

Enterprise Risk Management: A Case Study of a Moroccan Financial Institution

L. Benabbou 

Ecole Mohammadia d'Ingénieurs, Industrial Engineering Department,
Mohammed V-Agdal University, Rabat, Morocco.
benabbou@emi.ac.ma

Abstract. *The global business environment is more complex and uncertain than ever. The activities at all levels of an entity consider uncertainties, risks and opportunities. The Enterprise Risk Management (ERM) process enables entities to deal with uncertainty and provides decision makers reasonable assurance to achieve the entity's objectives (strategic, operations, reporting, and compliance). This paper presents an overview of ERM processes, including definitions, standards, evolution and benefits. Furthermore, some important considerations of ERM implementation are highlighted. A portfolio management structure case study is presented, illustrating the discussed ERM process.*

Key words: enterprise risk management, risk, operational risk, business objectives, business process.

1. Introduction

Risk is commonly referred to as uncertainty, loss and sometimes opportunity. There are many definitions of risk, generally linked to objectives [8,11,17,19]. Risk is often considered as an event that affects the achievement of objectives either negatively (risk) or positively (opportunity). Different classifications of risk have been suggested and the four classes usually adopted are: (i) strategic risks, (ii) financial risks, (iii) operations risks and (iv) other risks [19,38]. Strategic risks deal with the long term impact of important decision taking by institution. For example, developing a new product or entering into a new market. Financial risks are relative to financial operations and financial markets like credit risks and/or market risks. Operational risks result from processes, people and systems. Sometimes, operational risks are defined as any risk primarily devoid of market or credit risks. Finally, the fourth

category includes all other risks such as hazard risks (natural disaster), information risks (information access) and legal risks (regulation and taxation).

Financial institutions are primarily concerned with market and credit risks. These quantitative risks are studied and analyzed the most. Many measures exist to their quantification: Value at Risk (VaR), Conditional VaR (CVaR), Volatility, Duration, Convexity, Maximum of Loss and so on [21]. The availability of data, testable mathematical models and traded instruments render market and credit risks more manageable and quantifiable. Taking into account only market and credit risks in financial institution, however, by-passes important issues such as: (i) risks arising from operations and processes, (ii) huge loss from rare events (natural disaster), (iii) activity disruption, system failures and so on [18,19, 21,30].

This paper takes an opposite stance and presents Enterprise Risk Management (ERM) as a process which considers all risk categories at all levels of an entity. The case study presented herein illustrates the benefits of implementing the ERM process at a Moroccan financial institution. Section 2 presents the ERM with definitions, standards, evolution and benefits. Section 3 focuses on the ERM process based on COSO framework. Section 4 illustrates the implementation of ERM in a Moroccan financial institution.

2. Enterprise Risk Management

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published in 2004 the Enterprise Risk Management integrated framework [11]. This framework defines ERM as *“a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”*. This definition highlights three essential characteristics of ERM: (i) it is a governance activity (ii) a monitoring activity and (iii) a strategic one [3].

In fact, ERM combines risk appetite and strategy, and reduces surprising events and associated costs or losses. It considers risks and opportunities, and can increase business value [1,9,31]. It is a comprehensive, management-oriented and integrated approach. The purpose of the ERM process is to identify, assess and monitor any risks and opportunities that could affect the achievement of the company’s objectives. The ERM can also focus on managing all risks that can influence increasing value to shareholders. ERM is sometimes considered as an approach that treats risk holistically within an organization [35] by properly identifying risks and prioritizing appropriate responses [19].

In parallel with COSO, many risk management standards and frameworks studied ERM as depicted in Table 1. The majority are based on: COSO [11], ISO 31000 (2009) [17] and AS/NZ ISO 31000:2009 [8].

Standard or framework	Country	Year
The Group of Thirty Report in the United States [19,41]	US	1990
King Report on Corporate Governance in South Africa [23,32] King I King II King III	South Africa	1992 2002 2009
The Cadbury report in the United Kingdom [12,19,32]	Canada	1992 2000
Toronto Stock Exchange Day Report in Canada [39,19,32]	Canada	1994
CoCo: the Criteria of Control model: Canadian Institute of Chartered Accountants [19,32,38]	Canada	1995
Australian/New Zealand Standard for Risk Management [8] AS/NZ 4360:1995; AS/NZS 4360: 1999; AS/NZ 4360:2004; AS/NZS ISO 31000: 2009	Australia New Zealand	1995 1999 2004 2009
Risk Management Standard: AIRMIC, ALARM, & UK-IRM [6-7]. IRM: Institute of Risk management, AIRMIC: Association of Insurance and Risk Managers ALARM: The National Forum for Risk Management in the Public Sector	UK	2002 2010
FERMA; Federation of European Risk Management Associations Risk Management Standard [32]	EU	2003 2010
CAS ERM Process [5,32] CAS: Casualty Actuarial Society	US	2003
British Standard : [10,32] BS 31100 :2008 BS 31100 :2011	UK	2008 2011
Risk Management Standards [17] ISO 31000:2009 : Principles and Guidelines ISO Guide 73:2009 : Vocabulary ISO/IEC 31010:2009 : Risk assessment techniques	International: 26 national standards organizations	2009

Table 1: ERM standards and frameworks.

