Benefits Of Lean Six Sigma on Bank’s

Operational Risk Management.



University of Rome “La Sapienza”

Facoltà di Economia.

Master’s in Financial Risk and Data Analysis.

Student:

Nagib Stefano Souki

Student ID:

1793926

Thesis Advisor:

Valentina Lagasio

Academic Year 2021/2022.

**INDEX:**

Introduction…………..………………………………..………………………… 5

1. Risk management and Operational risk ……………………………………..6

1.1 ISO31000…………………………………………………………………….… 6

1.1.1 risk assessment……………………………………………………………... 7

1.1.2 risk treatment…………………………………………………………...….. 11

1.1.3 monitoring and review ...…………………………………………………..13

1.1.4 recordong and reportong ………………………………………………….13

1.2 EBA perspective of Operational risk...……………………………………...14

1.2.1 Operatioanl risk in banking ….…………………………………………... 15

* + - 1. Intrinsic difficulties faced by banks and interventions .……………. 15

2. Principles for the sound Management of operational risk and the role of supervisors…....…………..………………………………..…………………….. 22

2.1 role of supervisors ……………...……………………………………………..23

* 1. fundamental principles of operational risk manahement…………………27

3. Lean six sigma………………………………………………………………….. 41

3.1 Lean Management …………………………………………………………….41

3.2 Six Sigma methodology……………………………………………………… 43

3.3 lean six sigma ………………………………………………………………….45

3.3.1 Lean Aix Sigma Belt levels …….…………………………….……………. 46

3.3.2 LSS process ……………………………………………………….………… 47

3.4 Toyota’s study case ……………………………….…………………………. 49

3.5 Royal Bank pf Canada IT&S Luxembourg and Lean Six Sigma…………..………………………………..………………………………….50

Conclusion…………..………………………………..…………………………... 55

Referenxes …………..………………………………..……………………………56

**To my family**

Introduction.

When we talk about risk, we are talking about the possibility that we are exposed to face something unexpected. Risk involves the uncertainty of the effects of an activity in the human values, focusing on negative consequences. Having this basic knowledge we can agree with the international definition of risk, “effect of uncertainty on objectives”

The application of risk and all the process behind it can be applied on a wide range of interest, such as Finance, Business, Environment, Health, etc…

For the purpose of this study, we are going to see the definition and the improvement of a Risk in particular, the “Operational Risk”, that is a kind of risk that can affect all the branch where we can say that the risk exists.

Through the study of Operational Risk we will see one tool that have being studied during years and have been showing important benefits on the management of big companies, this is the Lean Six Sigma methodology, it helps the big corporation to offer their services with the minimum margin of error and reducing all the waste of the process; reducing the possibility of facing human errors that is one of the main problems when we talk about operational risk.

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 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.

**1.2.1 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)

**1.2.1.1 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)

**2. Principles for the Sound Management of Operational Risk and the Role of Supervision**

Sound Practices for the Management and Supervision of Operational Risk (Sound Practices) is a document that was published in February 2003 by the Basel Committee on Banking Supervision (Committee) that articulate a framework of principles for the industry and supervisors. After, in the “2006 International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version” known as “Basel II”, the Committee anticipated that industry sound practice would continue to evolve.

Since then, banks and supervisors have implied their knowledge and experience in implementing operational risk management frameworks (Framework). Loss data collection exercises, quantitative impact studies, and range of practice reviews covering governance, data and modelling issues have also contributed to industry and supervisory knowledge and the emergence of sound industry practice. [[18]](#footnote-18)

Given the changes, the Committee decided that the 2003 Sound Practices paper should be updated to reflect the improved sound operational risk management practices used in the industry. In this document is incorporated the evolution of sound practice and it detail 11 principles covering (1) governance, (2) risk management environment and (3) the role of disclosure. By keeping the paper updated, the Committee upgraded it with specific principles for operational risk management.

A Framework for Internal Control Systems in Banking Organisations (Basel Committee, September 1998) underpins the Committee’s current work in the field of operational risk. The Core Principles for Effective Banking Supervision (Basel Committee, October 2006) and the Core Principles Methodology (Committee, October 2006), both for supervisors, and the principles identified by the Committee in the second pillar (supervisory review process) of Basel II are also important reference tools that banks should consider when designing operational risk policies, processes, and risk management systems. [[19]](#footnote-19) The banks are encouraged by the Supervisors to continue developing more sophisticated tools and practices to face the operational risk.

The Committee believes that the principles mentioned establish sound practices relevant to all banks. The Committee intends that when implementing these principles, a bank will take account of the nature, size, complexity, and risk profile of its activities.

**2.1. Role of Supervisors**

Supervisors conduct, directly or indirectly, regular independent evaluations of a bank’s policies, processes and systems related to operational risk as part of the assessment of the Framework. Supervisors ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at a bank. [[20]](#footnote-20)

Supervisor also pursue to ensure that, if the banks are part of a financial group, the procedures and processes are inline to ensure that the operational risk management is appropriated across the group. To achieve this request the cooperation and exchange of information with other supervisors will be necessary.

If there are deficiencies on the supervisory review, should be faced by a range of actions. Depending on the situation the supervisors will use the most suited tool. To ensure that they are receiving the information from the banks, supervisors may will to stablish a reporting mechanism with the bank and external auditors.

Operational risk can be found in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank’s risk management programme. As a result, sound operational risk management reflects the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems. The Committee desires to promote and improve the effectiveness of operational risk management through the banking system.

Risk management generally covers the process of identifying risks to the bank, measuring exposures to those risks, ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank’s risk exposures and capital positions. Internal controls are typically embedded in a bank’s day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation. In practice, the two notions are in fact closely related and the distinction between both is less important than achieving the objectives of each. [[21]](#footnote-21)

Sound internal governance create the foundation of an effective operational risk management Framework. Though, internal governance issues related to the management of operational risk are likely those met in the management of credit or market risk.

The Committee is seeing sound operational risk governance practices adopted in an increasing number of banks. Common industry practice for sound operational risk governance often relies on three lines of defence

(i) business line management.

(ii) an independent corporate operational risk management function and.

