CHAPTER 1. RISK MANAGEMENT AND OPERATIONAL RISK:

RISK MANAGEMENT (ISO31000)

OPERATIONAL RISK (EBA PERSPECTIVE)

1. **Risk management.**

A general definition is that risk management consists of “coordinated activities to direct and control an organization with regard to risk".[[1]](#footnote-1)

* 1. **ISO31000.**

*ISO31000*is a group of standardsrelated to risk collected from the International Organization for Standardization, provides the principles and guidelines to manage risk that could have a negative impact (on economic performance or reputation) to the organization.

It aims to offer a universal standard for all the interested on the risk management process, replacing the limitless quantity of different existing standards and methodologies among the different industries and geographical area.

ISO31000 was published as a standard on 13 November 2009 and provides a standard on the implementation of risk management. The purpose of ISO 31000:2009 is to be applicable and adaptable for "any public, private or community enterprise, association, group or individual." It began the process for its first revision on May 13, 2015. A draft international standard (DIS), which was open for public comment, was published on February 17, 2017.

An update to ISO 31000 was added in early 2018. The update is different in that "ISO 31000:2018 provides more strategic guidance than ISO 31000:2009 and places more emphasis on both the involvement of senior management and the integration of risk management into the organization."[[[2]](#footnote-2)]](https://en.wikipedia.org/wiki/ISO_31000#cite_note-2)

The international standard for risk management, describes a risk management process that consists of the following elements:

* Communicating and consulting
* Establishing the scope, context, and criteria
* Risk assessment (this includes risk identification, risk analysis and risk evaluation).
* Risk treatment (selecting and implementing options for addressing risk).
* Monitoring and reviewing
* Recording and reporting

In general, the aim of risk management is to assist organizations in “*setting strategy, achieving objectives and making informed decisions*”. The outcomes should be “scientifically sound, cost-effective, integrated actions that treat risks while taking into account social, cultural, ethical, political, and legal considerations”.[[3]](#footnote-3)

**1.1.1 Risk assessment**

Risk assessment is a systematic approach to recognising and characterising risks, and evaluating their significance, to support decisions about how to manage them. [ISO 31000](https://en.wikipedia.org/wiki/ISO_31000" \o "ISO 31000) defines it in terms of its components as “the overall process of risk identification, risk analysis and risk evaluation”.[[4]](#footnote-4)

Risk assessment can be *qualitative, semi-quantitative or quantitative*:

* *Qualitative approaches* are based on qualitative descriptions of risks and rely on judgement to evaluate their significance.
* *Semi-quantitative approaches* use numerical rating scales to group the consequences and probabilities of events into bands such as high, medium, and low. They may use a [risk matrix](https://en.wikipedia.org/wiki/Risk_matrix) to evaluate the significance of combinations of probability and consequence.
* *Quantitative approaches*, including Quantitative risk assessment (QRA) and probabilistic risk assessment (PRA), estimate probabilities and consequences in appropriate units, combine them into risk metrics, and evaluate them using numerical risk criteria.

Risk identification

Risk identification is “the process of finding, recognizing and recording risks”. It “involves the identification of risk sources, events, their causes and their potential consequences.” [[5]](#footnote-5)

It is defined by ISO31000 as the first stage in a risk assessment process. In some cases, as in safety context it could be defined as “hazard identification”.

There are different methodologies to identify risk:

* Checklists or taxonomies based on past data or theoretical models.
* Evidence-based methods, such as literature reviews and analysis of historical data.
* Team-based methods that systematically consider possible deviations from normal operations.
* Empirical methods, such as testing and modelling to identify what might happen under circumstances.
* Techniques encouraging imaginative thinking about possibilities of the future, such as scenario analysis.
* Expert-elicitation methods such as brainstorming, interviews and audits.

Risk analysis

Risk analysis is the process of develop and understand the risk. ISO defines it as “the process to comprehend the nature of risk and to determine the level of risk”. [[6]](#footnote-6)

Risk analysis may include:[]](https://en.wikipedia.org/wiki/Risk#cite_note-ISO31010-41)[[7]](#footnote-7)

* Determining the sources, causes and drivers of risk
* Investigating the effectiveness of existing controls
* Analysing possible consequences and their likelihood
* Understanding interactions and dependencies between risks
* Determining measures of risk
* Verifying and validating results
* Uncertainty and sensitivity analysis

Risk analysis often uses data on the probabilities and consequences of previous events.

In the case of leak on the data or in a context of systems that are not considered operational or there is not experience, various analytical methods may be used to estimate the probabilities and consequences:

* *Proxy or analogue data from other contexts*.
* *Theoretical models*, e.g., Monte Carlo simulation and Quantitative risk assessment software.

Risk evaluation and risk criteria

Risk evaluation involves comparing estimated levels of risk against risk criteria to determine the significance of the risk and make decisions about risk treatment actions. [[8]](#footnote-8)

We can reduce the risk by increasing the controls or other treatment options, but at the same time this will represent an increase of the cost and the inconvenience. It’s difficult to eliminate risk without affecting the activity. That’s why we have the risk criteria, the give the guide decisions on the issues.

