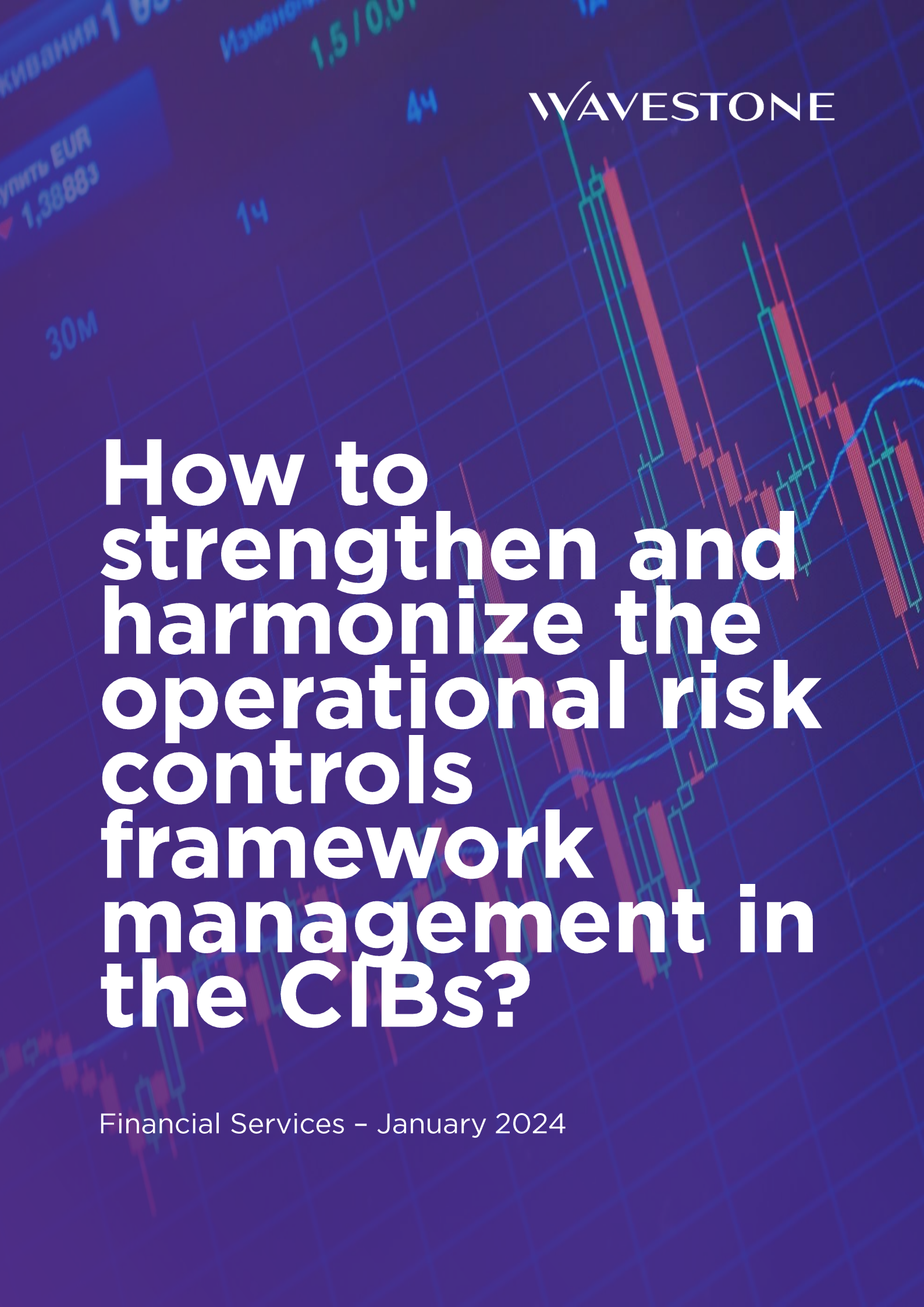


WAVESTONE

How to strengthen and harmonize the operational risk controls framework management in the CIBs?

