Advanced Operational Risk Management

in a Rapidly Evolving Landscape.

In a world brimming with changes,
Risk Management remains the compass toward sustainability.

Mr. Said Abdelmegeed

Head of ORM at National Bank of Egypt - NBE

Chair of the Operational Risk Committee at Federation of Egyptian Banks (FEB)

Disclaimer: **Information and examples provided in this presentation are based on publicly available events & data, and are intended strictly for educational and informational purposes only. They do not reflect the personal views of the presenter or his affiliated entity. All opinions expressed are solely for analytical and discussion purposes, and should not be construed as financial, legal, or commercial advice.**

Global Operational Risk:

Key Trends & Indicators

1- A Glance at Operational Losses in Banks

2- Operational Risk Sources

A Glance at Operational Losses in Banks

BIS

Basel III
Monitoring Report
March 2025

Operational Risk-Weighted Assets ranked second, right after credit risk, in terms of size.

O.R.X

Operational Risk data exchange Association
June 2024

Contributing Members **82**

External Fraud recorded the highest frequency of events from 2018 to 2023.

166,803

Average Annual Gross Loss (2018-2023).

€ 21.5bn

Operational risk stems from diverse and intertwined sources. Human elements, information technology, and processes are no longer merely origins of operational risk; rather, they are considered, at their core, significant business enablers.

Human Elements

Processes

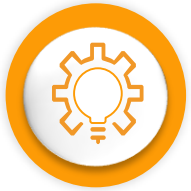
Information Technology

External Factors

During this session, we will cover the following key Pillers:

Key Challenges In a Rapidly Evolving Environment

Advanced Technologies For Operational Risk Management



Progressive Frameworks for Risk Management

Future Outlook and the Evolving Function of ORM

Key Challenges in a Rapidly Evolving Environment

1- Accelerated Technological Evolution

2- Evolving Nature of Risks

3- Increasing Data Volume and Complexity

4- Compliance with Regulatory and Supervisory Guidelines

1- Accelerated Technological Evolution:

Key Technologies Driving Change

- ❑ Artificial Intelligence (AI)
- ❑ Machine Learning (ML)
- ❑ Cloud Computing
- ❑ Blockchain

Associated Risks

- ❑ Cyber Risks
- ❑ Change Management Risk
- ❑ Bias in Application Design Risks
- ❑ Third-Party Risks

2- The Evolving Nature of Risks

"Operational risks are no longer confined to human error or traditional system failures. Instead, their scope has expanded significantly as the current environment is marked by new diverse emerging risk types. These notably include cyber risks, third-party risks, model risks, and those pertaining to sustainability and **ESG factors**. Concurrently, **Geopolitical risks** are significantly impacting global business continuity and supply chain."

3- Increasing Data Volume and Complexity

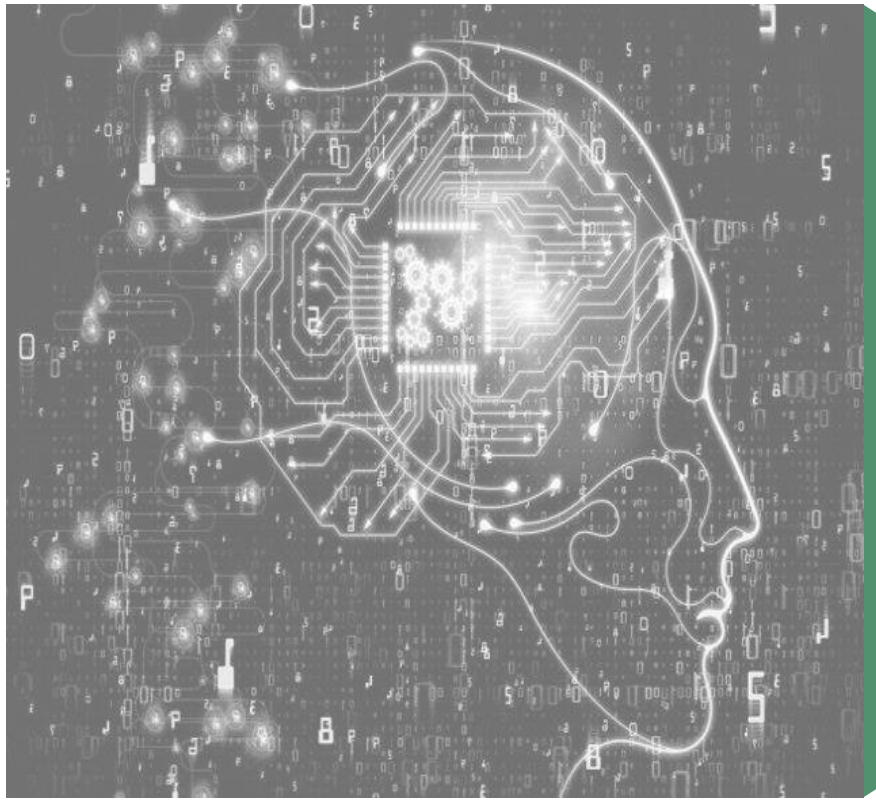
Although “Big Data” offers great opportunities to enhance the understanding of risks and enable more informed decision-making, its management and analysis present significant challenges.

