FINANCIAL SECTOR ADVISORY CENTER (FinSAC)

Renewed supervisory challenges in light of tightened financial conditions and economic slowdown

May 9–10, 2023 | Vienna, Austria

Session 4: Sanctions, conduct, IT, cybersecurity: challenges in operational risk supervision

Presentations by:

Kateryna Rozhkova – Deputy Governor, National Bank of Ukraine
Andrea Pozzi – Banco Santander S.A.
Philipp Hochreiter – Stiltskin consulting
Emil Abrahamyan – Central Bank of Armenia
David Papuashvili – World Bank Consultant

WORLD BANK GROUP
Finance, Competitiveness & Innovation
Financial Sector Advisory Center (FinSAC)

WWW.WORLDBANK.ORG/FINSAC

Contents

Operational and cybersecurity risks during the war

Kateryna Rozhkova
National Bank of Ukraine

Operational risk assessment Armenia 2023

Emil Abrahamyan
Central Bank of Armenia

Operational Risk Management in the Cryptoassets Sector

Philipp Hochreiter
Stiltskin

Contemporary Challenges in Operational Risk Management

David Papuashvili
World Bank

National Bank of Ukraine

Operational and cybersecurity risks during the war

8 May 2023

Financial Stress Index (FSI) declined from the highs of the early days of the war, yet remains volatile

Джерело: НБУ.

- War increased the level of stress in financial system, almost all components of the FSI have raised significantly.
- The FSI is still volatile and hovered around high levels.
- Attacks on energy infrastructure provoked FSI surge in October; however, in November, financial sector's sensitivity fell considerably; almost all sub-indices were subsiding until March.
- In March, 2023 increase in yields of government bonds led to the increase in FSI.

NBU had business continuity requirements for banks before the war

NBU Regulation No 64 of June 2018 set requirements for banks in the area of business continuity

Policy for business continuity management	Procedure for analysis of adverse factors impact upon bank's business processes	Business continuity plan (BCP)
• Sets principles and banks' approaches to ensuring business continuity	• Assess criticality of business processes, systems and ICT services, and other resources (staff, premises, equipment)	• Sets strategic objectives, priorities, and measures for ensuring business continuity • Revised annually, validated by the NBU

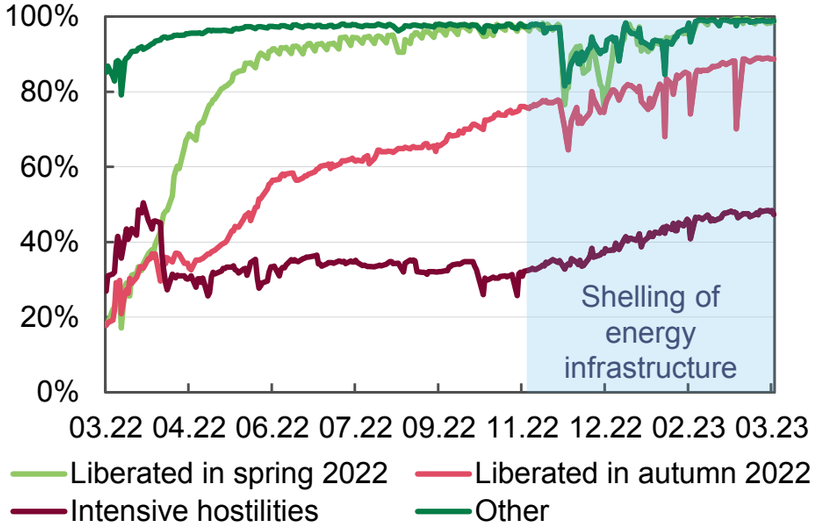
As the full-scaled war erupted, the NBU refined and enhanced its requirements (in line with NBU Regulation of February 2022)

- Ensuring at least 35% of branches in each region are open even during a blackout
- Keeping clients informed about open branches
- Ensuring safety of bank operations, including cash transactions
- Keeping critical process running, including those of critical infrastructure, ICT systems, and data back-up
- Ensuring operations even when cut from NBU SEP (RTGS) system – for headquarters and branches

NBU also had its own business continuity plan developed after 2014 invasion and regularly updated.

Banking network is functioning despite power outages

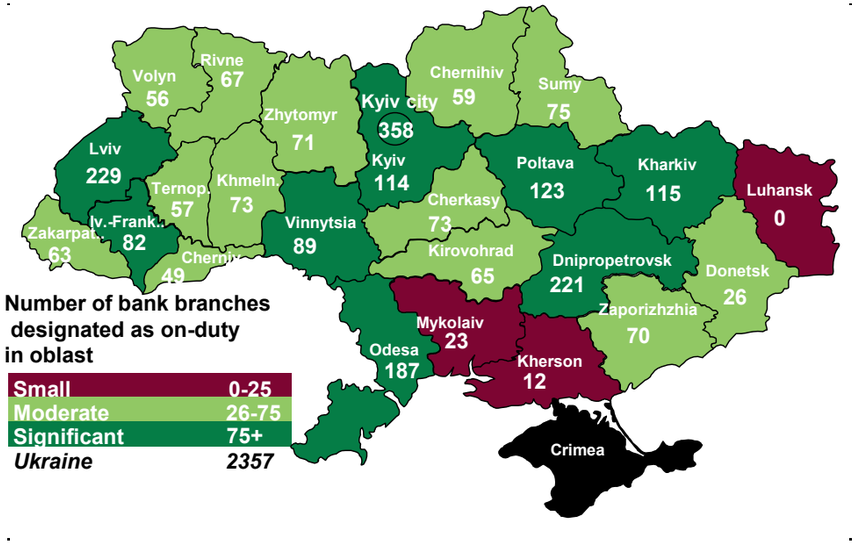
Share of working branches of systematically important banks



Regions are classified into groups. “Liberated in spring” comprise Kyiv, Sumy, Chernihiv oblasts, and city of Kyiv. “Liberated in autumn” comprise Mykolaiv and Kharkiv oblasts. “Intensive hostilities” comprise Donetsk, Luhansk, Zaporizhzhia, and Khesron oblasts.

Source: NBU, survey of systematically important banks important banks

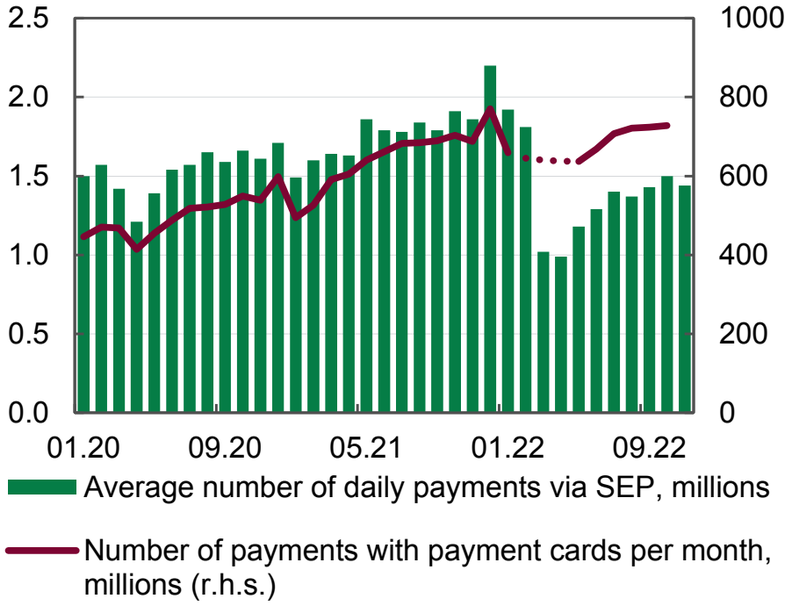
Number bank branches designated as on-duty by regions as of April 24, 2023



- The proportion of working bank branches gradually increased, but because of power outages, it sometimes dropped.
- Power outages was a new challenge for uninterrupted functioning of banks, additional operating expenses for arranging work under such conditions would exceed UAH 300 millions.
- Despite temporary threat reduction of missile attacks “Power Banking” network continues to rise and now includes 2300+ branches of 61 banks. This is a network of on-duty branches capable of operating and providing the necessary services during the blackout.

