# IMPLEMENTING ENTERPRISE RISK MANAGEMENT IN ROAD ORGANIZATIONS: CONSIDERATIONS AND A PROPOSED ROADMAP

Benekos, I.[1], Yannis, G.[2], Mavromatis, S.[3]

[1]Ph.D., Chair of the World Road Association (PIARC)'s Technical Committee A.3 (Risk Management).

Head of Laboratory A5 (Risk Management and Resilience), Hellenic Institute of Transport,

Centre for Research and Technology Hellas, 52 Egialias st., 15125, Marousi, Greece.

Tel: +30 211 10 69 555. Email: ibenekos@certh.gr (corresponding author)

[2]Ph.D., Professor; Department of Transportation Planning and Engineering, School of Civil Engineering,

National Technical University of Athens, 5, Heroon Polytechniou st., 15773, Athens, Greece.

Tel: +30 210 772 13 26. Email: geyannis@central.ntua.gr

[3]Ph.D., Assistant Professor; Department of Transportation Planning and Engineering, School of Civil

Engineering, National Technical University of Athens, 5, Heroon Polytechniou st., 15773, Athens, Greece.

Tel: +30 210 772 13 26. Email: stemavro@central.ntua.gr

**ABSTRACT**

Implementing risk management to an entire organization, though being increasingly applied, may appear challenging, often perceived as requiring substantial effort with unclear benefits. This paper aims at providing road transport organizations and practitioners with key references and a roadmap for designing and implementing Enterprise Risk Management. The methodology relies on synthesizing existing good practices from the road transport sector. A brief overview of state-of-art practices with applications using different structures are provided and implementation drivers, expected benefits and maturity levels are highlighted. Practical considerations and key success factors are discussed, followed by the suggestion of an integrated implementation framework including key concepts and tools.

**KEYWORDS**

Enterprise Risk Management, risk, organizational risk, risk management implementation.

## 1. INTRODUCTION

We all perform, unconsciously or consciously, on a daily basis, acting proactively or reactively, some process for managing consequences from different options we are faced with or events that may occur, whether these may involve simple considerations such as not missing the train and get late to an appointment or more complex ones such as investing in the stock market which requires expert knowledge of the subject matter.

Risk management (RM) process is, however, '*the systematic application of management policies, procedures and practices to the tasks of communicating, consulting, establishing the context identifying, analyzing, evaluating treating, monitoring, and reviewing risk'* [1].

Traditionally and/or intuitively, risk has been associated with threats. The upside of risk, namely opportunities, has been recognized and incorporated in all formal definitions provided by international standards and professional associations (e.g. [2], [3], [4]). For example, risk is considered as '*an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more objectives such as scope, schedule, cost and quality'* [5] referring to a project's objectives. Experts in technical fields often define risk as *'a measure of the probability of occurrence and the severity of related consequences of events'* to the examined objective [6]. The typical risk structure is shown with an example in Fig. 1.

The trigger event may be defined as the mechanism that leads to the realization of a hazard, i.e. the class-4 hurricane. Preliminary and intermediate events may amplify or mitigate the probability of occurrence and/or the related consequences. To society or to a company or institution responsible for a specific activity, the total damage due to a hazard is of prime interest. The societal risk R may be defined [7] as:

$$\boldsymbol{R} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{p_i} \times \boldsymbol{C_i} \tag{1}$$

where $n$ is the number of all independent and mutually exclusive event scenarios $i$, $p_i$ is the probability of occurrence (per year) of scenario $i$, and $C_i$ are the consequences of scenario $i$, for example in terms of fatalities. The consequences may include human, economic, and environmental consequences and can be measured in terms other than fatalities per year, for instance in, monetary units or emission of a given substance. An important aspect, thereby, is the combination of the various types of consequences under a common metric, such by assigning a monetary value to all types of consequences, since different types of impact cannot be directly compared. The societal risk criterion is usually used in the risk assessment studies where the calculated societal risk must fulfill the risk acceptance criteria, i.e. must be less than a specified minimum and acceptable value (threshold).

Enterprise Risk Management (ERM) is concerned with the management of risks that relate to the strategic objectives of an organization and risk may be defined as the '*effect of uncertainty on objectives'* [1]. ERM should support both the selection and the setting of the strategy for the organization [8]. Although the principles of risk management and application of relevant frameworks may be extrapolated and applied to entities that are larger than a simple project, such as programmes, portfolios and organizations, the scaling up includes additional challenges and considerations that need to be accounted for when planning for their implementation to an entire organization. As such application may also involve significant costs, pioneering for the implementation of an ERM and demonstrating the added value that this would create for the organization, would also call for a good understanding and analysis of the expected benefits.

Traditionally, organizations would restrict RM in the areas of insurance and financial operations. Institutions in the financial sector may be more adept to implement ERM frameworks as relevant legislative and regulatory provisions (e.g. Turnbull Report of 1999; Sarbanes-Oxley Act of 2002; Basel I, II and III Accords) have been providing motivation and guidance for doing so. The lack of significant prior experience, uniform guidance and regulatory provisions in the road sector may render the implementation of an ERM framework both dubious in relation to its necessity and challenging in relation to its application. Road transport related organizations may include road authorities and agencies, concessionaires, road and relevant infrastructure design and construction firms, whereas practitioners may include programme, project and risk managers. Whether belonging to the public or the private sector, road transport related organizations and risk management practitioners in the road sector face similar challenges when it comes to designing and implementing an ERM framework. Drivers for ERM for public organizations may spring from the nature of their mission to effectively and efficiently serve the society in general and support its resulting accountability, as opposed to drivers in the private sector that often consider in priority the firms' essential mission to generate (and often maximize) profits for its shareholders. Whereas one could argue that this difference could result in different prioritization of relevant risks/opportunities, nevertheless, the root-causes of the challenges, due to the absence, as aforementioned, of a comprehensive legislative and regulatory framework at the organization's level for implementing ERM implementation remain the same for all actors in the road transport sector. RM practices are often fragmented and applied ad-hoc or in specific regulatory context (e.g. road safety, risk analysis for tunnels, health and safety of workers) that do not account for the organization and its mission as a whole [9]. However, RM may affect significantly the effectiveness of transport and mobility management strategies. Such strategies combined with recent technological advances (e.g. ITS) may greatly improve safety and cost reduction in road transport systems and thereby support and further advance their

sustainability and reliability. Taking further the example of ITS in road transport risk management, such systems enable traffic authorities to coordinate and act more efficiently in case of planned or unexpected emergency situations [10]. By implementing risk treatment options during transportation design – construction – operation, some hazards may no longer apply, but new hazards may be detected rendering the RM process in road transport iterative.

The necessity of including governance policies and procedures in RM systems is increasingly being recognized [9], [11]. Therefore, we aim at providing road transport organizations and practitioners with key references, principles for designing, and a roadmap for implementing ERM with relevant tools and concepts for each step of the process. Our main goal besides synthesizing information that exists, is to bring further insight into the implementation process of an ERM framework, address the *'how to proceed'*, an aspect that seems not to have been extensively addressed by the recent revisions of major international ERM frameworks [12] and [13]. We do not aim at analyzing notions and tools that are known to the risk practitioner. Also, although a brief discussion on the challenges that exist in measuring the ERM's added value is provided and some proposals are formulated on potential ways to address this issue for completeness and in order to indicate potential avenues for future research, it is not within the scope of this study to provide an extensive analysis on how to measure the ERM added value which is a current and sensitive issue of concern among risk practitioners in various industries and sectors, thus meriting an in-depth examination at a later stage.

The paper is structured as follows: the research methodology and the methods used are first presented (Section 2); a literature review of existing ERM frameworks, implementation methods and state-of-practice are briefly presented first by considering RM and ERM both in a general and historical context and in relation to road organizations (Section 3); the proposed structures, maturity levels for RM and the drivers for ERM are discussed; the benefits and added value of an integrated ERM framework versus conventional RM are then argued (Section 4). The paper synthesizes the aforementioned analysis by providing practical considerations, application and benchmarking tools, presents current practices and challenges for measuring ERM's added value, and proposes a gradual, stepwise approach for its implementation (Section 5) to facilitate practitioners and organization boards to advocate for it. Section 6 summarizes the key points from this research and provides recommendations for further research.

## 2. RESEARCH METHODOLOGY AND METHODS

ERM implementation can greatly vary from organization to organization and existing literature and case studies may become overwhelming. However, as the literature review in the following section will reveal, though various journal papers report on the results of the operationalization of ERM in different contexts, there is lack of relevant scientific literature on *how to proceed* for actually implementing an ERM framework, which is even more pronounced in applications concerning the road transport sector. Therefore, we attempt to identify the general principles and benefits of ERM and provide a roadmap for its implementation by following a top-down and bottom-up iterative approach that moves from the general principles to context-specific ERM applications as indicated at the following methodology steps:

1. A desk-based literature search is first performed to collect information relevant to ERM principles, practices, and guidance for implementation. As aforementioned, this step revealed a lack of scientific literature, particularly in relation to the guidance for practical implementation. There exist propositions *on what* an ERM framework should consist of, or which factors are observed to correlate with increased level of ERM maturity but there is very limited information *on how* to proceed for establishing it.
2. Based on the previous finding, and as it is likely that existing regulatory context, use of standards and the state-of-practice in the sector could constitute important drivers in adopting ERM practice [14] and influence its implementation, our inquiry next moved from the generic to the sector-specific in a two-tiered approach:
    a. ERM frameworks from well-established international organizations and standardization committees that set the benchmark in ERM practice are first considered for obtaining insight into the general principles.
    b. ERM implementation in the road transport sector is then scrutinized for context-specific insight. ERM frameworks and RM applications established by country agencies that are considered by experts who are members of the World Road Organization (PIARC) to belong to the cluster of 'advanced' in terms of RM practice with the longest practical experience are considered for obtaining insight on actual ERM application in the road transport sector.
3. Based on the aforementioned desk-based search we synthesized commonly observed best practices by also considering relevant published papers from renowned management consulting firms. We produced a high-level coarse proposed roadmap for ERM implementation which was subsequently presented to focus group experts within the work proceedings of PIARC's Technical Committee (TC) A.3 (i.e. in its 5$^{th}$ Meeting in Brussels, Belgium, May 2018) dealing with RM and ERM, and International Seminars

(see step 4 below). The coarse proposed roadmap served as the *baseline* for further elaboration and refinement.

4. Focus groups discussions, insights and case studies obtained from experts and risk management practitioners that belong to different road-related organizations (governmental agencies, consultants, road design, construction and management companies) Technical Committees (TC) of PIARC (i.e. mainly from TC A.3 dealing with Risk Management but also to some extent from TC E.1 dealing with Adaptation / Resilience Strategies and TC E.3 dealing with Disaster Management as these TCs co-organized International Seminars on RM for road organizations) further refined different aspects of ERM implementation and considerations for practical application. In this respect, the following three major sources of data and information were considered:
    a. Focus group discussions and presentations performed within TC A.3 in relation to ERM best practices and the proposed roadmap.
    b. An international survey that was performed by Working Group A.3.1 of TC A.3 which provided further insight on ERM maturity levels and current practices. The results of the international survey are published in PIARC's Technical Report [11] that reflects the work that has been performed during the 2016-2019 cycle in relation to ERM.
    c. International Seminars and Workshops that were co-organized by PIARC with the active involvement of TC A.3:
        i. International Workshop on Risk Management for Road Organizations and Projects, Prague, Czech Republic, May 12, 2017.
        ii. International Seminar on climate adaptation, risk and disaster management for roads and road organizations, November 8-10, Havana, Cuba.
        iii. International Seminar on Disaster and Risk Management for Roads, Hanoi, Vietnam, November 7-9, 2018.
5. We iteratively updated and refined the synthesis of the best practices and experience in relation to the ERM principles and proposed implementation (baseline roadmap, Step 3) based on information obtained from the aforementioned international events and focus group discussions. The last International Seminar served as a mean of validation of our proposed theoretical roadmap [15] as it was well-received by Seminar participants and other presentations from countries with long standing experience in ERM implementation provided positive feedback and experience concerning actual ERM implementation [16]

that closely resembled the proposed roadmap. Following the International Seminar, [11] and [17] also include a brief overview of the proposed roadmap which underwent peer-evaluation within PIARC. Nevertheless, we are aware that a complete validation of such propositions may only be obtained by extensive practice from different stakeholders who follow the proposed steps and systematically document their experience. As this has not been performed for the purposes of this paper, we acknowledge that it is a limitation of our proposed approach, however, we believe that the extensive search that was performed and the relevant feedback that has been processed from experienced stakeholders, warrant its further consideration by the research community, the road transport and management industry and will eventually result in the systematic collection of additional data and information needed for such validation.

## 3. LITERATURE REVIEW AND STATE-OF-PRACTICE

### *3.1 Literature review and major ERM frameworks*

Academic research has produced few peer-reviewed articles in relation to ERM, mostly in finance and accounting journals, which relate to risks with well-defined statistical properties that spring from well-defined regulatory requirements and with limited application outside finance [3]. [3] provides a comprehensive review of ERM definitions, its conceptual roots and operationalization by researchers and practitioners, and identifies relevant areas where management research, which is even more limited in relation to ERM, could contribute. We avoid reproducing the extensive list of these references if not in the scope of this paper unless these provide some added value for contextual relevance.

Although the notion of 'holistic' or 'integrated' approach had appeared earlier (e.g. [18] and [19]) it is in 2001 that the ERM term is first used in the research literature [20] and [21]. [22] proposed combining scenario planning and real option analysis performed by finance researchers to account for uncertainty, in advocating an integrated approach to RM at Corporate Level based on qualitative assessments of real options. The paper emphasized monitoring of key contingencies, reviewing and reassessment of the exposures, flexibility in the design of organizational processes and structures and identification and training of responsible individuals for successful RM implementation.

