Notes of JFU CPA, Tax Advisors, and Digital Tools are prepared for sharing our thoughts on problems encountered in the course of our practice. Subscription is free. Questions and comments are welcome; feel free to write to the Editor, JFU Notes, enquiries@jfuconsultants.com

We will soon open our cloud-based risk management system. Companies that wish to build a formal enterprise risk management system are eligible for a free trial. If interested, you may register your intention to participate on JFU ONLINE REGISTRATION WEB PAGE. Space is limited.

Approaches to Managing Risks
Source: JFU | Digital Tools
28 September 2021

As we discussed in our last note, a firm can chart its growth by using a two-dimensional grid to match firm-specific capabilities to risks it is facing. It can do so by employing tools such as SWOT analysis, dynamic capabilities and enterprise risk management. This note focuses on risk management. A risk arising from changes or uncertainties can be an upside opportunity or a downside danger, depending on how one anticipates, responds to and manages the risk.

How do we detect, analyze and monitor risks?

The Intuitive Approach

Without a formal Enterprise Risk Management system, most companies follow the intuitive approach. To illustrate the intuitive approach, we can consider the human body.

Our body is an intricately successful ordered system that breaks down foods, converts nutrients into energy, removes waste and enables us to carry out what we need to accomplish. Our eyes, nose, ears, mouth and skin are all integrated to form a sensory system that detects changes around us. When changes occur, our brain is alerted and assesses the stimuli consciously and subconsciously. Both deliberate and instinctive decisions are redistributed as instructions to muscles to initiate a response, while the senses continue to monitor the feedback. Through this process, we learn, adapt to changes and evolve— an ability that characterizes us as intelligent beings.

The body's approach to managing risks is an intuitive 3-stage process: (1) a sensory system first detects changes and sends alerts, (2) relevant bodily processes receive and analyse the alerts and (3) at the end, a redistribution mechanism sends instructions to responsible organs to carry out adjustments and monitor feedback.

What evolution provides is an effective but grossly inefficient process. Through the intuitive method, advances can only be made through slow trial and error. While the human race is successful compared to other animals, many individuals are sacrificed in the process of natural selection. Applying this metaphor to companies, departmental units or even entire firms may fail in the face of market uncertainties, if reliant only on the slow and incremental process of figuring out the right response. To avoid becoming sacrificed in the process, it is only wise to adopt refinements through technological changes obtained from focused studies, researches and sophisticated tooling.

In the course of our practice, we have observed that many organizations— including resourceful multinationals and public companies— still rely on intuition and relative primitive tools to manage enterprise risks, like relying on guidelines, practice notes, employee discipline, warhorse experiences and internal audits.

A few years ago, several government agencies and well-known organizations were asked to explain why major infrastructural projects were allowed to proceed despite contractors failing to submit requests for inspections or surveys at critical junctures. Only a few months ago, a major developer informed homebuyers they needed to delay moving to their new homes. A completed high-rise had to be demolished and rebuilt due to a late-stage discovery that substandard materials had been used in construction. There exist ample examples to demonstrate learning is slow, mistakes are expensive and a tarnished reputation can be difficult to redeem.

Regulatory bodies in many jurisdictions have made it mandatory that public companies devise and implement appropriate risk management systems. It is time that the business community seriously consider the widespread adoption of enterprise management risk frameworks. Technical proposals are available, created by standard-setting bodies who have long been advocating for managing enterprise risks, including ISO 31000 and COSO (2017).

The ISO31000 approach

ISO 31000 falls under the umbrella of ISO standards developed by the International Organization of Standardization for aiding the production of good quality services, protecting consumers, minimizing risk and waste and more. The organization's website describes the standards as "like a formula that describes the best way of doing something." ISO standards can be about making a product, managing a process, delivering a service, or supplying materials. We refer specifically to ISO 31000 Risk Management, which addresses operational continuity, economic resilience, professional reputation and environmental and safety outcomes.

Principles

ISO 31000 holds that risk management should be:

- An integral part of all organizational activities;
- Structured and comprehensive;
- Customized to the organization's context and objectives;
- Inclusive of all stakeholders by enabling their views and supporting knowledge sharing;
- Dynamic in detecting and responding to changes
- Based on information with respect to past, present and future, taking into account limitations and uncertainties, and
- Made clearly available and in a timely manner to relevant stakeholders.

It also recognizes that human behaviour and culture affect risk management at all levels and all stages of implementation. ISO 31000 acknowledges that risk management is an iterative process, subject to continuous improvements in light of learning and experience. Adhering to this set of principles is essential for achieving the purpose of risk management— value protection and creation.