Undisrupted access to payment services promotes trust to banks

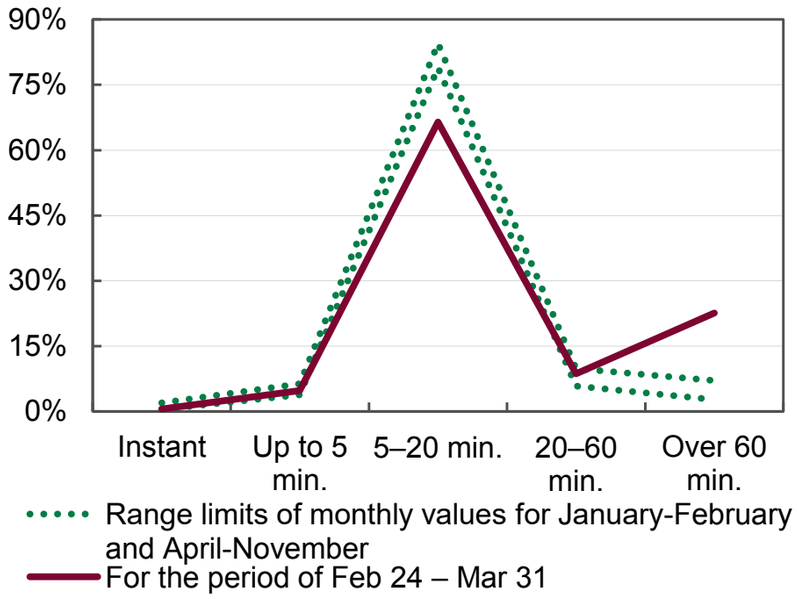
Number of payments through SEP and by cards



* In February–April 2022, static data submission was suspended.

Source: NBU.

Distribution of payments in SEP* by time a transaction takes in 2022



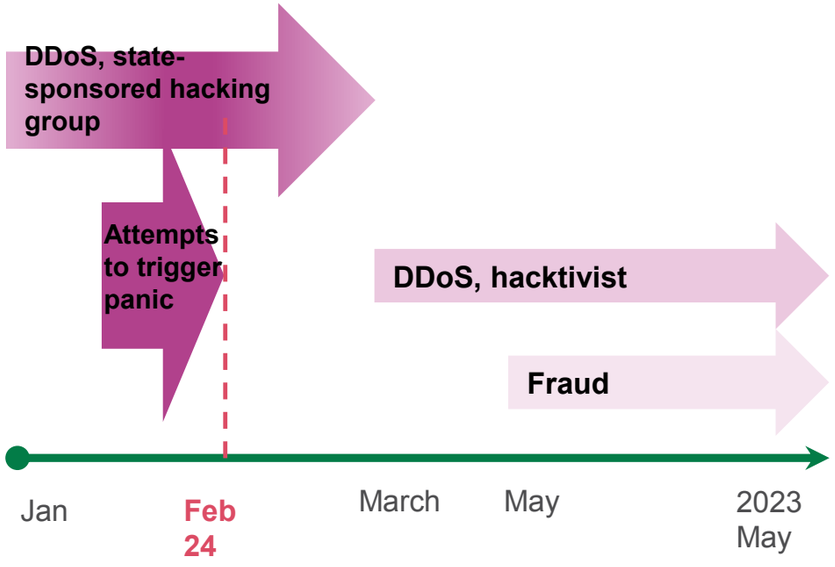
* By number of transactions in 2022.

Source: NBU.

- Despite of the full-scale war, payments were continuous, which prevented high demand for cash and saved banks' liquidity.
- The number of payments in the System of Electronic Payments (SEP) shows that the economy adapts to war conditions and gradually recovers. The number of card payments in summer-autumn 2022 has exceeded that for the same period in 2021.
- The SEP kept transactions regular. Only in the first days of the invasion and during massive bombardments some payments took more time to complete and were slightly postponed.

Nature of cyber attacks on Ukrainian banks continues to change

Evolving nature of cyber attacks



Banks survey results on the data storages

Indicator	Number of banks	Percentage of banks (out of 68)
Data storages located in Kyiv	53	78%
Backup storages located in Kyiv	53	78%
Realocated data storages	50	74%
incl. realocated to other cities	23	34%
incl. reallocated to the cloud	46	68%
Plan to use cloud permanently	24	35%

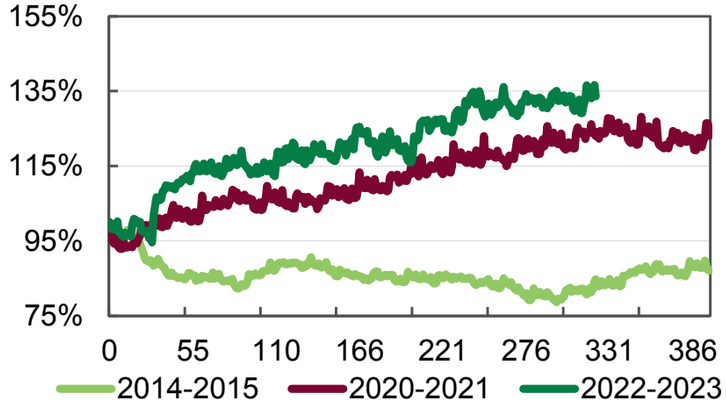
Source: Survey of banks, NBU estimates.

- Before the full-scale invasion started on 24 February 2022, the central bank and dozens of Ukrainian banks came under massive attacks, primarily DDoS. In 2022, the NBU registered a total of 50 attacks on NBU resources and 200 attacks on banks' ones, peaking in February.
- Russia used cyber-attacks to disrupt smooth functioning of the banking system and trigger panic, bank runs, and undermine stability of the financial sector.
- Almost 50 banks (out of 68) used the option to relocate or duplicate data to a cloud hardware located abroad. The relocation was an additional factor of data protection.
- In the first months of 2023, a total 20 of attacks on NBU resources and 50 attacks on banks' ones were reported. The scope of financial companies attacked widened.

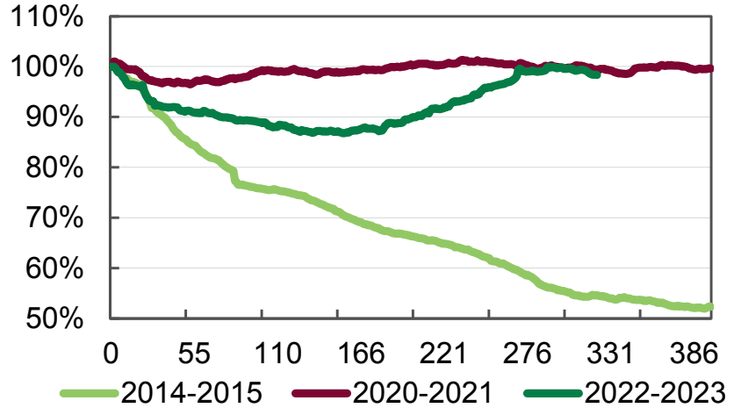
Term deposits in hryvnia are growing

Retail deposits the last day before the outflow*=100% *(at solvent banks as of 1 April 2023)*

All deposits in hryvnia



All deposits in FX

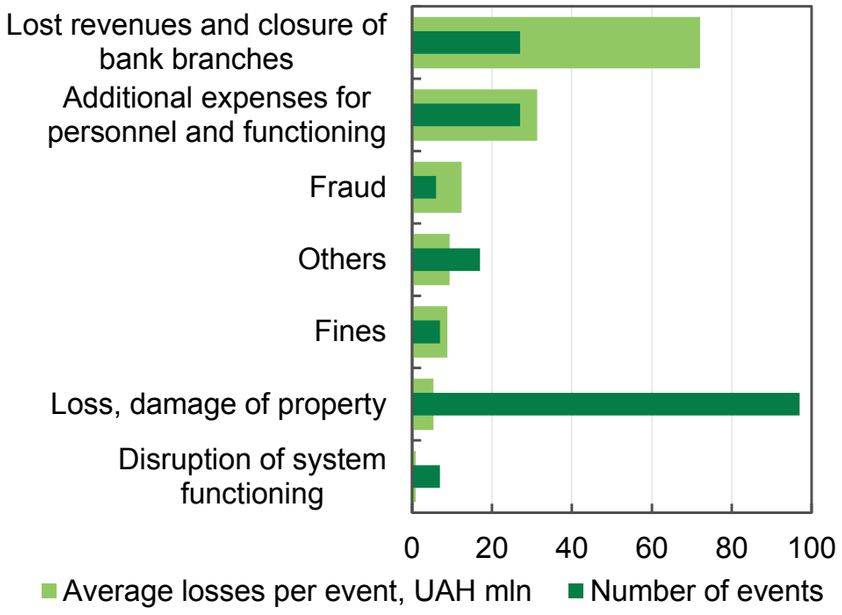


* The highest readings of hryvnia deposits recorded before the crises: 2014: 23 Jan 2014; 2020: 10 Mar 2020; 2022: 17 Jan 2022. X axis indicates number of working days.
Source: daily data, retail deposits include certificates of deposit. For 2022 – data at banks that were solvent as of 1 April 2023.