[23] analyzed survey data from 123 organizations that applied ERM, obtained from chief audit executives, to identify factors that are positively correlated with the advancement (i.e. stage; maturity level) of ERM implementation. [24] used Tobin's Q, a standard proxy for a firm's value, to statistically demonstrate the positive

effect of ERM on firm value. [25] used regression and residual analysis with empirical data obtained from 112 US firms to claim (as the study examined data only from a single year, i.e. 2005) that the following factors affect the ERM relation to the firm's performance: environmental uncertainty, industry competition, firm complexity, firm size, and board of directors' monitoring. [26] concluded by studying the ERM operationalization in two banks and the different types of ERM that may exist, that management control systems would benefit by accounting for the risk culture that is shaped by the respective ERM implementation. Both 'quantitative-enthusiasts' as well as 'quantitative-skeptic' risk cultures influenced strategic choices, albeit in a different way. However, for important risks, in lack of time, models or data, risk managers often rely on judgment. [27] proposed a three-type of risk taxonomy for classifying risks, preventable or internal risks arising from within the organization, strategy risks, and external risks with the latter being out of the organization's control. It emphasized the importance for risk management to question established biases, the tailoring of their management tools, processes and structures in accordance to the type of risk they examine, and for establishing close relationship with top management.

A survey performed for investigating the ERM maturity in Chinese Construction Firms (CCFs) based in Singapore, arguably the first of the kind performed in the construction sector, identified a low maturity of ERM. Similarly to [23] and [25], the ERM maturity level was positively correlated with the firm's size. Risk communication, RM in relation to objective setting and development of a risk-aware culture were reported as being perceived as the most essentials in ERM development and level of maturity [28]. [29] used literature review and a survey performed to CCFs to identify critical hindrances to ERM implementation. Lack of: a) resources, b) relevant procedures, c) leadership and senior-level support and d) high-quality data were identified among the most critical. [3] also mentions the lack of relevant historical data has also been mentioned as a hindrance to performing thorough probabilistic RM assessments.

As aforementioned, the scientific literature search revealed few cases (e.g. [28], [29]) in which ERM was studied in a context different than that of the accounting / financial sector, i.e. the construction industry, which is linked to the road transport sector only by association. Moreover, the focus of these studies was rather on the ex-post assessment or statistical observation of operationalization characteristics of ERM (i.e. structure; processes; maturity level) and few also proposed context-specific performance criteria for measuring ERM success. Although this may offer some insight to practical considerations for the desired features of, and the way to proceed for establishing, a comprehensive ERM framework, these findings need to be further enriched by looking at established ERM frameworks and context-specific applications for completeness and relevance.

The first comprehensive ERM frameworks originate from the field of internal controls, which are typically performed to ensure that business processes are carried out correctly, effectively, and efficiently. Two major ERM frameworks with a focus on internal controls may be distinguished.

The Committee of Sponsoring Organization of the Treadway Commission (COSO) published a well-known ERM framework that applied to internal control of private companies [30]. According to the COSO ERM, *'Enterprise risk management is 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'* [30]. Fig. 2 summarizes the components of the COSO ERM.

In the COSO ERM strategies and objectives are articulated by considering the internal environment in four categories: Strategic (high-level goals supporting the mission), Operations (effective and efficient use of resources), Reporting and Compliance to existing laws and regulations. RM through event identification, risk assessment, risk response and control activities supports the execution of the organization's strategies while performance evaluation and monitoring of the process is assured by high-level executives and internal audits who provide feedback through an integral flow of information and communication to improve the RM process and align it with the strategic objectives. All levels (entity-level, division, business unit and subsidiary) and functions of the organization are involved in the process. COSO ERM is also linked to Sarbanes-Oxley requirements for companies listed in the USA. In its 2017 update the focus is put on the performance and on the linkage of ERM with strategy-setting [4]. [25] proposed an Enterprise Risk Management Index that relates to COSO's four categories for measuring the organization's ERM effectiveness. Acknowledging the complexity of the COSO model, [31] claims that time is needed for the implementation of the ERM, however, design and initial implementation may be performed in a relatively shorter period by focusing on key strategic and business objectives.

Similar in its concept, though directed towards the performance and accountability of the public sector where different internal control constraints and work practice may exist, is the International Organization of Supreme Audit Institutions (INTOSAI) framework [32]. In the INTOSAI framework the 'Strategic' and 'Reporting' objectives of the COSO ERM are substituted by 'Accountability' and 'Safeguarding Resources' (i.e. against loss, misuse, and damage) that are perceived as more applicable to public administrations.

The ERM framework "The Orange Book: Management of Risks – Principles and Concepts" known as the Orange Book from the UK [33] is also geared towards public organizations, though by attributing more importance to the external environment and to the timeframe considered for identifying potential changes that may affect the risk profile for the organization than the INTOSAI framework. Internal control is viewed more as a response to an event and less as a proactive activity. RM is performed at three levels of the organization, the Strategic level where strategic decisions are defined, the Programme level that involves decisions transferring strategy into action, and the Project and Operational level that involves decisions required for the implementation of these actions, which constitute the routine activities of the organization. ERM is viewed as a circular, repetitive process, not a linear one (see Fig. 3), integrated in the organization and not performed in silos, aiming at balancing interwoven activities that interact with each other for supporting the implementation of the strategy. Importance is given to the monitoring, evaluation, and improvement of the established RM procedures.

The most recent RM framework that may be applied to organizations irrespectively of their size is the International Standard for Standardization (ISO) 31000:2009 framework, recently revised into ISO 31000:2018, as best practice by several road agencies [34]. The ISO 31000:2009 emphasizes the implementation and the integration of RM throughout the organization rather than the support of the process and it is based on a set of clearly defined principles. According to these principles an ERM to be effective must create value at all levels, be an integral part of the organizational processes and of decision-making, explicitly address the uncertainties, be systematic, structured and timely, based on the best available information tailored to the organization's needs and its external and internal environments, take human and cultural factors into account, be transparent and inclusive of stakeholder's views, be dynamic, iterative and responsive to change and, facilitate continual improvement of the organization [2].

The ISO 31000:2009 RM framework is based on the Plan-Do-Check-Act (PDCA) circle, which has received a clear mandate and commitment from the top management (see Fig. 4a). Mandate and commitment ensure that the RM policy is defined and endorsed, that appropriate RM performance indicators are selected and aligned with performance indicators of the organization, and that the RM objectives are aligned with the strategic objectives of the organization, its culture and risk appetite. The design of the framework involves a thorough understanding of the organization and its context, allocation of appropriate resources, establishing external and internal communication and reporting mechanisms and protocols, defining the RM policy and appropriate accountability and authority lines, establishing required competence and integrating these into the organizational processes. RM implementation involves selecting the right timing and strategy by communicating and consulting with

stakeholders regarding the application of the RM process (see Fig. 4b). The PDCA circle concludes with the monitoring and reviewing of the framework and its further improvement. [35] argues that though the standard resolves many inconsistencies and ambiguities that existed between the different proposed approaches and definitions, it may still create challenges for those that are mostly acquainted with approaches and language that are different from those proposed by the ISO. In its review of the ISO's recent update [36] where the organization's leadership role in initiating and pushing forward the integration across the organization and the iterative nature of the process are highlighted, [12] states that clearly demonstrating the added value of ERM in relation to the relevant allocation of resources for its implementation remains a challenge, fact also mentioned in their COSO framework review [13], and that it is still lacking a step-by-step checklist to implementation, a gap that we aim at partially bridging with our study. It also advised on flexibility needed in implementing ISO's principles and proposed components according to the context of the organization.

Despite their different backgrounds and however different development the RM and Internal Control may have followed, their goals are similar and practice has demonstrated the need for their integral management.

### *3.2 ERM implementation in the road sector*

In the road sector, key elements of RM may not be different from other management areas but need to be adapted to the specifics of the road operations. Design uncertainties, construction and operational safety, and challenges from natural or man-made events have always been in the spotlight and RM is commonly used for road project selection, planning, procurement, and construction by several road organizations [37], [10].

[38] presents the results of a comprehensive survey and interviews that aimed at assessing the RM state of art across the US Departments of Transportation (DoT) and identifying executive strategies for ERM. The survey indicated that only 39% possess a formal ERM program. Sponsorship by DoT executives and commitment from upper management, employee involvement at all levels and adequate provision of resources along with the development of a risk management culture were identified as essential to fostering organization-wide RM.

Technical Committee 1.5 of the World Road Association (PIARC), dealing with RM in the 2012-2015 cycle, performed an international survey across both private and public road organizations in 16 countries aiming to investigate the level of formalization and integration of RM policy and process within an organization. Road management activities covered by the survey included project selection, planning, design, procurement, financing, construction, operation and maintainance, tolling/charging, crisis management and emergency preparedness, human resource management and governance. The survey indicated that RM processes are often applied to a

departmental or functional level and often road organizations possess formal strategic objectives but without any formal risk policy. When formal RM policies exist, often, formal risk processes do not supplement these. Even fewer organizations apply integrated ERM framework to their whole organization [9].

Technical Committee A.3 of PIARC, dealing with RM in the 2016-2019 cycle, performed an international survey with 23 responses received from 16 countries to investigate on the maturity level of ERM applied to road organizations. Only 14 responses, all coming from Upper Income countries that are considered as being advanced in the practice of ERM, reported applying ERM at varying level of maturity. Interestingly, eight (8) responses indicated perceiving no added value in applying RM [11].

Road operation and maintenance typically rely on prevention and reaction but further work is needed to better anticipate and integrate risks associated with ageing infrastructure, natural hazards, and decision processes. Risk is increasingly being recognized as an asset rather than threat that may deliver competitive advantage and improve efficiency for a road organization when managed effectively. Road agencies in Australia, Canada, Denmark, Japan, New Zealand, Sweden, the UK and the USA are among the leaders in recognizing the added value of ERM and assimilating such framework into their organizations [34], [39].

RM frameworks in Australia, Canada, Denmark, New Zealand, and the USA, in general, follow the principles and processes outlined in the ISO 31000:2009, which is strongly based on the prior AS/NZS 4360:2004 RM standard [40], [41].

In South Australia's Road Authority project management system (PMS), project planning and delivery are incorporated within an integrated decision-support system to achieve the strategic objectives. RM is intrinsic to both the PMS and the decision support system. All aspects of the project are subjected to a thorough assessment of risks since the initiation phase of a project and RM is applied throughout the project's life cycle by development of a detailed RM plan. The ERM system identifies two levels of risk profiles, the organizational/strategic risk profiles and, the local risk profiles that cover risks at a local level or operational in nature, in detail aimed to be managed by the local business areas. The ERM has evolved after the recommendations of internal audit to promote transparency by providing open access to information about divisional operational risks to be shared by all staff and focusing on tailoring RM to meet departmental and business area needs while staying aligned to the strategic goals. In establishing a common language and criteria for assessing risks across the organization, risk information is reported to senior management and the established Audit and Risk Committee by using a standardized format and a risk matrix tailored to the organization's business groups is included in the RM policy [42].

In Canada, the Quebec Ministry of Transportation (MTQ) adopted a framework where the concept of risk in public safety explicitly considers the element of vulnerability ($V_i$) to the risk of its infrastructures needed to fulfill its mission, which is incorporated in the term of consequences ($C_i$) in aforementioned eq. (1), i.e. R = f ($p_i$, $C_i$, $V_i$) [43]. The Ministry of Public Security in Quebec proposes the same RM process for managing related risks [44].

In the Danish Road Directorate, RM is performed throughout the organization though with a clear orientation in meeting the project's schedule and budget. Risk assessments are performed quantitatively by using a simplified definition of eq. (1) where frequencies of occurrence and related consequences in terms of cost are determined in triplets (min, most likely, max for frequencies; $10^{th}$ percentile, most likely, $90^{th}$ percentile for cost). A standardized risk management software (RamRisk) stores all risk information and is used for reporting using a risk matrix [9]. The risk register along with environmental impact assessments and the construction cost estimate form the basis for the political decision in the initiation phase of a project. The process resembles a typical project RM framework with strong mandate from the top management.

The Swedish Transport Administration (STA) establishes the strategy in accordance with the "Ordinance on Internal Management and Control (2007:603)" [45]. RM is part of the annual operations analysis, presented and approved by the Director-General and the Board of STA at the start of the year, that focuses on the most critical threats (i.e. risks) and opportunities that have been identified by internal and external audits for operations, projects, and the strategic objectives in a bottom-up approach. Escalation, risk tolerance and acceptance criteria are defined on three levels, the Strategic, Tactical, and Operational with an emphasis for increased consideration toward societal risks. A hazard catalogue is used as a checklist for assessing the criticality of risks and opportunities relevant to maintaining operations and their resources and achieving the operational objectives. Risk analyses use the scenario approach in which a chain of events is considered starting from root causes of hazards and possible consequences of a realized event on assets of interest have been often practiced by the STA [34].

In the UK, the Highways Agency (HA) performs RM at two levels, the Strategic and the Operational level with overarching goal to provide better value for money aiming in a less risk-averse culture [46]. The CEO, the Board of Directors (BoD) and the Audit Committee are responsible for setting the RM philosophy or risk appetite, the culture, and expectations (risk tolerance) in regard to RM, the roles and responsibilities. A Corporate risk register is used and internal control policies are defined based on the HA's risk profile. At the Strategic level eight key business and administrative objectives are reflected in the HA's business plan. The Operational RM receives input from project risks and aims to ensure that risks identified for the key HA's strategic objectives are properly managed through appropriate risk assessments, performed using a uniform methodology to ensure consistency

throughout the HA. There are three *'lines of defense'* for the RM process: all personnel and line managers constitute the first one. Formal groups established to oversee management and investment arrangements constitute the second one. The third consists of a Corporate Risk Management Advisor, ultimately responsible for developing and maintaining the HA's RM arrangements who sits within the Internal Audit Committee that reviews the robustness of the framework and provides quarterly RM reports to the BoD.