Between the types of criteria, we have:

* Risk appetite, define the level of risk that can be accepted by pursuing some objective.
* Criteria that determine whether further controls are needed.
* Criteria that decide between different risk management options.

The simplest framework to face the risk criteria is assign a level to the different risk and dividing them on acceptable risks and risk that need treatment. The tolerability of risk framework, developed by the UK Health and Safety Executive, divides risks into three bands:

* Unacceptable risks: only permitted in exceptional circumstances.
* Tolerable risks: to be kept “As Low as Reasonably Practicable” (ALARP), considering the costs and benefits of further risk reduction.
* Broadly acceptable risks: not normally requiring further reduction.

## **1.1.2 Risk treatment**

Risk Treatment is about selection and implementation options to address the risk.

The process is the following:

* Formulating and selecting risk treatment options.
* Planning and implementing risk treatment.
* Assessing the effectiveness of that treatment.
* Deciding whether the remaining risk is acceptable.
* If not acceptable, taking further treatment.

### Selection of risk treatment options.

### We must balance the potential benefits derived from the achievement of the objectives with the cost and effort of the implementation, to be able to select the most appropriate risk treatment option.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. We can find different options to treat the risk:

* Avoiding the risk by discontinuing or not starting the activity that create the risk.
* Accepting the risk to pursuit the objective.
* Removing the risk source.
* Changing the likelihood.
* Changing the consequences.
* Splitting the risk.
* retaining the risk by informed decision.

Justification for risk treatment is wider than just economic considerations and should consider all the organization’s obligations, voluntary commitments, and stakeholder views. The selection of risk treatment options should be made in coordination with the organization’s objectives, risk criteria and available resources.

In the moment of selecting risk treatment options, the organization must consider the values, perceptions and involvement of stakeholders and the right way to communicate with them. Some risk treatments could be easier to accept than others by the stakeholders.

Risk treatment may not produce the expected results and could create unexpected consequences. To ensure that the different forms of risk treatment remain effective is necessary to have a Monitoring and Review process. If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review.

Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

### Preparing and implementing risk treatment plans.

The aim of the risk treatment plan is to specify how the selected treatment will be apply, so the plan can be explained and monitored. The treatment plan should clarify the order of implementation of the risk treatment. Treatment plans should be integrated into the management plans and processes of the organization, in consultation with appropriate stakeholders.

The information provided in the treatment plan should include: [[9]](#footnote-9)

* the rationale for selection of the treatment options, including the expected benefits to be gained.
* those who are accountable and responsible for approving and implementing the plan.
* the proposed actions.
* the resources required, including contingencies.
* the performance measures.
* the constraints.
* the required reporting and monitoring.
* when actions are expected to be undertaken and completed.

## **1.1.3 Monitoring and review**

The aim of monitoring and review is to ensure and upgrade the quality and efficiency of the process design, application, and results. Monitoring and review should be a planned part of the risk management process.

Monitoring and review should take place in all stages of the process. Monitoring and review include planning, gathering, and analysing information, recording results, and providing feedback. The results of monitoring and review should be incorporated throughout the organization’s performance management, measurement, and reporting activities. [[10]](#footnote-10)

## **1.1.4 Recording and reporting**

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting point to:

* communicate risk management activities and outcomes across the organization.
* provide information for decision-making.
* improve risk management activities.
* assist interaction with stakeholders, including those with responsibility and accountability for risk management activities. [[11]](#footnote-11)

Reporting is a vital part of the organization’s governance and should increase the quality of dialogue with stakeholders and support top management and oversight bodies in meeting their responsibilities.

Features to consider for reporting include:

* Contrary stakeholders and their specific information need and requirements.
* Cost, frequency, and timeliness of reporting.
* Methodology of reporting.
* Relevance of information to organizational objectives and decision-making.

1. **EBA perspective of Operational Risk:**

Operational risk is defined by EBA as “the risk of losses stemming from inadequate or failed internal processes, people, and systems or from external events”. It has been always in Banking and non-banking organizations, but the relevance has been increasing with the complexing and globalization of the financial system. Through the publication of its guidelines and regulatory technical standards on operational risk, the EBA aims at promoting and enhancing the effectiveness of operational risk management and supervision throughout the banking system.

The operational risk resumes the risk and hazards that a company could face during the day-to-day activities. It represents type of business risk, it can result from breakdowns in internal procedures, people, and systems.

These risks are associated with the active decision of the organization functions and priorities. 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.

Since operational risk reflects the human errors, we can summarize it as human risk; that is the risk of business operation failing because human error. It changes from industry to industry, but it’s present on all of them.

**2.1 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. 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 misspelling, 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. [[12]](#footnote-12)

**2.1.1 Intrinsic difficulties faced by the banks and interventions:**

even if the progress of the banks on operational risk is big, its management remains intrinsically difficult. Compared with the financial risks, operational risk is more complex, because of the quantity of diverse risk that we can find on this category. Second reason is that the operational risk requires oversight and transparency off almost all the organizational process and business activities. The individual definitions of the roles of the operational-risk function and other oversight groups have been fluid.