- Ukraine did not face a bank run thanks to a number of factors:
- The Banks worked on despite the challenges, especially in terms of online payment system
- The NBU introduced restrictions and measures to support banks, some of the restrictions are still in place
- Households' propensities and behavior has changed.

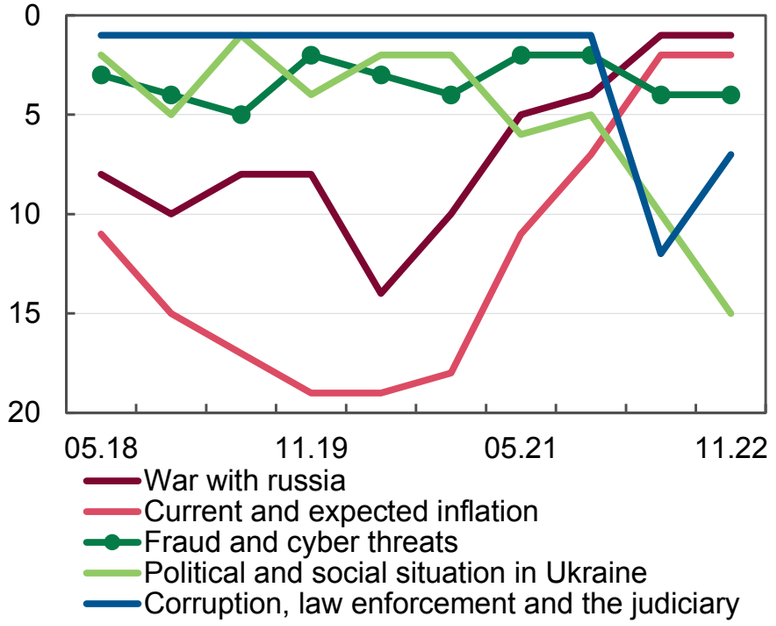
Banks' losses from operational risk will continue to rise

Classification of the largest war-related operational risk events of banks



Source: NBU, Survey of bank operations in wartime.

Rankings of major risk factors in financial sector*



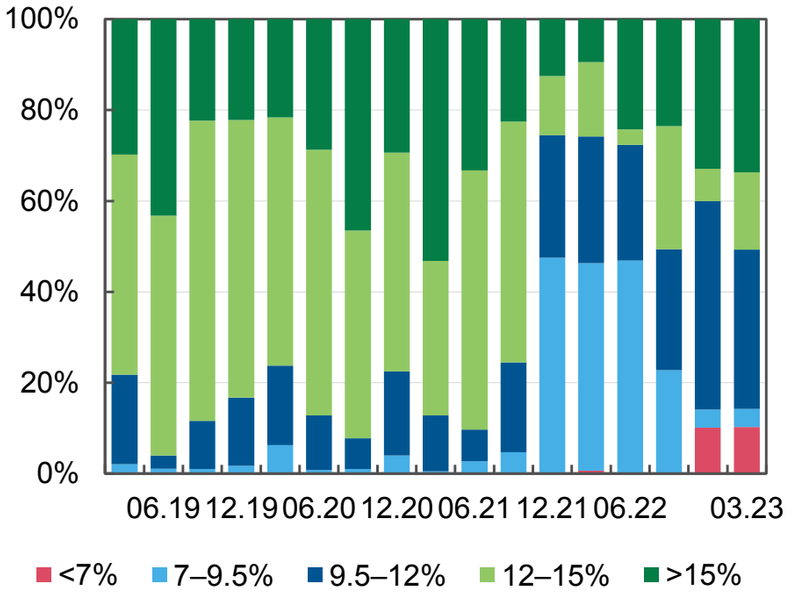
* Based on the balances of responses in the Systemic Risk Survey.

Source: NBU.

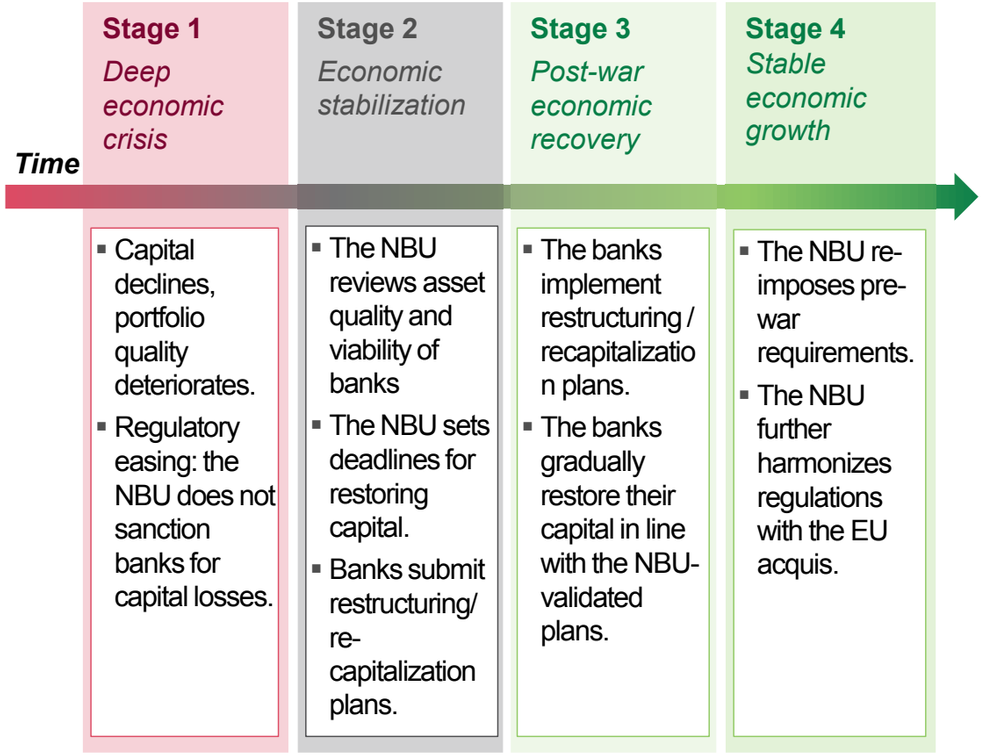
- In 2022, the amount of banks' losses and lost revenues from war-related operational risk has reached UAH 13 billion.
- Banks consider fraud and cyber risks to be among the TOP-5 risks for financial stability.
- High demand for online services raised attention to cyber security and banks investments in this area.

Next year, the NBU will conduct bank resilience assessment

Distribution of core capital adequacy by share of banking assets



Source: NBU.



- Banks maintain, sometimes build up capital despite of the war. Capital requirements partially include operational risk.
- In 2023, the NBU plans to review asset quality and estimate banks' viability next year.