The ERM is a result of risk management evolution into an enterprise-wide integrated approach. ERM is not a fad, more and more firms develop their ERM process based on presented standards [19]: Hydro one [37], (Infosys, GE Capital, JPMorgan Chase [34]) and (PepsiCo, Arcelor Mittal [30]). According to [22] nearly half of the insurance companies used an ERM process and had a Chief Risk Officer.

Major factors mostly over the past decade have provided an additional force to ERM. Such factors started with the application of Basel accords (I, II and III) [35]. The increased awareness of concentration and complexity of risks was also incorporated after September 11th. The wave of corporate accounting fraud (Enron, Tyco, WorldCom) between 2001 and 2002 also added new factors. Other contributing factors came from lessons about worst-case scenarios and natural disasters, vis a

vis, Hurricane Katrina. Since 2006, rating agency scrutiny has included ERM system deployment as a factor in its rating methodology (Standard & Poor's and Moody's). Additional legislative and regulatory factors were included after the 2007 financial crisis and significantly impacted the advancement of ERM [19,27,32,35].

Another aspect that raised the management awareness of risks and the need for an integrated approach as ERM is the occurrence of rare events, like H1N1 flu pandemic in 2009 and Fukushima nuclear disaster in 2011. Finally, technology evolution, especially computing power, and the maturity of consumers' requirements on information and forecasts have contributed to ERM evolution [19,27,32,35].

Moreover, ERM has branched out to several disciplines such as accounting, finance, insurance [4,18], management, operations management [13,20], management sciences, mathematics as well as probability and statistics [2,4,35].

3. The ERM Process

The COSO Framework defines a multidimensional ERM process; which applies across the entire organization as depicted in figure 1. The ERM is defined in three dimensions: (i) entity objectives, (ii) entity organizational structure and (iii) ERM process.

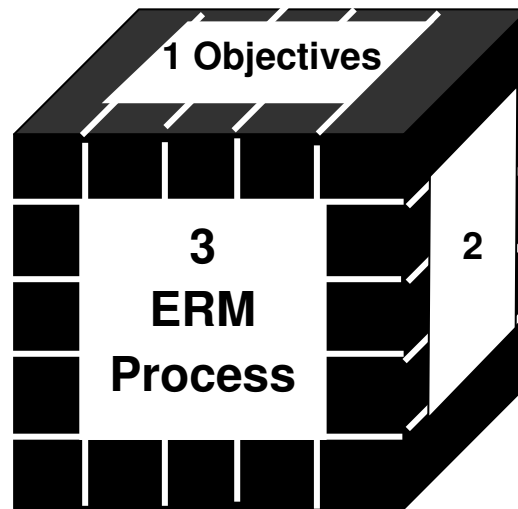


Figure 1: COSO ERM cube (adapted from [11]).

The first dimension-top of the cube-identifies four categories of objectives: Strategic, Operations, Reporting and Compliance. ERM compels organizations to understand and achieve their objectives. Risks are categorized according to affected business objectives. The second dimension -right-hand side of the cube- refers to all hierarchical levels within the organization where ERM has to be considered: Subsidiary, Business unit processes, Division and Entity-level. It reflects the importance of ERM at all organizational levels. The third dimension -the face of the cube- includes the eight interrelated ERM process components: (i) internal environment (ii) objectives setting (iii) events identification (iv) risk assessment (v)

risk response (vi) control activities (vii) information and communication (viii) monitoring.

3.1. Internal environment and objectives setting

The analysis of an internal environment is aimed at understanding the entity's risk culture: integrity, ethical values, risk awareness and management involvement in the ERM process. Having determined the internal environment, the next step consists on setting the objectives. As explained earlier, risks are defined as any event that may influence objectives' achievement. Before identifying risks, managers have to know and understand the organization's objectives and they have to define risk tolerance which measures the acceptable level of variation around these objectives. For example, the product quality index has to be between 4σ and 4.6σ . The risk appetite has to be specified, for example, (i) accept financial markets volatility, (ii) accept reduction of profit margins associated with competition (iii) do not accept the degradation of the organization reputation [11].

3.2. Risk identification

Having defined the internal environment and the objectives, one should identify internal and external risks and opportunities that could impact the achievement of objectives. Risk identification techniques, depicted in Table 2, are either Top-down or bottom-up. The top-down approach adopts a board perspective of risks, and guarantees the senior management continuous involvement and support to the ERM process. On the other hand, the bottom-up approach involves all individuals in the organization.

The best way to identify risks in practice is through carrying face to face discussion with concerned people. ERM is considered to be a "*contact sport*" [3]. The identified risks along with the description of risk causes and effects must be placed in a risk register. Risk identification is a continuous process. Since all risks will not be identified in this step, there needs to be provision for monitoring and reviewing to update the risk register [14, 27].

3.3. Risk assessment

Each identified risk has to be assessed taking into consideration the likelihood of occurrence and impact on the achievement of the organization's objectives over time horizon. The gross, net and residual risks are assessed in terms of likelihood and impact [11]. Quantitative and qualitative approaches are combined to assess risks. The Likelihood and impact may be quantified according to different measurement scales. In measurement theory, there are four types of scales: nominal, ordinal, ratio and interval. They are all based on three characteristics: order, distance and origin [5].

Internal interviewing and discussion	External sources	Tools, diagnostics and processes
<ul style="list-style-type: none"> • Interviews • Questionnaires • Brainstorming • Self-assessment and other facilitated workshops • SWOT analysis • Historic of risks • Audit and inspection reports 	<ul style="list-style-type: none"> • Comparison with other organizations • Discussion with peers • Benchmarking • Risk consultants 	<ul style="list-style-type: none"> • Checklists • Flowcharts • Scenario analysis • Value chain analysis • Business process analysis • Systems engineering • Process mapping

Table 2: Risk identification techniques (adapted from [40]).

