed discussion on these topics:

Information Security Technology Prevention

Information security technology prevention involves various technical measures aimed at protecting information and information systems from various threats and attacks. These measures include:

1. Encryption Technology:

Encryption technology, also known as encryption, is a fundamental security measure widely used in various fields such as e-commerce, data transmission, and information storage. It involves converting important data into a scrambled format (encryption) during transmission and restoring it to its original form (decryption) at the destination using the same or different means. Below is a detailed overview of encryption technology:

Basic Principles

Encryption technology relies on two core elements: algorithms and keys. Algorithms are the mathematical processes used to encrypt and decrypt data, while keys are the secret values that, in combination with the algorithm, enable the encryption and decryption processes.

Types of Encryption

1. Symmetric Encryption

Principles: Uses the same key for both encryption and decryption. Both the sender

Advantages: Fast encryption and decryption speeds, suitable for processing large amounts of data.

Disadvantages: Key management is crucial; if the key is compromised, security is compromised.

Common Algorithms: DES, 3DES, AES.

Applications: File encryption, database encryption, instant messaging, etc.

2. Asymmetric Encryption

Principles: Uses a pair of public and private keys. The public key is used for encryption, and the private key is used for decryption.

Advantages: Provides higher security as the private key does not need to be transmitted over the network.

Disadvantages: Slower encryption and decryption speeds, typically used for encrypting small amounts of data or exchanging symmetric keys.

Common Algorithms**: RSA, ECC (Elliptic Curve Cryptography), DH (Diffie-Hellman).

Applications**: HTTPS protocol, digital signatures, key exchange, etc.

3. Hashing

Principles: Although not strictly an encryption technique, hashing plays a crucial role in cryptography for verifying data integrity. Hashing functions map arbitrary-length data to fixed-length summaries, which are usually irreversible and highly sensitive to input changes.

Advantages: Irreversible, collision-resistant (different data is unlikely to produce the same hash value).

Common Algorithms: MD5, SHA-1, SHA-256.

Applications: Password storage, data validation, digital signature verification, etc.

Other Encryption Techniques

1. Message Authentication Code (MAC)

Principles: Combines a key and message content to generate a short, fixed-length authentication code. The receiver uses the same key to calculate the MAC and compares it with the received authentication code to verify the message's integrity and authenticity.

Advantages: Provides data integrity verification and message authentication.

Common Algorithm: HMAC (Hash-based Message Authentication Code).

Applications: Data integrity and authentication in network communications.

2. Transparent Encryption

Principles: Automatically encrypts and decrypts files at the operating system level without manual intervention. Files are decrypted when accessed and encrypted when saved, making the process "transparent" to users.

Advantages: User-friendly, operates transparently, enhances security without compromising user experience.

Applications: Enterprise document security management, mobile device data protection.

Applications and Importance

Encryption technology is widely used in various fields, including:

- Data Storage and Transmission**:** Encrypting sensitive data during storage and transmission to prevent unauthorized access.
- E-commerce and Online Transactions**:** Ensuring the confidentiality and integrity of transaction data.
- Network Security**:** Protecting network communications from eavesdropping and tampering.
- Digital Signatures**:** Verifying the authenticity and integrity of digital documents and messages.

Encryption technology is the cornerstone of network security technology. It provides a means to secure sensitive information and prevent unauthorized access, ensuring the confidentiality, integrity, and availability of data. With the continuous development of technology and the increasing sophistication of attacks, encryption technology continues to evolve, with new algorithms and techniques emerging to address emerging threats.

2. Firewalls:

- Firewalls are network security devices that monitor and control inbound and outbound network traffic, blocking unauthorized access and malicious traffic.
- Types include hardware firewalls, software firewalls, and next-generation firewalls (NGFW), which can filter based on IP addresses, ports, protocols, or applications.