In the USA, the American Association of State Highway and Transportation Officials (AASHTO) subcommittee on Asset Management has proposed an ERM guide with RM performed at four levels: the Enterprise level dealing with risks to strategic objectives, the Program level dealing with risks to group of projects, the Project level dealing with risks specific to individual projects and the Activity level dealing with risks specific to the functions that are supportive of the projects or programs [47]. RM is considered as being *complimentary* to performance and asset management in supporting the strategic objectives, *not a replacement* of these and the RM process is dynamic with a risk being able to rise or fall down a level. The guide proposes tools and resources to be developed for the RM process, a checklist to use when establishing ERM programs and a risk maturity matrix for measuring an organization's RM process level of maturity.

The presented literature is only indicative, nevertheless representative, as this contribution aims to provide base references and an overview of the general principles for the most established and widely used ERM frameworks with examples of the state-of-practice that have been implemented in the road sector.

## 4. STRUCTURE, DRIVERS, BENEFITS, AND MATURITY OF ENTERPRISE RISK MANAGEMENT

### *4.1 Levels of risk management, structure and risk taxonomy*

It has become apparent that RM may be performed at different levels in an organization. However, the segregation or characterization of those levels at which RM is applied differs in the proposed frameworks. The four levels of the COSO ERM framework rather pertain to the organizational structure of the enterprise.

The four levels proposed in the AASHTO ERM guide are rather differentiated on a more impact-based structure concerning the performance of operational tasks, major programs (e.g. pavements) or projects or the achievement of major objectives, in an increasing level of complexity. Some organizations consistent with the AASHTO's approach may even consider a fifth level of RM, the portfolio level (e.g. bridge and pavement programs), which would align specific programs and projects to specific strategic goals, to be an intermediate level between the enterprise level and the program level. AASHTO's activity level resembles to a sub-category of the operational level proposed by other agencies and may be justified by the large number of critically important activities that a

transportation agency performs such as maintenance of drainage structures and traffic signals, snow-removal operations, incident response, counting traffic, etc. The difference among these levels is the extent and scope of risks to be managed.

Three levels are proposed by the Orange Book and the Swedish Transport Administration, oriented towards the major phases of transferring the strategic decisions into actions for supporting the strategic goals. The UK Highways Agency opts for a coarser distinction with only two levels, the strategic and the operational, the latter encompassing all organizational and project elements required to achieve the strategic objectives. The ISO 31000:2009 framework abstains from proposing RM levels but rather focuses on the RM principles required irrespectively of whether these apply to an entire organization or to a sub-unit.

So, which is the appropriate level / structure for categorizing different risks and facilitate the RM process? In the financial sector, there is a clear and ubiquitous separation of risks at high level into market, credit, operational and liquidity risks. Further sub-categories are defined for each of these high-level categories. The difference in an organization as opposed to a bank is that a risk may be attributed to different categories or levels according to the way it may affect the organization. In the road sector for instance, a natural hazard such as a blizzard that may result to the closing of a motorway may be an operational risk for a concessionaire charged with the operation of the motorway, but it may constitute a strategic risk with severe implications for a road agency responsible for the operation of the transportation network. Another important difference arises from the fact that often an organization's register of most important risks may often include the so-called 'data-poor' risks where there is little available historical data to effectively support analytical quantitative risk approaches [48], [3], [26]. As a result, the integration of such risks into the risk profile of an organization may scale-back the overall level of quantification of the risk assessments.

The essence of ERM lies not in the number or type of risk categories (risk taxonomy) or levels that are defined but rather on how these support the integration of the RM process across the organization and the realization of its strategic objectives [49], [50], [4], [11], [26]. The appropriate structure for an organization should derive by considering its *RM policy* and *risk architecture*.

In the RM policy, the risk strategy, attitude, and philosophy are defined. These are usually reflected through the terms risk appetite, risk tolerance and risk threshold though confusion arises from the fact that sometimes organizations or even units within the same organization use these terms interchangeably but definitions may also vary [3], [51]. The PMI [5] defines these terms in a clear way that may help in avoiding confusion. Risk appetite

is the degree of uncertainty an entity is willing to accept in anticipation of a reward; risk tolerance is the degree or amount of risk an organization is willing to withstand. Usually this refers to the acceptable level of variation to the achievement of a specific objective. It may be defined as a range using the same unit of measure applied to the objective or in the form of a range of degree or amount of risk that applies in individual risks or to aggregate risks when compounding from different hazards that pertain to the specific objectives. Risk threshold refers to the specific limits that separate the different levels of risk characterization (e.g. low, medium, high) that relate to the risk tolerance or to upper or lower limits of risk values beyond which risks are considered unacceptable or acceptable without needing a response, respectively. Different risk tolerances may result in different risk treatment responses.

The risk architecture specifies the roles, responsibilities, accountabilities, the communication, and the reporting structure. The incorporation of the risk architecture and risk policy into the RM process and their integration across the organization is performed via guidelines, rules and procedures in the so-called risk protocols that specify the RM methodologies, tools, and techniques to be used [49].

For any resulting RM structure, it is important to note that RM should be dynamic irrespectively of the level or category that risks may be initially assigned to. Risks may be elevated or downgraded to different levels or switched categories according to the importance they exhibit in relation to the organization's strategic objectives as time evolves. There are two major categories of approaches that have been traditionally used in building an ERM: top-down approaches where risk identification is pushed down from the top of the organization and bottom up approaches where risks are identified at each business unit and then pushed up to the organization's top management. However, either method may present important shortcomings as listed in Table 1 [52].

### *4.2 Drivers for ERM and expected benefits*

Based on the COSO and the ISO 310000:2009 definitions for RM, it may be inferred that the overriding driver for implementing ERM is to support strategic planning by aligning the organization's strategy with its risk culture in achieving the strategic objectives. In complex and uncertain environments, the achievement of the organization's strategic objectives relies on managing both internal and external risks [47], [36], [4], [26]. Natural disasters are an example of an external infrastructure risk to a road organization whereas unreliable information technology systems could constitute an internal infrastructure risk. Failure to manage these risks may increase the likelihood of their occurrence, the severity of their consequences or both. Thus, drivers for RM may be externally and/or internally driven. It is recognized that external factors and events such as economic slowdown, regulatory

changes due to major disasters in the corporate and road sectors involving important reputational, economic and / or human losses (e.g. Enron scandal; major accidents in road tunnels such as at the Mont Blanc in Italy-France, 1999, with 39 deaths, the Tauern in Austria, 1999, with 12 deaths, and the St. Gotthard in Switzerland, 2001, with 11 deaths), or increasing competition may have a major impact on the organization mission's success and thus constitute major ERM drivers [53]. Risk taxonomies, such as the FIRM (Financial, Infrastructure, Reputational, Marketplace) risk scorecard [49], or the preventable—strategy-external categorization proposed by [26], may be used to identify risk drivers for strategic, tactical, and operational risks.

The potential benefits of RM are widely recognized. RM has become part of a suite of good management practices. It provides a sound and documented basis for decision-making in the face of these uncertainties. Traditional RM focused on protecting *tangible assets* of the organization such as physical assets (e.g. infrastructure; buildings; equipment; inventory) and financial assets reported on a balance sheet (e.g. cash; receivables; investments; equity). ERM broadens the scope of RM to also include the *intangible assets* [54] of an organization. These pertain to customer assets (e.g. customers; channels; affiliates), employee / supplier assets (e.g. employees; suppliers; partners) and organizational assets (e.g. strategy; leadership; knowledge; reputation; innovation; systems; processes; values). Differences between traditional RM and ERM are summarized in Table 2.

Hence, *'ERM redefines the value proposition of RM by providing an organization with the processes and tools it needs to become more anticipatory and effective'* [50] in managing the uncertainties and the relevant factors in achieving its strategic objectives but also, very importantly, provides a framework for communicating these inside, outside of, and across the organization, thus creating sustainable value for its stakeholders in an ever-changing operating environment. ERM elevates RM from a tactical to a strategic level within the organization and may create value for the organization both at the macro and micro level [55]. At the macro level, strategic plans consider relevant risks and become more substantive and robust. At the micro level, it establishes a common risk language across the organization and ensures that decision-making is not only a top management activity but also performed throughout the firm by middle managers that actively participate in assessing the risk-return tradeoff of their projects in relation to supporting the strategic objectives or to the marginal increase of the organization's total risk. Major benefits reported by risk and financial executives reported better-informed decisions, greater management consensus, increased management accountability and smoother governance practices [56].

ERM may contribute management to successfully protect and enhance the organization's value in three ways [50]: in establishing a competitive advantage, in optimizing the cost for RM and in improving business performance. Fig. 5 shows the sub-components of these, which are closely related to the benefits as listed in ISO 31000:2009.

The added value of ERM is recognized in the road sector and the aforementioned views are shared [9]. Other important considerations for ERM is the performing of due diligence and the sharing of responsibility for accepting unavoidable risks inherent in undertakings, when these are documented, with the executive and legislative branches of an organization.

ERM potential shortcomings and limitations should not be overlooked so that these may be properly addressed. ERM may be an expensive approach in terms of managerial time as it involves consistent and systematic involvement of top management. If not due attention is paid to opportunities and risk tolerances are not well defined, decisions may be driven by a 'keeping-out-of-the-red-zone' mentality as middle management may worry more about threat than opportunities. Substantiating and measuring the effectiveness and efficiency of an ERM framework may also be challenging. Clearly establishing the link between ERM implementation and derived benefits may not be trivial or obvious to all [3], [11]. Lastly, ERM is a group thinking approach that fosters consensus seeking but group thinking may not be appropriate for all decisions [57]. A survey performed by the Politecnico di Milano in Italy, identified that the major obstacles in implementing an effective ERM perceived by the respondents were insufficient funding, bureaucracy, and lack of knowledge and data [9].

### *4.3 Levels of ERM maturity*

ERM and more so RM, are not new concepts to road organizations, many of which have implemented a RM process either to the whole organization or to parts of it [11]. However, different levels of ERM maturity are observed with, as aforementioned, few road organizations possessing a comprehensive ERM implemented across the entire organization with RM being most common at the project level [9], [11].

A few maturity models have been proposed in the corporate sector that resemble the capability maturity model for improving the software developed by Carnegie Mellon University [58]. An example, oriented to financial applications, is the four-level maturity model proposed by [48] increasing in RM complexity from ad-hoc approaches to what ressembles most to a comprehensive ERM including a strong risk culture with systematic scenario analysis of profits and losses and diversification of the risk portfolio through contracting and markets.

In the road sector, the AASHTO ERM Guide [47] has compiled a five-scale maturity model, a composite of guidances issued by the British Treasury Department [59] and the Australian State of Victoria [60] for measuring the maturity level of an organization's RM process. Table 3 summarizes the key elements of this model.

Understanding the maturity level of RM in an organization and knowing the elements of full implementation is key to successfully implement a RM framework that may progressively become a comprehensive ERM across the entire organization [11]. The consideration to keep in mind is: how much added capability do we need to provide reasonable assurance we will continually achieve the strategic objectives and what are the expected costs and benefits in increasing these capabilities?

## 5. CONSIDERATIONS FOR IMPLEMENTATION AND BENCHMARKING

The analysis in the previous sections advocates that ERM necessitates some time to infiltrate in the organization's culture. Employees' attitude, perception, commitment, behavior, and performance towards RM may facilitate or hinder the implementation process [61]. Appropriate training, reward, and sanction systems in relation to RM are important in promoting the RM culture [62], though the very definition of 'culture' may be often challenging [3]. Employees need to clearly understand how RM may create value for them. The organization's maturity level in RM may dictate the subsequent steps to follow in advancing the integration and implementation of an ERM framework and it is a good first step for understanding current RM practice in the organizations and its further needs [11].

However, irrespectively of the RM maturity level, there are common principles and good practices that may highlight and boost the expected benefits of ERM practice. Due to the size of road networks, organizations or administrations in the road sector are often faced with decisions involving significant investments, often affecting the large public. Resource limitations make imperative that these decisions consider both threats and opportunities in a transparent and cost-efficient way. This section is structured as follows:

- First, we attempt to bring these good concepts, principles and practices forward without getting into the specifics of the RM process and related procedures for which extensive analysis and proposed methods exist in the literature and which, are highly dependent on the type of industry and level of maturity. To achieve this, we made use of the findings and recommendations provided in peer-reviewed academic journals, principles and practices proposed in established ERM frameworks (both international and national-specific to the road sector) and standards, high quality, peer-reviewed technical reports and publications from road-related international organizations (e.g. PIARC) with relevant case studies included, and high-quality reports produced by leading management consulting and accounting companies. Table 4 provides the relevant references that advocate for these good practices.

- Next, we propose an ERM implementation roadmap and relevant high-level tools for each step of the process that are highly applicable to the road sector which was iteratively enriched and refined following, as aforementioned in Section 2, focus (road and risk experts) group meetings, presentations and discussions at International PIARC Workshops. We also provide a brief discussion on the challenges for measuring the ERM added value so as to highlight a crucial point in ERM future promotion and wider acceptance that presents ample opportunities for further research.

### *5.1. Principles of ERM culture and key success factors*

*Context of the organization and objective-setting.*

Organizations are unique in their structure and composition and operate in diverse environments with various external and internal stakeholders. The strategic objectives and their timeframe for RM must be SMART (Specific, Measurable, Achievable, Relevant, Time-bound) and not overly broad with clear performance goals as risks also evolve with time. Longer planning horizons such as those imposed for road asset planning and management inevitably result in increased RM complexity as both the number and the uncertainties of risks become greater.

The external environment in the form of PESTEL (i.e. Political, Economic, Social, Technological, Environmental, and Legal) and competition may present important threats or opportunities in relation to the realization of the objectives. Changes, trends, and drivers having impact to the objectives need to be identified. Available infrastructure and human resources, technology and knowhow, capability and core competences, the organizational culture and structure including lines and limits of authority, roles and responsibilities and management processes constitute important considerations for ERM implementation concerning the internal environment. Unless RM addresses the pressing challenges and priority threats and opportunities from both the internal and external environments, in relation to the strategic objectives, it will be neither effective nor relevant.