Financial Services – January 2024

Introduction

The recent operational risk management failings witnessed at Credit Suisse testify once more of the attention Corporate and Investment Banks (CIBs) need to give towards efficiently manage their risks and towards planning operational controls.

Furthermore, the global and decentralized nature of CIBs leads to disparities in inherent risk evaluations and control framework deployed.

The importance of protecting banks against operational risks

Operational risk refers to events affecting processes, IT systems, people, and external events which can impact the bank's activity. It can lead to significant financial consequences, decreasing its value to shareholders, debtholders, and overall damaging the banks reputation. Effective management of operational risk is essential to ensure business continuity and protect banks' reputations.

In December 2021, the BaFin, Germany's central financial authority, fined Deutsche Bank €8.66 million and demanded corrective measures be implemented as punishment for insufficient internal controls. Indeed, the bank is accused of not implementing efficient control systems to prevent IBOR (Interbank Offered Rate) manipulation. The bank had to invest considerable resources to reinforce its control systems and train its personnel in managing operational risks.

This sanction underlines the importance for banks to identify operational risks, as well as maintaining a modern tech infrastructure supporting efficient operational risk management.

What major operational risks threat investments banks

Due to their essential role in the financial system, CIBs face different types of risks inherent to their operations. Understanding and controlling these risks is essential to assess the health and stability of a financial institution.

Referring to the classification of operational risks issued by the Basel Committee, CIBs face 7 types of major risks:

1. *Internal fraud*
2. *External fraud*
3. *Employment practices and workplace safety*
4. *Clients, products & business practices*
5. *Damages to physical assets*
6. *Business disruption and systems failures*
7. *Execution, delivery & process management*

It is essential to broaden this scope to include other types of risks, such as strategic and reputational risk.
Failure management can lead to an over or underestimation of the capital allocated to hedge the bank's operational risk. In addition, it can lead to excessive allocation of resources, additional investments, deterioration in profitability or poor strategic decisions, to mitigate an over or underestimated risk. Thus, a robust analysis is essential in valuing its inherent risk, accompanied by complementary indicators such as the risk occurrence rate.

The operational risks can impact inherent business, IT systems, security, and compliance processes. It is therefore crucial for banks to implement appropriate controls to mitigate those risks and ensure the smooth running of their operations.

What types of controls the banks can implement to mitigate their operational risks

Banking supervision aims to ensure regulation compliance, protect client's interests and prevent banking risks. The objective is also ensuring transparency of banking activities and the quality of the financial information issued.

Each bank should adopt and implement controls in accordance with its size, its organizational structure, its business strategy, as well as applicable regulatory requirements.

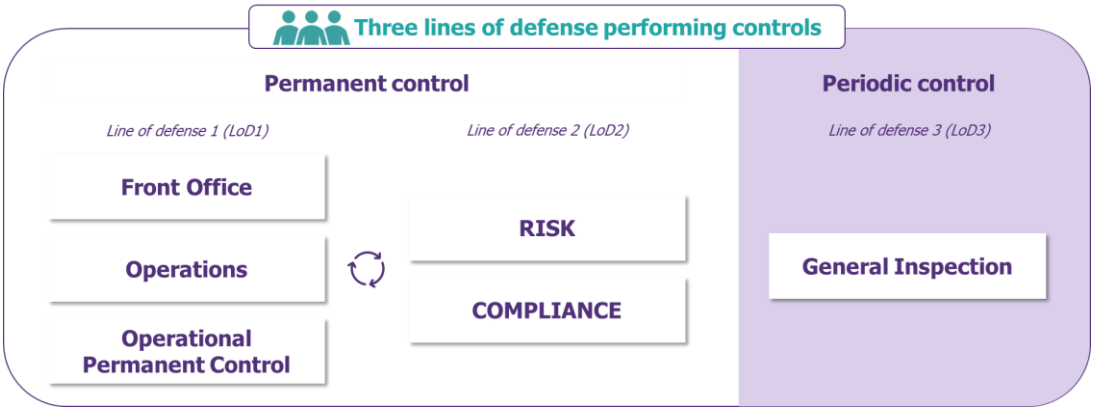
Operational controls aim to minimize operational risks related to internal processes of the banks. They include implementing policies and procedures, training staff, monitoring activities and adopting business continuity mechanisms.