Firewalls, also known as firewalls, are a critical component in the field of network security. The following is a detailed explanation of the firewall:

Definition and Function

A firewall is the first line of defense between networks, or between network security domains and insecure domains. Its main function is to prevent unauthorized access, effectively protecting network resources from attacks. Firewalls filter and monitor incoming and outgoing packets through the development and implementation of security policies, ensuring that only packets that meet security requirements can pass through.

Type

Firewalls can be divided into two types: hardware firewalls and software firewalls:

Hardware firewall : It is usually the entry point of the entire enterprise network, such as firewall devices from brands like Shenxin. They have powerful processing capabilities and rich security features, which can provide comprehensive network security protection for enterprises.

Software Firewall : Typically running on a single computer or server, it is used to protect the network security of that computer or server. Software firewalls can be open-source software or commercial software, with the characteristics of flexibility and ease of deployment.

Working principle

The working principle of a firewall is mainly based on packet filtering and

application awareness. Packet filtering refers to the firewall checking incoming and outgoing packets one by one according to preset security rules, and deciding whether to allow packets to pass through based on the inspection results. Application awareness refers to the firewall's ability to detect data at the application layer, conduct in-depth checks on malicious traffic, such as DDoS attacks, SQL injections, etc., and provide higher-level protection.

Development Trends

With the development of cloud computing and AI technology, firewalls are gradually migrating to cloud environments and integrating AI technology to achieve intelligent threat detection and automated defense. This trend enables firewalls to adapt more quickly to changes in the network environment and enhance the intelligence level of network security.

Application scenarios

Firewalls are widely used in key fields such as banking, government, and healthcare, providing critical protection to ensure data integrity and privacy. At the same time, firewalls are also an important component of enterprise network security architecture, which can work together with other security devices to build a secure and efficient network defense line.

In summary, as the guardian of network security, firewalls play an important role in protecting network resources from attacks. With the continuous development of technology, the functionality and performance of firewalls are also constantly improving, providing a more solid guarantee for network security.

3. Intrusion Detection and Prevention Systems (IDS/IPS):

- IDS monitors network traffic and system activities, detecting and reporting potential security incidents.
- IPS not only detects but also actively blocks and responds to attacks.
- Common techniques include signature-based detection, behavior-based detection, and hybrid detection methods.

IDPS is a device or software that can monitor the activity of a network or system, searching for possible malicious or policy violating behavior. When IDPS detects such

behavior, it can take a series of actions, such as sending warnings, blocking activities, or sending signals to other security devices (such as firewalls). Its main functions include:

Real time monitoring: IDPS can monitor all data traffic entering and leaving the network in real time, ensuring timely detection of anomalies.

Threat identification: Through in-depth analysis of data traffic, IDPS can identify patterns and abnormal behaviors that may indicate intrusion attempts.

Automatic response: In addition to detecting threats, IDPS can also perform automatic response measures to prevent or mitigate security incidents, such as blocking malicious traffic, isolating infected systems, etc.

Logging: The IDPS system records all monitored events and actions taken, facilitating post event analysis and compliance requirements.

Types and classifications

IDPS can be classified into various types based on their working mode and location, mainly including:

Network Intrusion Detection System (NIDS): an IDPS that monitors the entire network traffic and can detect network attacks such as denial of service attacks, scans, or botnets.

Host Intrusion Detection System (HIDS): monitors the IDPS of a single host (such as a server or workstation) and can detect host level attacks such as malware, Trojan horses, or privilege escalation.

Network Intrusion Prevention System (NIPS): Not only can it detect network attacks, but it can also prevent them. For example, NIPS can prevent traffic from denial of service attacks and protect the network.

Host Intrusion Prevention System (HIPS): Not only can it detect host level attacks, but it can also prevent them. For example, HIPS can prevent the behavior of malicious software and protect hosts.

Working principle

The working principle of IDPS mainly relies on two technologies: feature matching and anomaly detection.

Feature matching: Detecting attacks by comparing network or system activity with known attack features (also known as signatures). If the pattern of network traffic matches the known attack pattern, IDPS will consider it an attack.