In establishing the context of the organization and in setting objectives, an important issue is to identify the key success factors (KSFs) for thriving or leading in the industry. These concern certain resources, activities and capabilities that are more important than others in achieving superior performance in the specific industry. For example, for a road organization aimed at serving the public, public satisfaction may be a KSF to the organization. Top management must *tailor* the ERM framework to the organization's uniqueness and specific context in applying organizational resources for meeting those objectives.

*Risk culture and strategy*

A RM policy is the cornerstone in establishing a RM culture in an organization. The RM policy should aim in establishing risk awareness, commitment, insight, *transparency*, and clear understanding as to how and why the risks are managed across the organization. Relevant *risk information* should be available and accessible to keep people involved and informed and take advantage of the knowledge and experience sharing. In supporting RM culture and integration, human resources management may have a leading by providing effective RM plans for organizational activities that have a people dimension [9].

Mind-sets and behaviors in risk-taking of employees and decision-makers are very important. Employees must see benefit in practicing RM and take ownership. Important decisions need to be risk-based, in particular, significant operating decisions (e.g. how much contingency do we put aside for the eventuality of a natural disaster for business continuity?) and strategic planning decisions concerning important strategic choices related to the organization's objectives (e.g. mergers and acquisitions; planning a new highway corridor that may significantly alter the transportation profile in a road network with tolls). The cost-benefit trade-offs need to account for the relevant risks. A positive risk culture would also consider the opportunities, not only threats.

In this context, the risk appetite, risk tolerance and risk thresholds are very important in providing clear directions and boundaries to the possible options. Risk tolerances should emerge as the result of thought discussions at the board level and risk appetites should be conveyed to stakeholders. Clear thresholds and procedures need to be established for escalating or downgrading a risk to a different level.

ERM should be directed in exploiting to the maximum possible extent the areas where the organization excels relative to its competition while minimizing exposure to those risks, which lacks the competence to manage [50]. Core competencies (i.e. the skills and abilities that a company has that provide differentiation and advantage) are woven into the fabric of the company and its activities, are difficult for competitors to acquire or copy, and take years of effort to create. For maximum strategic value, core competencies should be developed and maintained in support of one or more KSFs for the industry.

Poor transparency on risk tolerance, lack of open access to pertinent risk information and overly conservative or optimistic behaviors are often experienced among different business units or departments within an organization.

*Championing ERM and governance*

Championing ERM by the board and top management is key to its success. Ultimately top management and the board are responsible for leading and sponsoring ERM implementation and establishing clear lines of accountability and responsibility for the implementation of the RM process to avoid diluting responsibility. In

practice ERM implementation may be either overseen by a *risk champion or a central risk team*, often reporting to the Chief Financial Officer, or by an independent ERM Group led by a *Chief Risk Officer (CRO)* who may be part of the Executive Board or report to a corporate *RM Committee* composed of board members. Both the risk champion and the CRO are accountable for developing and implementing the ERM program and the related high-level processes and methodologies. They form teams that conduct risk assessments, and they have an essential role in coordinating workshops, facilitating meetings and trainings, developing RM plans and registers, and providing overall program assistance and tools. Often, the risk champion basically acts as a facilitator and aggregates and compiles risk information received from risk-related functions usually embedded into the standard functional departments whereas, the CRO is a more empowered advisor, with direct visibility to the board, often through an independent line, by being part of top management decision forums with more substantive input to the functional heads or the program owners who often owns, monitors and manages key company risks. Intermediate schemes may also exist based on the level of risk aggregation and integration across the organization and the level of involvement of the risk champion in actively managing the risks in cooperation with the functional managers.

The choice of the CRO function is more associated with a more complex and rapidly evolving risk profile when the RM culture and processes are not sufficient or robust enough to allow functional managers to address their operational risks. For organizations in the corporate or the road sector, having a CRO is usually more pertinent to RM frameworks that exhibit the highest or the two highest levels of maturity as presented in Section 3.3. In composing a RM Committee care must be exercised to avoid limitations that may be inferred from lack of capabilities and/or specific mind-set. A RM Committee may instill the specialized vocabulary and the independent RM oversight needed but also account for risk-return trade-offs in strategic planning. Furthermore, existence of such teams and practices could not only balance the competing risk preferences of different stakeholders but are also well received by different stakeholders which, in turn could create value for the shareholders when perceived in the context of Corporate Social Responsibility, [63], [64].

Though there exist companies that have proven successful in managing risks as a core part of the management responsibilities without the existence of such explicit roles, usually such success derives from a strong RM culture and effective RM processes provided that risks do not overlap organizational boundaries, which is a rather exceptional combination of circumstances [52].

*Top-down and bottom-up approach*

The shortcomings of each approach have been discussed in Section 3.1. Instilling a RM culture and practice across the organization and balancing risk and rewards optimally is the responsibility of top management and that is where the ERM process should start, a claim that is also supported by studies in industrial and organizational psychology that find that macro-organizational factors significantly influence firm-level risk taking and profitability [65]. The organization's leadership with the assistance of the enterprise level Risk Committee and the CRO must determine the ERM framework and clearly define the dedicated resources, the RM policy and align it with the organization's strategic objectives. A risk taxonomy tailored to the organization's context may provide broad categories of risks or clarity with respect to the 5-10 most important risks that may influence the objectives to facilitate subsequent risk assessments and risk aggregation. This is a good starting point for risk owners, depending on the ERM structure, to conduct self-control risk assessments tailored to the specificities and resources of their units/programs in a bottom-up process.

What is important to comprehend is that the implications of ERM implementation and related risk treatment actions in the organization's objectives are a bottom-up exercise. Important elements of the bottom-up part of the ERM include the formation of a RM culture through detailed policies and guidelines on key risks, a regular and comprehensive process for risk identification, assessment, treatment, communication, and reporting and embed these into regular management processes, appropriate tools and methodologies, and escalation mechanisms that may elevate risks to different levels.

In this context, the organization's front-liners and middle managers possess better insight in relation to the risks faced and their input may modify or even expand the scope of the ERM in a continuous, circular, and integrated top-down and bottom-up process. ERM is a living process, not a one-off exercise. The importance of the top-down process is primordial as while bottom-up oversights may create RM inefficiencies, it is flaws and gaps in the top-down part of the cycle that may drastically limit the effectiveness of the ERM [52].

*Risk assessment, treatment, and RM tools*

The ISO 31000:2009 includes risk identification, risk analysis and risk evaluation in the risk assessment process. Risk identification is strongly dependent and influenced by the context setting and the experience of the team members involved. A thorough understanding of the nature of the risk, including how, why and where it is sourced, facilitates the selection of the risk treatment method and may indicate the appropriate level of depth for the risk analysis. Managers closest to the source of risks are often the best positioned to understand their nature and root

causes and propose appropriate actions called risk treatments. *Risk statements* that help differentiate actual risks from their causes and impacts are helpful to this respect [66].

In Section 3.1 we referred to the problem that 'data-poor' risks pose to their quantification. In the road sector there may be strategic, operational or reputational risks that may be difficult to quantify and assessments may rely on semi-quantitative or qualitative judgments. Risks fall under three categories: the known-knowns, the known-unknowns which may usually be quantified and constitute variability and the unknown-unknowns, which are considered as uncertainty and are difficult to measure, usually through qualitative expert judgments, scenario planning techniques or complex and computationally expensive modeling techniques such as Monte Carlo operations. The uncertainties in these risk assessments need to be thoroughly understood by decision makers.

Overly sophisticated models that rely on poor data or that are applied to non-crucial risks may result in excessive use of resources or to erroneous basis for decision-making. Risk matrices or heat maps do not always reflect the uncertainty that is inherent in these assessments. Qualitative and semi-quantitative techniques may be used for screening risks whereas more expensive quantitative methods may be used for a more in-depth analysis of selected key risks. When ERM is in the initial stages of implementation, starting with simple tools and systematically introducing more complex tools, as needed, as the process evolves and experience is gained may be the way to make ERM integration more appealing to the entire organization.

A special category of risks, those with low likelihood of occurrence but with catastrophic consequences, merits special consideration as it is often difficult to justify required resources to address these disasters ex-post or to defend the appropriateness of the ERM framework when these occur. Road organizations cannot adequately respond to these major disasters nor can they tolerate their likelihood. As a result, road management authorities tend to rely on gradually and continuously building the organization's and road network's redundancy, robustness, and resilience [47]. Redundancy may be defined as the excess or duplicative capacity that can be used in emergency situations. Robustness is the capacity in coping with stress and withstanding disturbances. Resiliency is the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events. A general RM treatment related to resiliency is scenario planning and preparedness through business continuity plans (BCPs) and Disaster Reduction Plans (DRPs) [67], [68].

Aggregating risk exposures across the organization will result in the organization-wide risk profile. Dashboards and risk maps are good tools to summarize these findings. However, aggregating risks is not always trivial and correlations between risks should not be overlooked but understood. The common way to aggregate risks is to

translate their consequences to a common metric such as a monetary value. Calculating monetary values though for certain types of risks (e.g. country risk, reputational risk) is not always easy or even possible.

Risk evaluations concern the comparison of the risks against the predetermined tolerances and thresholds and their prioritization for treatment. ISO 31010:2009 [69] includes a variety of risk assessment techniques and a description to which procedure of the risk assessment process these techniques are most applicable. Specific RM applications of these techniques and RM methodologies to road operations are reported in [70] and [39].

Risk treatment options include tolerating the risk (e.g. risk below threshold or outside of the organization's capability or authority), treating (mitigating), transferring (sharing; e.g. purchasing insurance or through private public partnerships) and terminating (e.g. eliminate a source of risk or stop a practice). It is important to recognize that risk treatment actions may change these correlations or even introduce new risks. Thus, risk analysts should not only be aware of the original risks but also of residual risks after treatment, new risks that may be introduced by risk treatment actions and risk interactions.

Risk treatment, though carrying a connotation that is mostly relevant to threats, should also apply to opportunities (i.e. sharing, exploiting, enhancing) as a regularly selected or at least considered option so that an opportunity may be pursued when its potential benefit exceeds the likelihood of negative consequences. Examples in the road sector may include trying new construction materials and techniques, PPPs, implementing information technology systems or dropping low-return assets processes and functions. All risk treatment recommendations would need approval from higher-level risk owners before being implemented.

There are three major tools in providing RM capabilities:

- Training and coaching of employees and key personnel in regard to risk-related competencies is a must for an organization that aspires to implement an integrated ERM. People should understand how to deal with the risks and the inherent uncertainties and become familiar with basic risk concepts and frameworks.
- RM plan and handbook: a RM plan is the *'result of the process that determines the approach, the design of actions and the resources for managing risks'* [1] and may be elaborate to the extent of becoming a RM guide or handbook. RM plans may include RM processes, methodology, areas of practice, roles and responsibilities, budget, time sequence of activities, measurement methods, thresholds, and units. RM guides or handbooks are usually more comprehensive and detailed than RM plans in that they may include templates for risk registers, risk policy and RM plan, reporting formats and cycles, reporting and communication protocols, relevant training and performance levels expected and guidance on how to

develop risk statements that help differentiate actual risks from their sources and effects, conduct risk analyses and develop risk tolerances.

- Risk website or other repository for sharing risk relevant information (e.g. risk registers, risk analysis and relevant data) and facilitate transparency.

*Communication, monitoring and reporting*

Clear, two-way communication is essential for an effective ERM and should extend to both internal and external stakeholders in a consultative approach with clear protocols for information and communication flow up, down, across, in and out of the organization. Stakeholders are often needed to support RM actions. Their expectations should be clearly defined and communicated and ascertained that are in concordance with the mission and vision of the organization. The CRO of risk expert needs to foster dialogue between the involved parties in creating a common sense of risk appetite, tolerance, and language [31].

The monitoring and review framework should aim in validating that the RM process is relevant, documented and performs according to expectations. The scope and frequency altogether with who and how must be defined in a documented procedure such as a RM plan or guide. Regular, fact-based and timely discussions on the RM scope, objectives, processes, review findings, risk considerations and relevant actions should extend beyond a risk register or a risk heat map and must be clearly communicated to the relevant parties in form and timeframe that allow people to carry out their responsibilities.

Risks are dynamic in their nature, keep evolving and thus need both periodic and ad hoc review. Estimates of relevant threats and opportunities and their likelihood and related consequences may change over time. Monitoring the organization's context for changes in risks or emerging risk exposures should rely on the good understanding of its context, the established processes and procedures and existing controls. Appropriate indicators, often referred to as *Key Risk Indicators (KRIs)*, that signal emerging trends and anticipate changes in the context setting (external and internal), should complement monitoring the evolution of identified risks. KRIs may also notify about the emergence of new risks not previously identified, or that have been identified but for which risk treatment is not effective in bringing these to the defined tolerance levels.

Relevant risk information should be stored in risk repository or website and regularly updated. A risk register usually forms the basis for reporting and communicating risks to risk owners and stakeholders. Transparency induced by RM documentation and access to relevant information in relation to the rationale for RM choices are

reported as key success factors for implementing an ERM framework and add to the organization's credibility, often crucial to stakeholders [66].

### *5.2 ERM implementation guidance*

Implementation of an ERM framework involves significant change management, and relies on the degree to which leadership embraces the change, the centralization, complexity, and cohesiveness of the internal management structures for accepting direction and the degree of the external influence and its infiltration to the organization [71].

The essence of the aforementioned key principles is that ERM should be kept simple enough and not expensive in order to be embraced by the organization's staff. Expert judgment and experience are important assets in ERM. Complex analysis tools may not substitute for active management of risks by risk managers. As complex as ERM implementation may appear, it does not have to be and in practice successful practitioners report that '*only a few key staff are needed to support it as long as leadership embraces it and staff throughout the organization incorporate it into normal management activities'* [47].