(iii) an independent review. [[22]](#footnote-22)

Depending on the bank’s nature, size and complexity, and the risk profile of a bank’s activities, the degree of formality of how these three lines of defence are implemented will vary.

As discussed in the Committee’s paper Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, June 2011, independent review includes the following components:

1. Verification of the Framework done on a periodic basis and is conducted by the bank's internal or external audit.
2. Verification activities test: the effectiveness of the overall Framework consistent with policies approved by the board of directors, and test validation processes to ensure they are independent and implemented in a manner consistent with established bank policies.
3. Validation: ensures that the quantification systems used by the bank is sufficiently robust and provides assurance of the integrity of inputs, assumptions, processes, and outputs. Specifically, the independent validation process should provide enhanced assurance that the risk measurement methodology results in an operational risk capital charge that credibly reflects the operational risk profile of the bank. In addition to the quantitative aspects of internal validation, the validation of data inputs, methodology and outputs of operational risk models is important to the overall process.

Sound Practices for the Management and Supervision of Operational Risk 3 governance function should be fully integrated into the bank’s overall risk management governance structure.

In the industry practice, the first line of defence is business line management. This means that sound operational risk governance will recognise that business line management is responsible for identifying and managing the risks inherent in the products, activities, processes, and systems for which it is accountable. A functionally independent corporate operational risk function (CORF) is typically the second line of defence, generally complementing the business line’s operational risk management activities. The degree of independence of the CORF will differ among banks. For small banks, independence may be achieved through separation of duties and independent review of processes and functions. In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance, and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting. A key function of the CORF is to challenge the business lines’ inputs to, and outputs from, the bank’s risk management, risk measurement and reporting systems. The CORF should have enough personnel skilled in the management of operational risk to effectively address its many responsibilities. The third line of defence is an independent review and challenge of the bank’s operational risk management controls, processes, and systems. Those performing these reviews must be competent and appropriately trained and not involved in the development, implementation, and operation of the Framework. This review may be done by audit or by staff independent of the process or system under review but may also involve suitably qualified external parties. [[23]](#footnote-23)

It's an important characteristic the use of a strong risk culture and good communication among the 3 lines of defence. Internal audit coverage should be adequate to independently verify that the Framework has been implemented as intended and is functioning effectively.

Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank. Internal audit should not simply be testing for compliance with board approved policies and procedures but should also be evaluating whether the Framework meets organisational needs and supervisory expectations.

Given the evolution of operational risk management and the environment’s continuously changing management should ensure that the Framework’s policies, processes, and systems remain sufficiently robust. Improvements in operational risk management will depend on the degree to which operational risk managers’ concerns are considered and the willingness of senior management to act promptly and appropriately on their warnings. [[24]](#footnote-24)

**2..2 Fundamental principles of operational risk management:** [[25]](#footnote-25)

As introduced in the biggening of this chapter, we will analyse the evolution of sound practice and the 11 principles covering governance, risk management environment and the role of disclosure.

*Principle 1:* “the board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation”.

While higher is the culture of risk management and ethical business practices, the banks are less likely to face damaging operational risk events and are better positioned to deal whit the potentially events that may occur. The actions of the board and senior management, and policies, processes and systems provide the foundation for a sound risk management culture.

The board must create a code of conduct that reflect clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices and prohibited conflicts. It ensures that the bank staff understand the roles and responsibilities and authority to act again risk. Strong and consistent senior management support for risk management and ethical behaviour strongly supports codes of conduct and ethics, compensation strategies, and training programmes.

The compensation policies should be in line to the bank’s statement of risk appetite and tolerance, strategy, and objectives. The proper balance between risk and reward must be found.

Senior management must ensure that a proper level of operational risk training is available at all levels through the organisation. The provided training must be in line with the seniority, role, and responsibilities of the employees.

*Principle 2:* “banks should develop, implement, and maintain a Framework that is fully integrated into the bank’s overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity, and risk profile”.

The main goal of sound risk management is that the board of directors and managers understand the nature and complexity of the risk related in the products, services, and activities.

A fundamental means of understanding the nature and complexity of operational risk is to have the components of the Framework fully integrated into the overall risk management processes of the bank. The Framework should be appropriately integrated into the risk management processes across all levels of the organisation.

Sound Practices for the Management and Supervision of Operational Risk including those at the group and business line levels, as well as into new business initiatives’ products, activities, processes, and systems. In addition, results of the bank’s operational risk assessment should be incorporated into the overall bank business strategy development processes.

The Framework must be well documented in the board of directors, and they should approve policies and include definitions of operational risk and loss. If they don’t the effectiveness of the framework will be harm.

**Framework documentation should clearly**[[26]](#footnote-26)**:**

1. identify the governance structures used to manage operational risk, including reporting lines and accountabilities.
2. describe the risk assessment tools and how they are used.
3. describe the bank’s accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments.
4. describe the bank’s approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure.
5. establish risk reporting and Management Information Systems (MIS).
6. provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives.
7. provide for appropriate independent review and assessment of operational risk.
8. require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs and revised as appropriate.

**Governance:**

*Principle 3:* “The board of directors should establish, approve, and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes, and systems are implemented effectively at all decision levels.”

The board of directors should[[27]](#footnote-27):

1. establish a management culture, and supporting processes, to understand the nature and scope of the operational risk inherent in the bank’s strategies and activities, and develop comprehensive, dynamic oversight and control. An inconsistent taxonomy of operational risk terms may increase the likelihood of failing to identify and categorise risks, or allocate responsibility for the assessment, monitoring, control, and mitigation of risks that are fully integrated into or coordinated with the overall framework for managing all risks across the enterprise.
2. provide senior management with clear guidance and direction regarding the principles underlying the Framework and approve the corresponding policies developed by senior management.
3. regularly review the Framework to ensure that the bank has identified and is managing the operational risk arising from external market changes and other environmental factors, as well as those operational risks associated with new products, activities, processes, or systems, including changes in risk profiles and priorities (e.g., changing business volumes).
4. ensure that the bank’s Framework is subject to effective independent review by audit or other appropriately trained parties; and
5. ensure that as best practice evolves management is availing themselves of these advances.

