**Operational Risk:**

**EBA (European Bank Authoruty) definition of operational risk:**

is defined as the risk of losses stemming from inadequate or failed internal processes, people and systems or from external events. Operational risk includes legal risks but excludes reputational risk and is embedded in all banking products and activities. It has always existed in banking, and non banking, organizations but it has acquired a greater relevance given the increased complexity and globalization of the financial system and the recent materialization of unprecedented extremely large losses. Through the publication of its guidelines and RTS on operational risk, the EBA aims at promoting and enhancing the effectiveness of operational risk management and supervision throughout the banking system.

Operational risk summarizes the uncertainties and hazards a company faces when it attempts to do its day-to-day business activities within a given field or industry. A type of business risk, it can result from breakdowns in internal procedures, people and systems—as opposed to problems incurred from external forces, such as political or economic events, or inherent to the entire market or market segment, known as systematic risk.

Operational risk can also be classified as a variety of unsystematic risk, which is unique to a specific company or industry.

Understanding Operational Risk

Operational risk focuses on how things are accomplished within an organization and not necessarily what is produced or inherent within an industry. These risks are often associated with active decisions relating to how the organization functions and what it prioritizes. While the risks are not guaranteed to result in failure, lower production, or higher overall costs, they are seen as higher or lower depending on various internal management decisions.

Because it reflects man-made procedures and thinking processes, operational risk can be summarized as a human risk; it is the risk of business operations failing due to human error. It changes from industry to industry and is an important consideration to make when looking at potential investment decisions. Industries with lower human interaction are likely to have lower operational risk. **Investopedia**

**Operational risk in banking.**

Operational risk is a relatively young field: it became an independent discipline only in the past 20 years. While banks have been aware of risks associated with operations or employee activities for a long while, the Basel Committee on Banking Supervision (BCBS), in a series of papers published between 1999 and 2001, elevated operational risk to a distinct and controllable risk category requiring its own tools and organization.1 In the first decade of building operational-risk-management capabilities, banks focused on governance, putting in place foundational elements such as loss-event reporting and risk-control self-assessments (RCSAs) and developing operational-risk capital models. The financial crisis precipitated a wave of regulatory fines and enforcement actions on misselling, questionable mortgage-foreclosure practices, financial crimes, London Inter-bank Offered Rate (LIBOR) fixing, and foreign-exchange misconduct. As these events worked their way through the banking system, they highlighted weaknesses of earlier risk practices. Institutions responded by making significant investments in operational-risk capabilities. They developed risk taxonomies beyond the BCBS categories, put in place new risk-identification and risk-assessment processes, and created extensive controls and control-testing processes. While the industry succeeded in reducing industry-wide regulatory fines, losses from operational risk have remained elevated (Exhibit 1). Mckinsey.

**Intrinsic difficulties**

While banks have made good progress, managing operational risk remains intrinsically difficult, for a number of reasons. Compared with financial risk such as credit or market risk, operational risk is more complex, involving dozens of diverse risk types. Second, operational-risk management requires oversight and transparency of almost all organizational processes and business activities. Third, the distinguishing definitions of the roles of the operational-risk function and other oversight groups—especially compliance, financial crime, cyberrisk, and IT risk—have been fluid. Finally, until recently, operational risk was less easily measured and managed through data and recognized limits than financial risk.

This last constraint has been lifted in recent years: granular data and measurement on operational processes, employee activity, customer feedback, and other sources of insight are now widely available. Measurement remains difficult, and risk teams still face challenges in bringing together diverse sources of data. Nonetheless, data availability and the potential applications of analytics have created an opportunity to transform operational-risk detection, moving from qualitative, manual controls to data-driven, real-time monitoring.

As for the other challenges, they have, if anything, steepened. Operational complexity has increased. The number and diversity of operational-risk types have enlarged, as important specialized-risk categories become more defined, including unauthorized trading, third-party risk, fraud, questionable sales practices, misconduct, new-product risk, cyberrisk, and operational resilience.