Infrastructure and Analytical Capabilities

Data Integration

Data Quality

Data Privacy Protection



4- Compliance with Regulatory and Supervisory Guidelines

The banking sector faces continuous regulatory and supervisory updates aimed at enhancements, that places significant challenges on risk management functions and demands high flexibility.

- **Capital Adequacy**
- **Stress Testing**
- **Recovery Plans**
- **Operational Resilience**
- **New Product Requirements and Financial Inclusion**

Key Challenges in Developing and Implementing Stress Testing

- Data Limitations and Quality Issues
- Resistance from Stakeholders
- The Need for Staff Development
- Availability of Quantification Models
- Confusing Stress Testing and Scenarios

CHALLENGES

Advanced Technologies for Operational Risk Management

1. Leveraging Sophisticated Data and Advanced Analytics
2. Applications of Artificial Intelligence (AI) and Machine Learning (ML)

Adopting these technologies is not merely about keeping pace with advancements; it represents an opportunity to evolve the operational risk management function from a supporting role into a strategic partner that contributes to achieving operational excellence and safeguarding organizational values.

1-Leveraging Sophisticated Data and Advanced Analytics

To address the challenges that have been discussed, banks need to adopt more advanced and effective technologies and frameworks.

This goes beyond traditional compliance and oversight, focusing instead on proactivity, deep data analysis, and enhanced resilience.

Here are the key characteristics of this approach:

- ❑ Shift from traditional, manual risk & control assessments to continuous, data-driven, real-time or near real-time monitoring. This includes using dynamic Key Risk Indicators (KRIs) and trend analysis to identify deviations and recognize unusual patterns.

2- Applications of Artificial Intelligence (AI) and Machine Learning (ML)

Process Automation

Leverages AI to automate repetitive tasks in risk management, such as classifying events, testing controls, and generating and analyzing reports.

Predictive Modeling

Involves developing advanced predictive models that anticipate the probabilities of operational losses by analyzing a wide range of internal and external risk factors.

Advanced Scenarios Analysis

Utilizing Machine Learning (ML) to analyze complex scenarios enables the assessment of potential impacts from extreme or interconnected risk events.

Progressive Frameworks for Risk Management

1. Strengthening Operational Resilience
2. Developing Governance and Measurement Frameworks
3. Effective Third-Party Risk Management
4. AI Risk Management in Banks

1- Strengthening Operational Resilience

Operational Resilience: is a bank's ability to deliver banks' essential and critical operations during times of disruption. This enables the bank to identify and protect the bank from potential threats and failures, respond, adapt, recover and learn from disruptive events to minimize their impact on the continuity of essential and critical operations. A bank must consider the overall risk appetite, maximum risk tolerance, and risk framework.

As per the CBE's directives issued on January 4, 2021.

