Managing Risk

in a Volatile, Uncertain, Complex, Ambiguous World

在VUCA世代 如何管理風險

Gary Seib FHKIoD

How do leaders manage risk in a VUCA – *volatile, uncertain, complex, ambiguous* – world? What are some best practices that leaders can adopt in Hong Kong?

What risks are out there? To coin Donald Rumsfeld: there are known unknowns and there are *"unknown unknowns – the ones we don't know we don't know."*

Increasingly, effective corporate governance requires executives and boards to plan strategically, carefully and in advance about the range of risks that this big, wide, VUCA world may present to the enterprise.

This article will look at risk, governance and some best practices that leaders should adopt in identifying, assessing and managing risk.

What is Risk?

Risk is an exposure to the possibility an adverse or unwelcome circumstance.

Paraphrasing – *stuff happens*. Leaders don't have perfect foresight and cannot forecast, or avoid, *"stuff"* happening. Risk management is all about minimising the risk of negatives occurring, or when (more than if) they do, mitigating or limiting their impact.

Risk can be operational, strategic or *existential*. Strategic risk analysis and management needs closely to consider not only the nature of the risks facing the enterprise, but also the likelihood of each occurring and their impact if they do.

Risk and Disruption are Everywhere

We live in a complex and dynamic world. My role as a Disputes lawyer, and yours as a leader, is to simplify and navigate that complexity.

My colleagues and I have done a lot of analysis around risk, and have worked with hundreds of executives and leaders across a range of sectors to help identify, articulate and manage risk proactively. Our recent reports on **Business Complexities, Belt & Road: Opportunity & Risk** and **Mega-Trends & Legal Solutions** draw out the issues confronting corporate leaders across sectors, and address solutions that can, and should, be put in place before the prospect of a risk event becomes a reality.

What are the risks that leaders told us *"keep them awake at night"?*

There's a lot around technology and disruption. Here's the top four issues (of the 10 we look at in the Complexities Report) leaders identified:

1. The need to innovate via new technologies (i.e. internally driven);
2. Pressure on margins;
3. Disruption via technology (i.e. externally driven);
4. Compliance and regulatory risk.

Other vital issues are also in the mix, such as cyber security, trade uncertainties, economic and environmental risk; geopolitics.

These results highlight a key issue around risk – it can be internally driven, or an external "shock" over which you may have little or no control.

And while it's important to take a view *"from 30,000 feet"*, the analysis also needs to drill down to sectoral and then to organisational levels.

What is consistent across all sectors we looked at is that every industry sees business becoming more, not less, complex. But the types of issues differ across the sectors. For example, the No 1 issue identified by the Energy Mining and Infrastructure sector is regulatory risk. Business model innovation is pretty well down the list (which might be surprising given issues around climate change and the move away from fossil fuels). But in Technology, Media and Telecommunications, business model innovation is the No 1 sectoral issue. For Retail, it's acquisition risk.

The take-away: it's important to take a high-level, strategic perspective. But risk profiles differ across sectors and from organisation to organisation. Risk needs to be assessed and managed in the particular context of your organisation. And you will have a range of stakeholders whose welfare will depend on you doing so effectively.

Best Practices

As ever, there is no *"one size fits all"* solution for risk management. But there are a number of steps that reflect best practice in this key area of governance.

First, **Risk Committees.**

Establishing a Risk Committee sometimes is mandated. For example, listed companies must establish a committee to be called the "Risk Management Committee" under the Securities and Futures Ordinance in Hong Kong. But whether or not mandated, establishing a dedicated, independent and specialist Risk Committee, with suitable mandate and authority, in my opinion is a first, essential step in effective risk management.

The Hong Kong Stock Exchange describes its major roles and functions broadly as:

- Advising the Board on the Group's risk appetite, profile and tolerance.
- Overseeing the risk management framework.
- Reviewing the Group's risk management policies, reports and any breaches.
- Considering current and emerging risks and ensuring appropriate mitigation is in place.
- Reviewing the effectiveness of the Group's controls and mitigation tools.

It requires at least 4 meetings per year, and more if appropriate, with annual reporting.