Annex

Banking system relaxations

Capital Conservation	• Sanctions for breeching certain capital, liquidity, and FX requirements are not applied • Capital distribution, including dividend payouts, are forbidden • The counting of days past due for prudential provisions temporarily suspended (eased pressure on regulatory capital) (**canceled in July 2022**)
Postponing new requirements	• The introduction of capital buffers postponed • The NSFR kept at 90% (until April 2023)
Easing pressure on operating activities	• Banks' AQR and stress tests for 2022 were canceled • Submission of financial statements and some statistical reports postponed • Revaluation and verification of collateral postponed • Simplified verification temporarily expanded; onsite AML inspections suspended
Opening up opportunities	• The use of cloud data services allowed • A number of customer identification requirements eased • The upper limit amount for simplified remote verification increased • Banks temporarily allowed not to recognize loans that have been restructured because of the war as in default
Other	• Transactions with related parties forbidden

The NBU promptly adjusts specifics of banking regulation under martial law, taking into account current situation in the financial sector

May 2023

STILTSKIN

REGULATORY CONSULTING

Operational Risk Management in the Cryptoassets Sector

Philipp Hochreiter

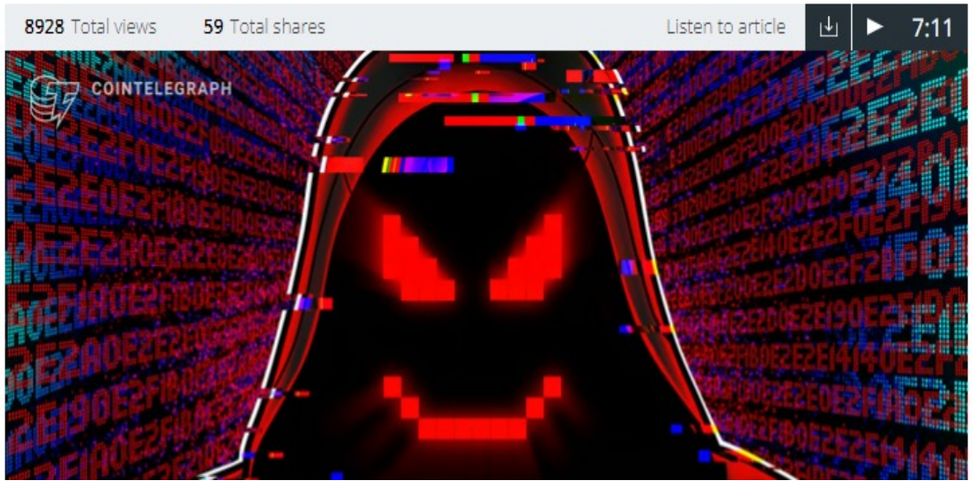
The Cryptoassets Sector and OpRisk

- Crypto exploits tend to affect all sectors of the crypto industry (exchanges, DAOs, DeFi) – hinting at structural deficiencies in OpRisk management practices across the entire industry.

JESSE COGHLAN DEC 30, 2022

The 10 largest crypto hacks and exploits in 2022 saw $2.1B stolen

Just the top 10 major cryptocurrency exploits garnered over $2 billion for malicious actors in a year that was marred with bankruptcies and collapses.



CRIME

2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers

FEBRUARY 1, 2023 | BY CHAINALYSIS TEAM

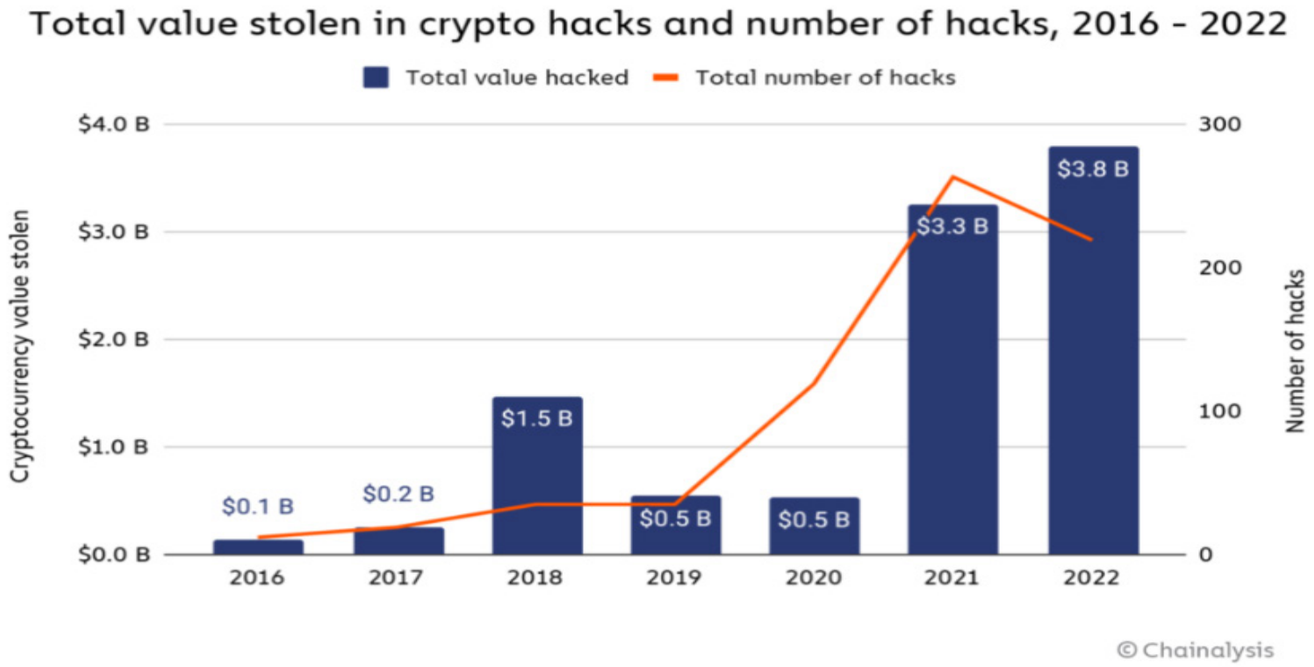
- **Wormhole,** February 2, $325 million
  - A hacker exploited smart contracts on the Solana-to-Ethereum bridge to mint and cash out on wrapped ether without depositing collateral. Jump Crypto, the venture capital firm behind Wormhole, replenished the stolen funds to keep Solana-based platforms affected by the hack solvent. Wormhole renamed its bridge Portal and currently holds over $480 million, according to crypto data firm DeFi Llama.

- **Crypto.com**, January 17, $35 million
  - In late January, a hacker managed to disable two-factor authentication on the crypto exchange Crypto.com and extract bitcoin and ether from customer accounts. CEO Kris Marszalek initially denied customer funds were lost before acknowledging the hack days later. The company said it is transitioning to "multi-factor authentication" in response to the exploit.

Sources: https://cointelegraph.com/news/the-10-largest-crypto-hacks-and-exploits-in-2022-saw-2-1b-stolen ; https://blockworks.co/news/the-nine-largest-crypto-hacks-in-2022 ; https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/ ; https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/Technology/ie_the_dao_attack.pdf

The Cryptoassets Sector and OpRisk (cont.)

- Despite some fluctuations in numbers and volumes, crypto exploits appear to have become an ever increasing issue in the industry.



Source: https://blog.chainalysis.com/reports/2022-biggest-year-ever-for-crypto-hacking/

The Cryptoassets Sector and OpRisk (cont.)

- **Idiosyncratic characteristics of the industry may help explain the industry's vulnerabilities for exploits:**
  - **Hypergrowth and hypercompetition** – business strategy tends to focus on rapid expansions and a race for market share, arguably at the expense of prudent OpRisk management and the build-up of adequate internal systems & controls ("Minimum Viable Product (MVP) Approach").
  - **Hyperflexibility** – hire & fire culture and remote working environment may compromise the effectiveness of internal coordination mechanisms, build-up of mutual trust among staff, formal and informal internal controls, and business continuity management (e.g. handover procedures).
  - **Around the clock ubiquity** – expectation of 24/7 access from anywhere significantly reduces the availability of "breathing space" to adapt and optimize internal systems and governance structures.

    High volatility in crytpoasset prices regularly leads to extreme spikes in customer demand, often overwhelming exchange's systems.
  - **Complex and opaque corporate / governance structures** – corporate structures can be unnecessarily opaque and complex, including ample use of outsourcing (also for internal control functions).

    Decision-making power (and access to custody wallets) tends to be concentrated with founder-owners.
  - **Lack of regulatory pressure** – until recently, regulatory requirements in the EU almost exclusively focused on AML/CTF requirements, arguably leading to a competitive race to the bottom in terms of risk management structures.
  - **Low level of regulatory literacy and cyberpunk mentality –** until recently, the crypto industry – born in the wake of the great financial crisis – has particularly attracted talent that tends to challenge the status quo and government intervention, leaving regulatory concerns not on top of the to-do list.

EU Regulatory Initiatives

- The EU has brought forward two important regulatory initiatives that are likely to have a positive impact on the crypto industry's (operational) risk management practices:

  - **The Digital Operational Resilience Act** (DORA, adopted in Nov 2022) requiring, among others, Cryptoassets Service Providers (CASPs) to...

    ✓ follow key principles for their internal control and governance structures;
    ✓ have in place sound, comprehensive, and well-documented ICT risk management frameworks (including third parties) that are periodically reviewed and audited;
    ✓ have in place ICT-related incident reporting;
    ✓ implement robust and comprehensive testing plans.

  - **The Markets in Crypto-assets Regulation** (MiCA, pending formal adoption by Council), requiring, in particular, CASPs to...