A nominal scale is the lowest level of measurement; it does not involve any kind of ranking. The measurement is based on assigning symbols or names to events. Ordinal scale refers to the presence of order without origin or distance. The choice of the order's degree depends on a number of subjective considerations [13]. Order and distance are known in interval scale with numerically equal distances. When order, distance and origin (true zero) are known, then a ratio scale is defined. It allows to conclude for example that if the impact level "four" is assigned to event "1" and the impact level "eight" to event "2", event "2" has twice the potential impact of the first [11]. Examples of scales and characterization are given in table 3 adapted from [5].

Scale	Admissible transformation	Examples
Nominal	Any bijective function	Etiquette, color
Ordinal	$x > y \Leftrightarrow \phi(x) > \phi(y)$	Preferences: high, medium or low
Interval	$\phi(x) = \alpha x + \beta$	Temperature, intelligence
Ratio	$\phi(x) = \alpha x$	Mass

Table 3: Characterization of measurement scales.

In the COSO framework, nominal and ordinal scales are considered as qualitative techniques. On the other hand, interval and ratio scales are considered quantitative. For more consistency, likelihood and impact scales are identical throughout the organization. Qualitative techniques, especially with ordinal scale, are largely used in practice. This makes risk prioritizing possible, based on the knowledge and judgment of the risk owners [11,17,24]. Generally, five levels are used to measure likelihood and impact as shown in figure 2.

Quantitative techniques are usually used to assess financial risks. However, with a large history of events, we can quantify the likelihood and impact of operational risks using interval or ratio scales. COSO classifies quantitative techniques in to three categories [11]: (i) probabilistic (Value at Risk, Cash Flow at Risk, Earnings at Risk, assessment of loss events and back-testing), (ii) non-probabilistic (Sensitivity Analysis, Scenario Analysis, and Stress Testing), (iii) benchmarking techniques.

(Reader interested in detailed risk quantification can refer to the work of [2], [13] and [21].)

Catastrophic	5					Critical Risk
Major	4			High Risk		
Moderate	3		Medium Risk			
Minor	2					
Insignificant	1	Low Risk				
		1	2	3	4	5
		Rare	Unlikely	Possible	Likely	Almost Certain

Figure 2: Likelihood and Impact ordinal scales.

Some other well-established methods such as HAZOP (HAZard Analysis and OPerability study) [36]; FMECA (Failure Modes, Effects, and Criticality Analysis) [26]; (FTA) Fault Tree Analysis [42]; Sigma process, especially by using DMAIC (Define, Measure, Analyze, Improve, and Control) [16] can be used to identify, asses and treat risks.

Risk maps are commonly used to portray an organization's risk assessment. These maps are clear, concise and constructive. They can summarize the qualitative measurement of risks in one visual representation [40]. It is more prudent to use risk maps than multiplying the likelihood and the impact (likelihood x impact) [29]. Using the multiplication (likelihood x impact) is erroneous and sometimes dangerous because it can lead to wrong decisions making [13]. Figure 2 shows a traditional risk map that highlights four risk exposure regions: Critical, High, Medium and low.

3.4. Risk responses

Once risks are assessed, the next stage involves selecting risk responses: avoidance, reduction, transfer and acceptance. The selected treatments have to bring net risks to tolerable levels. Definitions and examples of response strategies are presented in figure 3.

3.5. Control activities

Generally, control activities are aligned with every risk response: avoidance, reduction, transfer and acceptance. Control activities guarantee that risk responses are carried out properly and in a timely manner. They can also be considered as risk responses, to reduce the likelihood and/or impact of risks. Routine maintenance, for example, can be considered as a control activity and risk response [11].

Risk Avoidance

Discontinue activity that causes certain risks when the returns are not attractive in comparison to the risks faced, example:

- Disposing of a business unit, product line or geographical segment

Risk Reduction

Preventive measures reduce the likelihood of risks and corrective measures reduce the impact of risks, examples:

- Establishing operational limits
- Establishing control activities

Risk Transfer

Transfer risks to a third party, examples:

- Insurance mechanisms
- Hedging risks through capital market Instruments
- Outsourcing business processes

Risk Acceptance

Accept risks with attractive potential returns and contingency planning is not necessary, example:

- Accepting risks that conform to risk tolerances

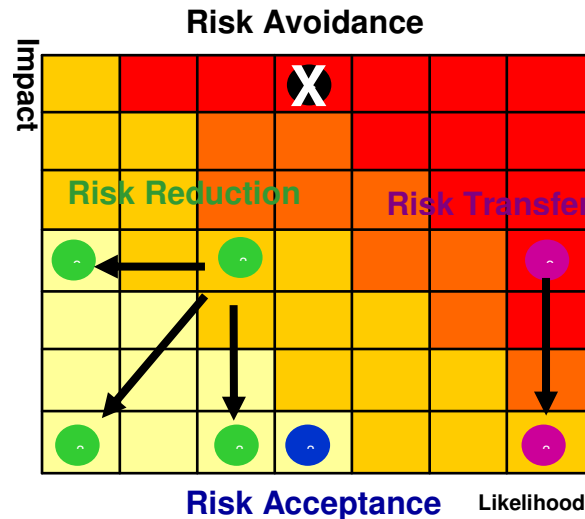


Figure 3: Risk response strategies.