The generic value proposition of ERM may not be sufficient to top management for moving forward with a full-scale implementation. In light of scarce resources, an enterprise risk assessment complemented by a gap analysis of the organization's RM capabilities concerning its priority risks should provide the more detailed articulation to drive top management's decision in investing in ERM infrastructure. The greater the gap between the existing capabilities and the desired state of RM, the more compelling is the need for ERM implementation [50]. The following sections propose an ERM implementation framework and discuss considerations in measuring the ERM added value, which is an active area for research.

*Implementation roadmap, concepts, and practical tools*

ERM implementation roadmap steps are proposed and briefly discussed by considering the ERM principles in Table 5. Practical concepts and tools that apply to these steps are also listed.

*Measuring ERM added value*

While an effective ERM provides a better understanding and management or threats and opportunities, it nevertheless does not eliminate the threats. As such, highly unlikely risks may still materialize and thus the effectiveness of the ERM should not be based on this account. Also, ERM may offer valuable insights in relation to *potential* risks that have not necessarily materialized or happened, which is not necessarily reflected through

actual financial or other performance [3]. The role of the ERM is to limit the probability of such outcomes to an agreed-upon value-maximizing level to support informed decision-making [55]. Risk communication and stakeholder engagement are vital in this process. When risks are well managed, understood and communicated, stakeholders should be able to differentiate between bad luck and bad management and keep in the confidence and trust the organization needs for attracting resources that may be allocated in valuable projects. Integration of RM into strategic planning and operational processes, improved risk identification and preparedness, increased risk awareness, fact-based risk assessments and decision-making that replace guesswork should be apparent or "felt" at the very least to practitioners. But, how to concretely measure the ERM implementation success and added value?

Skepticism may be raised in the RM practice and research community in the absence of a consistent measure and widely accepted measure of effectiveness of ERM implementation that uncontestably demonstrates its added value [3]. Difficulty also arises because managerial perceptions may interpret or assess risks differently from objective measures of risk, which in turn influences their behavior [72]. A way of measuring its direct cost to the organization would be to keep track of personnel time that relates to RM activities, especially in the early stages of ERM implementation. However, as ERM becomes progressively ingrained into the organization's daily activities, it becomes more difficult to distinguish ERM related activities from regular managerial activities and measuring the relevant costs and benefits is not an easy process. Scaling-back projects and programs to focus on their most important risks is a way of bringing the RM cost in more commensurate levels. For example, a risk analysis may indicate that mechanical ventilation and time closure after an accident may be the key factors in successfully responding to a tunnel accident and focus in addressing these issues in priority.

Measuring the benefits is a different challenge. It has been argued that standard corporate performance criteria (e.g. Tobin's Q, ROA, Economic Capital, RAROC, TCOR) do not necessarily fully capture the ERM performance or added value in relation to the achievement of the firm's objectives that may be beyond shareholder profit [3], [73]. Organizations outside of the financial and accounting sectors tend to rely on key performance indicators (KPIs). Ex-post quantitative indicators of ERM performance of events (ERM KPIs) that occurred during a reporting period and summarize the frequency (e.g. number of road accidents in a time period) and impact severity (e.g. maximum duration of disruption of the road network; number of fatalities; cost of mitigation measures) may be used for measuring the ex-post added value of ERM. Reduced performance variability in KPIs is another way though it may be challenging to delineate the ERM contribution from other managerial activities. Use of traditional financial metrics such as the cost of capital (borrowing cost over share valuations), ROI and ROE or non-financial

(e.g. customer satisfaction, market share, brand image) may be indirect measures of ERM effectiveness, however the exact correlation may be difficult to infer.

KRIs are emerging for anticipating and monitoring risks. These differ from KPIs in the sense that they are forward-looking in time by providing advance warning, often referred to as early warning indicators whereas KPIs are backward looking by evaluating achieved performance. In establishing KRIs, risk registers may provide the necessary insight on to which KRIs may be selected in forecasting likelihood of achieving performance goals. Monitoring commodity prices (e.g. oil, diesel, cement, steel), construction price trends, equipment downtime, staff sick-days and achievement of early project milestones may be examples of KRIs for the road transport sector.

As road transport agencies perceive RM to be the mirror image to performance management [47], integrating RM with KPI reporting in the form of risk maps for each of the KPIs on its balanced scorecard or including KRIs in the balanced scorecard [74] may provide means to decision makers for risk-based decision making and could guide prioritization in addressing those risks and improving performance over time. Tracking the performance evolution of key risks over time, risk incidents and near misses could guide prioritization in addressing those risks and improving performance over time and constitute good practices in support of the ERM added value. Nevertheless, producing metrics that clearly demonstrate the added value of the ERM framework and link its implementation with the improved performance of an organization in achieving its strategic objectives remains a challenge and very active area of research [3].

## 6. SUMMARY AND CONCLUSIONS

Implementation of ERM frameworks in the road sector is lagging in comparison to the financial sector and often needs broader considerations that expand beyond the traditional focus on financial and regulatory risks primarily addressed in financial risk management. However, the benefits and added value obtained from implementing organization-wide RM frameworks are being increasingly recognized and ERM practice is expanding in the road sector. This study presented a variety of ERM frameworks applied in the road sector that considered different approaches and structures in implementing organization-wide RM.

There is no single methodology for implementing an ERM framework that suits all organizations. An ERM framework should be tailored to the unique context and culture of each organization. Imagination and creativity are powerful tools when designing an ERM framework. Experience and expert knowledge of the subject matter though are required competences for the aspiring practitioner. Due to the variety of existing methodologies,

techniques and tools, the task may appear daunting, with unclear benefits and often difficult to quantify, and this may discourage top management from pursuing it. This study presented the key drivers and benefits to be expected from ERM implementation, identified the different configurations for ERM structure and summarized the key principles that need to be considered in implementing an ERM framework. An ERM implementation framework with a roadmap, relevant concepts and tools and a discussion on the challenges of measuring the added value of the ERM framework, which is critical in advocating for it, have been presented. As aforementioned in Sections 2, a limitation of our study is that only a preliminary validation of our proposed framework has been performed the matching of our theoretical proposition with implementation practice presented at an International Conference and the positive feedback in relation to their experience from road risk management experts participating in focus groups and international seminars. A full validation would need to consider feedback from several actors that actually implemented ERM through the proposed approach.

Management must recognize that ERM is a journey, neither a project nor a destination, within the context of strategy setting that represents a commitment to continuous improvement. Organization-wide RM practices and culture take time to develop. The following conclusions are drawn:

a) ERM is a key component of strategy setting and management that may improve an organization's achievement of strategic objectives by supporting strategic planning with performance management.

b) Several governmental road agencies and private road organizations have introduced ERM to some extent. Every successful organization faces, takes, and responds to risks. Different RM approaches may be followed at the enterprise level. The organization's context, the strategic objectives and the stakeholder's expectations and perceptions will greatly influence the selection of appropriate methods and tools in moving forward with ERM implementation. Communication and consultation with stakeholders, transparency and information sharing are key in establishing the trust and confidence to the endeavor. Ensuring ownership and accountability of critical risks and establishing a thorough understanding of the organization's threats and opportunities and RM capabilities is critical to successful implementation.

c) ERM must be kept simple and not overly complicated. Only a few staff are needed on a full-time basis to advance the process. However, ERM will fail if a risk culture is not conveyed to all personnel of the organization. Defining the risk culture with clear risk policies, risk appetites, tolerances and thresholds is the responsibility of top management. Top management must lead the endeavor and be genuinely committed and actively engaged to it to allow the organization to embrace and practice the risk culture.

d) ERM implementation must be a gradual and progressive process. Road organizations should develop their own risk taxonomies that reflect the mechanisms through which the different risks may affect them to properly anticipate, prepare, monitor, and respond to these in a continuous exercise. Attempting to consider everything at once when lacking the experience and the maturity in the process may prove highly inefficient with dubious outcome. Considering the limitation of resources, a practical approach is to select a few key risks that pertain to the strategic objectives and proceed with managing these across the organization in a progressive process that establishes the infrastructure and instills the experience needed to bridge gaps between current and intended performance and advance the maturity level of ERM. Documentation of the process and of the learned lessons, monitoring and measuring the process, and appropriate reporting and review must be performed for ERM capacity building.

e) PIARC [9] recommends that key to ERM promotion is the proofing that *'spending money on RM can generate net benefits in the form of avoided future documented consequences'.* Those consequences should cover both direct (e.g. damages to road infrastructures, financial losses from tolls, lawsuits costs and claims) and indirect costs (e.g. damages to surrounding infrastructures, medical costs, environmental and other economic impacts, time loss). It further recommends that RM policies should focus in making the evaluation of such risks costs a mandatory activity and consider these costs along with the proposed optimal risk treatment solutions in managing the risks.

f) [75] argue that project management should be business-focused and linked to the organization's strategies to effectively deliver those strategies. To this respect, performance measures should be *outcome-based* and oriented in measuring the effectiveness of the project in relation to the business' objectives instead of being *output-based* and measure how well the project management process is delivered (efficiency) with the traditional budget, cost, and quality considerations. In relation to ERM, the KSFs articulated in the business case may be used to evaluate the ERM proposition over time and establish the linkage between the achievement of strategic objectives and the management of risks. The present overview of ERM practice has identified a few key areas of potential interest for further research:

A more complete understanding is needed regarding the distribution of an organization's value and how this is affected by the achievement of the strategic objectives to which ERM aims at supporting. As such, a recommendation for further research is the development of appropriate metrics and methodologies that relate the effectiveness of ERM performance to achieving the organization's strategic objectives to clearly demonstrate the resulting benefits.

In evaluating organization-wide risk, aggregating risks from different sources and levels is often needed. However, individual risks do not use the same metric for consequences. Moreover, correlations between different types of risk are also essential in measuring organization-wide risk and some risks such as reputational and strategic are often difficult to reliably quantify. As *the measurement of risk presents a variety of research opportunities for management scholars,* so does their aggregation in an organization-wide context and even more so, as *different casual mechanisms may occur* that *may influence managerial and firm behavior* [3]. In practice, risk maps and dashboards are used that rely on imposed rules of thumb (e.g. if more than two risks pertaining to a certain project or risks from two different projects under a common program are above their risk tolerance levels then the risk level is elevated to the Program level) as existing literature provides little insight for aggregating different risks and for estimating these correlations. Advanced modeling techniques such as computationally expensive Monte Carlo simulations are used when risk aggregation is possible. Consistent methods for accounting for risk correlations and for risk aggregation with quantifiable metrics need to be developed that do not overly complicate the risk assessment effort and may provide reliable risk oversight at the enterprise level.

We believe that our work offers a systematic implementation framework for ERM that addresses the *'how to proceed'* question. The proposed roadmap could be implemented by road transport sector related organizations irrespectively of their maturity level as they may be able to identify elements or processes that can be added to their current practice for further advancing it either in depth, breadth, or both so as to achieve better use of their resources, including time, in a systematic and structured ERM implementation approach in support of their organization's strategic objectives notwithstanding of course of the aforementioned limitations and challenges in measuring the ERM's added value. The basic concepts and roadmap steps that are proposed may be also suitable for industries other than the road transport sector that lack specific regulatory context and guidance for implementing an ERM framework.

**REFERENCES**

**[1] International Organizations for Standardization (ISO). 2009a.** ISO 73:2009 Risk Management – Vocabulary. Geneva, Switzerland.

**[2] International Organizations for Standardization (ISO). 2009b.** *ISO 31000:2009 Risk Management – Principles and Guidelines*. Geneva, Switzerland.

**[3] Bromiley P, McShane M, Nair A, Rustambekov E. 2015.** *Enterprise Risk Management: Review, Critique, and Research Directions*. Long Range Planning. Aug 1, 48(4):265–76. DOI: 10.1016/J.LRP.2014.07.005.

**[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2017.** *Enterprise Risk Management – Integrating with Strategy and Performance*. AICPA. NJ, USA. June.

**[5] Project Management Institute (PMI). 2013.** *A Guide to the Project Management Body of Knowledge. PMBOK Guide – 5th Edition*. ISBN 978-1-935589-67-9. Project Management Inc., Pennsylvania, USA.

**[6] Merna, T. and F. F. Al-Thani. 2008.** *Corporate Risk Management*. 2nd Edition. ISBN 978-0-470-51833-5. John Wiley & Sons, Ltd. West Sussex, UK.

**[7] CIB TG 32, 2001.** *Risk assessment and risk communication in civil engineering.* Report 259. ISBN: 90-6363-026-3. Rotterdam.

**[8] Chapman, J. R. 2011.** *Simple Tools and Techniques for Enterprise Risk Management*. 2nd Edition. ISBN 978-1-119-98997-4. John Wiley & Sons, Ltd. West Sussex, UK.

**[9] PIARC (World Road Association). 2016a.** *Role of Risk Assessment in Policy Development and Decision-Making*. PIARC Technical Committee 1.5 – Risk Management. 2016R09EN. ISBN: 978-2-84060-388-7. Paris, France.

**[10] Benekos, I., Mavromatis, S., Laiou, A., Yannis, G., 2019.** *The use of Intelligent Transportation Systems (ITS) in risk and emergency management for road transport planning and operation*, ITE Journal, January, pp. 44-49.

**[11] PIARC (World Road Association). 2019.** *Evaluation of Organizational Approaches to Risk*. Technical Committee A.3 – Risk Management, 2019R16EN. ISBN: 978-284060-535-5. Paris, France.

**[12] Institute of Risk Management (IRM). 2018.** *A Risk Practitioners Guide to ISO 31000:2018 – Review of the 2018 version of the ISO 31000 risk management guidelines and commentary on the use of this standard by risk professionals*. London, UK.

**[13] Institute of Risk Management (IRM). 2018.** *From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks – Review of the 2004 and 2017 Enterprise Risk Management (ERM) frameworks published by COSO and commentary on the use of these frameworks by risk professionals*. London, UK.