    ✓ obtain a fully-fledged license (as opposed to the current AMLD-registration regime);
    ✓ act "honestly, fairly and professionally in the best interests of clients";
    ✓ comply with certain prudential requirements (e.g. own funds requirements);
    ✓ comply with certain governance requirements, including fit & proper, ICT, BCM, and outsourcing requirements.

EU Regulatory Initiatives (cont.)

- While MiCA and DORA certainly will improve the operational resilience and the quality of OpRisk management in the industry, MiCA's effectiveness will to a non-negligible degree depend on the more detailed requirements of the Level-2 texts.
- It also remains to be seen to what extent, if any, the lack of internationally agreed standards / standards setters will jeopardize MiCA's effectiveness by entities engaging in regulatory arbitrage.
- From an operational and systemic risk perspective, certain aspects of MiCA might warrant specific attention for supervisory authorities:

  - **Level-1 OpRisk requirements are rather broad** -> clear communications of regulatory expectations and tight supervision arguably necessary (even more so in an industry with a relatively low level of regulatory literacy);
  - **Own funds requirements are not risk sensitive**, e.g. no specific capital requirements for OpRisk or possibility for systemic risk buffers -> additional supervisory attention on OpRisk and systemic risk arguably warranted;
  - **Conduct requirements are rather broad** -> supervisors may want to pay additional attention to the development of a prudent and robust risk culture - and corporate culture more generally - as the "backbone" of prudent conduct in an extraordinarily dynamic sector;
  - **MiCA allows for comparatively easy access for traditional finance institutions** such as credit institutions or investment firms (notification instead of license) to the crypto space -> supervisors may want to monitor closely the development of direct and indirect interlinkages between the crypto– and the traditional finance space to anticipate and mitigate potential spill-overs and feedback loops;
  - **By raising the barrier for market entry, concentration in the crypto industry may increase**, potentially leading to an increase in systemic risks in the crypto industry and potential spill-overs to the traditional finance sector -> additional monitoring arguably warranted.

Conclusion

- **Certain idiosyncratic characteristics of the crypto industry make the industry especially prone to the materialization of OpRisk**.
  - Supervisory authorities may want to put particular emphasis on “the basics” in their supervisory approach, e.g. focus on regulatory and risk management awareness / knowledge, integrity within the firms and vis-à-vis customers, proper documentation, outsourcing arrangements (especially of internal control functions) and the fitness & propriety of management and key personnel.
- **Recent legislative initiatives on the EU level are likely to increase the operational resilience and the quality of risk management practices of crypto service providers and could serve as a blueprint for non-EU jurisdictions**.
  - However, MiCA’s risk management and conduct requirements are arguably - at least as far as the Level-1 is concerned - only a first step and not (yet) entirely comparable to the requirements in the traditional finance sector.
- **As recent events in the US have shown, there is a non-negligible potential for direct and indirect spill-overs between the crypto– and the traditional finance sector**.
  - Regulators and supervisory authorities may want to consider devising and implementing sector-specific regulatory policy measures and monitoring tools to minimize the potential systemic risk stemming from the crypto sector.

STILTSKIN

REGULATORY CONSULTING

Thank you.

WORLD BANK GROUP
Finance, Competitiveness & Innovation

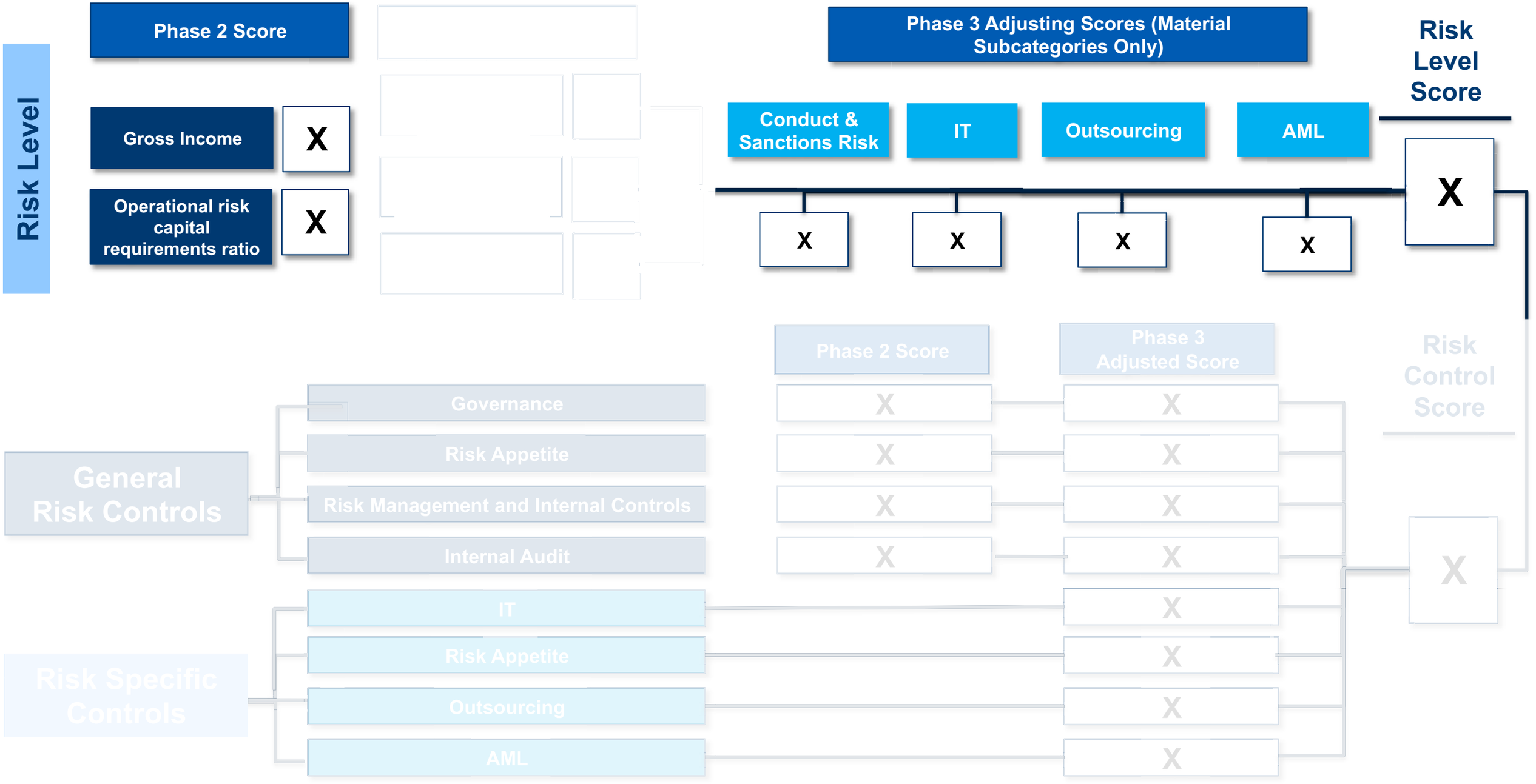
CENTRAL BANK OF ARMENIA

OPERATIONAL RISK ASSESSMENT
Armenia 2023

OUTLINE

- ✓ Methodology of Operational Risk Assessment in Banks
  - ✓ Outsourcing Risk Assessment Methodology
  - ✓ IT and IT Security Risk Assessment Methodology
  - ✓ Sanctions Risk Assessment Methodology
  - ✓ AML Risk Assessment Methodology

Operational Risk Assessment map



OUTSOURCING RISK

RISK LEVEL ASSESSMENT

STAGE 1

INFORMATION GATHERING
- List of outsourced services
- Expenditure on outsourcing

STAGE 2

AUTOMATED SCORING

1. Volume (outsourcing expenditure)
2. Offshoring
3. Concentration (type I)

STAGE 3

SUPERVISOR JUDGEMENT
1. Materiality
2. Country Risk
4. Concentration (type II)

RISK CONTROL ASSESSMENT

STAGE 1

INFORMATION GATHERING
- Banks were asked to fill in control questionnaire

STAGE 2

Control Component	Score
Outsourcing Policy	12
Record Keeping	3
Exit Strategy and Business Conitnuity	6
Internal Audit	3
MI and Senior management approval	3
Risk Analysis	3

STAGE 3

SUPERVISOR JUDGEMENT
1. Practical Assessment of 1-2 outsourcing contracts
2. Risk Interviews