3.6. Information and Communication

The goal of this step is to ensure the availability of relevant risk information for decision-making at all respective management levels. Important risk information are gathered and communicated in the right format at the appropriate time. This enables the right personnel to carry out their responsibilities. The acquisition and design of information systems can be critical and helpful in implementing the ERM process and consequently, achieving the organization's objectives [40].

3.7. Monitoring

Monitoring is a continuous activity. It is accomplished through various management activities, separate evaluations, or both. Monitoring tracks implementation of risk responses and enables the timely notification of fundamental changes to the risks or their response plans.

In this step, the ERM process has to be evaluated using the appropriate techniques: checklists, questionnaires, and flowcharting techniques. The evaluation process is a four steps process: planning, performance, reporting and corrective actions. The ERM documentation is updated, or created, for better ERM comprehension. ERM deficiencies should be reported, as soon as they are detected, to ensure that necessary decisions are made.

To facilitate proactive management of response measures, Key Risk Indicators (KRI) are widely used. KRIs indicate levels or trends of risks [33]. KRIs measure the achievement level of the objectives and makes it possible to detect changes at the right time. There is no standard KRI, it depends on the nature of the organization. However, many propositions of KRI were put forward for each organization function (Audit, human resources, information technology, finance, legal/ compliance, and risk management) with different levels of granularity [33].

Other techniques can be used for monitoring. The conventional Balanced Score Card (BSC) can be integrated with ERM to manage and monitor risks related to the objectives in each of the four perspectives: (i) customer (ii) internal processes (iii) innovation and learning, and (iii) financial [40].

4. Case study: Implementation of Enterprise Risk Management within a Moroccan Financial Institution

The purpose of this study is to illustrate the successful implementation of the ERM process at a Moroccan financial institution, which will be referred to "FInst" for confidential reasons. Initially, the idea of an ERM project being implemented in the Portfolio Management Department (PMD) as a pilot project was accepted by the FInst board.

Three factors were presented to explain the PMD's choice: (i) the PMD is one of the most vulnerable FInst department and faces too many types of risks (market risks, credit risks, liquidity risks, operational risks, strategic risks) (ii) the people awareness of risk management is more important than other FInst departments, they manage different classes of risky assets (iii) the technical backgrounds and qualifications of people-more than 70% are engineers or have masters degree-will facilitate the implementation of ERM process and will show if ERM can be setup throughout the FInst units. The failure of ERM implementation in PMD will highlight challenges and difficulties in implementing similar projects. Many risk workshops were organized for all project stakeholders to prepare the internal environment for ERM implementation and to guarantee their enthusiasm.

The ERM project was launched, beginning with the establishment of project goals and the creation of a project team. The project team was composed entirely of internal resources: the chief of PMD (part-time), the risk manager (the project chief, full-time), a Fixed Income Securities manager (part-time), an Equities manager (part-time) and the internal controller of the middle office (part-time). Generally, it's more beneficial to implement ERM with internal resources in order to guarantee comprehension of the internal environment and knowledge transfer [37].

A kickoff meeting, lead by the risk manager, had been organized to explain to all project stakeholders the ERM process objectives, steps and guidelines to achieving the objectives of the organization, to manage risks and to deal with uncertainty. This meeting also highlighted the determining factors for the project's success or failure and a project scheduling of six months. This section analyzes the different stages of FInst ERM implementation process (Figure 4). Various tools and techniques for risk identification are described. Risk assessment and monitoring are also discussed.

4.1 Objectives and internal environment

As explained earlier, PMD considers risks in every activity, from the asset allocation strategy and execution to its daily operations. PMD supports ethical values, transparency and integrity by respecting the code of conduct, values and mission of the FInst. This mission has been outlined based on strategic, financial and operational objectives. Even though the FInst objectives had been established, those objectives were not clearly understood by all PMD employees. The ERM Project was an opportunity for discussing and helping to clarify strategic objectives. The risk tolerance and appetite were identified for financial and strategic objectives. For example, the PMD has to respect the asset allocation fixed by Strategic Allocation Committee. PMD accepts and deals with the volatility of financial markets (stock market, Interest rate). The financial risk tolerance is measured primarily in terms of volatility, duration, tracking error and performance with regards to the benchmark.