A critical aspect of the operational risk is the strong internal controls, and it must be stablished by the board of directors with clear lines of management responsibility and accountability. The control environment should provide proper independence of duties between operational risk management functions, business lines and support functions.

*Principle 4:* “The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume”.

While approving and reviewing the risk appetite and tolerance statement, all the relevant risks, bank’s risk aversion, financial situation and strategic direction must be considered. The risk appetite and tolerance statement should summarise the various operational risk appetites within a bank and ensure that they are steady. Then the board of directors must approve suitable limits for specific operational risks, and an overall operational risk appetite and tolerance. It should be regularly reviewed by the board of directors, considering changes in the environment, materials and activity volumes, the quality of the control environment, the effectiveness of risk management or mitigation strategies, loss experience, and the frequency, volume, or nature of limit breaches. The board should supervise management adherence to the risk appetite and tolerance statement and provide for appropriate detection and remedy of breaks.

Principle 5: “Senior management should develop for approval by the board of directors a clear, effective, and robust governance structure with well defined, transparent, and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes, and systems for managing operational risk in all the bank’s material products, activities, processes, and systems consistent with the risk appetite and tolerance”.

Senior manager is the responsible for creating and keeping robust challenge mechanisms and appropriate problems-solving processes; must include reporting systems, track, and analyse issues to ensure the solving. Banks must be able to prove that the three lines of defence methodology is operating adequately and to clarify how the board and senior management ensure that this approach is implemented and operating in an appropriate way.

Senior management must interpret the operational risk management Framework established by the board of directors into specific policies and procedures that can be implemented and verified within the different business units. Senior management should clearly assign authority, responsibility, and reporting relationships to encourage and maintain accountability, and to ensure that the necessary resources are available to manage operational risk in line within the bank’s risk appetite and tolerance statement. Moreover, senior management should ensure that the management oversight process is appropriate for the risks inherent in a business unit’s activity. Senior management should ensure that staff responsible for managing operational risk coordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those in the bank who are responsible for the procurement of external services such as insurance risk transfer and outsourcing arrangements. Failure to do so could result in significant gaps or overlaps in a bank’s overall risk management programme. [[28]](#footnote-28)

Senior management must guarantee that bank activities are led by staff with the required experience, technical capabilities, and access to resources. The responsible staff for monitoring and applying the compliance with the institution’s risk policy must have independence from the units that they supervise.

A bank’s governance structure should be commensurate with the nature, size, complexity, and risk profile of its activities. When designing the operational risk governance structure, a bank should take the following into consideration: [[29]](#footnote-29)

1. Committee structure – Sound industry practice for larger and more complex organisations with a central group function and separate business units is to utilise a board-created enterprise level risk committee for overseeing all risks, to which a management level operational risk committee report. Depending on the nature, size and complexity of the bank, the enterprise level risk committee may receive input from operational risk committees by country,

business or functional area. Smaller and less complex organisations may utilise a flatter organisational structure that oversees operational risk directly within the board’s risk management committee.

1. Committee composition – Sound industry practice is for operational risk committees (or the risk committee in smaller banks) to include a combination of members with expertise in business activities and financial, as well as independent risk management. Committee membership can also include independent non-executive board members, which is a requirement in some jurisdictions.
2. Committee operation – Committee meetings should be held at appropriate frequencies with adequate time and resources to permit productive discussion and decision-making. Records of committee operations should be adequate to permit review and evaluation of committee effectiveness.

**Risk Management Environment:**

*Principle 6:* “Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood”.

The risk identification and evaluation are important characteristics for an effective operational risk management, it considers internal and external factors. The sound risk assessment allows banks to understand its risk profile and position the risk management resources and strategy in a more effective way.

Examples of tools that may be used for identifying and assessing operational risk include: [[30]](#footnote-30)

1. Audit Findings: While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors.
2. Internal Loss Data Collection and Analysis: Internal operational loss data provides meaningful information for assessing a bank’s exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic. Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses to obtain a more complete view of their operational risk exposure.
3. External Data Collection and Analysis: External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank. External loss data can be compared with internal loss data or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures.
4. Risk Assessments: In a risk assessment, often referred to as a Risk Self-Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact. A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls is considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls is considered). Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment.
5. Business Process Mapping: Business process mappings identify the key steps in business processes, activities, and organisational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action.
6. Risk and Performance Indicators: Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank’s risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks. Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss. Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans.
7. Scenario Analysis: is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome. Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions. Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process.
8. Measurement: Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return.
9. Comparative Analysis: Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank’s operational risk profile. Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank’s exposure to potential risk events.

The bank must ensure that the internal pricing and performance measurement mechanisms properly consider the operational risk. If isn’t, risk-taking incentives could not be properly aligned with the risk appetite and tolerance.

Principle 7: “Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk”.

A bank’s operational risk exposure is enlarged when a bank participates in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Besides, the level of risk may intensify when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business critical operations. A bank must ensure that its risk management control infrastructure is suitable at origin and that it keeps pace with the rate of growth of products activities, processes, and systems.

A bank must have policies and procedures that report the process for review and approval of new products, activities, processes, and systems. The review and approval process should consider:

1. inherent risks in the new product, service, or activity.
2. changes to the bank’s operational risk profile and appetite and tolerance, including the risk of existing products or activities.
3. the necessary controls, risk management processes, and risk mitigation strategies.
4. the residual risk.
5. changes to relevant risk thresholds or limits.
6. the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process must also ensure that appropriate investment has been made for human resources and technology infrastructure before new products are introduced. The application of new products, activities, processes, and systems must be checked to identify any differences to the expected operational risk profile, and to manage any risks.

*Principle 8:* “Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk”.

Banks are stimulated to improve the quality of operational risk reporting. A bank must ensure that its reports are comprehensive, accurate, consistent, and actionable across business lines and products. Reports must be adaptable in scope and volume; effective decision-making is obstructed by excessive amounts and scarcity of data.

Reporting must be appropriate, and a bank should be able to produce reports in normal and stressed market conditions. The regularity of reporting should reflect the risks involved and the pace and nature of changes in the operating environment. The outcome of the monitoring must be included in regular management and board reports, as must evaluate the Framework performance done by the risk management functionaries. Reports generated by supervisory authorities should also be reported internally to senior management and the board, where requires.