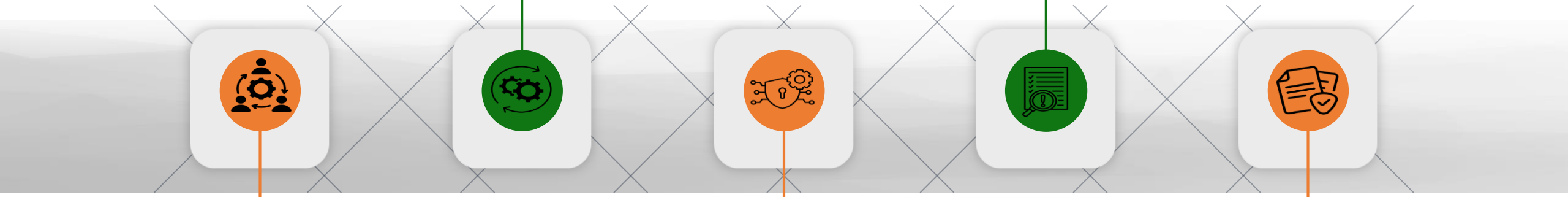
Principles of Operational Resilience

- Governance
- Operational Risk Management
- Business Continuity Planning and Testing
- Mapping Interconnections and Interdependencies
- Third-Party Dependency Management
- Incident Management
- Information and Communication Technology (ICT), including Cyber security

Stress Testing in the context of Operational Resilience

Focusing on impact, and the ability for an entity to recover under extreme conditions

Assesses systems, people and process resilience in real-world crisis scenario.



Simulates disruptions, validates resilience strategies

Testing critical services (IBS), including cyber, IT and third-party risks.

Meet regulatory requirements, proves firms can operate within impact tolerances.

2-Developing Governance and Measurement Frameworks

Integrated Governance:

Adopting an integrated governance approach moves beyond working in isolation silo approach ; This means that all relevant departments, such as operational risk management, business units as first liners, and other control functions like compliance, audit, and information security, must work in complete harmony and coordination.

To achieve this, it's essential to clearly define the roles and responsibilities for each party and to standardize risk classifications.

Quantitative Measurement

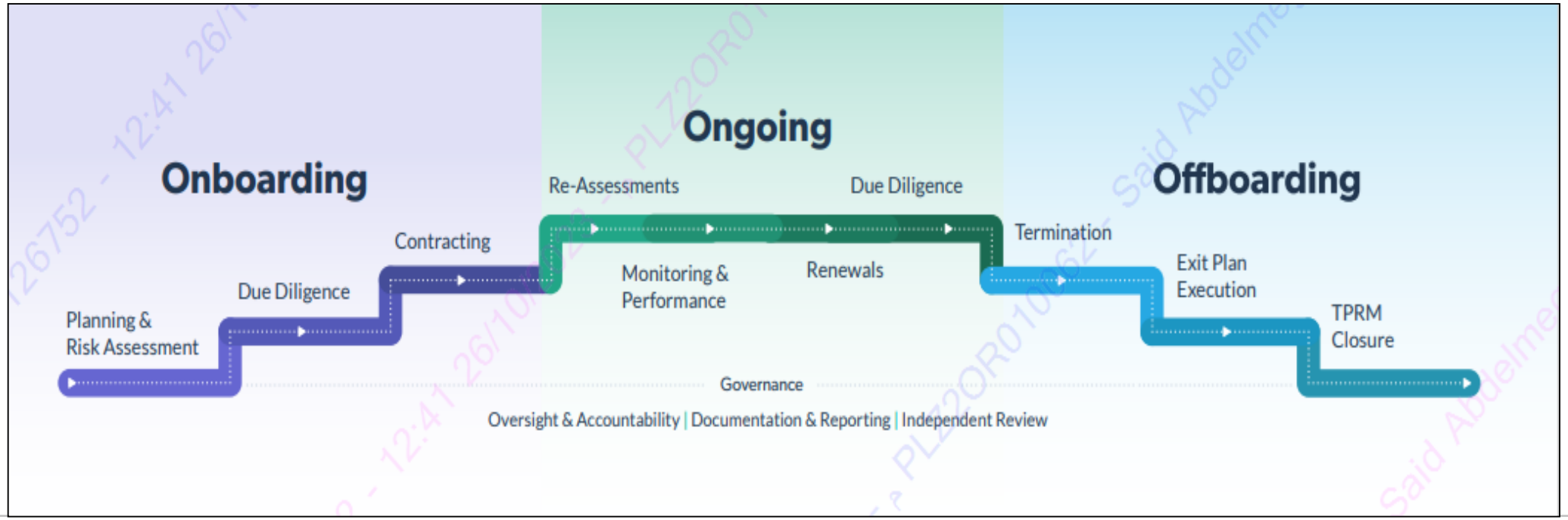
Continuous development of quantitative methods for operational risk; This includes utilizing historical loss data, risk assessments, and statistical analysis. A key aspect of this involves leveraging the new standardized approach for measuring operational risk capital.