**[14] Plambeck, N., Weber, K., 2010.** *When the glass is half full and half empty: CEOs' ambivalent interpretations of strategic issues.* Strategic Management Journal, 31 (7), 689-710. DOI: 10.1002/smj.835.

**[15] Benekos, I. 2018.** *A Proposed Roadmap for Implementing Enterprise Risk Management*. International Seminar on Disaster and Risk Management for Roads, Hanoi, Vietnam, November 7-9, 2018, Seminar Proceedings.

**[16] Van Den Bossche, E. 2019.** *Lessons Learned from Application of Organizational Risk Management*. International Seminar on Disaster and Risk Management for Roads, Hanoi, Vietnam, November 7-9, 2018, Seminar Proceedings.

**[17] Benekos, I., Yannis, G. 2019.** *A Proposed Approach for Implementing Enterprise Risk Management in Road Organizations*, World Road Association (PIARC), Roads/Routes, Issue No 380, pp. 22-25.

**[18] Haimes, YY., 1992.** *Toward a holistic approach to total risk management*. The Geneva Papers on Risk and Insurance 17 (64), 314-321. DOI: 10.1057/gpp.1992.20.

**[19] Colquitt, L.L., Hoyt, R.E., Lee, R.B., 1999.** *Integrated risk management and the role of the risk manager*. Risk Management and Insurance Review 2 (3), 43-61. DOI: 10.1111/j.1540-6296.1999.tb00003.x.

**[20] Dickinson, G., 2001.** *Enterprise risk management: its origins and conceptual foundations*. The Geneva Papers on Risk and Insurance-Issues and Practice 26(3), 360-366. DOI: 10.1111/1468-0440.00121.

**[21] D'Arcy, S.P., Brogan, J.C., 2001.** *Enterprise risk management*. Journal of Risk Management of Korea 12 (1), 207-228.

**[22] Miller KD, Waller HG. 2003.** *Real Options and Integrated Risk Management*. Long Range Planning. Feb 1;36(1):93–107. DOI: 10.1016/S0024-6301(02)00205-4.

**[23] Beasley MS, Clune R, Hermanson DR. 2005.** *Enterprise risk management: An empirical analysis of factors associated with the extent of implementation*. J Accounting and Public Policy. Nov 1; 24(6):521–531. DOI: 10.1016/J.JACCPUBPOL.2005.10.001.

**[24] Hoyt RE, Liebenberg AP. 2011.** *The Value of Enterprise Risk Management*. J. Risk Insurance. Dec 1; 78(4):795–822. DOI: 10.1111/j.1539-6975.2011.01413.x.

**[25] Gordon LA, Loeb MP, Tseng C-Y. 2009.** *Enterprise risk management and firm performance: A contingency perspective*. J Accounting and Public Policy. Jul; 28(4):301–327. DOI: 10.1016/J.JACCPUBPOL.2009.06.006.

**[26] Mikes, A. 2009.** *Risk management and calculative cultures*. Management Accounting Research. Mar; 20(1):18–40. DOI: 10.1016/J.MAR.2008.10.005.

**[27] Kaplan, R.S., Mikes, A. 2012.** *Managing risks: A new framework*. Harvard Business Review 90 (6): 48-60.

**[28] Zhao X, Hwang B-G, Low SP. 2014.** *Investigating Enterprise Risk Management Maturity in Construction Firms*. J. of Construction Engineering and Management. Aug; 140(8):05014006. DOI: 10.1061/(ASCE)CO.1943-7862.0000873.

**[29] Zhao X, Hwang B-G, Pheng Low S, Wu P. 2015.** *Reducing Hindrances to Enterprise Risk Management Implementation in Construction Firms*. J. of Construction Engineering and Management. Mar; 141(3):04014083. DOI: 10.1061/(ASCE)CO.1943-7862.0000945.

**[30] Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004.** *Enterprise Risk Management – Integrated Framework*. AICPA. NJ, USA. September.

**[31] Bowling, DM, Lawrence R. 2005.** *Success factors for implementing enterprise risk management: building on the COSO framework for enterprise risk management to reduce overall risk*. Bank Accounting & Finance, Apr.-May 2005, p. 21+. Academic OneFile.

**[32] International Organization of Supreme Audit Institutions (INTOSAI). 2004.** *Guidelines for Internal Control Standards for the Public Sector*. INTOSAI Professional Standards Committee. Copenhagen, Denmark.

**[33] HM Treasury. 2004.** *The Orange Book – Management of Risk – Principles and Concepts*. HM Treasury, U.K. Government, London, UK. October.

**[34] PIARC (World Road Association). 2012a.** *Managing Operational Risks in Road Operations*. PIARC Technical Committee C.3 – Managing Operational Risks in Road Operations. 2012R13EN. ISBN: 978-2-84060-265-2. Paris, France.

**[35] Purdy G**. **2010.** *ISO 31000:2009-Setting a New Standard for Risk Management*. Risk Analysis. Apr 8; 30(6):881–6. DOI: 10.1111/j.1539-6924.2010.01442.x.

**[36] International Organizations for Standardization (ISO). 2018.** *ISO 31000:2018 Risk Management – Principles and Guidelines*. Geneva, Switzerland.

**[37] PIARC (World Road Association). 2010.** *Towards Development of a Risk Management Approach*. PIARC Technical Committee 3.2 – Risk Management for Roads. 2010R01EN. ISBN: 2-84060-230-X. Paris, France.

**[38] Hallowell MR, Molenaar KR, Fortunato BR. 2013.** *Enterprise Risk Management Strategies for State Departments of Transportation*. Journal of Management in Engineering. Apr.; 29(2):114–21. DOI: 10.1061/(ASCE)ME.1943-5479.0000136.

**[39] PIARC (World Road Association). 2016b.** *Methodologies and Tools for Risk Assessment and Management Applied to Road Operations*. PIARC Technical Committee 1.5 – Risk Management. 2016R12EN. ISBN: 978-2-84060-394-8. Paris, France.

**[40] Standards Australia. 2004.** *Risk Management AS/NZS 4360:2004*. 3rd Edition. ISBN 0-7337-5904-1. Standards Australia International Ltd., Sydney, Australia and Standards New Zealand, Wellington, New Zealand. August.

**[41] Standards Australia. 2005.** *Risk Management Guidelines: Companion to AS/NZS 4360:2004*. Standards Australia International Ltd., Sydney, Australia and Standards New Zealand, Wellington, New Zealand. December.

**[42] New South Wales Treasury. 2012.** *Risk Management Toolkit for NSW Public Sector Agencies Volume 1: Guidance for Agencies*. New South Wales Government, Sydney, Australia.

**[43] Ministry of Transportation of Quebec (MTQ) 2011.** *Report on Risk Management in the Road Sector.* Ministère des Transport du Québec. ISBN: 978-2-550-62581-0. Montreal, Canada. August.

**[44] Ministry of Public Security of Quebec (MPS) 2009.** *Risk Management Guide in Civil Protection*. Gouvernement du Québec. ISBN: 978-2-550-54257-5. Montreal, Canada.

**[45] Hansen, J. and Nilsson, L. 2006.** *Risk Management Method in the Swedish Road Administration*. The Swedish Road Administration. Sweden.

**[46] Highways Agency (HA). 2009.**

http://webarchive.nationalarchives.gov.uk/20091115020651/http://www.highways.gov.uk/aboutus/10873.htm.

**[47] American Association of State Highway and Transportation Officials (AASHTO). 2016.** *AASHTO Guide for Enterprise Risk Management.* 1st Edition. AASHTO. USA.

**[48] McKinsey. 2012.** *Enterprise risk management: What's different in the corporate world and why*. McKinsey Working Papers on Risk, Number 40. McKinsey & Company. December.

**[49] The Association of Insurance and Risk Managers (AIRMIC), The Public Risk Management Association (ALARM) and The Institute of Risk Management (IRM). 2010.** *A structured approach to Enterprise Risk Management (ERM) and the requirements to ISO 31000*.

**[50] Protivity. 2006.** *Guide to Enterprise Risk Management: Frequently Asked Questions*. Protivity Inc., January.

**[51] Power, M. 2009.** *The risk management of nothing*. Accounting Organization and Society. Aug; 34(6–7):849–855. DOI: 10.1016/J.AOS.2009.06.001.

**[52] McKinsey. 2010.** *Top-down ERM: A Pragmatic Approach to Managing Risk from the C-Suite*. McKinsey Working Papers on Risk, Number 22. McKinsey & Company. August.

**[53] Brancato, C., Tonello, M., Hexter, E. and Newman, K.R. 2006.** *The Role of U.S. Corporate Boards in Enterprise Risk Management*. The Conference Board Research Report No R-1390-06-RR. The Conference Board, Inc. ISBN: 0-8237-0878-0. USA.

**[54] Boulton, E. S. R., Libert, D. B., and Samek, S. M. 2000.** *A Business Model for the New Economy.* Journal of Business Strategy, Vol. 21 Issue: 4, pp.29-35, https://doi.org/10.1108/eb040102.

**[55] Nocco, W. B. and R. M. Stultz. 2008.** *Enterprise Risk Management: Theory and Practice*. Journal of Applied Corporate Finance. Vol. 18 (4).

**[56] Gates, S. 2006.** *Incorporating Strategic Risk in Enterprise Risk Management*. International Conference on Strategic Management. Geneva, Switzerland. June.

**[57] Vroom, V.H. 2000.** *Leadership and the Decision-Making Process.* Organizational Dynamics. 28(4): 82-94.

**[58] Carnegie Mellon University (CMU). 1994.** *The Capability Maturity Model: Guidelines for Improving the Software Process*. Software Engineering Institute, Carnegie Mellon University. USA.

**[59] HM Treasury. 2009.** *Risk Management Assessment Framework: A Tool for Departments*. HM Treasury, U.K. Government, London, UK. July.

**[60] Victoria Department of Treasury and Finance (Victoria DTF). 2012.** *Victorian Government Risk Management Framework*. Victorian Governement. Melbourne, Australia. March.

**[61] PIARC (World Road Association). 2012c.** *Social Acceptance of Risks and Their Perception*. PIARC Technical Committee C.3 – Managing Operational Risks in Road Operations. 2012R30EN. ISBN: 978-2-84060-298-9. Paris, France.

**[62] Brooks, D.W., 2010.** *Creating a risk-aware culture.* In Fraser, J., Simkins, B., (Eds.), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives.* Kolb series in Finance. John Wiley & Sons, Inc., Hoboken, NJ, pp. 87-95. ISBN: 978-0-470-49908-5.

**[63] Godfrey PC, Merrill CB, Hansen JM., 2009.** *The relationship between corporate social responsibility and shareholder value: an empirical test of the risk management hypothesis.* Strategic Management Journal, 30(4):425–445. DOI: 10.1002/smj.750.

**[64] Adam AM, Shavit T., 2009.** *Roles and responsibilities of boards of directors revisited in reconciling conflicting stakeholders interests while maintaining corporate responsibility.* J. Management & Governancel, 13(4):281–302. DOI: 10.1007/s10997-008-9076-3.

**[65] Power, M. 2009.** *The risk management of nothing.* Accounting Organization and Society. Aug; 34(6–7):849–855. DOI: 10.1016/J.AOS.2009.06.001.

**[66] Bromiley, P., Rau, D., 2010.** *Risk in strategic decision-making.* In: Zedeck, S. (Ed.), American Psychological Association's Handbook of Industrial and Organizational Psychology, pp. 161-182.

**[67] PIARC (World Road Association). 2016c.** *Risk Management for Emergency Situations*. PIARC Technical Committee 1.5 – Risk Management. 2016R26EN. ISBN: 978-2-84060-424-2. Paris, France.

**[68] PIARC (World Road Association). 2016d.** *Risk Management for Emergency Situations – APPENDIX A&B*. PIARC Technical Committee 1.5 – Risk Management. 2016A26EN. ISBN: 978-2-84060-426-6. Paris, France.

**[69] International Organizations for Standardization (ISO). 2009c.** *ISO 31010:2009 Risk Management – Risk Assessment Techniques*. Geneva, Switzerland.

**[70] PIARC (World Road Association). 2012b.** *Risks Associated with Natural Disasters, Climate Change, Man-Made Disasters and Security Threats*. PIARC Technical Committee C.3 – Managing Operational Risks in Road Operations. 2012R12EN. ISBN: 978-2-84060-333-7. Paris, France.

**[71] Rogers, E. 2003.** *Diffusion of Innovation.* 5th Edition. Free Press. ISBN: 978-074322-209-9. London, UK. August.

**[72] March, J.G., Shapira, Z., 1987.** . *Managerial perspectives on risk and risk taking*. Management Science 33 (11), 1404-1418. DOI: 10.1287/mnsc.33.11.1404.

**[73] Freeman, R.E., Harrison, J.S., Wicks, A.C., Parmar, B.L., De Colle, S., 2010.** *Stakeholder Theory: the State of the Art*. Cambridge University Press, Cambridge.

**[74] PricewaterhouseCoopers (PwC). 2008.** *A Practical Guide to Risk Assessment: How Principles-Based Risk Assessment Enables Organizations to Take the Right Risks.* PricewaterhouseCoopers Inc. December.

**[75] Frigenti, E. and Comninos, D. 2002.** *The Practice of Project Management: a guide to the business-focused approach*. ISBN: 0-7494-3694-8. Kogan Page. London, UK.