Operational risk reports may contain internal financial, operational, and compliance indicators, as well as external market or environmental information about events and conditions that are relevant to decision making.

**Operational risk reports should include:**

1. breaks of the bank’s risk appetite and tolerance statement and limits.
2. Details of the recent significant internal operational risk events and losses.
3. relevant external events and any possible impact.

It’s necessary to analyse periodically the data capture and risk reporting processes to continuously enhancing risk management performance and advanced risk management policies, methodologies, and practises.

*Principle 9:* “Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies”.

A sound internal control programme consists of five components that are essential to the risk management process: 1) control environment; 2) risk assessment; 3) control activities; 4) information and communication; 5) monitoring activities.

An effective control environment also requires proper separation of duties. Assignments that create conflicting duties for individuals or a team without double controls may enable cover-up of losses, errors, or other inappropriate actions. Consequently, areas of potential conflicts of interest should be identified, minimised, and be subject to careful monitoring and review.

Effective use and sound implementation of technology can contribute to the control environment. The use of technology related products, activities, processes, and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring, and managing technology risks.

Management must ensure that the technology infrastructure meets the business requirements by providing sufficient capacity for the activity levels in normal and stress situation, ensuring data and system integrity, security, and availability; and supporting integrated.

*Technology infrastructure refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data, and the operating environments.*

Mergers and acquisitions resulting in divided and separated infrastructure, cost-cutting measures or scarce investment can challenge a bank’s ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth. Management must elaborate an appropriate capital’s investment or always provide for a robust infrastructure, before mergers are completed, high growth strategies are started, or new products are added.

*Principle 10:* “Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption”.

Banks are exposed to disrupting events, that may be severe and result in an incompetence to achieve some business obligations. Incidents that harm the bank’s facilities, telecommunication or information technology infrastructures can result in significant financial losses to the bank. A bank must establish business plans in accordance with the nature, size, and complexity of their operations to provide resiliency against the risk. The plans should consider different types of possible scenarios in which the bank may be vulnerable.

Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes. A bank should identify critical business operations, key internal and external dependencies, and appropriate resilience levels.

Possible disrupting circumstances must be evaluated for their financial, operational, and reputational impact, and the result of the risk assessment must be the basis for recovery priorities and objectives. Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, and suppliers.

To ensure that the contingency strategies remain consistent with the current operations, risk and threats, resiliency requirements and recovery priorities, the bank should execute periodically reviews on its continuity plans.

A bank should participate in stress testing with key service providers. The results must be reported to the directives and managers.

**Role of Disclosure**

*Principle 11:* “A bank’s public disclosures should allow stakeholders to assess its approach to operational risk management”.

Internal controls should be designed to provide reasonable assurance that a bank will have efficient and effective operations; safeguard its assets; produce reliable financial reports; and comply with applicable laws and regulations.

A bank’s public disclosure of relevant operational risk management information can lead to transparency and the development of better industry practice through market discipline. The amount and type of disclosure should be commensurate with the size, risk profile and complexity of a bank’s operations, and evolving industry practice. A bank should disclose its operational risk management framework in a manner that will allow stakeholders to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively. [[31]](#footnote-31)

A bank’s disclosures should be consistent with how senior management and the board of directors assess and manage the operational risk of the bank.

A bank should have a formal disclosure policy approved by the board of directors that addresses the bank’s approach for determining what operational risk disclosures it will make and the internal controls over the disclosure process. In addition, banks should implement a process for assessing the appropriateness of their disclosures, including the verification and frequency of them. [[32]](#footnote-32)

**3. LEAN SIX SIGMA:**

In recent years, some practitioners have combined Six Sigma ideas with [lean manufacturing](https://en.wikipedia.org/wiki/Lean_manufacturing) to create a methodology named [Lean Six Sigma](https://en.wikipedia.org/wiki/Lean_Six_Sigma).[[7]](https://en.wikipedia.org/wiki/Six_Sigma#cite_note-WalsheHarvey2010-7) The Lean Six Sigma methodology views lean manufacturing, which addresses process flow and waste issues, and Six Sigma, with its focus on variation and design, as complementary disciplines aimed at promoting "business and operational excellence".[[7]](https://en.wikipedia.org/wiki/Six_Sigma#cite_note-WalsheHarvey2010-7)

**3.1 Lean management:**

Lean management is a way of management for the companies that helps on a process of continuous improvement, it’s a long-term methodology that aims to achieve small and incremental improvements in the process, particularly on the efficiency and quality.

The main objective of Lean Management is to create value for the final costumer through the optimization of the resources and elaborate a stable workflow respecting the costumers’ requirements, it do it eliminating all the wastes and the unnecessary efforts of the process by an identification of each step of the business process and reviewing and eliminating the steps that do not add a value.

It focusses on defining the value from the starting point to the final costumer; limiting the waste; continuously improve of the process.

Lean Management enables a shared leadership and responsibilities. Through the continuous improvement they can ensure that each single employee contributes to the improvement process. Lean Management acts as a guide to build a successful and strong organization that continuous progressing, recognizing the real issues and fixing them.

The roots of Lean Management are in the Toyota production system stablished in the late 40’s. By applying the 5’s principles of Lean Management, Toyota decreased the amount of non-valued processes, being known as the “Toyota Way”.

### 5 principles of lean management:

### The 5 principles of Lean Management that are applied by managers are:

* **Identifying value**: the initial step in Lean Management, it means finding the problem that the costumer is facing and trying to resolve. The offer product must be part of the solution that the costumers need. Any not value-added activity must be removed.
* **Value stream mapping:** in this step, we proceed by doing a map of the company’s workflow, including all people and actions who makes part of the process of creating and delivering the final product to the costumer. It’s a tool for managers to visualize the processes and identifying the people responsible for measuring, evaluating and improvement of the process. This step helps managers to define which parts of the system are not adding value to the workflow.
* **Creating a continuous workflow:** it consists of ensuring that each team’s workflow progress in the most efficient way and avoid any interruptions that may occur with the cross-functional teamwork. Between the techniques we can find the Kanban, it utilizes a visual track to trigger actions, it enables the easiest communication between teams, helping them to identify what needs to be done and when it must be done. The Kanban works by breaking the total process into a smalless sets and visualizing the workflow facilitating a feasible remotion of process interruptions and barriers.
* **Developing a pull system:** this step consists of ensuring that the continuous workflow keep being stable and the teams can deliver the work faster and with less effort; it is a specific technique that reduce the waste of any production process by ensuring that new work is started only if there’s a demand for it, minimizing the overhead and optimizing the storage costs.
* **Facilitating continuous improvement:** represent a variety of techniques that are used to identify what an organization has done, what it needs to do, any possible obstacles that can be found in the process and evaluating how all the members of the organization can improve their process. Since the Lean Management is a cyclical process, the problems could occur in any of the 4 steps. This is the last but most important step of the process.

