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

---

Risk Management Practical Problems - 1
Magnitude of Risk and Effectiveness of Control
Source: JFU | Digital Tools
21 July 2020

The Hong Kong Listing Rules require the board to oversee the issuer's risk management and internal control systems on an ongoing basis, ensuring that the systems' effectiveness be reviewed regularly, at least once a year, and report accordingly.

How can one tell if the systems are effectively run?

Tracking change

IEC[1] 31010, the supporting standard of ISO[2] 31000 on risk management, suggests the magnitude of a risk depends on the assumptions made about the presence and effectiveness of relevant controls. Thus, the level of risk is a function of effectiveness of control - tracking change in the level of risk can tell us the effectiveness of the controls and hence how effective the systems are managed.

Risk management practitioners describe levels of risk by using notions of **inherent risk** (or gross risk) for situations where relevant controls are absent or fail to function and **residual risk** (or net risk) for situations where relevant controls are considered operating as intended. These two indicators should appear in a typical risk register and the absence of such indicates the risk management function of the organization is fundamentally flawed.

Residual risk and inherent risk provide useful information about the significance of a particular risk at the point when a risk is identified and initially assessed. They give risk managers a sense of the worst-case and best-case scenarios. In reality, an organization's risk profile is at neither end of the spectrum but sits somewhere in between.

We, therefore, devise in our risk management tool a new indicator. It gives expression to an informed judgment on the **current** level of risk while accounting for how effective a risk is managed and the level of risk that the organization is facing now with respect to the best-case and worst-case scenarios. This information is as useful as what the speedometer can tell the driver of a car maneuvering on the road.

Level of current risk

Enterprise risk management is a process important for the survival and growth of an organization maneuvering through a path strewn with risks arising from changes in circumstances. Risk managers cannot mitigate risks by merely putting them down on the risk register. Rather, someone in the organization who knows the risks need to devise and implement appropriate treatments and someone will need to monitor the implementation and make a conscious judgment on the progress made. The **current risk** reflects the judgments made which tell risk managers and the board if the organization is under effective control in maneuvering through the uncertainties along its path.

Concerns over accuracy often arise when forming judgments on the effectiveness of control and hence the level of risks. Such concerns are misplaced. In risk management, the real concern is whether or not a **risk is known** and the **actions taken** to mitigate threats and seize opportunities. A ball dodged is a ball dodged regardless of whether or not you can accurately determine the speed of the ball.

Thus, it is not necessary to devise complex mathematical model to calculate the level of current risk. A simple one will do, as long as it provides a good sense about the risk so that appropriate response can be made timely. The following outlines the mathematical model that we use.

A simple yet effective model

A risk event is typically measured in two dimensions: likelihood and impact. The inherent risk of a risk event is the value obtained assuming nothing is done or can be effectively done along these two dimensions, represented as,

$$\text{Risk}_{\text{Inherent}} = \text{Likelihood}_{\text{Inherent}} \times \text{Impact}_{\text{Inherent}}$$

If the inherent risk is greater than the risk tolerance of the organization, risk managers have to initiate treatments and controls to reduce the likelihood of the event from happening or reduce the impact on the organization. The residual risk is the value obtained assuming the treatments and controls can operate effectively as intended, represented as,

$$\text{Risk}_{\text{Residual}} = \text{Likelihood}_{\text{Residual}} \times \text{Impact}_{\text{Residual}}$$

Current risk has a value same as the inherent risk if the treatments have not been implemented or if they are ineffective. On the other hand, the current risk has a value same as the residual risk if the treatments operate fully as intended. In other words, the treatment must have been well managed and controlled, or mathematically speaking, 100% effective in control over the implementation of the treatment.

As explained above, sophisticated calculation on the degree of control effectiveness is usually superfluous and a reasonable judgment should suffice. An organization only needs someone with reasonable knowledge about the risk and control initiatives to make a considered and informed judgment on the effect of actions taken. For instance, the reviewer or monitor determines in his / her judgment that the actions taken reduce the likelihood by X% and impact by Y%, the values of current likelihood, current impact and current risk can be estimated with simple formulas as follows.

$$\text{Likelihood}_{\text{Current}} = (\text{Likelihood}_{\text{Residual}} - \text{Likelihood}_{\text{Inherent}}) * \text{Effectiveness}_{\text{Likelihood}} + \text{Likelihood}_{\text{Inherent}}$$

$$\text{Impact}_{\text{Current}} = (\text{Impact}_{\text{Residual}} - \text{Impact}_{\text{Inherent}}) * \text{Effectiveness}_{\text{Impact}} + \text{Impact}_{\text{Inherent}}$$

© 2018 JFU Consultants (Beijing) Limited, JFU Consultants (Hong Kong) Limited, JFU Consultants (Canada) Limited. All rights reserved. | Legal | Privacy

$$Risk_{Current} = Likelihood_{Current} \times Impact_{Current}$$

The above outlines the basic mathematical operation for arriving at the value of the current risk of an event that may happen with an impact on the outcome of efforts made by an organization in pursuing an objective. The operation will have to be modified or expanded to reflect the effects of multiple risks or multiple treatments of a risk.

Achieving effectiveness

We often see risk managers using spreadsheets to register risks identified and show the level of inherent and residual risks. With the above, we would share our view that it is not quite possible to run risk management efficiently and effectively, and present a clear view of current risks without digitalizing the process and to prompt organizations to take timely actions to dodge dangers and seize opportunities.

---

[1] The International Electrotechnical Commission

[2] The International Organization for Standardization

© 2015 JFU Consultants (Beijing) Limited, JFU Consultants (Hong Kong) Limited. All rights reserved. | Legal | Privacy