Anomaly detection: Detecting attacks by comparing network or system activity with normal behavioral patterns. If the behavior of the network or system deviates from the normal baseline, IDPS may consider it an attack.

4、 Configuration and usage

The configuration of IDPS mainly involves defining the normal behavior patterns of the network or system, as well as selecting the attack features to be detected. For example, it is necessary to define the normal traffic pattern of the network, including the size, frequency, destination, etc. of the traffic, while also selecting the attack characteristics to be detected, such as known malware features, attack tool features, etc.

When using IDPS, the following points should be noted:

Regularly updating the signature library: With the continuous evolution of network threats, the signature library of IDPS also needs to be constantly updated to ensure the detection of the latest attacks.

Reasonable configuration rules: The rule configuration of IDPS needs to be adjusted according to specific network environments and business requirements to avoid false positives and false negatives.

Timely handling of warnings: When IDPS issues a warning, it is necessary to analyze and handle it in a timely manner to ensure network security.

Challenges and Development Trends

Although IDPS plays an important role in network security defense, it also faces some challenges such as handling encrypted traffic, preventing zero day attacks, and handling a large number of warnings. To address these challenges, IDPS needs to continuously develop and improve. The future development trends include:

Integrating big data and artificial intelligence technology: Through big data analysis and artificial intelligence technology, the detection capability and response speed of IDPS can be improved, enabling it to more accurately identify abnormal

activities.

Adapting to cloud computing and IoT environments: With the popularity of cloud computing and IoT technologies, IDPS needs to adapt to these new environments and provide seamless protection across physical and virtual networks.

Enhance automation capability: By enhancing automation capability, IDPS can more effectively manage security alerts and respond to security events, improving the efficiency and accuracy of network security defense.

4. Antivirus and Anti-Malware Software:

- These software tools detect, block, and remove viruses, worms, Trojans, and other malicious software from computer systems.

- Functions include real-time monitoring, periodic scanning, malware isolation and removal, and behavior analysis.

Antivirus software, also known as antivirus software, is a software specifically designed to detect, remove, and prevent computer viruses. It usually integrates monitoring and recognition, virus scanning, cleaning, and automatic upgrading functions, and some antivirus software also has data recovery functions.

working principle:

Real time monitoring: Antivirus software detects and prevents potential virus intrusions by monitoring the real-time activity of the system or network.

Virus scanning: Regularly scanning the computer's files, memory, registry, etc. to find and remove known viruses.

Virus library update: Antivirus software regularly updates its virus library to include the latest virus features and signatures, enabling it to detect and remove newly emerging viruses.

Common antivirus software:

Norton AntiVirus (Norton antivirus software)

Avast Antivirus

360 antivirus

Jinshan Poison Overlord

Rising Antivirus

2、 Anti malware Software

definition:

Anti malware software, also known as anti malware, is a more comprehensive protection program that can not only detect and remove viruses, but also defend against other types of malware such as worms, Trojan Horses, ransomware, spyware.

working principle:

Signature detection: Using known malware signatures to detect and remove malicious software.

Behavioral analysis: Identifying potential malicious software by analyzing its behavior, even if they have not yet been added to the signature library.

Real time protection: Provides real-time malware protection to prevent the installation and operation of malicious software.

Common anti malware software:

Emsisoft Anti Malware: Provides an advanced anti malware system with multiple levels of protection to protect computers from various types of malware threats.

Malwarebytes Anti Malware: A free anti malware detection and removal software suitable for both households and businesses, with features such as anti malware and anti spyware protection, malicious website interception, real-time protection, and more.

3、 The difference and connection between Antivirus and Anti Malware difference:

Antivirus software mainly detects and removes viruses.

Anti malware provides more comprehensive protection against various types of malware, including viruses.

Contact:

Both are important components of the field of network security, working together to protect computers from malicious software.

In practical applications, antivirus software and anti malware software often

complement each other, jointly improving the computer's protection capabilities.