**3.2 Six Sigma Methodology:**

Six Sigma (**6σ**) is a set of techniques and tools for the process improvement. It was presented by the Bill Smith, an American engineer.

Six Sigma aim to improve manufacturing quality by identifying and removing the causes of defects and reducing the variability in the process. This is done by applying empirical and statistical method and by working with Six Sigma experts. Each Six Sigma project follows a defined methodology and has specific value targets.

International Organization for Standardization (ISO) published in 2011 the first standard definition of Six Sigma “ISO13053:2011. Other standards have been made by universities and companies.

Six Sigma origins are from Statics, from the field of Statistical Quality Control. It refers to the ability of the processes to produce a high proportion of output. The process that operates with “Six Sigma Quality” in a short term are assumed to produce long-term defects levels under the 3.4 defects per 1.000.000 opportunities (DPMO). The 3.4 DPMO is based on a shift of ± 1.5 sigma explained by Mikel Harry.

Specifically, say that there are six [standard deviations](https://en.wikipedia.org/wiki/Standard_deviation)—represented by the [Greek letter](https://en.wikipedia.org/wiki/Greek_alphabet) σ ([sigma](https://en.wikipedia.org/wiki/Sigma))—between the [mean](https://en.wikipedia.org/wiki/Mean)—represented by μ ([mu](https://en.wikipedia.org/wiki/Mu_(letter)))—and the nearest specification limit. As process standard deviation goes up, or the mean of the process moves away from the centre of the tolerance, fewer standard deviations will fit between the mean and the nearest specification limit, decreasing the sigma number, and increasing the likelihood of items outside specification. According to a calculation method employed in process capability studies, this means that practically no items will fail to meet specifications. [[33]](#footnote-33)

Six Sigma emphasises that [[34]](#footnote-34):

* It’s necessary to make continuous efforts to achieve a stable and predictable process results.
* Manufacturing and business processes have characteristics that can be defined, measured, analysed, improved, and controlled.
* Achieving sustained quality improvement requires commitment from the entire organization, particularly from top-level management.

Features that set Six Sigma apart from previous quality-improvement initiatives include [[35]](#footnote-35):

* Focus on achieving measurable and quantifiable financial returns
* Emphasis on management leadership and support
* Commitment to making decisions based on verifiable data and statistical methods rather than assumptions and guesswork

Lean Management and Six sigma shared some methodologies and tools. The difference is on the focus of the approach, Lean Management aims to eliminate waste through tools that aim organizational efficiencies by the integration of a performance improvements system and Six Sigma by eliminating the variation. Both are led by data, but Six Sigma depends on more accurate data.

The main and most evident goal on Six Sigma is to improve the process but not necessarily to 3.4 DPMO level. The organization must select a proper sigma level depending on the importance of the processes.

### Methodologies of Six Sigma:

Six Sigma projects follow two project methodologies, inspired by W. Edwards Deming's Plan–Do–Study–Act Cycle, each with five phases.[[36]](#footnote-36)

* **DMAIC**: is used for projects aimed at improving an existing business process.
* **DMADV**: is used for projects aimed at creating new product or process designs.

**Six Sigma in practice:**

Six Sigma is normally applied on large organizations, according to Thomas Pyzdek and J. Kullmann, Industry consultants, the companies that will find Six Sigma more suitable for it processes are the companies with more than 500 employees, but it also has tools that could fit on smallest organizations. E.g., the difficult to afford a Black Belt specialist (higher level on the Six Sigma pyramid, does not mean that they cannot apply the other tools of Six Sigma.

### In the financial field, Six Sigma has shown an important role by improving the accuracy of the allocation of cash, automatic payments, more accurate reports, and documents, among others.

### On the Bank of America, Six Sigma helped to increase the customer satisfaction by 10.4% and reduce the costumer issues of 24%. Between the big financial companies that have applied Six Sigma on their processes there are American Express, GE Capital and JPMorgan.

**3.3 Lean Six Sigma:**

Lean Six Sigma is a methodology that apply a collaborative team effort to improve the performance by limiting the waste and variation. It’s a combination of Lean Management and Six Sigma to eliminate the wastes, called *Muda*.

Lean Six Sigma uses the DMAIC phases as in Six Sigma. There are 5 phases used on Lean Six Sigma to identify the root of the inefficiencies and work with any process and services that have a big amount of data.

Fujio Cho defined the waste (Muda) as “anything other than the minimum amount of equipment, materials, parts, space, and workers time, which are absolutely essential to add value to the product".

Different types of waste have been defined in the form of a [mnemonic](https://en.wikipedia.org/wiki/Mnemonic) of "downtime":

* **D**efects: is a product that is not able to be used, requires the interventions or to be discarded. This creates a cost to the company on time and money.
* **O**ver-production: excessive quantity of production or in produced at the wrong moment.
* **W**aiting: refers to the delays in the process and there are 2 kinds, waiting for material or weak equipment.
* **N**on-Used Talent: refers to the waste of human resources and skills. The main problem is when the employees does not have the opportunity to give a feedback and assessments to managers to improve the process.
* **T**ransportation: not proper movements of materials, products, people, equipment, and tools. It represents a value-add to the products and processes.
* **I**nventory: represent an excessive quantity of products and materials that are unprocessed. It is a problem since the product may become useless to the costumer, creating a useless cost of storage.
* **M**otion: unnecessary movement of people.
* **E**xtra-processing: is doing more steps than necessaries to finalize the product.