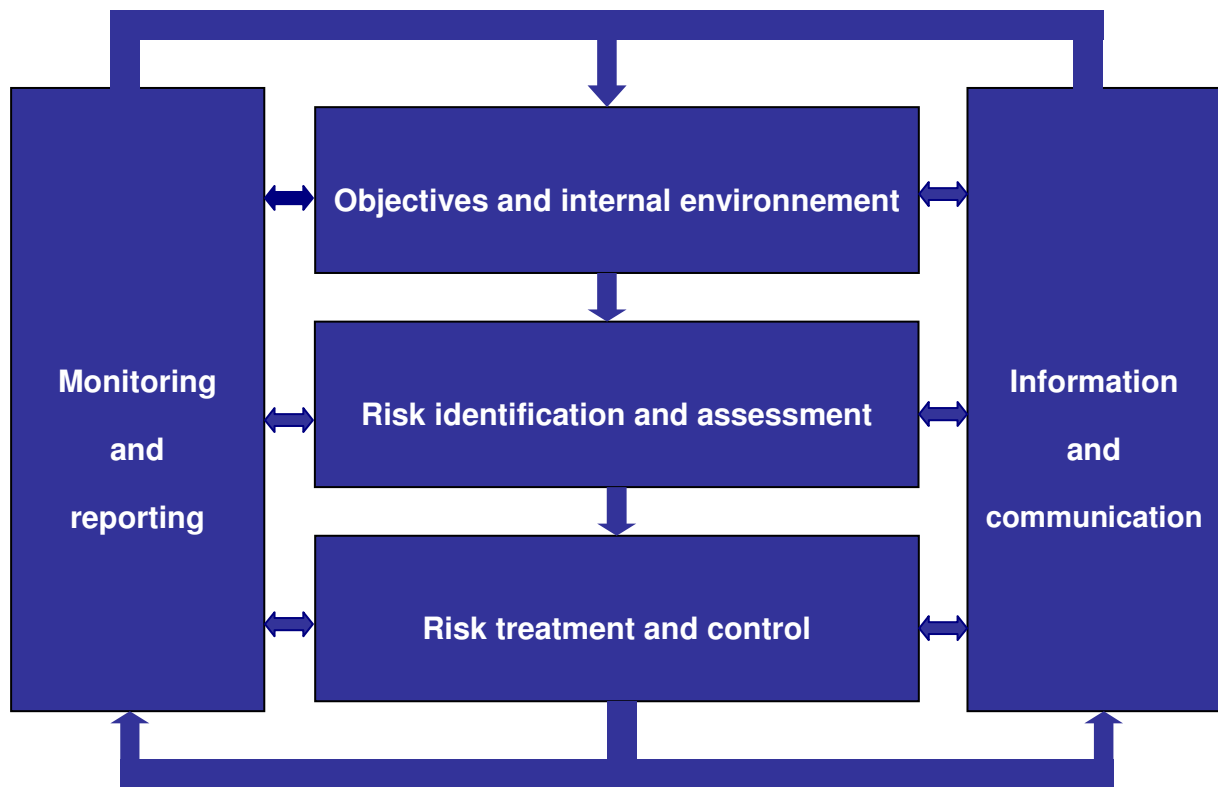


Figure 4: PMD ERM process.

4.2 Risk identification and assessment

For more efficiency, the risk identification and assessment, in terms of impact and likelihood, had been executed at the same time. At first, a brainstorming workshop was organized but only a few operational risks were identified. The ERM project team proposed a questionnaire but generally, asset managers didn't have the time to give their feedback. As explained in section 3, the most efficient strategy in identifying risks is sharing ideas with people.

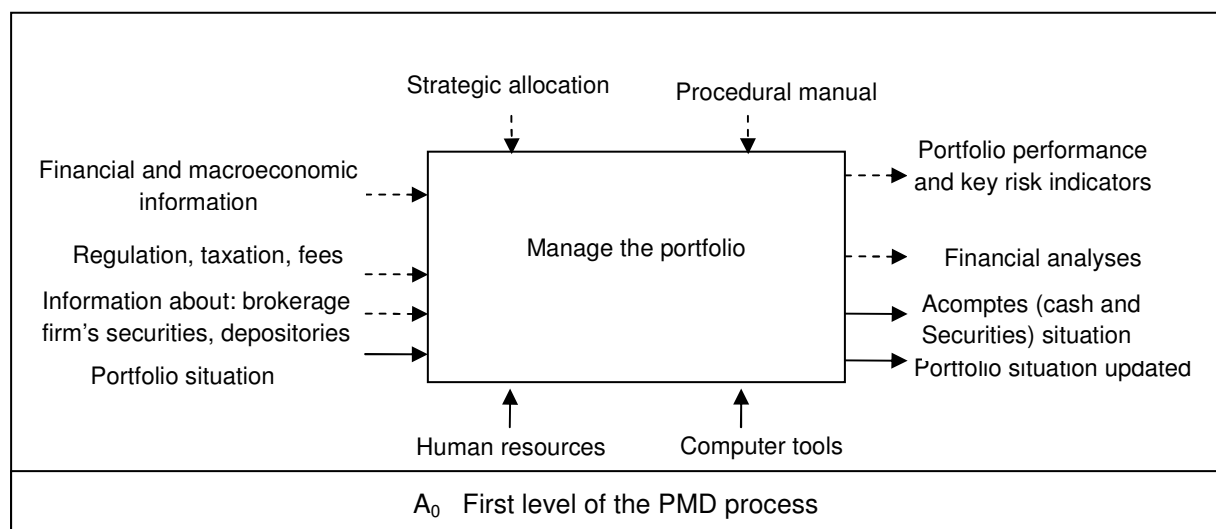


Figure 5: Representation of the first level of the PMD process.

Many risks may be due to operational events which can be identified by building PMD functional diagrams. Diagrams can be used to represent PMD with hierarchical perspectives and describe the PMD functions. A combination of Structured Analysis and Data Techniques (SADT) and other techniques (BPMN, SIPOC, WMS) was used to give a visual representation of the PMD process with all the activities involved and the interactions between them. Figure 5 shows the first level of the PMD functional diagram: function, inputs, outputs, mechanisms (resources) and constraints.