Different types of controls operates in the banking sector

In addition to traditional control measures, financial institutions should implement specific controls to manage operational risks, covering a larger scope of internal processes and human factors liable to cause disruptions and losses within the bank.

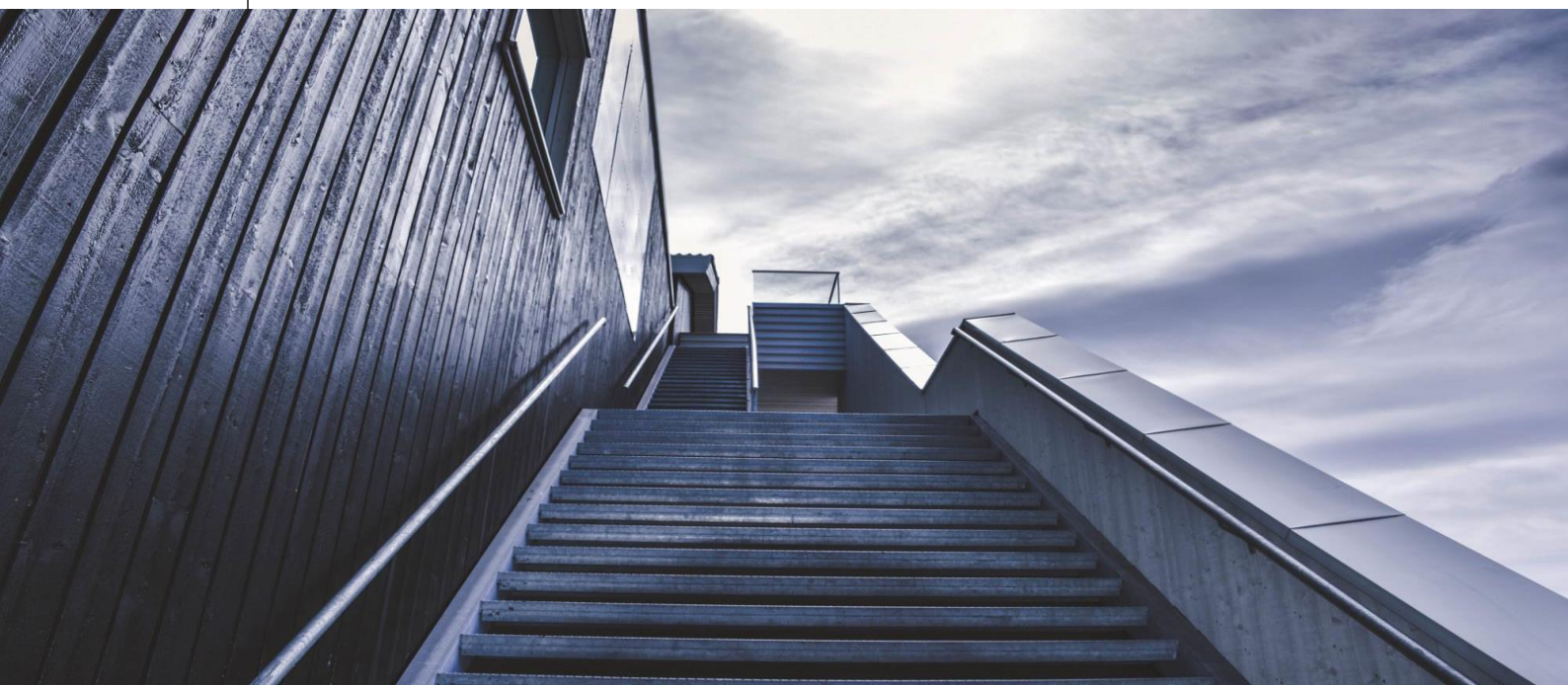
Said controls can be both preventive and detective, by anticipating potential risks or identifying existing anomalies. Furthermore, those controls can be done manually, requiring direct human intervention, or automatically, relying on technological systems and tools. A periodic review of risk management and operational controls is to be realized by the three lines of defense (LoD 1, LoD 2, LoD 3).