At the same time, digitization and automation have been changing the nature of work, reducing traditional human errors but creating new change-management risks; fintech partnerships create cyberrisks and produce new single points of failure; the application of machine learning and artificial intelligence (AI) raises issues of decision bias and ethical use of customer data. Finally, the lines between the operational-risk-management function and other second-line groups, such as compliance, continue to shift. Banks have invested in harmonizing risk taxonomies and assessments, but most recognize that significant overlap remains. This creates frustration among business units and frontline partners.

**Looking ahead**

Against these challenges, risk practitioners are seeking to develop better tools, frameworks, and talent. Leading companies are discarding the “rearview mirror” approach, defined by thousands of qualitative controls. For effective operational-risk management, suitable to the new environment, these organizations are refocusing the front line on business resiliency and critical vulnerabilities. They are adopting data-driven risk measurement and shifting detection tools from subjective control assessments to real-time monitoring.

The objective is for operational-risk management to become a valuable partner to the business. Banks need to take specific actions to move the function from reporting and aggregation of first-line controls to providing expertise and thought partnership. The areas where the function will help execute business strategy include operational strengths and vulnerabilities, new-product design, and infrastructure enhancements, as well as other areas that allow the enterprise to operate effectively and prevent undue large-scale risk issues.

The operational-risk discipline needs to evolve in four areas: 1) the mandate needs to expand to include second-line oversight, to support operational excellence and business-process resiliency; 2) analytics-driven issue detection and real-time risk reporting have to replace manual risk assessments; 3) talent needs to be realigned as digitization progresses and data and analytics are rolled out: banks will need specialists to manage specific risk types such as cyberrisk, fraud, and conduct risk; and 4) human-factor risks will have to be monitored and assessed—including those that relate to misconduct (such as sexual harassment) and to diversity and inclusion.

The evolution includes the shift to real-time detection and action. This will involve the adoption of more agile ways of working, with greater use of cross-disciplinary teams that can respond quickly to arising issues, near misses, and emerging risks or threats to resilience.

New frameworks and tools are therefore needed to properly evaluate the resiliency of

business processes, challenge business management as appropriate, and prioritize

interventions. These frameworks should support the following types of actions:

Map processes, risks, and controls. Map the processes, along with associated risks and controls, including overall complexity, number of handoffs involved, and automation versus reliance on manual activities (particularly when the danger is high for negative customer outcomes or regulatory mistakes). This work will ideally be done in conjunction with systemic controls embedded in the process; end-to-end process ownership minimizes handoffs and maximizes collaboration.

Identify supporting technology. Identify and understand the points where processes rely on technology.

Monitor risks and controls. Create mechanisms and metrics (such as higher-than-normal volumes) to enable the monitoring of risk levels and control effectiveness, in real time wherever possible.

Link resource planning to processes. Link resource planning to the emergent understanding of processes and associated needs. Be ready to scale capacity up or down according to the results of process monitoring.

Reinforce needed behavior. Ensure reinforcement mechanisms for personal conduct, using communications, training, performance management, and incentives.

Enable feedback. Establish feedback mechanisms for flagging potential issues, undertaking root-cause analysis, and updating or revising processes as needed to address the causes.

Establish change management. Establish systematic, ongoing change management to ensure the right talent is in place, test processes and capacity, and provide guidance, particularly for technology.

**Using data and real-time analytics to face operational risk**

Advanced analytics has applications in all, or nearly all, areas of operational risk. It is creating significant improvements in detecting operational risks, revealing risks more quickly, and reducing false positives. Whether in information security, data, compliance, technology and systems, process failure, or even personal security and other human-factor risks, the advanced-analytics advantage is becoming increasingly evident. Some applications are described below:

Anti–money laundering. Replacing rules-driven alerts with machine-learning models can reduce false positives and focus resources on cases that actually require investigation.

Conduct. Analytics engines can identify suspicious sales patterns, connecting the dots across sales, product usage, incentives, and customer complaints (for example, increases in nonactivated deposits, accounts sold by a retail banker, or trades triggered by a wealth-management adviser as they approach compensation breakpoints). Trade-monitoring analytics can mine trading and communication patterns for potential markers of conduct risk.