Once all PMD functions and interactions between them have been represented, each function's gross risks were identified through interviews with each risk owner. Those interviews were an opportunity to describe causes, effects, existing means to manage risks and assessment of net risks. Given that we did not have enough historical data for operational and strategic risks, we used a qualitative approach to assess their impact on PMD objectives. For practical reasons, the project team established an Ordinal Measurement Scale. As explained earlier, five levels are generally used, but two intermediary levels were necessary for accrued representation of risks. Table 4 illustrates seven levels of the likelihood and impact of risks according to their effects on PMD objectives.

Level	Kelihood	Level	Impact
7	Once a week	7 : Fatal	Events call into question the achievement of several or all key institution objectives
6	Once a fortnight	6 : Major	Events call into question the achievement of several or all key departmental objectives but without affecting all institution objectives
5	Once a month	5 : Critical	Events call into question the achievement more than one department objectives but without affecting all institution objectives
4	Once a quarter	4 : High	Events call into question one departmental objective or the performance of a service in the department
3	Once a year	3 : Moderate	Events partially call into question service process or performance
2	Between 1 and 5	2 : LOW	Near neutral events across the service
1	> 5 years	1 : Insignifiant	Near neutral events across desks of the service

Table 4: Likelihood and impact measurement scales.

To measure impact of risks on PMD objectives, a participative approach was used in a focus group. A weight was allocated to each participant; with risk owner getting more. Each participant completed an electronic voting sheet, and a weighted sum was calculated to measure an aggregate risk impact. The ERM project team identified around fifty risks. For confidential reasons, only a sample of the identified risks is presented in Table 5. As expected, more than 50% of the overall risks identified were operational risks, and most of them were associated with the non application or misunderstanding of existing controls. Identified and assessed risks were documented in a risk register.

Ref	Risk	Category	Effects	Causes	Means to treat risks	Impact	Likelihood
1	Inappropriate Timing	Operational	Loss of investment opportunity	Delay in decision making or in taking to account an information	Facilitating communication and rapid decision making when faced with important market information in the specified interval risk tolerance.	3	4
2	Inappropriate reaction to rumors	Operational	Underestimate or overestimate an investment opportunity	Unreliable sources information and using incorrect information	Authenticate information and their sources before making a trading decision Create a watch unit for collecting and communicating relevant information	3	4
3	The lack of information or the overflow of information	Operational	Asset managers concurrently execute the same transaction at different price ranges	Lack of coordination between asset managers and information is not communicated instantly to all asset managers	Centralize all data in a single database and instantly share the portfolio situation with all asset managers within the same interface	3	2
4	Cash does not cover a transaction	Operational	Overdue in payment of transactions	Operation missed, portfolio and cash situations are not updated	Apply procedures and plan cash flow	3	2
5	Exceed accepted tolerance risks	Operational	Exceed regulatory or strategic thresholds	Incorrect or missing data Files are not updated	Apply procedures and centralize all data in a single database	5	2
37	Non compliance with legal and regulatory requirements	Strategic / operational	Sanctions	Absence of control and non application of procedures	Implementation of an integrated portfolio management software with automatic control system	7	1
38	Computer system Failures	Strategic / operational	Momentary suspension of operation Loss of data Loss of investment opportunity	Absence of backup and recovery systems	Implementation of portfolio management software	7	5
39	Inability to respond appropriately to market uncertainty	Strategic / operational	Loss of investment opportunity Loss of portfolio performance	Lack of training or information	Organize training and frequent meetings to explain market uncertainty Create a watch unit for collecting and communicating relevant information	6	6
40	Inadequate Business Activity Plan (BPA)	Strategic / operational	Interruption of activity in the case of a disaster	BPA not updated	Keep in line with BPA update frequency	7	1

Table 5: Examples of PMD risks.

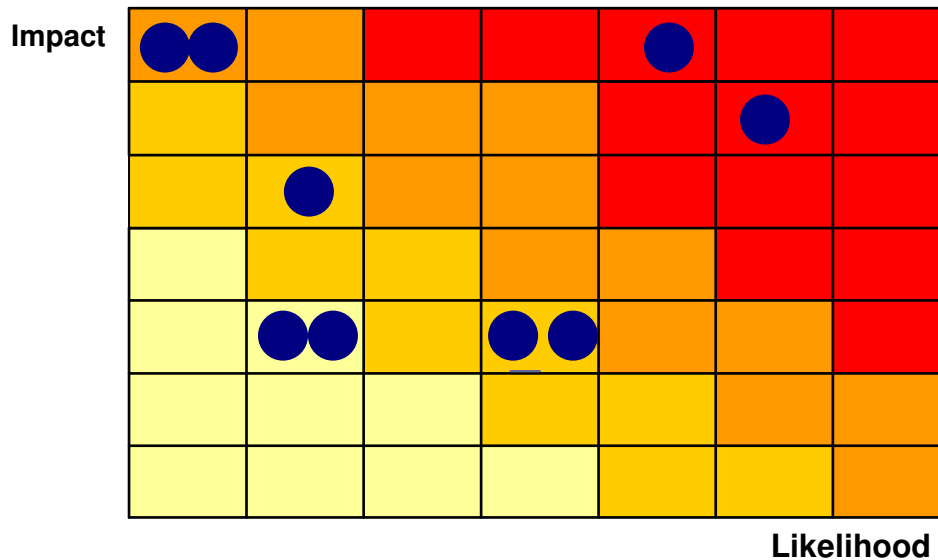


Figure 6: PMD risk map.