The 3 Lines of Defense in charge of performing controls



Wavestone recommends a 5-step approach to reinforce CIBs operational risk and control management framework

1. Define a methodology to identify operational risks scenarios
2. Define and implement a control library
3. Implementing management tools and reports
4. Identify controls automation
5. Implementing a strong risks and controls governance



1. Identifying and defining operational risks scenarios

As experts in Corporate and Investment Banking activities, we have successfully implemented key programs to optimize the operational risk and associated controls frameworks of leading French CIB Banks. Our experience on similar projects enables effective integration by leveraging on our accelerators and our hands-on approach to deliver on large and complex programs to a successful end. In order to harmonize and strengthen your risk management and operational control frameworks, we suggest addressing the following five key subjects.

Before implementing any protective measure, it is crucial to clearly understand the dimension of operational risk at hand. This implies an in-depth analysis of current internal processes, information systems, human resources and external factors which could affect the proper functioning of the bank. This task will allow to identify the risk points and prioritize protective actions.

The establishment of a methodology for identifying and defining inherent risks is essential to create a harmonized and standardized library of risk scenarios for each CIB activity at worldwide level. The aim is to standardize risk definitions and ensure a common understanding of these risks within the bank globally.

Once those risks are identified, it is important to assess the level of inherent risk based on a quantifiable methodology and consistent with the underlying activity specificities. Assessing risk evaluation helps prioritize risks and focus efforts on the most important and frequent risks. To assess the frequency of a risk, we recommend mostly analyzing historical data (internal and external) and relying on the business expertise.

Our key success factors to build a robust RCSA methodology

a. Clearly define the process and responsibilities from the outset of the project: ensures a strong commitment to proactive operational risks management

b. Implement a continuous iteration between LOD1 and LOD2 at each key step of the project

c. Leverage control test results and key performance indicators: to evaluate the controls' efficiency and reinforce control framework.

d. Demonstrate the added value of the program to reinforce trust between stakeholders

2. Define and implement a control library

As mentioned, different types of control exist to manage operational risks. It is therefore essential to establish a common control framework at the bank's level to ensure a harmonized and coherent approach. However, it is also essential to acknowledge the risks that may be intrinsic to a region or to a business activity specificities, and thus adapt the control framework accordingly.

A consolidated and harmonized vision of its control library, dedicated to each activity and region, is paramount, and shall include a clear view of each control component (objective, description, value chain, execution rate, proof, etc.)

Once the controls selected, it is necessary to evaluate their performance to determine their efficiency in reducing inherent risks. Finally, it is then necessary to assess the residual risks, i.e., the risk that is still effective despite the performance of controls, in order to put in place additional corrective actions or mitigation measures to further reduce and maintain an acceptable level of risk.

Harmonizing controls and risk libraries may require significant changes to existing processes and practices. Change management becomes therefore crucial to help teams adapt to the new practices and integrate them in their business as usual.

We recommend assessing all potential optimization levers through an in-depth analysis of existent processes and automation opportunities.