IT and IT security Risk

- ✓ Risk assessment is similar to the process adopted by ECB Banking supervision
- ✓ Every year supervised entities complete the annual 'Information Technology Risk Questionnaire' (ITRQ)

STAGE 1

Banks are given one month to complete IT RISK SELF-ASSESSMENT QUESTIONAIRE

- **Risk Level:** 26 questions in 4 risk level areas
- **Risk Control:** 100 questions in 8 risk control areas

Self-Assessment Score — **X**

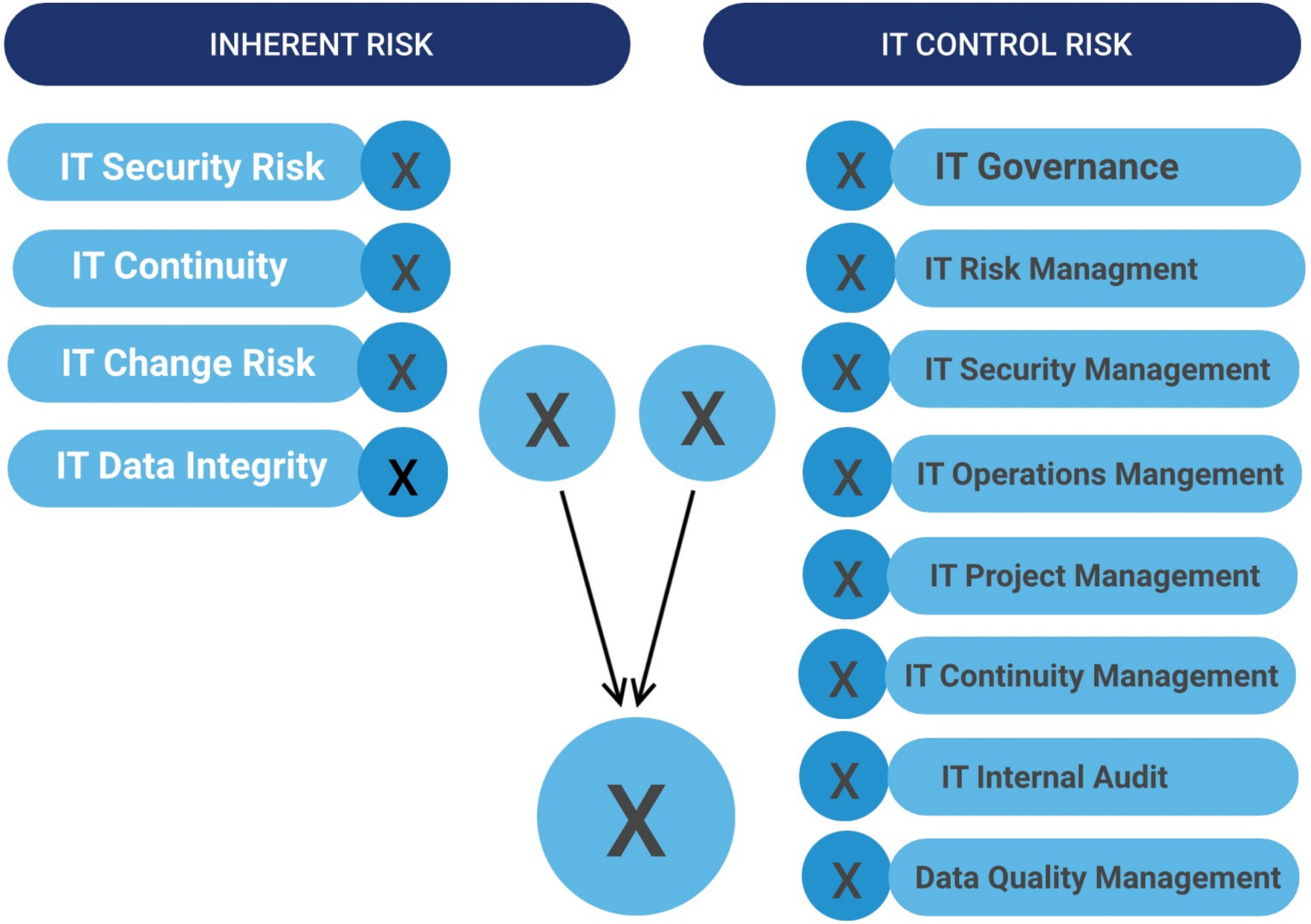
STAGE 2

Supervisory Re-adjustment of Self-Assessment Score

- **Offsite information gathering and assessment** of the most significant areas based on stage 1 findings
- **Onsite inspections** lasting 1-2 weeks to conduct further onsite checks and risk interviews with key individuals

Supervisory Re-Adjusted Score — **X**

IT RISK SELF-ASSESSMENT QUESTIONAIRE



Sanctions Risk Assessment

✓ Every year supervised entities complete the Sanctions Risk Assessment Questionnaire

SANCTIONS RISK

RISK LEVEL ASSESSMENT

AUTOMATED SCORING

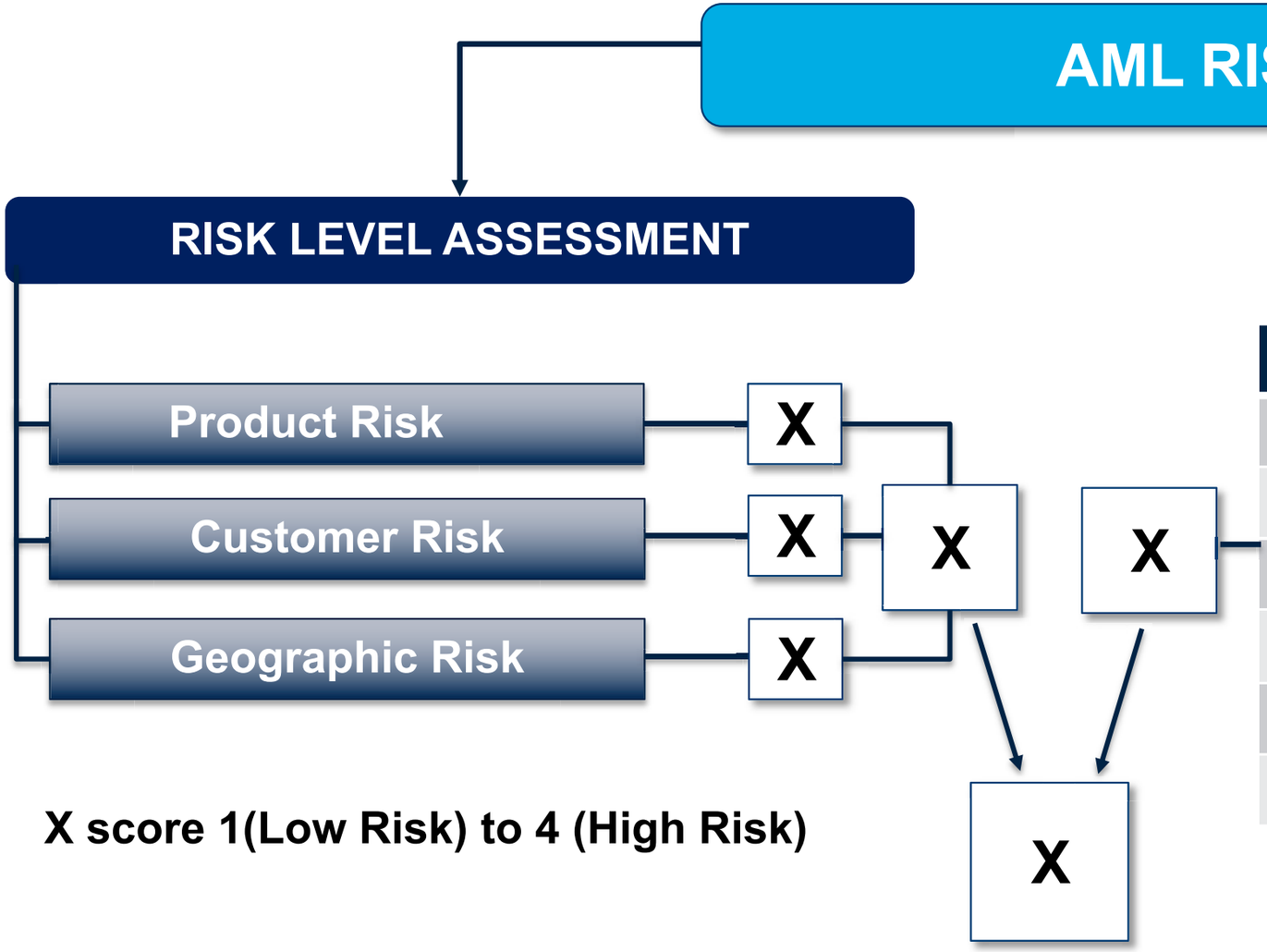
1. **Exposure to customers residents of sanctioned jurisdictions**
2. **Transactions with sanctioned jurisdictions**
3. **Dual-use goods**
4. **Enquiries from correspondent banks**
5. **Customers found in major regulatory sanctions lists**