4、 Selection and usage suggestions

choice:

Choose appropriate antivirus or anti malware software based on your own needs and computer environment.

Consider factors such as software update frequency, virus library size, detection rate, false positive rate, etc.

use:

Regularly update software to ensure it can detect and remove the latest malicious software.

Regularly conduct a comprehensive scan to identify and remove potential malicious software.

Be careful not to click on unknown links or download files from unknown sources at will to reduce the risk of malware infection.

5. Access Control Technologies:

- Access control technologies ensure that only authorized users can access specific information and resources, achieved through authentication and authorization processes.

- Methods include role-based access control (RBAC), attribute-based access control (ABAC), and multi-factor authentication (MFA).

Access control technology refers to the use of a series of policies and mechanisms to control access to resources in an information system, ensuring that only authorized users or systems can access specific resources. Its main functions include:

Identity verification: Confirm the user's identity and ensure that the user is a legitimate user.

Permission management: Assign corresponding access permissions based on the user's identity and role.

Access control: Control user access behavior to resources based on permission management policies.

Audit and monitoring: Record user access behavior and conduct real-time

monitoring to detect and handle abnormal behavior in a timely manner.

2、 Common Access Control Models

Access Control List (ACL):

Maintain access control to a resource in the form of a list.

Intuitive and easy to implement, but with high maintenance costs, especially when there are a large number of users.

Autonomous Access Control (DAC):

The owner of a resource can assign their permissions to other users.

High flexibility, but relatively low security, as the allocation of permissions relies entirely on the judgment of resource owners.

Mandatory Access Control (MAC):

All access control policies are formulated by system administrators and cannot be changed by users.

High security, but low flexibility because users cannot adjust permissions according to their own needs.

Role Based Access Control (RBAC):

Transform the relationship between users and permissions into the relationship between roles and permissions.

Simplifying permission management and reducing maintenance costs is currently the most popular access control model in commercial applications.

Attribute based Access Control (ABAC):

To achieve access control based on any combination of attributes.

The flexibility is extremely high, but the implementation is complex and currently not widely popular.

3、 Application scenarios of access control technology

Enterprises and organizations:

Protect sensitive data and critical resources through access control technology within the internal network of the enterprise.

By setting different roles and permissions, ensure that employees can only access the resources necessary for their work.

Cloud computing platform:

In cloud computing environments, user data and privacy are protected through access control technology.

By implementing multi tenant isolation and access control policies, ensure that data between different users does not interfere with each other.

Internet of Things (IoT):

In IoT devices, access control technology is used to protect the security and data privacy of the devices.

By setting access control policies, illegal access and operations on devices are restricted.

Smart Home:

In smart home systems, access control technology is used to protect the security and privacy of households.

By setting different user roles and permissions, ensure that family members can only access the devices and features they need.

Development Trend of Access Control Technology

Integration and Intelligence:

With the continuous development of technology, access control technology will gradually be integrated into a wider range of security solutions.

By introducing artificial intelligence and machine learning technologies, smarter access control and risk management can be achieved.

Cross platform and cross domain:

With the popularity of cloud computing, the Internet of Things and mobile Internet, access control technology will gradually achieve cross platform, cross domain and cross organization interoperability.

Users will be able to seamlessly access the resources they need on different devices and platforms.

Privacy Protection and Compliance:

With the increasingly strict regulations on data privacy protection, access control technology will pay more attention to privacy protection and compliance

requirements.

By using encryption, anonymization, and data anonymization techniques, users' privacy and data security are protected.

6. Endpoint Detection and Response (EDR):

- EDR technologies continuously monitor and analyze the activities of endpoint devices (e.g., computers, mobile devices) to detect and respond to security threats.

- Functions include behavior monitoring, threat detection, automated response, and forensic analysis.

Data Protection

Data protection refers to the measures taken to safeguard sensitive data from unauthorized access, use, disclosure, modification, or destruction. The following are key aspects of data protection:

1. Data Classification and Labeling:

- Classifying and labeling data based on its sensitivity and importance helps in implementing appropriate protection measures.