Control optimization should be realized in accordance with the following 4 levers

3. Implementing management tools and reports

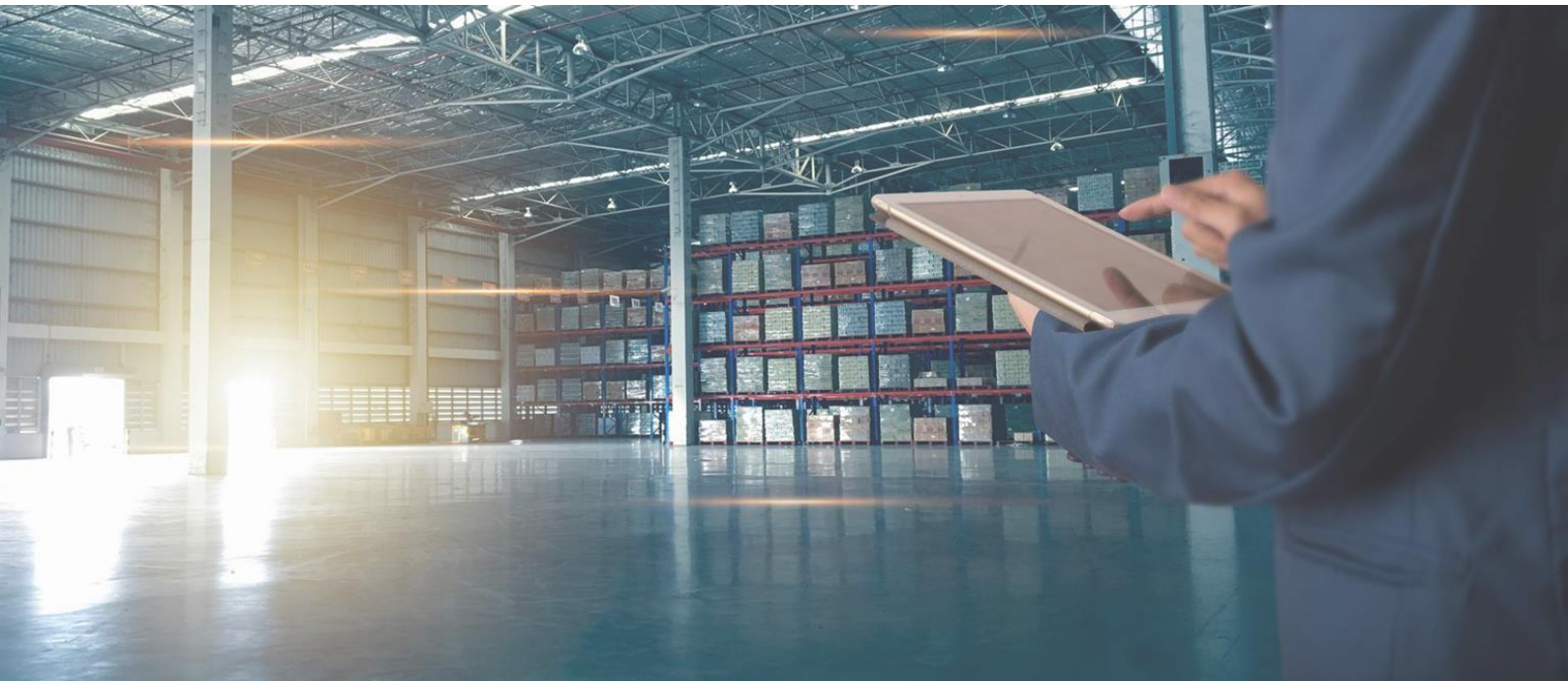
The change brought to the risk management processes and operational controls must come together with proper steering and reporting tools to ensure a close follow-up and constant improvements.
It is essential to perform a gap analysis in the functionalities of existing tools. This assessment will identify and challenge the necessary improvements, whether by customizing current tools or considering new tools offering functionalities more in line with the bank's expectation and needs.

We also recommend assessing a robustness analysis of regulatory reporting capabilities in the context of increasing requirements from regulators and reinforce the process relying on tools offering advanced reporting features.

4. Identify controls automation

We recommend carrying out an in-depth analysis of potential control that can be automated. It would assess in detail every step of the control process to identify areas where automation could provide significant improvements (such as targeting repetitive tasks, compliance verification or continuous monitoring of operational tasks).
Following this, a maturity assessment of existing automation will need to be assess. This assessment should consider available resources and capabilities, as well as the tools and technologies used in control management.
Using new technologies (RPA, OCR, etc.) is also recommended to support risk and control functions, as they allow reducing costs, improving operational efficiency and risk management.