Risk Culture

Fostering a robust risk culture across the organization rather every employee must be accountable for identifying and managing operational risks within their scope of work.

3. Effective Third-Party Risk Management

- Effectively managing Third-Party risks is crucial for enhancing bank's resilience, given the increasing reliance on third parties for services and products. Consequently, Third-Party Risk Management (TPRM) across the banking group has become even more vital.
- The definition of a "Third-Party" now extends beyond outsourced services to include service providers and suppliers.
- It is essential to focus on risk management throughout the entire third-party lifecycle, from pre-contracting through to termination, to ensure efficient and effective risk management.



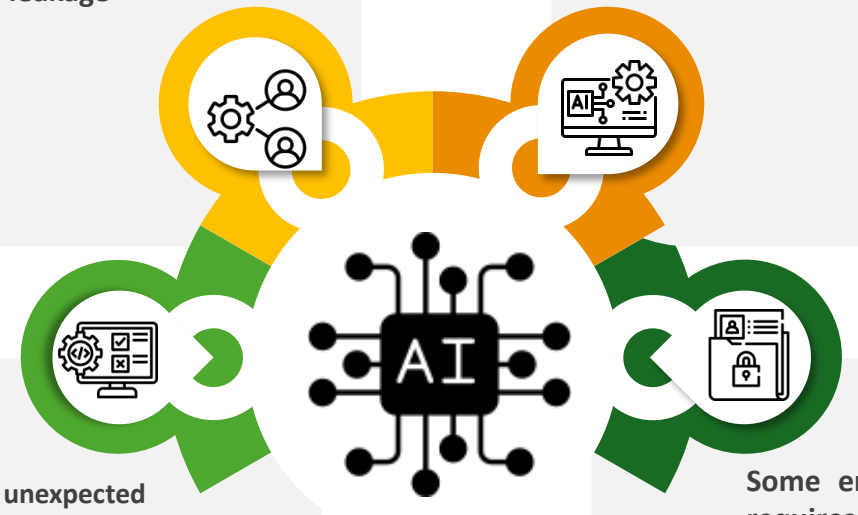
4- AI Risk Management in Banks

Data Privacy and Information Security

The use of AI models requires a massive amount of data, which may lead to increase the possibility of data leakage or misuse by service providers or other parties.

Dependence on Third Parties (AI Programs / Applications Developers)

Relying on SW providers could lead to great challenges due to lack of control on the technological aspect.



Biased in AI outputs

AI may produce inaccurate or biased information, resulting in unexpected responses or incorrect advice. These errors may also occur in areas such as credit score or the rejection of customer requests without logical justifications.

Inadequate Testing of AI Models:

Some errors may appear in AI models and applications, which requires conducting a number of tests to ensure the validity of these models before launching the application or service.

(Testing involves a range of approaches to ensure functionality, performance, and user experience. These tests are crucial and can include: Performance Testing, Stress Testing, Load Testing, UAT Testing, Usability Testing , Integration Testing & Security Testing).

Key Takeaways

Focus on investing in infrastructure and employee skills: Successful implementation of AI requires investments in technical infrastructure and employee skills development.

Due diligence: Before entering into contractual relationships with AI service providers.

Perform a detailed assessment of risks and controls: The assessment of risks and controls should not only involve ICT technical aspects but also other relevant functions such as cyber security, legal, information security, operational risk and external third parties. It should identify controls that need to be in place before testing starts or before an AI tool goes live

Test prototypes internally first: Focus on low-risk use cases before expanding externally.

Periodic review of model results: Especially in assessing credit scoring and critical decisions.

Source: Euromoney, "AI in Banking Best Practices Playbook"