A Risk Committee is an independent committee, whose remit is responsibility for the risk management policies of the enterprise. That does not mean it is the owner or manager of all risk – that must stay within the remit of day-to-day management (I make further observations as to the ownership and mitigation of risk below).

Risk Committees can be charged with establishing and implementing a risk management framework/strategy for the enterprise, tailored to its business and focused on the material risks it confronts. A Risk Committee, when utilised well, can identify and manage risk proactively; align governance with strategy; support stakeholders; ensure clear oversight; and implement lines of communication across specialist committees within a governance structure.

Next, establish the Risk Committee's **mandate, structure and composition.** How does it fit with the board/other committees? What is its remit and what are its responsibilities? What is its structure, and who, therefore, should sit on the Risk Committee? How will it be supported: what resources – internal as well as external – can it call on?

Consider also whether it's necessary or appropriate to appoint a **Chief Risk Officer.** Does this function reside – in

practice or formally – in the General Counsel function? Often it will, and often that is appropriate. But consider whether a CRO role needs to be established formally, and if so, how it should fit within the current governance structure.

Risk Management By Numbers

The analytics then need to be undertaken. If risk is seen in probability terms – the probability of an uncertain, adverse event occurring, then a framework that provides a degree of objective analysis will assist, and can enable the Risk Committee to draw on the expertise of the different business lines/functions within the enterprise.

To that end, risk can be estimated and allocated a numeric value, based on a pretty straightforward analysis (perhaps deceptively so, because it will be dependent on the underlying judgments). Effectively, using an appropriate scale:

$$\text{Magnitude of Risk} = \text{Likelihood of Occurrence} \times \text{Severity of Outcome}$$

That scale may be 1-10 (or higher), but it may not help to be too nuanced, so I would recommend 1-5.

A *value* can then be attributed to the identified risk, and considered against the *risk appetite* of the enterprise.

To take an example, let's look at a risk to recovering a receivable. The risk may be reasonably high (the chance of incurring a bad debt is pretty high in any business with volume) but the impact of a bad debt to the enterprise isn't likely to be critical. Hence, the analysis may be:

$$\text{Magnitude of Risk} = \text{Likelihood of Occurrence} \times \text{Severity of Outcome}$$
$$= 4^{*} \times 1$$
$$= 4$$

*Perhaps that risk is even at 5 – a virtual certainty

Other risks can be assessed in the same way. For example a Denial of Service cyber attack might be (depending on the nature of the enterprise):

$$\text{Magnitude of Risk} = \text{Likelihood of Occurrence} \times \text{Severity of Outcome}$$
$$= 4 \times 4$$
$$= 16$$

Hence, the cyber risk is a much higher risk to the enterprise, and should be addressed with that priority in mind.

Developing a Risk Register

Based on that analysis, across all business lines and functions, the Risk Committee should oversee the preparation of a robust **Risk Register and Mitigation Plan**.

A Risk Register is a tool that documents the risks identified in this process, values them, and identifies mitigation steps for each. The Risk Register should also identify the **owner of each risk** – who is responsible for the risk and for its mitigation? Of course, the process doesn't end there – the key then is to **implement the steps required** to mitigate those risks, and **to monitor** progress against the mitigation plan.

Ongoing Dynamics of the Environment

I opened this article by observing that we live in a VUCA world. Inevitably, this means a process of **continual monitoring and review**, because our operating environments, and the nature of risk, are not static. Take the example of the key risks confronting the EMI industry. I expect that business model innovation will become an increasingly key issue; indeed it may have shifted to some extent since the survey we reported.

Thus it is critical that the Risk Committee address two important issues: **implementing** the mitigation plan, and

the **regular review and update** of the Risk Register itself. The Risk Committee should meet regularly (e.g. quarterly, or more frequently as the process is initiated or circumstances merit). The nature, magnitude and priority of different risks should be reassessed periodically, as of course should the mitigation plans developed for those risks.

Wrap up

All enterprises, and their leaders, need to be strategic about how they manage risk. Sophisticated businesses are increasingly alive to the value of doing so, especially since the global financial crisis of a decade ago, and in an ever more complex and disruptive world.

Establishing a framework within which the risks facing an enterprise can be identified, prioritised and mitigated is an essential objective of rigorous risk governance, and helps leadership better understand, and address, those risks.