Our 3 methodological tools servicing a more efficient control framework:
1. Data collection: we deploy tools that facilitate the collection and transformation of data, allowing us to compute and analyze data in an efficient manner.
2. Automation: we implement automation tools according to static rules, allowing repetitive and manual tasks to be managed more efficiently.
3. Analysis and machine learning: we use AI to improve the management of complex processes, such as the identification of models, detect correlations and anomalies among large volumes of data.



5. Implementing a strong risks and controls governance

Implementing an efficient governance is essential in maintaining the best management of its RCSA over the long term, and to continuously improve its operational risk and control framework management. Local and global governance committees, with a definition of stakeholder's roles and responsibilities, must be established. Reports must be communicated regularly to convey the bank's procedures and directives. It is also important to follow-up and evaluate the efficiency of the implemented risk management measures though harmonization and continuous evolution of reporting tools.

The continuous assessment of inherent risk and control framework performed by the business is at the center of this governance and must also be revised and improved through internal audits, independent evaluations by regulators, and regular reviews by the 3 Lines of Defense.

Wavestone main key success factors to lead operational risks transformation program successfully within CIBs

1. Set-up a change management team from the start of the project to quickly onboard all stakeholders to understand the project, its objectives and the new methodology for redefining operational risks and control framework.

2. Identify key project participants by combining the first two lines of defense.

3. Outline the roles and responsibilities of each actor upstream to offer a clear vision of everyone's involvement and heir role in the project's ecosystem, at all levels, from central areas to operational perimeters and business activities, including different geographical perimeters.

4. Adopt a flexible approach throughout the project by iterating with other project dependencies and ensuring coordination between the RCSA approach and the definition of operational control framework.

5. Ensure a quick onboarding with the support of our experienced teams and their knowledge of the operational risk subjects, as well as with our project accelerators (methodology, management tools, best practice benchmarks, etc.)

Conclusion

The operational risk management process must be efficient, reliable, harmonized and deployed consistently across all regions and activities of the bank. It is essential to ensure standardized and harmonized methodologies, as well as coherent and efficient governance, with local and global operational control principles implemented.

In this context, Wavestone supports CIBs to strengthen their operational control framework, with a guided RCSA at local and global levels, as well as fine-tune their control libraries based on best market practices for better control of operational risks.

This methodological approach allows for better cost allocation and avoids over-estimating risk-related costs. It also promotes optimization, mutualization, and control coherence by avoiding unnecessary duplications and targeting resources where most needed. In addition, it allows to implement a strong risk management culture, meets regulatory requirements, improves decision-making and ensures bank activities stability and sustainability.

CONTRIBUTORS

AUTHORS

DAYDE Flavia
Senior Consultant
flavia.dayde@wavestone.com

MAJOULET Clara
Analyst
clara.majoulet@wavestone.com

CONTRIBUTORS

With the participation of other contributors from the Financial Services team:

PRACHE Hélène
Senior Manager
helene.prache@wavestone.com

FEL Damien
Manager
damien.fel@wavestone.com

ETTER Sébastien
Manager
sebastien.etter@wavestone.com

FABRIZI Daphné
Manager
daphne.fabrizi@wavestone.com

TEODOR Dan
Analyst
dan.teodor@wavestone.com

ABOUT WAVESTONE

Wavestone, a leading independent consultancy headquartered in France, and Q_PERIOR, a consulting leader in the Germany-Switzerland-Austria region, joined forces in 2023 to become the most trusted partner for critical transformations.
Drawing on more than 5,500 employees across Europe, North America and Asia, the firm combines seamlessly first-class sector expertise with a 360° transformation portfolio of high-value consulting services.

The Positive Way

WAVESTONE

www.wavestone.com