**3.3.1 Lean Six Sigma Belt Levels.**

Lean Six Sigma’s levels of certification are structured in belt colours. Being the highest level the Master Black Belt, after this there are the Black Belt, Green Belt, Yellow Belt, and White Belt. To be part of the different levels, is necessary to success on an exam about Lean Six Sigma and applications.

White Belt: employee understands the meaning and goals of Lean Six Sigma. They know the terms associated with the methodology and report any process problems to colleagues with either Green or Black Belts.

Yellow Belt: an employee understands essential Lean Six Sigma concepts, tools, and techniques. They report process problems to colleagues with either Green or Black Belts.

Green Belt: employee has some expertise in Lean Six Sigma strategy and can launch and manage Lean Six Sigma projects. They focus on the use of tools and the application of DMAIC and Lean principles.

Black Belt: employee with advanced Lean Six Sigma expertise who reports to Master Black Belts. They can be full-time, cross-functional project team leaders, as well as a coach or mentor to Green Belts. They are responsible for putting Lean Six Sigma changes into place.

Master Black Belt: employee with a Master Black Belt has extensive Lean Six Sigma expertise is typically responsible for the Lean Six Sigma initiative. They can act as coach or mentor and monitor projects. They work with company leaders to identify efficiency gaps and training needs. They report to C-Suite executives.

**3.3.2 Lean Six Sigma Process:**

In Lean Six Sigma the process is defined by a DMAIC, that is a data-driven quality strategy that aim to improve the processes. DMAIC stands for Define, Measure, Analyse, Improve, Control. That represent the 5 parts of the process.

**Define**: this step aims to clarify the business problem, goal, resources, scope, and timeline. This phase is normally used on the project chapter creation, that consist of an explanation of the current situation of the process. It aims to clarify, define objectives, and develop the project team. It defines the following:

* Problem
* Costumer, using a SIPOC.
* Voice of the customer (VOC) and Critical to Quality (CTQs)

### Measure: this step represents the measurement of the specification of the problem and goal. Here the data is collected. The performance metric for this phase will be compared to the final metric of the project to analyse if the improvement were achieved. The team decides about what should be measured and how, normally here the teams spend big quantity of time to assess the appropriateness of the proposed measurement system. Good data is the heart of the DMAIC.

### Analyse: the aim of this step is identified, validate, and select the root cause of the elimination. Most of the potential root causes are identified through a root cause analysis (e.g., Fishbone diagram). The roots are choose using a multi-voting consensus for other validations. A data collection plan is created, and data are collected to establish the relative contribution of each root causes to the project metric. This process is repeated until valid root causes can be identified.

### Improve: the aim of this step is to identify, test and apply a solution to the issues, partial or full depending on the situation. To fix or prevent the issues is necessary to identify creative solutions, e.g., apply tools like Six Thinking Hats and Random Word. The aim of the improve step could be also find the solution without implementing it. The idea is to:

* Create
* Focus on simple solutions.
* Test solutions using plan-do-check-act cycle
* Depending on PDCA results, try to anticipate any preventable risks related to the improvement using Failure mode and effects analysis (FMEA)
* Stablish a detailed implementation plan
* Organize improvements

### Control: the aim of this step is to insert the changes and guarantee sustainability, it’s the final step if the DMAIC method. In this step, the following processes are undertaken amend ways of working, quantify and sign-off benefits, track improvement, officially close the project, and gain approval to release resources.[[37]](#footnote-37)

* A control chart can be useful during the Control stage to assess the stability of the improvements over time by serving as a guide to continue monitoring the process and providing a response plan for each of the measures being monitored in case the process becomes unstable.
* Standard operating procedures (SOP's) and Standard work
* Process confirmation
* Development plans
* Transition plans
* Control plan
* Benefit delivery

**3.4 Toyota’s Study Case:**

**Toyota Motor Corporation** is a Japanese multinational automotive manufacturer headquartered in Toyota City, Aichi, Japan. It was founded by Kiichiro Toyoda and incorporated on August 28, 1937. Toyota is one of the largest automobile manufacturers in the world, producing about 10 million vehicles per year.The company was originally founded as a spinoff of Toyota Industries, a machine maker started by Sakichi Toyoda, Kiichiro's father. Both companies are now part of the Toyota Group, one of the largest conglomerates in the world. While still a department of Toyota Industries, the company developed its first product, the Type A engine in 1934 and its first passenger car in 1936, the Toyota AA[[38]](#footnote-38).

**Application of Six-Sigma in Toyota[[39]](#footnote-39):**

Toyota applied the phases of the Six Sigma Methodology to start the project, then improved the processes. The DMAIC was applied in the following way:

**Define:** since the automobile industry was facing numerous changes, Toyota was not able to ensure their leadership’s position on the market for the future. The managers defined the current situation and understood the conflicts and problems.

After the understanding of the problem the company created a project plan including the Costumer to Quality.

**Measure:** Toyota managers found a processed the information available to find new solutions through Value Stream Mapping*,* Data Gathering, Data measurement validation.

**Analyse:** At this stage, the management had reliable information about the problem or areas of potential problem the information was be analysed to get the root cause of the problems. Cause and Effect Analysis, FMAE (Failure modes and effects), Correlation and regression studies and DOE (design of experiments).

**Implement**: the management/implementation team understood the problem at hand, had a well-defined picture of what is going on in an organization, understood departments with inefficiencies and the financial implications of the gaps (Wheelen and Hunger, 1998). The next step is to devise several possible solutions to be implemented. Here staffs should be fully included.

**Control:** Toyota Management at different regional offices developed a control and monitoring team. When controlling there is an already set path, through which processes had to be followed. They had to start from somewhere heading to another area.

**3.5 Royal Bank of Canada IT&S Luxembourg and Lean Six Sigma:**

For more than 120 years, RBC Investor & Treasury Services (RBC I&TS) has provided asset and payment services to corporate investors and financial institutions globally.

Are a financially strong partnertrusted with CAD 4.1 trillion in assets under administration2 with offices in 13 countries.