## TABLES AND TABLE CAPTIONS

**Table 1.** Shortcomings of top-down and bottom-up ERMs

| ERM approach | Common problems |
|---|---|
| **Top-down** | • Limited insight and depth of discussions relevant to risks<br>• Major decisions are not risk-based or contain insufficient information on risks involved<br>• Insufficient follow-up on risk mitigation actions by top management and ineffective risk oversight due to poor reporting<br>• Uniformity of views / perspective relative to risks shared by a small group of top management may hinder the bredth and open mind needed for effective RM<br>• Confusion instilled to middle management by the support of a performance management culture that does not balance risks and rewards and that is inconsistent with the RM policy |
| **Bottom-up** | • Timely identification and response to emerging risks<br>• Challenges in translating RM policy into action<br>• Difficulty in RM integration and RM culture establishment throughout the organization<br>• Variety of risk processes that collect relevant information<br>• Consideration of RM by middle management as a burden that adds to managerial tasks |

**Table 2. Differences between ERM and traditional RM**

| Attribute | RM | ERM |
|---|---|---|
| Objective | Protect the organization value | Protect *and enhance* the organization value |
| Scope | Finance, insurance and operations | Applies across all types of organizations and levels |
| Focus | Physical and financial (tangible) assets | Portfolio risk view including both tangible *and intangible* assets |
| Application | Selected risk areas primarily in finance, operations and internal controls | Strategy setting and RM tool applied across the organization to all sources of value in support of the strategic objectives while considering both internal and external factors |

**Table 3. Risk maturity model as adapted from AASHTO [47]**

| Maturity Level | Elements | Notes |
|---|---|---|
| 1. Awareness | • Adhoc and crisis driven<br>• Requires individual initiative<br>• Only threats managed | RM is done on an adhoc basis based on external pressures to achieve performance or to manage threats by motivated individuals without formalized RM process or policy. |
| 2. Initiating | • Only threats managed<br>• Some definitions and policies documented | Basic RM processes and procedures are developed. Key risks to strategic objectives or to critical project and programs may be identified, however, risks are not clearly defined and the RM process, policies and procedures are not clearly documented. |
| 3. Emerging | • Definitions and policies documented<br>• Covers most programs and activities<br>• Training offered but limited | Formal processes, policies, definitions and procedures are used to identify and manage risks. Opportunities are not regularly identified or exploited. Training is limited to key personnel only and the RM process does not extend to activities nor it affects frontline workers. |
| 4. Competent | As above but with widespread training plus:<br>• Mature policies and procedures<br>• Opprtunities managed<br>• Risk influences programming and activities<br>• Mature monitoring and communication of risks | RM is integrated in the organization with well-defined policies, processes, procedures, tools and training. Personnel understand risk appetites and tolerances applicable to their programs, projects and activities. Opportunities with potential for greater reward are pursued; RM influences decision making in strategic planning, programming and project selection. Risks are regularly monitored and stakeholders adequately informed. |
| 5. Excellence | As above plus:<br>• Costs and benefits documented<br>• Opportunities recognized and seized<br>• Leading risk indicators used<br>• Front lines manage risk and opportunities | Long standing experience and culture in RM. Documented history of cost savings, performance improvement and risk reduction. Risk are considered at all levels of the organization; all employees are properly trained and practice RM; metrics are established to justify the added value of RM. RM becomes a source of competitive advantage. |

**Table 4. References advocating for the proposed ERM practices**

| Practice | Relevant references |
|---|---|
| *Context of the organization and objective-setting* | [2], [4], [6], [8], [11], [15], [16], [17], [22], [27], [28], [30], [32], [33], [35], [36], [37], [40], [41], [42], [44], [47], [49], [50], [60], [66], [73], [74] |
| *Risk culture and strategy* | [2], [3], [4], [5], [8], [9], [11], [15], [16], [17], [28], [29], [30], [32], [33], [34], [36], [38], [40], [41], [42], [47], [49], [50], [52], [59], [60], [61], [62], [74] |
| *Championing ERM and governance* | [2], [3], [4], [8], [11], [15], [16], [17], [23], [24], [26], [29], [30], [32], [36], [38], [40], [41], [42], [47], [49], [50], [52], [53], [59], [63], [64], [74] |
| *Top-down and bottom-up approach* | [26], [38], [50], [52], [53], [55], [65], [74] |
| *Risk assessment, treatment, and RM tools* | [2], [4], [8], [11], [15], [16], [17], [30], [33], [36], [39], [47], [50], [66], [67], [68], [69], [70], [74] |
| *Communication, monitoring and reporting* | [2], [4], [5], [6], [7], [8], [11], [15], [16], [17], [22], [27], [28], [30], [31], [32], [33], [34], [35], [37], [36], [40], [41], [42], [43], [44], [45], [47], [49], [52], [53], [50], [59], [60], [66], [67], [73], [74] |

**Table 5. ERM framework implementation roadmap**

<table>
<tr><th colspan="3">1. LINK TO STRATEGIC PLANNING, SCOPE, AND MANDATE</th></tr>
<tr><th colspan="2">1A. Context of ERM in relation to strategic planning</th><th>1B. Executive mandate, ERM team and initial implementation plan</th></tr>
<tr><td colspan="3">Considerations: In step 1A the vision and scope of ERM are defined in relation to the strategic objectives using foresight methods (e.g. expert panels, SWOT analysis, Delphi analysis, PESTEL, scenario analysis, trend analysis, cross-impact analysis) that provide a systematic way in identifying changes, future needs, drivers, threats, and opportunities for building medium and long-term visions of RM development and support strategic decisions. The external environment is defined (PESTEL) and the organization’s context and strategic objectives in relation to the external environment are determined (SWOT). Stakeholder perceptions, their expectations and the KSFs are clearly understood and communicated. Ideally, the strategic planning (SP) team would consist of 6-8 members with relevant expertise in PESTEL factors and include the risk champion and, if possible, also members external to the organization. Performance goals and KPIs in relation to the strategic objectives are determined. An initial discussion of the major threats and opportunities relevant to the objectives may be conducted and documented. A brief RM policy statement may be elaborated to articulate the key benefits of ERM and provide initial direction in ERM implementation.<br><br>In step 1B top management establishes the central ERM team and ensures the necessary mandate, sponsorship and authority needed by the team to proceed with the scanning of the RM status and provide a proposition for further implementation. Senior management from key functions of the organization and the strategic planning team should compose the core ERM team to ensure active executive commitment, support and linkage to strategy setting. The team may be ideally composed of 8-12 members of different backgrounds, including external members, if possible, to provide the necessary width of views without compromising the efficiency and must be led by the risk champion who possesses in depth RM expertise. At this stage, a common risk language is established and ERM is considered more like a project. An initial plan and a project management system is put forward that specifies available resources, timing, project phases and milestones for investigating the ERM value proposition. Lines of accountability and responsibility are identified and communication protocols between the ERM team and executive management are defined.</td></tr>
<tr><td colspan="3">Concepts and tools</td></tr>
<tr><td>• PESTEL<br>• SWOT<br>• Brainstorming / Delphi</td><td>• Scenario planning<br>• Objective setting<br>• Balanced scorecard</td><td>• RACI matrix<br>• Stakeholder analysis<br>• KPIs – financial ratios</td></tr>
<tr><th colspan="3">2. RM STATUS, CAPABILITY ASSESSMENT AND VALUE PROPOSITION</th></tr>
<tr><th colspan="2">2A. Assessment of RM current practice and capabilities</th><th>2B. Value proposition</th></tr>
<tr><td colspan="3">Considerations: Top management may be reluctant to commit further resources to RM unless they clearly see the benefit from doing so. Step 2A aims at scanning the organization’s internal context and use it in conjunction with the external context and the applied strategy as a frame of reference in conducting an initial risk identification by defining broad categories of risks (risk taxonomy) or by using checklists in relation to the strategic objectives. An assessment of the current RM practice, existing capabilities (e.g. knowledge, infrastructure) and processes in place including relevant policies (formal and informal) must be conducted. The aim is to fully determine the prevailing RM culture and practice and level of ERM maturity and produce an organization-wide, portfolio view of risks and risk prioritization from usually qualitative or semi-quantitative risk assessments that mostly rely on expert judgments.<br><br>Step 2B aims at providing top management with the justification, economic if possible, for moving forward in committing additional resources for ERM implementation. A gap analysis of the current state of capabilities in relation to key risks or key risk categories may indicate further RM needs. This step should ultimately address the vision for the “how” for ERM capacity building and integration in terms of policy, infrastructure, and timeline. A compelling vision for the desired state of ERM capabilities and infrastructure (changes in the organization’s policy, competencies, RM oversight, processes, IT systems, tools, reporting and databases needed) must be articulated and risk appetite, tolerances and thresholds formulated at the level of analysis of Step 2A. Initially, ERM implementation may appear daunting to apply to the entire organization. Identifying the key business processes and decisions that pertain to the strategic objectives and arrange to support these with relevant risk-based processes, methodologies and tools is a good starting point. The expected key benefits from implementing the ERM vision must be clearly defined and communicated to stakeholders and relevant costs determined. The ERM vision, risk portfolio, and risk appetite, tolerances and thresholds should be reviewed by the SP team and the Board and endorsed to commit the necessary funds and personnel for ERM capacity building.</td></tr>
<tr><td colspan="3">Concepts and tools</td></tr>
<tr><td>• Risk checklists / databases<br>• Process / organizational flowcharts / maps<br>• Stakeholder risk profile analysis</td><td>• SWOT, workshops<br>• Gap analysis<br>• Risk taxonomy / dashboard / map</td><td>• Nominal group techniques<br>• Risk appetite, tolerance, thresholds<br>• Questionnaires, interviews</td></tr>
<tr><th colspan="3">3. ERM CAPABILITY DEVELOPMENT</th></tr>
</table>

| 3A. ERM architecture, policy, and protocols | 3B. RM process integration and implementation |
|---|---|

**Considerations:** Unless the maturity level of the organization's ERM framework is high, the aim of this step is to advance the organization's RM capabilities for selected *key risks* based on their prioritization and on cost-benefit and risk-return considerations performed in Step 2B to provide a starting point for ERM capacity building. Now that the ERM vision is elaborate, step 3A consists of *detailing* the risk management oversight, the roles and responsibilities, and the communication and reporting protocols for the ERM framework. In conjunction with the intended RM culture (risk appetite, tolerance, and thresholds), this step will ultimately lead to the identification of the different levels of the ERM structure to be also included in the RM policy with reference to the appropriate protocols for the integration of the RM process for the selected *key risks*. For the road sector and project-driven organizations that rely on programs, projects, and activities a structure similar to the one proposed by AASHTO [47] may be the most suitable structure.

Step 3B aims at precisely defining the context for the RM process and integrating the risk assessment (risk identification, risk analysis and risk evaluation) process with existing management structures, processes and procedures (e.g. strategic planning and management, performance measurement and assessment, new product or service launching), modifying these or even introducing new processes, through the development and implementation of detailed risk protocols supported by appropriate technology and tools. Training of key staff is key to the implementation. Scales of likelihood of event occurrence and of consequence severity and the risk classification system and risk appetites, tolerances and thresholds must be developed for each sub-level of the ERM framework. Escalating or downgrading criteria for risks must be clearly defined. It may be that, in light of the more detailed analysis, risk appetites, tolerances or thresholds be modified as these are dynamic statements and uncertainties may be revealed, or even risks not identified in Step 2A be considered by the ERM team. In such case, these alterations need approval from the SP team and the Board. Risk assessments may utilize a variety of quantitative or qualitative methods depending on the available resources and data and should also aim in identifying and evaluating existing controls. Documentation of the Step 3B rules and procedures, and RM methodologies, tools and techniques may vary in detail from a brief RM plan to a detailed RM guide. The RM process steps proposed by ISO 31000:2009 (see Fig. 4b) is a good example of the implementation steps with the end-result being populating the risk registers and risk repositories with risk information from the risk assessments and proposed risk responses, residual risks, implementation timelines and responsibilities. Proposed risk responses must be reviewed and approved by risk owners. Risk tables of heat maps are typical outputs from the risk assessment process.

**Concepts and tools**

| | | |
|---|---|---|
| • RACI matrix<br>• RM policy<br>• RM processes and procedures | • Risk classification systems<br>• RM plan and/or guide<br>• ISO 31010:2009 techniques | • Risk tables / maps<br>• Risk registers, website<br>• Training workshops |

**4. ERM EVALUATION AND REFINEMENT OF INFRASTRUCTURE AND PERFORMANCE**

| 4A. ERM monitoring and success measurement[1] | 4B. ERM review and refinement |
|---|---|

**Considerations:** Step 4 aims in evaluating the existing ERM infrastructure capability and develop a strategy for refining it.

Step 4A aims in monitoring and assessing the cost-effectiveness of existing controls for the selected *key risks* and the performance of the current ERM infrastructure. It also aims at providing assurance that relevant information is available for risk assessments and that adopted procedures are efficient, understood and followed. Levers that management has direct control over, referred to as Key Risk Drivers (KRDs – e.g. number of training hours; number of automated vs. manual processes; time to resolve outstanding audit findings), and Key Control Indicators (KCIs – e.g. number of days before deficiencies are identified; number of breaches identified by internal audit; number of errors eliminated) in conjunction with ERM KPIs are also measures that enable to monitor the effectiveness of the ERM procedures established. Important factors in ERM oversight, measurement and monitoring are to consider risk correlations and interdependencies and the selection of appropriate aggregation metrics to compound the combined effects from different risks. Risk dashboards and registers provide good ways for compiling major risks from each risk category and providing organization risk oversight when aggregation proves challenging. Effective risk dashboards should complement or be an extension of the regular reports and documentation top management regularly uses. Risk-adjusted performance indicators, KRIs and valuation metrics should be developed and communicated to stakeholders to allow taking risks into consideration in decision-making and for measuring the ERM's contribution to the achievement of objectives. Collected information should be stored in the risk repository for processing and later use.