Once net risks had been assessed, the following step consisted of producing a risk map for global representation of risks and to track their evolution. Figure 6 illustrates a representation of risks. Depending on the likelihood and impact of respective risks, four risk exposure levels were determined: Critical, high, medium and low. The treatment and monitoring requirements depend on risk exposure levels.

4.3 Risk treatment and control

Risk map classifies net risks as critical, high, medium and low. Depending on the exposure of each risk, a treatment strategy is chosen: accept, transfer, avoid and reduce. For each risk, the risk owner decides the appropriate strategy. In view of the fact that the potential returns of some financial risks are attractive in comparison to the risks faced, some PMD financial risks were accepted, and risk owners (asset managers) had to manage their risks under the appropriate risk tolerance which. These are fixed by Flnt board and Allocation Strategic Committee.

Reducing strategies were undertaken in two different ways. First, preventive measures reduce the likelihood of risks. For example, to reduce the critical and certain risk of the failure of computer systems (risk 38: likelihood=5, Impact=7); Flnt decided to have a Portfolio Management Software. Second, corrective measures reduce the negative impact of risks. For example, to reduce the fatal and rare risk of inadequate Business Activity Plan (BPA) (risk 40: likelihood=1, Impact=7), PMD decided to review PCA annually to reduce the PMD inactivity time in case of a catastrophic event. The control process was also reviewed and new procedures were established to reduce the likelihood of PMD operational risks.

The response strategy of transfer was also recommended for reducing some asset management risks. The FInst board decided to externalize the management of investment funds, to challenge internal asset managers and to reduce financial risks.

4.5 Risk monitoring and reporting

ERM is a continuous process, risks are not statics and they have to be monitored. For example, the transfer of funds to external managers may decrease the exposure of financial risks, but it will create other types of risks. FInst created a risk management service that tracks the implementation of treatment strategies and continually monitor identified risks and any changes in risk exposure. This new service also carries out trend analyses to measure the risk assessment changes; KRIs were used for financial risks. Finally, the risk register was updated, and a risk dashboard was setup to report the results and the performance of ERM in all PMD structure and the FInst Board.

4.6 Information and communication

In each step of the ERM process, relevant information is produced in terms of risk identification, assessment, treatment and monitoring. The aim of the information and communication step is to ensure the availability of relevant risk information for decision-making. Significant internal and external information used in managing risks, have to be communicated also to each ERM process step. The implementation of Portfolio Management Software will support the transmission of relevant information.

5. Conclusion

Creating value for shareholders is always associated with uncertainty and risk. Financial institutions traditionally manage their financial risks. However, many operations and rare events can be more damaging than classical market and credit risks. This paper presents ERM as an integrated approach which manages risks and opportunities that affect all organizational objectives. ERM definitions, standards and evolution have been discussed. An ERM process based on COSO framework was presented. To illustrate the importance of ERM implementation in a financial institution, a Moroccan case study was presented. This case study highlights some considerations for implementing ERM in a financial institution. It illustrates how the ERM implementation process contributes in increasing operational risk awareness and understanding strategic objectives from the board to individual employees. Many strategic decisions were made: (i) implementing a Portfolio Management Software, to reduce the likelihood and impact of computer system risks (ii) allocating resources to the new control and risk management service to monitor and review the ERM process (iii) reviewing the current control process and procedural manual to reduce the likelihood of strategic, financial and operational risks (iv) externalizing the management of funds to transfer and share some financial risks (v) updating BPA to reduce the inactivity time in case of catastrophic events. The ERM implementation in PMD

was a success. At this time of time, Flnst is generalizing the ERM implementation in all departments.

Acknowledgements

I am grateful to ERM project team, especially to the Chief of PDM, and to Y.K. Hamidi and A. Berrado for their comments.

References

- [1] A. Brodeur, G. Pritsch. Making Risk Management a Value-Adding Function in the Boardroom. Mckinsey Working Papers on Risk, 2008.
- [2] A. J. McNeil, R. Frey, P. Embrechts. Quantitative Risk Management Concepts, Techniques and Tools. Princeton University Press, 2005.
- [3] A. Mikes, R.S. Kaplan. Managing Risks: Towards a Contingency Theory of Enterprise Risk Management. Working Paper 13-063, Harvard Business School, 2013.
- [4] A. N. Hitchcox, P. J. M. Klumpes, K. W. Mcgaughey, A. D. Smith, AND N. H. Taverner. ERM For Insurance Companies Adding The Investor's Point Of View. Institute of Actuaries and Faculty of Actuaries, 2010.
- [5] A. Rebaï, J. M. Martel. Que Doit-On Attendre D'une Procedure D'agregation Multicritère Pour Des Evaluations Non Cardinales Ou Mixtes? Working Paper 10-1998, Université Laval, 1998.
- [6] AIRMIC, ALARM, & UK-IRM. A Risk Management Standard. London, UK: AIRMIC, ALARM and UK-IRM. 2002.
- [7] AIRMIC, ALARM, & UK-IRM. A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000. London, UK: AIRMIC, ALARM and UK-IRM. 2010.
- [8] Australian/New Zealand Standard. AS/NZS ISO 31000:2009, Risk management Principles and guidelines. Sydney/Wellington: Standards Australia/Standards New Zealand. 2009.
- [9] B. W. Nocco, R. M. Stulz. Enterprise Risk Management: Theory and Practice. Journal of Applied Corporate Finance, Volume 18, Issue 4, (2006), 8–20.
- [10] British Standard. BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000. British Standards Institution. 2011.
- [11] Committee of Sponsoring Organizations of the Treadway Commission (COSO). Enterprise risk management framework. New York, NY: American Institute of Certified Public Accountants. 2004.
- [12] Committee on the Financial Aspects of Corporate Governance. The Financial Aspects of Corporate Governance, (Cadbury Report), London: Gee and Co. Ltd., 1992.
- [13] D. Wu, D. L. Olson. Enterprise risk management: coping with model risk in a large bank. Journal of the Operational Research Society (2010) 61, 179–190.