2. Access Control and Authentication:

- Implementing strict access controls and authentication mechanisms to ensure that only authorized users can access sensitive data.

- Multi-factor authentication can be used to enhance security.

3. Encryption:

- Encrypting sensitive data during storage and transmission to prevent unauthorized access.

- Both symmetric and asymmetric encryption techniques can be used depending on the specific requirements.

4. Data Backup and Recovery:

- Regularly backing up data to prevent data loss and ensure quick recovery in case of a disaster.

5. Data Loss Prevention (DLP):

- DLP technologies detect and prevent the leakage and unauthorized

transmission of sensitive data.

- Functions include content recognition, policy enforcement, incident reporting, and response.

6. Security Information and Event Management (SIEM):

- SIEM systems collect, analyze, and correlate security event logs from various sources, providing real-time monitoring, alerting, and reporting.

- Functions include log management, event correlation analysis, threat intelligence integration, and compliance reporting.

7. Incident Response and Forensics:

- Establishing incident response teams and procedures to quickly respond to security incidents and minimize their impact.

- Forensic analysis can be used to investigate and understand the root cause of incidents.

The construction of internal control and risk management mechanism is a crucial aspect of modern corporate governance, as it directly relates to a company's ability to maintain its competitive edge, mitigate risks, strengthen internal governance, and achieve sustainable development. Below is a detailed discussion on this topic:

Internal Control

Internal control refers to a series of policies, procedures, and measures implemented by an organization to safeguard its assets, ensure the accuracy and reliability of its financial information, promote operational efficiency and compliance with laws and regulations, and ultimately achieve its strategic objectives.

The development of internal control can be broadly divided into several stages, including internal checks and balances, internal control systems, internal control structures, the overall framework of internal control, and the overall framework of enterprise risk management. The COSO framework, issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1992, is a widely recognized internal control framework. It emphasizes five key elements: control environment, risk assessment, control activities, information and communication, and monitoring.

Internal control is a process designed to provide reasonable assurance regarding the achievement of an entity's objectives related to operations, reporting, and compliance. It encompasses a series of policies, procedures, and measures implemented by an organization to safeguard its assets, ensure the accuracy and reliability of its financial information, promote operational efficiency, and ensure compliance with laws and regulations.

The key elements of internal control typically include:

Control Environment : This refers to the overall atmosphere within an organization that influences the development and implementation of internal control policies and procedures. It includes factors such as management's philosophy and operating style, organizational structure, assignment of authority and responsibility, and human resource policies and practices.

Risk Assessment : This involves identifying and analyzing potential risks that may affect an organization's ability to achieve its objectives. Risk assessment helps organizations determine the level of risk they are willing to accept and the measures needed to mitigate those risks.

Control Activities : These are the policies and procedures that help ensure that management's directives are carried out. Control activities can include approvals, authorizations, verifications, reconciliations, reviews of operating performance, asset safeguards, and segregation of duties.

Information and Communication : Effective information and communication systems ensure that relevant information is timely and accurately communicated to those within the organization who need it to perform their responsibilities. This includes financial and operational information, as well as information related to internal control and risk management.

Monitoring and Evaluation : This involves ongoing monitoring of internal control systems to ensure their effectiveness, as well as periodic evaluations and audits to identify any weaknesses or deficiencies. Monitoring and evaluation help organizations make necessary adjustments to their internal control systems to maintain their effectiveness over time.

Internal control is not just a set of rules and procedures, but rather a continuous process that requires active participation and commitment from all levels of an organization. It is essential for organizations to establish a strong internal control system to safeguard their assets, ensure the accuracy and reliability of their financial information, promote operational efficiency, and ensure compliance with laws and regulations.

By implementing effective internal control, organizations can reduce the risk of fraud, error, and noncompliance, and improve their overall performance and reputation. Additionally, internal control can provide a foundation for managing risks and achieving organizational objectives, which is critical for sustainable success.