With clients at the heart of their service offering, safeguard assets and leverage data and technology solutions to: [[40]](#footnote-40)

* Deliver meaningful insights
* Simplify our clients’ operations
* Support their growth

**Application of Lean Six Sigma on RBC IT&S in Luxembourg:**

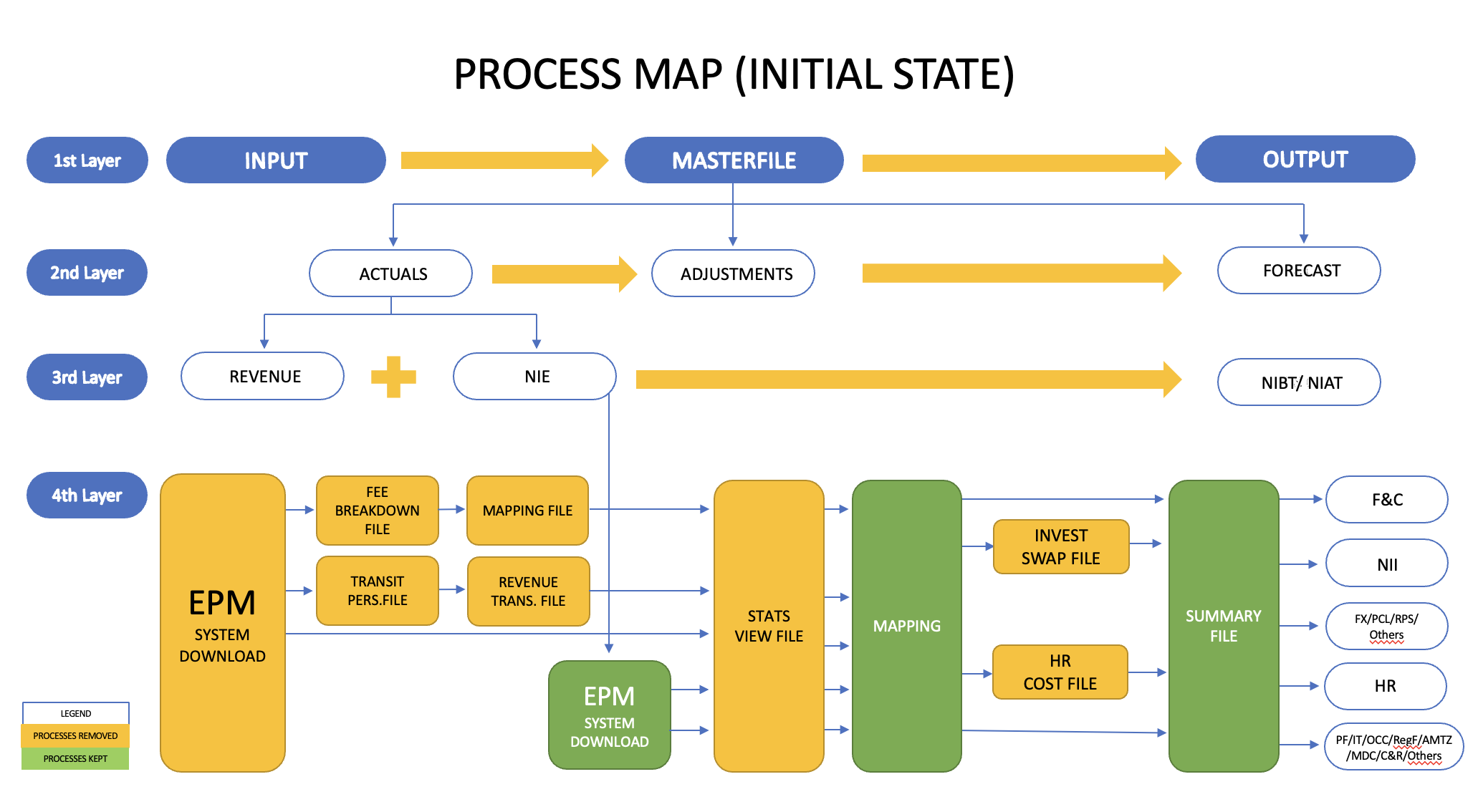
RBC IT&S, after the capacitation of the relevant employees for the project and acquired the certifications and necessary belt, is applying the Lean Six Sigma philosophy to upgrade the processes to achieve a lean organization and reducing all the wastes on the process.

The initial process of RBC IT&S Luxembourg is done by creating a Short-Range-Outlook. Objective of this Short-Range-Outlook report is to produce a P&L view with actual, budget and forecast to our CFO:

* This is an Excel report including several tabs with EPM tool data (Actual Budget, Forecast and Manual adjustments).
* The report is produced twice a month: after month end closing and one week before month end closing.
* Only the forecast figures are supposed to change considering the business input i.e., exceptional events.
* Adjustments are done at the reporting level i.e., not granular and are only available in the document.
* Business partners must be involved in the forecasting process to obtain realistic values.
* The excel report is used to produce a PowerPoint slide.

During it application they identified some issues on the processes that are creating a more exhaustive and expensive workflow. Between the issues we have:

* The SRO report was built incrementally by adding the sponsor’s (Chief Financial Officer, CFO) requirements.
* It is necessary to add comments to be able to monitor the adjustments
* We depend on the business partners collaboration to be able to create a forecast of the SRO figures thar are accurate.



The goal that RBC IT&S Luxembourg wants to achieve through Lean Six Sigma application is to:

* Clean-up the report (clean any data/files/links not used at this level of granularity and reformat/rebuilt).
* Potentially the tracking of the change can be lost when explaining the variances: therefore, create a tracker to discuss the variances (through comments of others).
* Partnership with business stakeholders must continue to be enhanced to get the right support at the right time: explain the objective of the exercise and implement SLA or clear instructions.

These improvements will result on a decrease of the time spent month by month and increase the efficiency, enhance clarity on the figures and provide a bigger accuracy on the results.

The Lean Six Sigma tools that have being applied inside of the bank’s management and analysis is the DMAIC process to stablish the interventions and identify the issues, Fishbone scheme to have a complete view of the process and applying the Kanban strategy to organize the daily task between the team members.

The future process will be achieved by reducing some of the process and interventions necessary to achieve the SRO in the best way possible.