- [14] E. O'Donnell. Enterprise risk management: A systems-thinking framework for the event identification phase. *International Journal of Accounting Information Systems*, Volume 6, Issue 3, (2005), 177–195
- [15] Enterprise Risk Management Committee. *Overview of Enterprise Risk Management*. Casualty Actuarial Society, Arlington, VA, USA, 2003.
- [16] F. W. Breyfogle. *Implementing Six Sigma: Smarter Solutions Using Statistical Methods*. John Wiley & Sons. 2003.
- [17] International Standards Organization (ISO). *ISO 31000:2009, Risk Management Principles and Guidelines*. Geneva: International Standards Organization. 2009.
- [18] J. Cummins, C. Lewis, R. Wei. The Market Impact of Operational Risk Events for U.S. Banks and Insurers. *Journal of Banking and Finance*, 30(10), (2006): 2605-2634.
- [19] J. Fraser, B. J. Simkins. *Enterprise Risk Management*. Wiley & Sons, Inc. 2010.
- [20] J. Hallikasa, I. Karvonenb, U. Pulkkinenb, V.M. Virolainenc, M. Tuominena. Risk management processes in supplier networks. *International Journal of Production Economics*. Volume 90, Issue 1, 8 (2004), 47–58
- [21] J. Hull. *Risk Management and Financial Institution*. Upper Saddle River, NJ, Pearson Education, 2007.
- [22] J. Miccolis. *ERM lessons across industries*, Tillinghast-Towers Perrin report. 2003.
- [23] King III. *Code of and Report on Governance Principles for South Africa (King III)*. Parklands : Institute Of Directors In Southern Africa. 2009.
- [24] KPMG. *Managing Operational Risk Beyond Basel II*. KPMG Germany. 2007.
- [25] L. Condamin, J. P. Louisot, P. Naïm. *Risk Quantification Management, Diagnosis and Hedging*. Wiley Finance, Jhon wiley & sons, 2006.
- [26] M. Rausand, A. Hoyland, *System Reliability Theory; Models, Statistical Methods and Applications*, Wiley: New York, 2004.
- [27] M. S. Beasley, M. L. Frigo. ERM and Its Role in Strategic Planning and Strategy Execution. *Enterprise Risk Management*. Chap 3, (2010), 31-50.
- [28] M. S. Beasley, M. L. Frigo, *ERM Frameworks*. *Enterprise Risk Management*. Chap 7, (2010), 97-124.
- [29] P. Mestchian, M. Makarov, B. Mirzai. Operational risk –COSO re-examined , *SAS Journal of Risk Intelligence*, (2005), 19-22.
- [30] PricewaterhouseCoopers. *Extending Enterprise Risk Management (ERM) to address emerging risks*. PricewaterhouseCoopers. 2009.
- [31] R. E. Hoyt, A. P. Liebenberg. The Value of Enterprise Risk Management. *Journal of Risk and Insurance* Volume 78, Issue 4, (2011), 795–822.
- [32] R. Matthews, R. D. P. Vanek. Enterprise Risk management (ERM) – Failure is not an option. *Second Annual General Business Conference Proceedings*, Sam Houston State University, 2010.
- [33] R. S. Kaplan, J. A. Colica, M. D. Ranganath, B. L. Zubrow, *Enterprise Risk Management*. Harvard Business School. The centennial business summit. Summit Report 2008.

- [34] R.S. Kaplan, A. Mikes. Managing Risks: A New Framework. In Harvard Business Review, 2012.
- [35] S. Segal. Corporate Value of Enterprise Risk Management: The Next Step in Business Management. Wiley & Sons, Inc. 2010.
- [36] T. A. Kletz. Hazop – past and future. Reliabil. Eng. Syst. Safety, vol. 55, (1997) 263-266.
- [37] T. Aabo, J.R.S. Fraser and B.J. Simkins. The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One. Journal of Applied Corporate Finance 17(3) (2005): 62–75.
- [38] The Canadian Institute of Chartered Accountants. CoCo: Criteria of Control Board. The Canadian Institute of Chartered Accountants, Toronto, 1995.
- [39] Toronto Stock Exchange, Committee on Corporate Governance in Canada. “Where Were the Directors? Guidelines for Improved Corporate Governance in Canada,” (the Dey Report), TSE, Toronto, 1994.
- [40] W. G. Shenkir, T. L. Barton, P. L. Walker. ERM Frameworks: Lessons from the Field. Enterprise Risk Management. Chap 24, (2010), 441-463.
- [41] Working Group on Global Derivatives. Derivatives: Practices and Principles. Group of Thirty, Washington, DC. 1993.
- [42] W. Lee, D. Grosh, E. Tillman, C. Lie. Fault tree analysis, methods and applications—a review. IEEE Trans. Reliabil., R-34, no. 3,(1985).194-203.