To conclude, operational risk was less easily measured and managed through data and recognized limits than financial risk.

The last limit has been lifted lately, since the most relevant data necessity have been acquired through different process. But the measurement stays a limit since it remains difficult. However, 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.

Whit the operational complexity increase, we can also see an increase of the number and diversity of operational risk types, such as unauthorized trading, third-party risk, fraud, questionable sales practices, misconduct, new-product risk, cyber-risk, and operational resilience.

Digitalization and autonomation are creating a change on the process, by reducing the human intervention and by that the human risk, but at the same time have been creating new change management risk. E.g., fintech partnerships create cyber-risks 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.[[13]](#footnote-13)

To be able to face these challenges, risk managers are looking to develop better instruments, frameworks, and talent. 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.

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:

* the mandate needs to expand to include second-line oversight, to support operational excellence and business-process resiliency.
* analytics-driven issue detection and real-time risk reporting must replace manual risk assessments.
* 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 cyber-risk, fraud, and conduct risk; and.
* 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.[[14]](#footnote-14)

The evolution embraces the change to real-time recognition and action. This will create a more agile way of working, with greater use of cross-disciplinary teams that can respond quickly to appearing issues, near misses, and emerging risks or threats to resilience.

New instruments and frameworks are needed to evaluate the resiliency of the business processes, challenge business management and prioritize interventions. These frameworks should support the following types of actions:[[15]](#footnote-15)

* **Map the processes,** along with associated risks and controls. 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 behaviour.** 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.

Advanced analytics has applications in 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[[16]](#footnote-16):

* Anti–money laundering. Replacing rules-driven alerts with machine-learning models can reduce false positives and focus resources on cases that 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.
* Cyber-risk. Machine learning can analyse sources of signals, identify emerging the eats, 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 analyse 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 cyber-risk levels, fraud, and potential money laundering. As long as all privacy measures are respected, institutions can use natural-language processing to analyse calls, emails, surveys, and social-media posts to identify spikes in risk topics raised by customers in real time.

The emerging risk that are part of the operational risks, present new challenges for the banks. To manage it, the banks will need specialized knowledges and tools. The operational risk officers will need to rethink their operational risk organization and look for new talent to support the risk management and advanced analysis.

The bank’s employees are a potential source of operational risk. Previously, HR was mainly responsible for lecturing conduct risk, as part of its oversight role in hiring and investigating conduct issues. As the potential for human-factor risks inflicting 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 behavioural 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. Analysing 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. [[17]](#footnote-17)

1. Risk Management | British Columbia Midwives Protection Program. (n.d.). Retrieved from www.bcmpp.org website: https://www.bcmpp.org/?q=node/9

   ‌ [↑](#footnote-ref-1)
2. ISO 31000:2009. (2017, November 8). Retrieved from ISO website: https://www.iso.org/standard/43170.html [↑](#footnote-ref-2)
3. ISO. (2018). ISO 31000:2018(en) Risk management — Guidelines. Retrieved from Iso.org website https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

   ‌ [↑](#footnote-ref-3)
4. ISO. (2018). ISO 31000:2018(en) Risk management — Guidelines. Retrieved from Iso.org website https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

   ‌ [↑](#footnote-ref-4)
5. ISO. (2018). ISO 31000:2018(en) Risk management — Guidelines. Retrieved from Iso.org website https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

   ‌ [↑](#footnote-ref-5)
6. ISO. (2018). ISO 31000:2018(en) Risk management — Guidelines. Retrieved from Iso.org website https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en [↑](#footnote-ref-6)
7. IEC 31010:2019. (n.d.). Retrieved from ISO website: https://www.iso.org/standard/72140.html

   ‌ [↑](#footnote-ref-7)
8. IEC 31010:2019. (n.d.). Retrieved from ISO website: https://www.iso.org/standard/72140.html

   ‌ [↑](#footnote-ref-8)
9. IEC 31010:2019. (n.d.). Retrieved from ISO website: https://www.iso.org/standard/72140.html

   ‌ [↑](#footnote-ref-9)
10. IEC 31010:2019. (n.d.). Retrieved from ISO website: https://www.iso.org/standard/72140.html

    ‌ [↑](#footnote-ref-10)
11. IEC 31010:2019. (n.d.). Retrieved from ISO website: https://www.iso.org/standard/72140.html

    ‌ [↑](#footnote-ref-11)
12. The future of operational risk management | McKinsey. Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/riskand-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-12)
13. The future of operational risk management | McKinsey. (n.d.). Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-13)
14. The future of operational risk management | McKinsey. (n.d.). Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-14)
15. The future of operational risk management | McKinsey. (n.d.). Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-15)
16. The future of operational risk management | McKinsey. (n.d.). Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-16)
17. The future of operational risk management | McKinsey. (n.d.). Retrieved from www.mckinsey.com website: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

    ‌ [↑](#footnote-ref-17)