Utilising some of the tools and best practices outlined here will, I hope, assist leaders in managing risk in a VUCA world, simplifying complexity, and continuously monitoring their responses to our ever-changing environments.

在VUCA*（波動、不確定、複雜、充斥灰色地帶）*的世代，公司領導階層應該如何管理風險？他們可採用什麼最佳實務措施？

我們面對什麼風險呢？套用Donald Rumsfeld的話：有「已知的未知」及*「未知的未知」，後者更嚴重，我們有機會不知道自己不知道甚麼，換言之亦難以作出準備」*。

要有效管治公司，行政人員和董事會日益有需要預先小心並有策略地估算VUCA世代企業可能造成的風險。

本文會探討風險、管治和領導階層人員在鑑識、評估和管理風險方面應採取的一些最佳實務措施。

何謂風險？

風險是指面對可能不利的情況。

換言之，*是會發生的事情*。領導階層人員沒有完全準確的預見能力，亦無法預測或避免將會發生的*「事情」*。風險管理是旨在盡量減少發生不利情況的風險，或當發生風險（不單止假如發生）時緩減或限制風險影響。

風險可能是營運、策略性或*存活層面*。策略性風險分析和管理不單必須密切考慮公司面對的風險性質，還要考慮每次發生風險的可能性及風險發生時產生的影響。

風險及破壞無處不在

我們活在複雜多變的世代。我和您的角色分別是處理糾紛的律師和領導階層人員，負責簡化複雜的情況和領導公司前航。

我跟同事們做過不少風險分析，並曾協助數以百計不同行業的行政人員和領導階層人員積極鑑識、明確界定及管理風險。我們近期發表多份報告**有關商業複雜性、一帶一路：機會與風險**及**大趨勢與法律解決方案**。該些報告提述各行業公司領導階層面對的問題，並說明於潛在風險發生之前可以並且應該採取什麼解決方案。

有什麼風險是領導階層人員囑咐我們要*「使他們在夜裡警醒」*的？

很多風險是關乎科技和破壞。以下是領導階層人員鑑識的四大問題（我們在「複雜性報告」中探討的十個問題其中四項）：

1. 透過新科技創新的需要（內部帶動）；
2. 毛利壓力；
3. 透過科技癱瘓市場（外部帶動）；
4. 合規及規管風險。

另外還有其他不同的重大問題，例如網絡安全、貿易不確定性、經濟風險、環境風險及地緣政治。

這些結果反映風險的一個主要情況 — 風險可能是內部帶動、或者是您難以或無法控制的外部「衝擊」。

雖然必須*「從30,000呎外」*作宏觀分析，但亦有必要深入至從行業及機構層面探討。

我們探討的所有行業都有一個共通點，就是各行各業的業務均日趨複雜，但不同行業面對不同種類的問題。例如，能源、礦業和基建業的首要問題是規管風險，但業務模型創新卻在較低的關注程度（鑑於氣候變化問題及棄用化石燃料，這令人感意外）。不過，在科技、媒體和電訊業，業務模型創新卻是行業的首要問題，零售業則面對收購風險。

由此得知，必須採用高層的策略性觀點。不過，風險承受能力因行業和機構而異，必須根據貴機構的情況來評估及管理風險，貴公司在這方面的效率會影響不同持份者的福祉。

最佳實務

一如往常，風險管理並無*「一體適用」*的方法，但有多個步驟反映此重大管治範疇的最佳實務。

首先是**風險委員會**。

有時候，成立風險委員會是強制性規定。例如，上市公司必須根據香港的《證券及期貨條例》成立「風險管理委員會」。不過，我認為不管是否強制，成立具適當任命和權限的獨立專責風險委員會是有效管理風險的必要第一步。

香港交易所粗略說明委員會的主要角色和功能如下：

- 就集團的風險胃納、承受能力和耐受能力向董事會提供意見。
- 監督風險管理框架。
- 檢討集團的風險管理政策、報告及任何違規。
- 考慮現有風險及新興風險，並確保已實施適當措施緩減風險。
- 檢討集團的風險管制和緩減工具的成效。

