



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](mailto: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.



## **ERM in Practice – Tooling Up the System**

**Source: JFU | Digital Tools**

**4 October 2021**

Enterprise risk management (ERM) is about value creation or business growth. The ERM guidelines discussed in our recent Notes tell us how to achieve this methodically. While the methodologies can be difficult to apply, better training and better tools will help perfect the practice.

### **Risk Management & Internal Control System (RMIC)**

Continuing from the discussion of Enterprise Risk Management leads us to the RMIC system. An RMIC System is an essential business system for an organization to ensure controls are exercised and risks managed.

While risk management deals with uncertainties that may bring surprises, (whether favourable or unfavourable), internal controls ensure that what must be done is properly done. Risk management (RM) and internal control (IC) are two sides of the same coin. Thus, an organization can combine them to form one integrated RMIC System for exercising control and for steering business towards its objectives.

Effective running of the RMIC System requires the maintenance of two registers: first, a Control Register for documenting controls devised to ensure an organization's internal policies and procedures are observed, and second, a Risk Register for capturing identified risks and monitoring corresponding measures.

The prerequisite to maintaining a proper Control Register is good documentation of internal policies and procedures. Compliance tests on the controls can be performed to assess if policies and procedures are being followed in practice. The contents of a Control Register should be relatively

static, because the policies and procedures of an organization generally do not change when the business system has been reasonably well-established.

On the other hand, maintaining a proper Risk Register requires that risk management principles and practices are extensively integrated into an organization's structure and processes— including governance, management and operations. Such extensive integration allows risks to be crowdsourced from a spectrum of members working in different functions at different levels of the organization. Thus, the Risk Register can sufficiently capture risks that the organization faces in different respects and allow risks to be identified, evaluated and treated in a timely manner. The contents of a Risk Register should be relatively dynamic, to account for the constant changes in environment, scope and context in an organization.

### Tooling Up the System

A system or practice is good if it is sufficiently efficient and effective. It should, primarily, be adequately equipped to deal with complexities in particular situations. Otherwise, it offers a false sense of comfort. The famous sinking of the Titanic in 1912 was particularly shocking due to its unexpected nature. Titanic was reportedly underequipped with lifesaving facilities, but all the passengers had felt safe on board, believing they were aboard one of the most advanced passenger liners of its time.

In Enterprise Risk Management, one common practice is the use of questionnaires or interviews for gathering risk inputs from mostly senior members of an organization. Practitioners should be aware that such a practice is prone to be self-serving, merely showing what was done to meet certain compliance requirements. Real risk management is about watching out for and dealing with potential occurrences that may destroy or create value.

Another example is acquiring a "risk universe" off the shelf, which is a self-defeating practice. A Risk Universe is a comprehensively researched list of risks that an organization may face. There are function or industry-specific Risk Universes that one may acquire from credible sources. They can be good reference tools filled with useful textbook examples. However, an organization must watch out for occurrences that may arise within its unique context. The officers of the Titanic were certainly aware of the risk of floating icebergs to ships in the ocean. Nonetheless, this known risk still materialized into a devastating tragedy. Mere knowledge on the shelf is inadequate; it is actual risk managing actions that work to prevent the occurrence of real danger.

### The Art of Managing Risk

Risk management is more than an attitude; it is a series of actions carried out systematically by people who know what they are doing and are conscious of what may prevent them from achieving what they want to do. We call these people Risk Owners. What are these actions and how do Risk Owners carry them out, efficiently and effectively?

The diagram on the right shows an effective sequence of actions separated into four categories.



It begins by defining the organization's environment: first, one identifies the operating **scope** that the risk management system covers. Second, the **context**— the organizational structure and components— is defined. Finally, the **criteria**, or working definitions of what is considered significant to the organization is determined.

The next category involves the core actions of **risk assessment**: identifying and locating risks, analyzing identified risks in terms of impact and likelihood, and evaluating risks in terms of significance for prioritization and allocation of management resources.

The third category is **treating risks** or designing measures to tackle risks that should not be left to the organization's own devices or cannot be ignored. At this point, decisions must be made by leadership at multiple levels to mobilize people and resources toward the appropriate risk-mitigating or risk-cancelling actions.

In the final category, an accounting is made of all risks and **reporting** is completed on the decisions that were made throughout the risk management process. This stage is concerned with whether decisions made are being effectively carried out. Please remember that the **effectiveness** of the risk management system should be a critical management focus for the board of directors or the organization's governing team.

We shall discuss in our next Note how Risk Owners can direct these risk managing actions.