Future Outlook and The Evolving Function of ORM

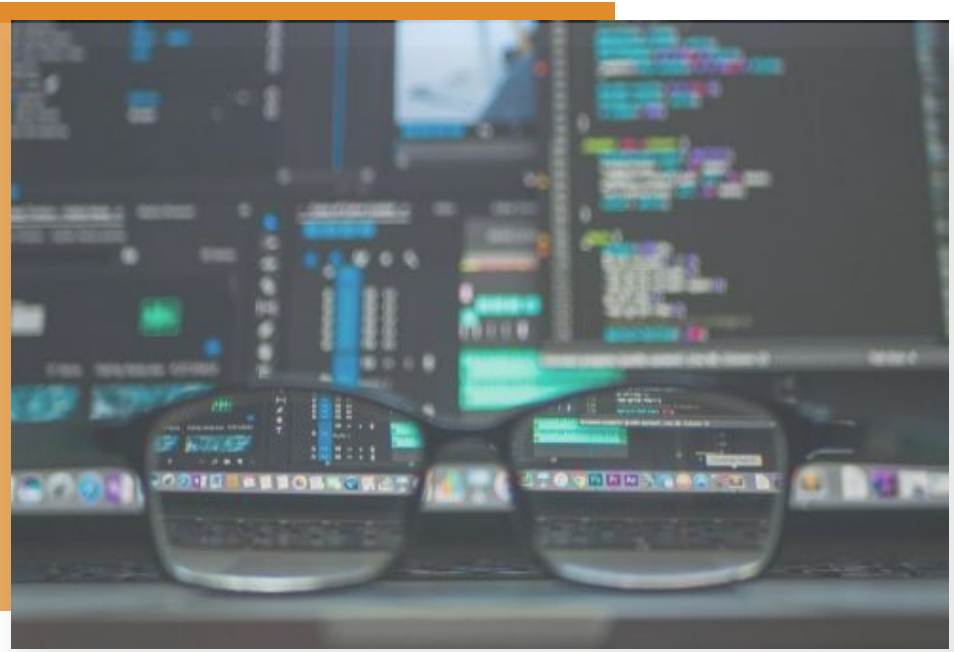
1- Strategic Partnership with Business Lines

2- Increased Focus on Non-Financial Risks

3- Integrated Risk Management

4- Evolution of Skills and Talent

5- Automation and Artificial Intelligence



1- Strategic Partnership with Business Lines

The operational risk management function will no longer be solely confined to the traditional scope of oversight and reporting. Instead, it will evolve into an integral strategic partner for the business lines. Risk experts will provide insights into operational strengths and areas requiring development, participate in the study and assessment of new products, contribute to infrastructure improvement, and support strategic decision-making. This ensures the realization of the bank's strategies and objectives while concurrently managing risks effectively.

2-Increased Focus on Non-Financial Risks

As the significant increase of non-financial risks, encompassing cyber risk, third-party risk, climate and ESG risks; risk departments will be compelled to develop specialized expertise and implement advanced tools or the effective management of these evolving and complex risk typologies.

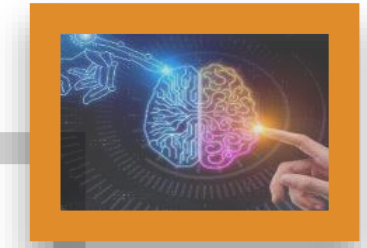
3- Integrated Risk Management

The trend towards integrating Operational Risk Management with other key risks (e.g., Credit, Market, and Liquidity Risk) and control functions (e.g., Compliance, Audit, and Security) will accelerate. This is essential for establishing a holistic Enterprise Risk Management (ERM) framework that provides a comprehensive view of risk across the bank.

4- Evolution of Skills and Talent

Operational Risk Management teams will need a diverse blend of competencies , combining deep banking expertise, a robust understanding of technology, advanced analytical capabilities, and strong communication and influential leadership skills. Investing in the development and recruitment of the appropriate talent will be critical.

5- Automation and Artificial Intelligence



The expanded utilization of automation and Artificial Intelligence (AI) will continue to enhance the efficiency and effectiveness of risk management, starting from continuous monitoring to predictive modeling and scenario analysis.

Key Takeaways

01

Adopt a Proactive Mindset

Transform from reactive responses to anticipating and preparing for potential risks.

02

Invest in Technology and Data

Build the necessary capabilities for effective data collection and analysis, and adopt advanced technology tools such as Artificial Intelligence and Machine Learning.

03

Foster a Risk Culture

Promote awareness regarding the importance of operational risk management throughout the bank.

04

Talent Development

Investment in personnel training and development is crucial to ensure they possess the necessary skills for future challenges. This involves updating educational content and establishing specialized training programs to build a highly capable workforce that can adapt to the rapid advancements within the field.

05

Focus on Resilience

Build robust operational resilience capabilities to ensure business continuity in the face of disruptions and secure supply chains through third-party risk management.

THANK YOU