Step 4B aims at closing the gap between the current and desired state of ERM. The ERM plan and vision produced in Steps 1B and 2B are refined by adding the necessary depth in the existing ERM infrastructure and introducing improvements as needed. Quarterly reviews of ERM monitoring and performance may indicate the need for refinement of the ERM project management system with additional resources, roles and responsibilities (e.g. a Chief Risk Officer), training, knowledge sharing and/or the modification of existing processes, risk appetites, risk tolerances and thresholds, and the introduction of new technology as time evolves and considered future scenarios tend to realize. Ultimately, the integration process and the risk culture initiated in Step 3B will embrace other management activities and become integral part of these. Embedding risk analyses and risk responses into key business processes (e.g. strategic planning, outsourcing) and including high-level risk resisters with a discussion of strategic risks into key organization documents and reports (e.g. annual budget; cash flow projections; business, work or operational plans) are common practice for conveying risk information relevant to the organization's future performance and creating high-level focus and awareness

| | | |
|---|---|---|
| in relation to the strategic priorities and the relevant threats and opportunities. ERM KPIs may also be included in a modified balanced scorecard to relate to strategic objectives and integrate ERM with strategy setting. | | |
| **Concepts and tools** | | |
| • KPIs, KRDs, KCIs, KRIs<br>• Internal audits<br>• Interviews / questionnaires | • Risk registers / dashboards<br>• BCPs, DRPs<br>• Industry benchmarking | • Risk and control workshops<br>• Gap analysis<br>• Modified balanced scorecard with ERM KPIs |
| **5. CHANGE MANAGEMENT AND ERM ADVANCEMENT** | | |
| **Considerations:** This step aims at strengthening and advancing the ERM vision, capabilities and maturity level. The depth as well as the breadth of the strategic objectives and the nature of risks considered, and/or the extent of coverage across the organization's operating units may be expanded. As experience in ERM implementation is progressively gained, an annual review of the ERM framework that will consider the refinements imposed in Step 4B and the metrics developed in Step 4A will reassess the organization's RM capabilities and effectiveness in managing the selected risks and revisit the scope of the ERM vision.<br>Learned lessons thoroughly documented in the risk repository (website) may indicate the actions and the desired capabilities needed to be deployed and developed respectively bridging the gap between the current and desired state for ERM and advancing the maturity of the organization in managing the *selected key risks*, and for effectively implementing change management in considering and addressing *additional key risks*. Such considerations should be supported by relevant cost and benefit analyses, reward mechanisms and identification of the most pressing exposures and uncertainties to the achievement of the strategic objectives. This step concludes with the reporting of lessons learned, ERM performance to stakeholders (external and internal), and future trends with recommendations for future ERM development and as per the legal requirements. | | |
| **Concepts and tools:** similar to those listed in Step 4 with emphasis in: | | |
| • Change management | • Risk reporting, KRIs | • Cost and benefit analysis |

Notes: 1: For definitions and a more comprehensive discussion on measuring ERM success, the reader should refer to the next Section

## FIGURE CAPTIONS

**Fig. 1.** Typical risk structure

**Fig. 2.** COSO ERM framework schematic representation

**Fig. 3.** Orange Book RM framework schematic representation (adapted from [33])

**Fig. 4a:** ISO 31000:2009 ERM framework components (adapted from ISO 31000:2009)

**Fig. 4b:** ISO 31000:2009 RM process (adapted from ISO 31000:2009)

**Fig. 5.** The value proposition of ERM (adapted from [50])

**FIGURES**

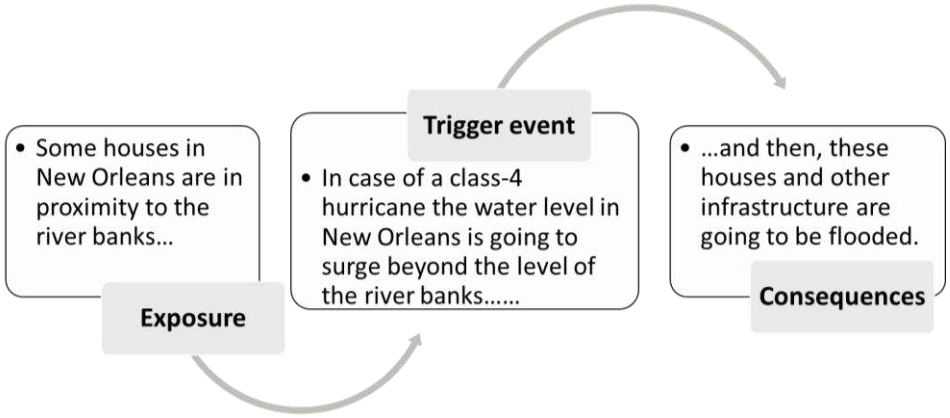


**Fig.1**

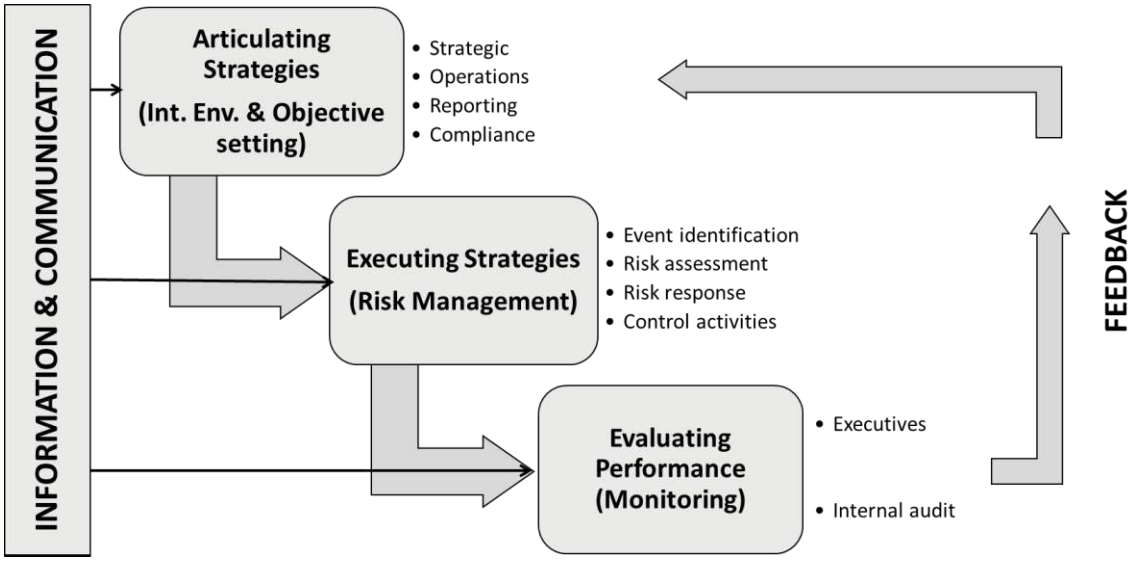
INFORMATION & COMMUNICATION
Articulating Strategies
(Int. Env. & Objective setting)
• Strategic
• Operations
• Reporting
• Compliance
Executing Strategies
(Risk Management)
• Event identification
• Risk assessment
• Risk response
• Control activities
Evaluating Performance
(Monitoring)
• Executives
• Internal audit
FEEDBACK

**Fig. 2**


Risk Environment/Context
The Extended Enterprise
Laws and Regulations
Government
Other Government Departments
Parliament
Reviewing and reporting risks
Identifying risks
Communication and learning
Capacity
Partner Organizations
Communication and learning
Addressing risks
Assessing risks
Sponsored / Sponsoring Organizations
Stakeholder Expectations
The Economy
Corporate Governance Requirements

**Fig. 3**

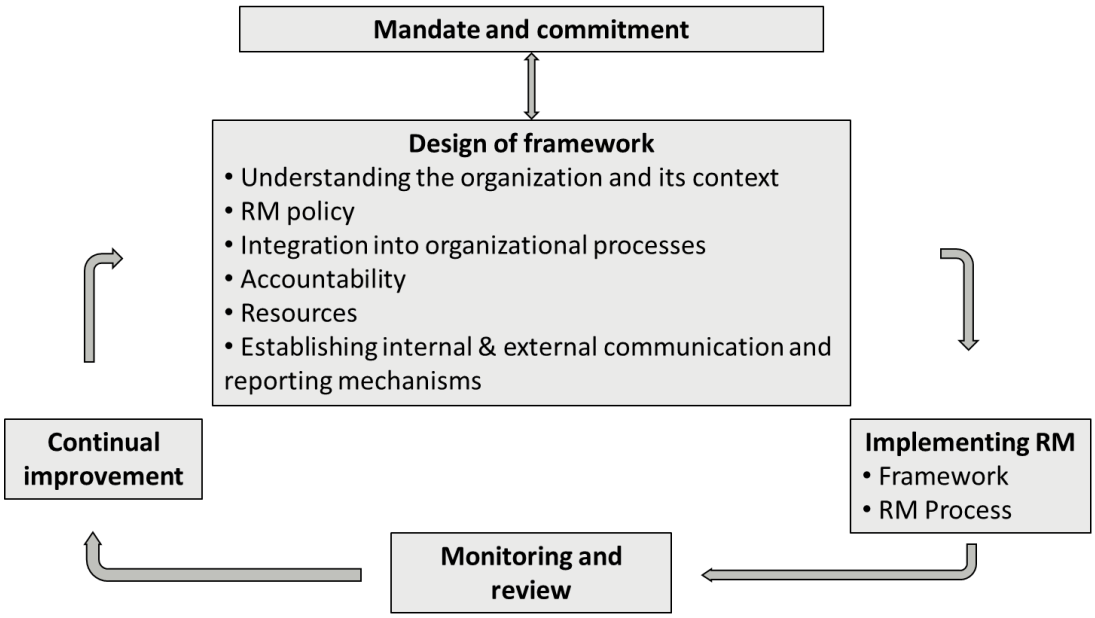
Mandate and commitment
Design of framework
• Understanding the organization and its context
• RM policy
• Integration into organizational processes
• Accountability
• Resources
• Establishing internal & external communication and reporting mechanisms
Implementing RM
• Framework
• RM Process
Monitoring and review
Continual improvement

**Fig. 4a**

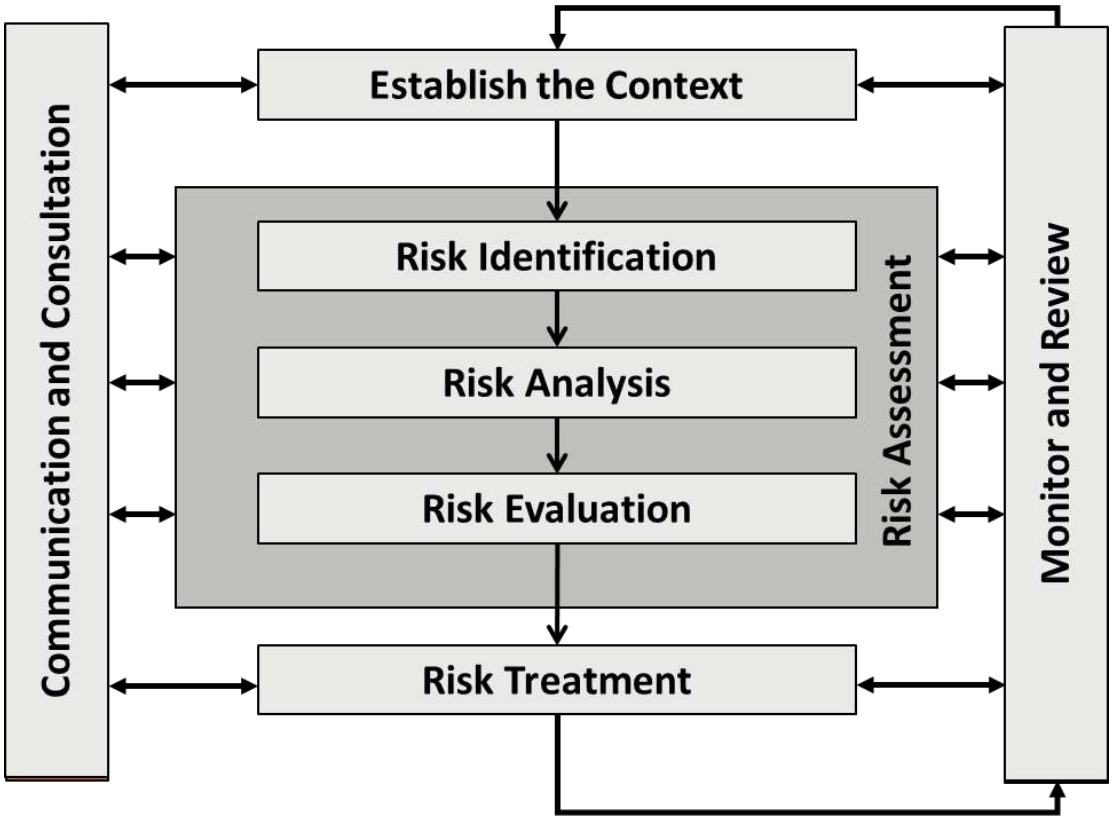
Communication and Consultation
Establish the Context
Risk Identification
Risk Analysis
Risk Evaluation
Risk Assessment
Risk Treatment
Monitor and Review

**Fig. 4b.**


PROTECT AND ENHANCE ENTERPRISE VALUE
Establish Competitive Advantage
• Integrate Risk Management w/ Business Management and Strategy Setting
• Implement More Robust Risk Assessment Process
• Improve Management of Common Risks Across the Enterprise
• Improve Capital Deployment and Resource Allocation
• Configure Risk Taking w/ Core Competencies
• Protect Reputation and Brand Image
Optimize Risk Management Cost
• Align Risk Appetite and Strategy
• Properly Price Risk Inherent in Transactions
• Aggregate Risk Transfer and Acceptance Decisions
• Eliminate Redundant and Unnecessary Activities
Improve Business Performance
• Instill Confidence from Systematic Risk Evaluation Process
• Enhance Understanding of Risks Affecting Earning and Capital
• Anticipate and Communicate Uncertainties Inherent in Performance Goals
• Improve Regulatory Compliance and Risk Responses
• Reduce Operational Losses and Surprises
• Improve Change Readiness

**Fig. 5**