Risk Management

Risk management involves identifying, assessing, and addressing potential risks that may affect an organization's ability to achieve its objectives. It is closely related to internal control, as both aim to safeguard the organization's assets, ensure the accuracy of financial information, and promote compliance.

Risk management typically includes risk identification, risk assessment, risk response planning, risk monitoring and control, and continuous improvement. By identifying potential risks and developing appropriate response plans, organizations can mitigate the negative impacts of these risks on their operations and financial performance.

1、 Definition and Importance

Risk management refers to the process of identifying, assessing, and controlling potential risks to minimize losses and maximize opportunities. With the accelerated development of globalization and digitization, the risks faced by enterprises and organizations are becoming increasingly complex and diverse. Effective risk management is crucial for protecting enterprise assets, ensuring business continuity, improving decision quality, and enhancing stakeholder confidence.

2、 Main steps

Risk identification: Identify potential risks, including internal risks (such as personnel turnover, equipment failure) and external risks (such as market changes,

regulatory changes). This step requires collecting possible risk factors and categorizing them for subsequent analysis.

Risk assessment: Evaluate identified risks, consider their probability of occurrence and degree of impact, and prioritize them. The evaluation methods include quantitative evaluation and qualitative evaluation, such as using Monte Carlo simulation for quantitative evaluation or using risk matrix for qualitative evaluation.

Risk response: Based on the results of risk assessment, develop corresponding risk response strategies, including risk avoidance, risk transfer, risk mitigation, and risk acceptance. For example, transferring potential losses to insurance companies through purchasing insurance, or taking measures to reduce the likelihood or impact of risk events.

Risk monitoring: Establish monitoring mechanisms, regularly track and evaluate changes in risks, and take necessary control measures to mitigate the impact of risks. This includes developing emergency plans and disaster recovery plans to address potential risk events.

3、 Practical methods

SWOT analysis: Identify and evaluate risks by analyzing the strengths, weaknesses, opportunities, and threats of an organization or project, and develop corresponding risk response strategies.

Risk map: Mark risk factors on the map to form a risk distribution map, which facilitates a visual understanding of the geographical location and distribution of risks.

Risk assessment tools: Use various risk assessment tools such as storyboards, sensitivity analysis, etc. to conduct a more in-depth assessment and analysis of risks.

4、 Application Fields

Risk management is widely applied in various fields, including project management, finance and investment, enterprise management, information technology, etc. In project management, risk management is a crucial aspect that can reduce the risk of project failure and increase the likelihood of project success. In the fields of finance and investment, risk management is an important means of protecting funds and investments. Risk management is one of the key factors in ensuring the sustainable

development of an organization in business management. In the field of information technology, risk management helps organizations assess and manage risks to information systems and network security.

5、 Development Trends

With the continuous advancement of technology and changes in the market, risk management is also constantly evolving. Modern risk management has gradually expanded to various fields such as strategy, operations, marketing, and reputation, emphasizing comprehensive management and optimization of risks. Meanwhile, risk management also places greater emphasis on data analysis and quantitative evaluation to provide more accurate risk predictions and response strategies.

In summary, risk management is a complex and important process that requires organizations and individuals to continuously learn and practice to improve their risk management capabilities. Through effective risk management, organizations and individuals can better cope with the challenges brought by uncertainty, achieving sustainable development and long-term success.

Construction of Internal Control and Risk Management Mechanism

To construct an effective internal control and risk management mechanism, organizations should consider the following aspects:

Establish a Sound Internal Control System : Based on the COSO framework, organizations should establish a comprehensive internal control system that covers all key business processes and risk points. This system should include clear policies, procedures, and responsibilities, as well as effective monitoring and evaluation mechanisms.

Strengthen Risk Assessment and Management : Organizations should regularly conduct risk assessments to identify potential risks and their potential impacts. Based on the assessment results, they should develop risk response plans and implement effective risk mitigation measures.