RISK CONTROL ASSESSMENT

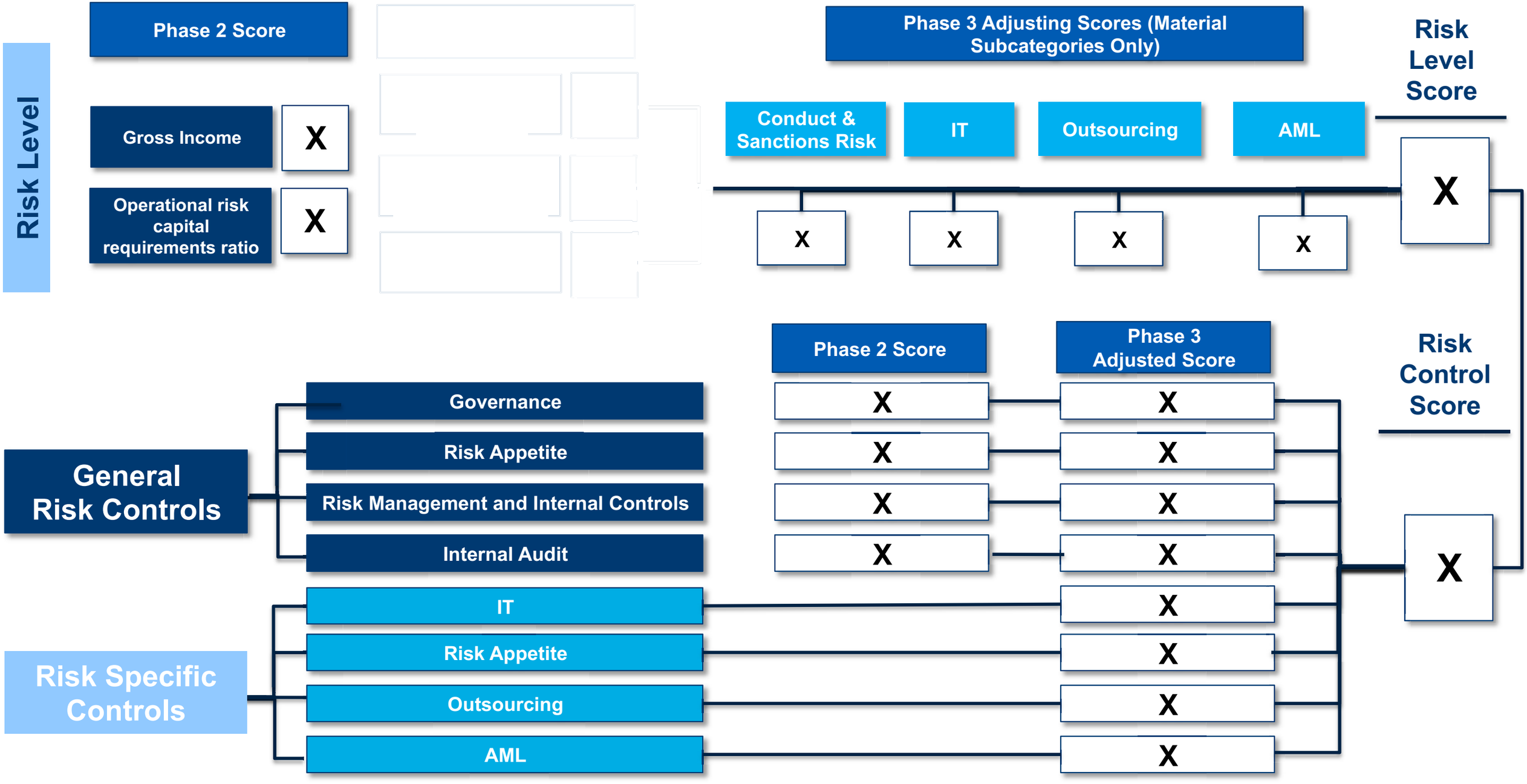
Control Component
Sanctions Compliance Policy
Effectiveness of Automated Screening Solutions
Quality of Customer Due Diligence Procedures
Staff Training
Internal Audit
Quality of Sanctions Enterprise-Wide Risk Assessment

AML RISK ASSESSMENT

✓ Every year supervised entities complete the AML Risk Assessment Questionnaire



Operational Risk Assessment map



WORLD BANK GROUP
Finance, Competitiveness & Innovation

CENTRAL BANK
OF ARMENIA

THANK YOU

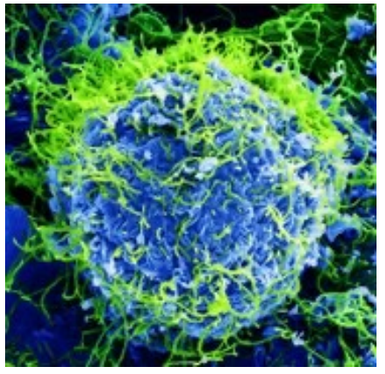
Contemporary Challenges in Operational Risk Management

David Papuashvili

FinSAC Annual Conference

May 9-10, 2023

Vienna, Austria



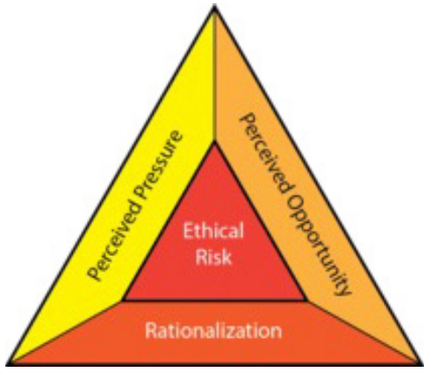
Note: The views expressed in this presentation represent those of the author and do not necessarily represent the views of the World Bank.

Why Should We Care about Operational Risk?

- Operational risk (including cyber risk) has become a key risk for the financial system.
- Some of the largest losses in the financial system have come from operational risk events.
- Pandemics, war and other events can have a significant impact on financial institutions.
- Cyber risk can be a direct threat to financial stability and is a source of systemic risk.

Risks Typically Included Under Operational Risk

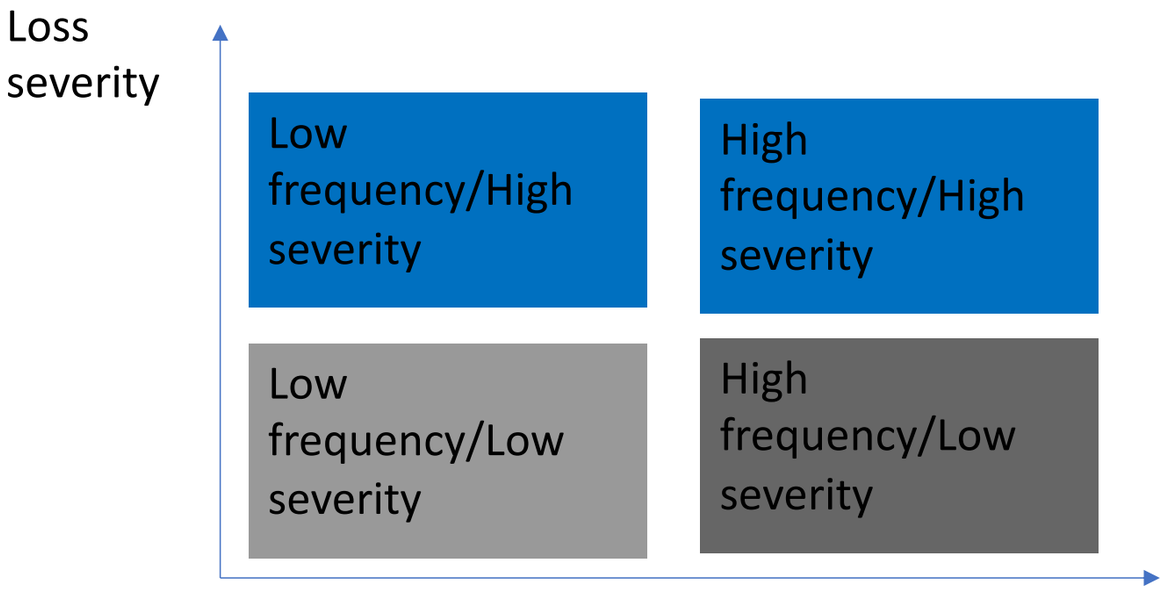
- Process Risk
- Technology Risk
- Business Continuity Risk
- Fraud Risk
- Cyber and Information Security Risk
- Outsourcing Risk
- Conduct Risk
- Legal Risk