Cyberrisk. Machine learning can analyze sources of signals, identify emerging threats, replace existing rules-based triggers, and reduce false-positive alerts.

Fraud. Machine learning, including unsupervised techniques, can identify fraudulent transactions and reduce false positives; synthetic-ID-fraud analytics use external, third-party data, in accordance with all local regulation, to analyze the depth and consistency in the identity profiles of new customers.

Process quality and regulatory risks. Automated call surveillance using natural-language processing can monitor adherence to disclosure requirements. Systemic quality-control touchpoints can check the accuracy of decisions, disclosures, and filings against customer-provided information and regulatory rules (for example, the accuracy of a bankruptcy filing against the system of record information).

Third-party risk. Models can be developed that quantify the reliance on key third parties (including hidden fourth-party exposures) to drive better business-continuity planning and bring a risk-based perspective to vendor assessment and selection.

Banks can now tap into large repositories of structured and unstructured data to identify risk issues across operational-risk categories, moving beyond reliance on self-assessments and subjective controls. These emerging detection tools might best be described in two broad categories:

Real-time risk indicators include real-time testing of operational processes and controls and risk metrics that identify areas operating under stress, spikes in transaction volumes, and other determinants of risk levels.

Targeted analytics tools can connect the data dots to detect potential risk issues (see sidebar “Targeted analytics tools”). By mining sales and customer data, banks can detect potentially unauthorized sales. Machine-learning models can detect cyberrisk levels, fraud, and potential money laundering. As long as all privacy measures are respected, institutions can use natural-language processing to analyze calls, emails, surveys, and social-media posts to identify spikes in risk topics raised by customers

in real time.

**Develop talent and the tools to manage specialized risk types**

A range of emerging risks, all of which fall under the operational-risk umbrella, present new challenges for banks. To manage these risks—in areas such as technology, data, and financial crime—banks need specialized knowledge and tools. For example, managing fraud risk requires a deep understanding of fraud typologies, new and emerging vulnerabilities, and the effectiveness of first-line processes and controls. Similarly, oversight of conduct risks requires up-to-date knowledge about how systems can be “gamed” in each business line. In capital markets, for instance, some products are more susceptible than others to nontransparent communication, misselling, misconduct in products, and manipulation by unscrupulous employees. Operational-risk officers will need to rethink their risk organization and recruit talent to support process-centric risk management and advanced analytics. These changes in talent composition are significant and different from what most banks currently have in place (see sidebar “Examples of specialized expertise”).

Manage human-factor risks

Bank employees drive corporate performance but are also a potential source of operational risk. In recent years, conduct issues in sales and instances of LIBOR and foreign-exchange manipulation have elevated the human factor in the nonfinancial-risk universe. In the past, HR was mainly responsible for addressing conduct risk, as part of its oversight role in hiring and investigating conduct issues. As the potential for human-factor risks to inflict serious damage has become more apparent, however, banks are recognizing that this oversight must be included in the operational-risk-management function.

Developing effective risk-oversight frameworks for human-factor risks is not an easy task, as these risks are diverse and differ from many other operational-risk types. Some involve behavioral transgressions among employees; others involve the abuse of insider organizational knowledge and finding ways around static controls. These risks have more to do with culture, personal motives, and incentives, that is, than with operational processes and infrastructure. And they are hard to quantify and prioritize in organizations with many thousands of employees in dozens or even hundreds of functions.

To prioritize areas of oversight and intervention, leading operational-risk executives are taking the following steps. They first determine which groups within the organization present disproportionate human-factor risks, including misconduct, mistakes with heavy regulatory or business consequences, and internal fraud. Analyzing functions within each business unit, operational-risk leaders can then identify those that present the greatest inherent risk exposure. The next step is to prioritize the “failure modes” behind the risks, including malicious intent (traditional conduct risk), inadequate respect for rules, lack of competence or capacity, and the attrition of critical employees.

**continuar leyendo esta pagina mas tarde… https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services**