Improve Information and Communication : Effective information and communication are crucial for the successful implementation of internal control and risk management. Organizations should establish a transparent and efficient

communication mechanism to ensure that relevant information is timely and accurately communicated to all stakeholders.

Strengthen Monitoring and Evaluation : Organizations should regularly monitor and evaluate the effectiveness of their internal control and risk management mechanisms. Based on the evaluation results, they should make timely adjustments and improvements to ensure the continuous improvement of the mechanism.

Promote Compliance and Ethical Culture : Organizations should establish a strong compliance and ethical culture, encourage employees to abide by laws and regulations, and strengthen their awareness of risk prevention and control.

sessions, stakeholder interviews, and external data sources.

Analyze risks using risk matrices, impact/likelihood assessments, and other tools.

Develop a risk register to document all identified risks, their potential impacts, and mitigation strategies.

Risk Mitigation Strategies :

Develop and implement strategies to reduce the likelihood and impact of identified risks.

Consider insurance, hedging, diversification, and other risk transfer mechanisms.

Monitor the effectiveness of mitigation strategies and adjust as needed.

Risk Monitoring and Reporting :

Establish a risk monitoring framework to track the progress of identified risks.

Report risk status, mitigation efforts, and any changes in risk profiles to senior management and stakeholders.

Use risk metrics and key performance indicators to measure the success of risk management efforts.

Integration of Internal Control and Risk Management

Align Objectives and Strategies :

Ensure that internal control and risk management objectives are aligned with the organization's overall strategy.

Develop integrated plans and policies that support both internal control and risk management objectives.

Coordinate Efforts :

Establish a risk management committee or similar governance structure to oversee internal control and risk management efforts.

Coordinate between internal control and risk management teams to avoid duplication of efforts and ensure consistency in approach.

Leverage Technology :

Utilize enterprise risk management (ERM) software and other technology solutions to streamline internal control and risk management processes.

Integrate internal control and risk management systems with other business processes, such as finance, operations, and compliance.

Continuous Improvement :

Foster a culture of continuous improvement in internal control and risk management.

Regularly review and update internal control and risk management policies and procedures based on new risks, regulatory changes, and technological advancements.

By following these guidelines, organizations can establish a robust internal control and risk management mechanism that supports their strategic objectives, enhances operational efficiency, and protects against potential risks. This, in turn, will contribute to the organization's long-term success and sustainability.

CONCLUSIONS

Ensuring the financial security of the banking system under international conditions requires a comprehensive approach that includes strengthening international financial regulation and cooperation, enhancing risk management capabilities, strengthening internal controls and governance, fostering financial innovation and technological advancements, strengthening investor and consumer protection, and monitoring international financial markets and economic trends. By adopting these strategies, countries can help ensure the stability and resilience of their banking systems in the face of global financial challenges.rs should.

REFERENCES

LAWS

1. Law of Ukraine «On Banks and Banking Activity» dated December 7, 2000 № 2121-III. URL: <https://zakon.rada.gov.ua/laws/show/2121-14#Text>
2. Law of Ukraine «On State Regulation of the Securities Market in Ukraine». VVR 1996 № 51. Art. 292. URL: <https://zakon.rada.gov.ua/laws/show/448/96-%D0%B2%D1%80#Text>
3. Law of Ukraine «On Investment Activity» dated September 18, 1991 № 1560-XII (with amendments and additions). VVR 1991. No. 47. Art. 646. URL: <https://zakon.rada.gov.ua/laws/show/1560-12#Text>

EDUCATIONAL LITERATURE

4. Methodology of scientific research in diagrams, tables, examples: teaching. manual / auto..col.; under the editorship of Dr. Econ. Science, Prof. G.M., Azarenkova – K.: UBS NBU, 2014. – 223 p.
5. Doronina M.S. Technology of scientific research (diagrams and examples): Study guide / Compiled by Doronina M.S. - Kh.: VD "INZHEK", 2010. – 118 p.
6. Yurchenko, S.O., Yurchenko O.E., Basics of scientific research: teaching. manual Kharkiv: Publishing House of KhNU named after V.N. Karazina, 2017. 203p.