Framework

ISO 31000 provides a framework to guide an organization in integrating risk management into organizational activities and functions.

The framework outlines a 5-stage iterative program for the introduction and maintenance of a risk management practice:

1. Integration
2. Design
3. Implementation
4. Evaluation
5. Improvement

Effective risk management requires commitment from overseeing bodies and leadership so that resources are made available company-wide, and that efforts, strategies and objectives are aligned.

Process

ISO 31000 proposes that the risk management process be embedded as an integral part of management and decision making, and be also integrated into the organization's structure, operations and processes at all levels, whether that be strategically, tactically, operationally, transactionally, through programs or within projects. **Exhibit D** shows that the risk management process has six essential components:

- Firmwide communication for integrating all stakeholders;
- Determining scope and context for customization;
- Defining risk criteria and alignment of objectives
- Establishing risk capabilities for the 3-step process of detecting, analyzing and evaluating risks
- Building risk treatment abilities to devise options for addressing risks, and
- Ability to monitor progress and feedback.

Exhibit D
ISO31000 Risk Management Process

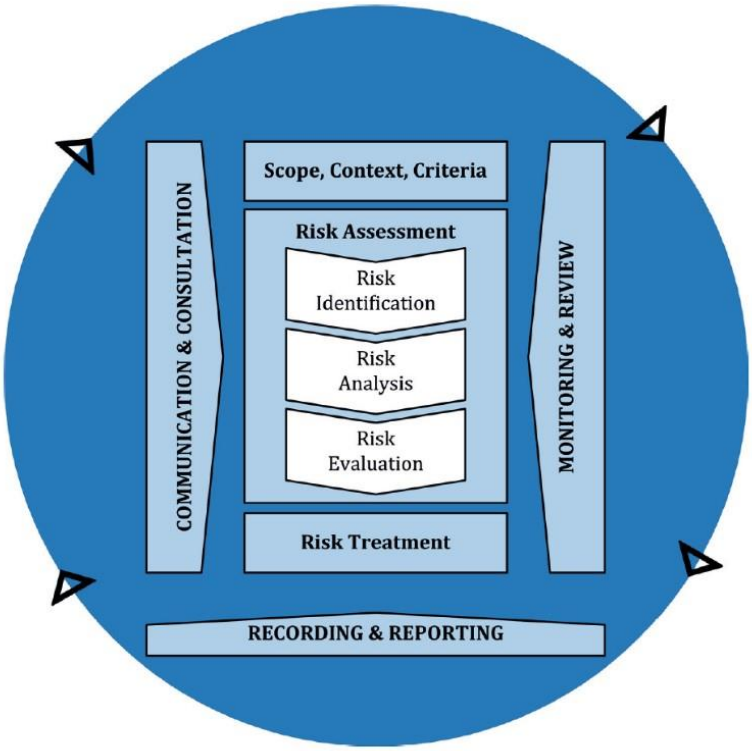

Figure 4 — Process

The COSO (2017) approach

We refer specifically to the risk management focus of COSO, known as COSO Enterprise Risk Management. COSO, or the Committee of Sponsoring Organizations, has a mission to help organizations improve performance by developing thought leadership that enhances internal control, manages risk, improves governance and deters fraud. While the notion and approach to risk management under COSO is similar to what ISO 31000 advocates, COSO presents it quite differently, making the importance of integrating risk management with strategy and performance more notably visible.

COSO conceptualizes enterprise risk management as a framework or process consisting of five components arranged in a double helix, very much like that of a DNA molecule. You may recall DNA is a chainlike molecule found in every living cell, directing the formation, growth and reproduction of cells in living beings. This concept suggests that risk management has to be embedded into an organization's functional units and operate at every stage of its value chain:

- Vision
- Strategy
- Objectives
- Performance
- Value

Only with such integration, can COSO Enterprise Risk Management prove useful in directing each unit and supporting the organization's overall production and growth. COSO's risk management concept and the five risk management components are depicted in **Exhibit E**.

<u>Exhibit E</u>
COSO ERM Components

Putting Concepts into Practice

From a risk practitioner's point of view, it is helpful to study the COSO concept and its components together with those that ISO 31000 advocates. The two approaches are similar in purpose but different in presentation.

COSO emphasizes the integration of risk management processes with governance, strategy and the rest of the organization. Like the metaphor of the DNA, the COSO approach focuses on interweaving risk management throughout the organization's overseeing bodies.

In contrast, ISO 31000's risk management framework is highly structured. It provides a 3-step risk assessment process— identification, analysis and evaluation—along with separate elements for treatment, monitoring and risk accounting.

Now that you have obtained an overview of Enterprise Risk Management, our next note will discuss how one can put these concepts into practice.