Diagram

Description automatically generated

**How Lean Six Sigma will help RBC IT&S Luxembourg to reduce operational risk:**

On the 2 schemes showed below, we can see the changes in the process of RBC IT&S Luxembourg, there we can find 3 main changes:

* Addition of the phase called “ONE OFF”, that represent an additional analysis on the events that affect the bank having a monetary value of over 1.000.000€.
* The further development of the adjustments, to understand properly the reason of the necessary adjustment from the plan.
* The autonomation, that reduce the intervention of the employees on the process, creating a more autonomous and developed system.

All of the changes have a positive impact when it comes to operational risk management, since they will reduces the possibility of human errors that is the main loss on the operational risk and analyse the other motivations of the losses through the “ONE OFF” analysis and the further development of the adjustments; applying this new process, RBC IT&S Luxembourg will be able to reduce the losses and identify and measure more accurately the issues and will be able to intervening at a good moment before that the losses are of big impact.

**Conclusion.**

Risk management and operational risk are 2 concepts that must be known for all the companies and risk officers. Authorities are doing everything that they can to incentive the companies to evolve their Risk Management process and the understanding of all the possible operational risk roots and effect that can be negative to the company.

As we saw before, there is a big interest from the Authorities to continue avoiding the damage coming from operational risk on the banking system, since the damage could be reflected just in the bank or also could have a systemic impact on the Banking sector, creating a damage for a big amount of clients.

Knowing this, and after seeing all the tools that Lean Six Sigma could bring to the management of the companies and can be used on an Operational Risk Management perspective, I consider that the banks should start to invest on the develop of the employees on this methodology; or in any other methodology that will help them to reduce, in the best way, the Operational Risk damage.

**References.**

*Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from <https://www.bis.org/publ/bcbs195.pdf>

IEC 31010:2019. (n.d.). Retrieved from ISO website: <https://www.iso.org/standard/72140.html>

ISO. (2018a). 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>

ISO. (2018b). 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>

ISO 31000:2009. (2017, November 8). Retrieved from ISO website: <https://www.iso.org/standard/43170.html>

RBC Investor & Treasury Services | Who We Are. (n.d.). Retrieved from www.rbcits.com website: <https://www.rbcits.com/en/who-we-are.page>

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

Six-sigma in Toyota Motor Corporation - 2486 Words | Report Example. (n.d.). Retrieved from Free Essays website: <https://ivypanda.com/essays/six-sigma-in-toyota-motor-corporation-report/>

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>

Wikipedia Contributors. (2019, February 26). Toyota. Retrieved from Wikipedia website: <https://en.wikipedia.org/wiki/Toyota>

Acknowledgements:

I dedicate this research and all my success in the university to my family and friends that were close to me during all this time. Also, to my angels that are always protecting me.

In particular to my mother, grandmother and brother that are the engine of my motivation to start and achieve this goal and continue looking forward in my professional life. Thank you for all your help and support.

Also, to my closest friends for being there each time that I needed help in the university and for personal things.

Andres, Andrea, Alex, Alessio, Pier, Fausto, and Rami. You became my family during these years in Rome. More than friends you are brothers to me.

I’m grateful to Rome because it gave me the pleasure to meet all of you, making me feel a city 8.500km away from my family like my “home” for 5 years. It was possible only because of you, the people that I meet here.

I would like to thanks to my friends from Bucharest, you became part of my family as well during the 6 months that I spent there, arriving without friends to a country that I have never being before, I found support on you and that’s why after almost 2 years we are still close friends. Chiara, Ivana, Manuel, Beppe, Giuseppe, Laneve, Javier, Davide, Concetta, Giulia, Flaminia and all the rest that created an impact on me.

I would also like to thank my friends from Venezuela, even if we were not together these 5 years, you all are part of what I’m today and the person that I will become in a future. Particularly to Stefania, but you are not my friend you are my sister; and Amanda because you have always been there for me and helping me with everything.

In general, I’m grateful to all of you that I meet and supported me the last 5 years that I will remember as the happiest five years of my life. And for sure I will remember all of you each time that I will talk to someone about my years in Italy and Rumania.

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)
18. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-18)
19. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-19)
20. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-20)
21. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-21)
22. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-22)
23. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-23)
24. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-24)
25. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-25)
26. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-26)
27. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-27)
28. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-28)
29. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-29)
30. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-30)
31. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-31)
32. *Basel Committee on Banking Supervision Principles for the Sound Management of Operational Risk*. (2011). Retrieved from https://www.bis.org/publ/bcbs195.pdf

    ‌ [↑](#footnote-ref-32)
33. Tennant, Geoff (2001). [SIX SIGMA: SPC and TQM in Manufacturing and Services](https://books.google.com/books?id=O6276jidG3IC). Gower Publishing, Ltd. p. 25. [↑](#footnote-ref-33)
34. Tennant, Geoff (2001). [SIX SIGMA: SPC and TQM in Manufacturing and Services](https://books.google.com/books?id=O6276jidG3IC). Gower Publishing, Ltd. p. 25. [↑](#footnote-ref-34)
35. Tennant, Geoff (2001). [SIX SIGMA: SPC and TQM in Manufacturing and Services](https://books.google.com/books?id=O6276jidG3IC). Gower Publishing, Ltd. p. 25. [↑](#footnote-ref-35)
36. De Feo, Joseph A.; Barnard, William (2005). JURAN Institute's Six Sigma Breakthrough and Beyond – Quality Performance Breakthrough Methods. Tata McGraw-Hill Publishing Company Limited. [↑](#footnote-ref-36)
37. ["DMAIC | Control Stage - InvisibileConsultant.co.uk"](https://invisibleconsultant.co.uk/dmaic-control-stage/). *InvisibileConsultant.co.uk*.  [↑](#footnote-ref-37)
38. Wikipedia Contributors. (2019, February 26). Toyota. Retrieved from Wikipedia website: https://en.wikipedia.org/wiki/Toyota [↑](#footnote-ref-38)
39. Six-sigma in Toyota Motor Corporation| Retrieved from Free Essays website: https://ivypanda.com/essays/six-sigma-in-toyota-motor-corporation-report/

    ‌ [↑](#footnote-ref-39)
40. RBC Investor & Treasury Services | Who We Are. Retrieved from www.rbcits.com website: https://www.rbcits.com/en/who-we-are.page

    ‌ [↑](#footnote-ref-40)