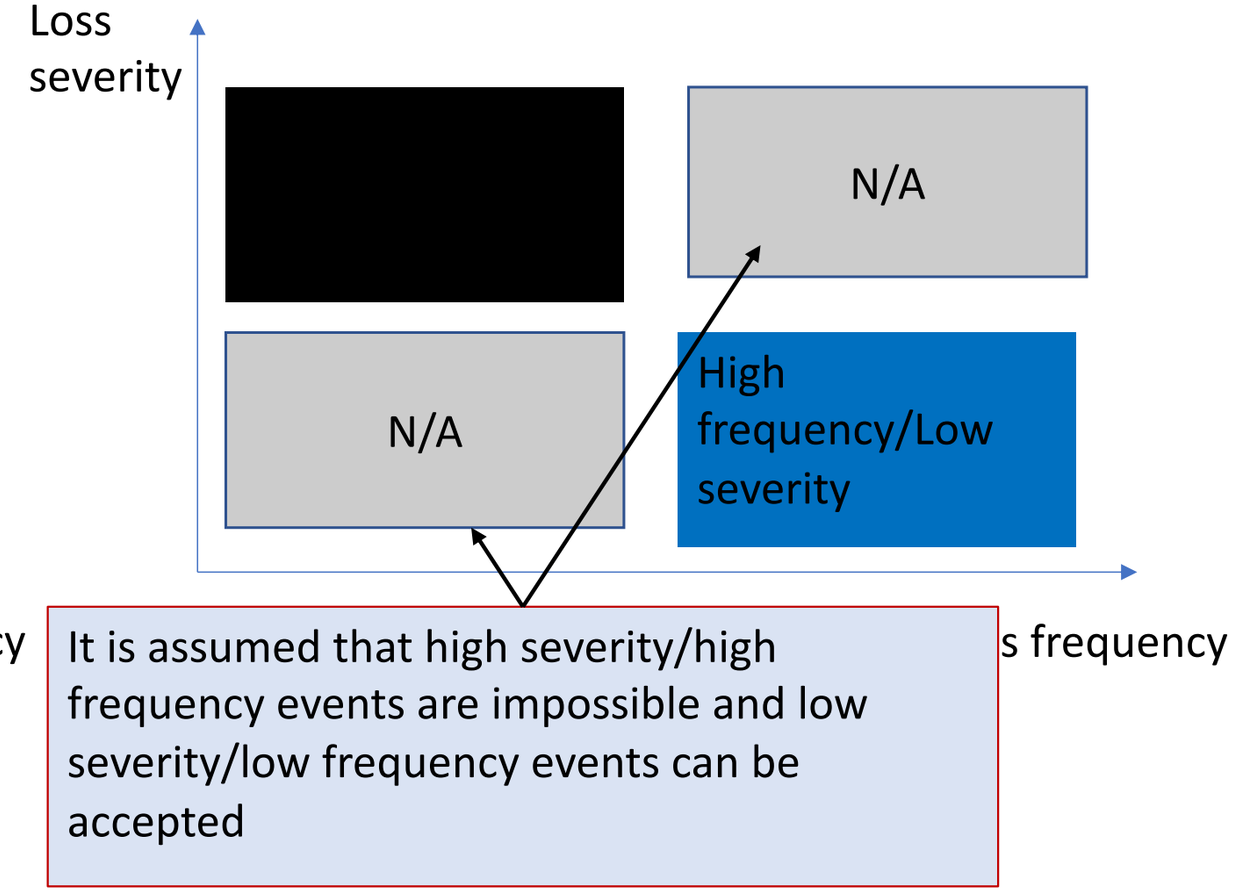


Key Points for Operational Risk Management

- The objective is to prevent operational losses, especially large losses.
- Large operational risk events can be due to fraud, technical disruptions, sales practice violations.
- The main goal of operational risk management is to lower the frequency and severity of large-loss events.
- **The primary challenge for operational risk management is to ensure a low frequency of major events (high severity) that can cause large losses.**
- Large operational risk events (i.e. internal fraud) can put an organization out of business.

Operational Loss Event Classification: unrealistic view (left) and realistic view (right)

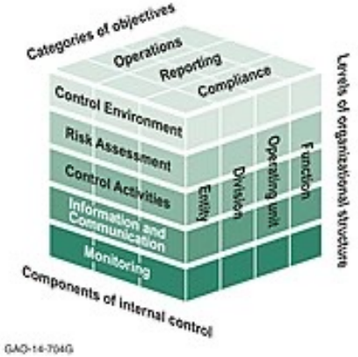




Source: Chernobai, Rachev and Fabozzi

Internal Control Environment

- Are there effective controls in place?
  - Preventive
  - Detective
  - Corrective
- Make sure that at least **sufficient detective controls** are in place if:
  - No adequate preventive controls have been implemented
  - No corrective controls such as business continuity and incident response



Supervisory Reviews

- Supervisory reviews are a good way to assess both inherent risk and the quality of management and internal controls.
- Reviews should generally use a risk-based approach.
- On-site examinations are important for understanding a bank's risk environment.
- On-site examinations include:
  - Interviews with key staff
  - Observation of select business processes (such as reporting, loan disbursements, money transfers, cash operations, etc.)
  - Assessment of contracts, agreements, etc. for compliance and accuracy.
  - Consumer protection-related considerations
    - i.e. data protection

What is IT Risk?

- IT is a business risk
  - i.e. No longer confined to an organization's information technology department.
- IT has become key to most business operations today
- Many companies still have not adjusted their processes to manage IT risk properly.
- IT risk is often closely associated with outsourcing of critical processes and functions

Information Technology (IT) Risk Supervision

- 4A - A commonly used supervisory framework for assessing IT Risk
- Developed at MIT by George Westerman and Richard Hunter for IT Risk management.
- Each step in the pyramid is dependent on the step that lies below.

Source: Westerman & Hunter

Key IT Risk Observations

- Complexity of information systems
  - Use of legacy systems
- New financial products and services increasingly use sophisticated technology that is not always well-understood.
- Failure to identify emerging risks
- Technical disruptions can lead to reputational risk
- Cloud computing is on the rise
  - **Can be an effective risk mitigation tool**

Contingency and Resilience Planning

- Key questions that need to be addressed:
  - What is the degree of protection provided by a bank's contingency plan against major unexpected events affecting the bank?
  - What is the time it would take to recover from an event and return to normal operations?
- External operational failures are far harder to control and require comprehensive contingency plans.
  - i.e. cyber-attacks can bring down a bank's internet-based operations.
- Quality of a contingency plan is proportional to the time and effort that staff have put into it.
  - Supervisors should make sure that adequate resources are put into the development of a business continuity plan
- Problem is that if risk managers do not take into consideration some of the relevant unexpected risks, the contingency plan may not be effective.

Outsourcing Risk

- Cloud computing has emerged as a significant form of outsourcing.
  - Can be a useful risk mitigation tool.
- Outsourcing Risk Assessments Need to Answer:
  - What is the reason for outsourcing?
  - Is the outsourcing activity in line with the overall strategy and direction of the organization?
  - What are the benefits and risks of outsourcing?
  - Are there qualified and experienced outsourcing service providers?
  - Can the organization monitor and manage the relationship with the outsourcer?
  - What are the operational risks (information security, fraud, etc.)?

Oversight and Monitoring of Outsourcing Risk

- What is acceptable in terms of service provider's performance?
- Specific metrics should be established
- Bank's employees that monitor the service provider should have sufficient expertise in the field
- Reporting should be risk-based
- Financial condition:
  - Has the financial condition of the outsourcer changed in any way?
- Internal Controls
  - Has the internal control environment changed?

Thank You