ARTICLES

7. Azarenkova G. Operational control over the financial stability of banking / A. Kuznetsova, B. Samorodov, G. Azarenkova, K. Oryekhova, M. Babenko // Banks and Bank Systems; Business Perspectives. – Volume 15, 2020. – Issue # 1. – PP. 51-58. - URL: [http://dx.doi.org/10.21511/bbs.15\(1\).2020.06](http://dx.doi.org/10.21511/bbs.15(1).2020.06).
8. Azarenkova G. Financial stability management in banks: strategy maps/ B. Samorodov, G. Azarenkova, O. Golovko, K. Oryekhova, M. Babenko // Bank and Bank Systems; Business Perspectives. – 2019. – Issue# 4. – P. 10-21.

LINKS TO INFORMATION RESOURCES ON THE INTERNET, VIDEO LECTURES, OTHER METHODOICAL SUPPORT

1. The official website of the Ministry of Education and Science of Ukraine URL: <http://www.mon.gov.ua>
2. The National Library of Ukraine named after Vernadskyi URL: <http://www.nbuv.gov.ua>

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 23:01:50 18.05.2025

Назва файлу з підписом: KMP_Lyudannier_bank_Galych.pdf.p7s[1].p7s[1].p7s
Розмір файлу з підписом: 762.3 КБ

Назва файлу без підпису: KMP_Lyudannier_bank_Galych.pdf.p7s[1].p7s[1]
Розмір файлу без підпису: 709.7 КБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач - 1: ГАЛИЧ РОМАН ВОЛОДИМИРОВИЧ

П.І.Б.: ГАЛИЧ РОМАН ВОЛОДИМИРОВИЧ

Країна: Україна

РНОКПП: 3271209038

Організація (установа): ФІЗИЧНА ОСОБА

Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 19:10:07 12.12.2024

Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"

Серійний номер: 5E984D526F82F38F0400000086D01A01A0838205

Тип носія особистого ключа: Незахищений

Алгоритм підпису: ДСТУ 4145

Тип підпису: Удосконалений

Тип контейнера: Підпис та дані в одному файлі (CAAdES enveloped)

Формат підпису: З повними даними ЦСК для перевірки (CAAdES-X Long)

Сертифікат: Кваліфікований

Підписувач - 2: АЗАРЕНКОВА ГАЛИНА МИХАЙЛІВНА

П.І.Б.: АЗАРЕНКОВА ГАЛИНА МИХАЙЛІВНА

Країна: Україна

РНОКПП: 2571514226

Організація (установа): ФІЗИЧНА ОСОБА

Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 19:35:48 12.12.2024

Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"

Серійний номер: 5E984D526F82F38F04000000E4DA710112DF3D05

Тип носія особистого ключа: Незахищений

Алгоритм підпису: ДСТУ 4145

Тип підпису: Удосконалений

Тип контейнера: Підпис та дані в одному файлі (CAAdES enveloped)

Формат підпису: З повними даними ЦСК для перевірки (CAAdES-X Long)

Сертифікат: Кваліфікований

Підписувач - 3: Омеляненко Денис Олегович

П.І.Б.: Омеляненко Денис Олегович

Країна: Україна

РНОКПП: 3634714115

Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 15:05:05 19.12.2024

Сертифікат виданий: "Дія". Кваліфікований надавач електронних довірчих послуг

Серійний номер: 382367105294AF9704000000EF5A070009B10B03

Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301

Серійний номер носія особистого ключа: Не визначено

Алгоритм підпису: ДСТУ 4145

Тип підпису: Кваліфікований

Тип контейнера: Підпис та дані в одному файлі (CAAdES enveloped)

Формат підпису: З повними даними ЦСК для перевірки (CAAdES-X Long)

Сертифікат: Кваліфікований