委員會必須每年舉行四次會議（若有需要可增加開會次數），並須每年作匯報。

風險委員會是獨立的委員會，職權範圍是為公司制定風險管理政策。這並不表示委員會是所有風險的責任人或管理人 — 這些必須依舊屬於日常管理職權範圍（以下是我對風險責任及減減風險的更多觀察所得）。

風險委員會可負責因應公司業務及針對當前重大風險制定及實施風險管理框架／策略。風險委員會若運用得宜，可以積極鑑識和管

理風險、以策略配合管治、支援持份者、確保監督具透明度及在管治架構內不同專責委員會之間進行溝通。

第二是確立風險委員會的**任命、結構和構成**。風險委員會如何跟董事會／其他委員會互相配合？風險委員會的職權範圍和責任是什麼？風險委員會的結構如何及由誰人出任委員？風險委員會可獲得什麼支援：內部資源及外部支援。

另外還必須考慮是否需要或適宜委任一名**風險總監**。這項職責是否已由首席法律顧問執行或正式包括在其職能內？雖然此舉往往有必要而且往往適宜，但必須考慮是否需要正式設立風險總監的崗位，若果有需要則如何將之加入現行管治結構。

按數值管理風險

接著必須**分析**。如果認為有可能出現不明確的不良事件，制定框架以某程度的客觀分析會有幫助，並讓風險委員會得以運用公司不同業務線／職能的專業知識。

為此之故，可以根據頗直接了當的分析（也許是看似直接了當，因為實際上要視乎相關的判斷）以評估風險然後分配一個數值。可採用適當的評分表來評估：

$$\text{風險強弱程度} = \begin{matrix}\text{發生的可能性} \\ \mathbf{x} \\ \text{後果的嚴重性}\end{matrix}$$

評分表可以採用1至10分（或更高分）。分得過份細微可能沒有幫助，故我建議採用1至5分。

接著可給鑑識的風險分配一個*數值*，然後對比公司的*風險胃納*作考慮。

例如，讓我們分析收回一筆應收款項的風險。雖然風險可能合理地高（任何具規模的公司出現壞帳的機會都頗高），但壞帳對公司的影響不會很大，故此可能得出以下分析：

$$\begin{aligned}\text{風險強弱程度} &= \begin{matrix}\text{發生的可能性} \\ \mathbf{x}\ \text{後果的嚴重性}\end{matrix} \\ &= 4^{*} \times 1 \\ &= 4\end{aligned}$$

*風險甚至是 5 — 幾可肯定

其他風險亦可以用相同的方式評估，例如阻斷服務網絡攻擊可能得出以下分析（視乎公司的性質）：

$$\begin{aligned}\text{風險強弱程度} &= \begin{matrix}\text{發生的可能性} \\ \mathbf{x}\ \text{後果的嚴重性}\end{matrix} \\ &= 4 \times 4 \\ &= 16\end{aligned}$$

因此，公司的網絡風險遠高得多，故應該優先處理。

編彙風險記錄冊

根據該項分析，不論哪種業務和職能，風險委員會都應該監督高效的**風險記錄冊和風險緩減計劃**的制定。

風險記錄冊是一種工具，用以記錄本流程鑑識的風險，並且評估其數值和確定每項風險的緩減措施。風險記錄冊亦應確定**每項風險的責任人**，即由誰人負責處理該風險及加以緩減。當然，流程並非到此為止，接著下來的關鍵步驟是**實施所需的措施**緩減風險，並且按照緩減計劃來**監督**流程。

環境持續變動

我在本文的開首即指出我們活在VUCA世代，基於我們的營商環境和風險性質都非一成不變，故無可避免地需要**持續監督和檢討**。以企業製造智慧業面對的主要風險來說，我預期業務模式創新會日益重要。誠然，自我們報告有關的調查後，該行業亦已作出某程度的轉變。

因此，風險委員會必須負責兩項重要工作：**實施**緩減計劃及**定期檢討和更新**風險記錄冊本身。風險委員會應該定期舉行會議（即每季舉行會議；在展開流程後或若情況有需要應該更頻密舉行會議）。另外，如果已就風險制定緩減計劃，應該定期重新評估不同風險的性質、強弱程度和優次。

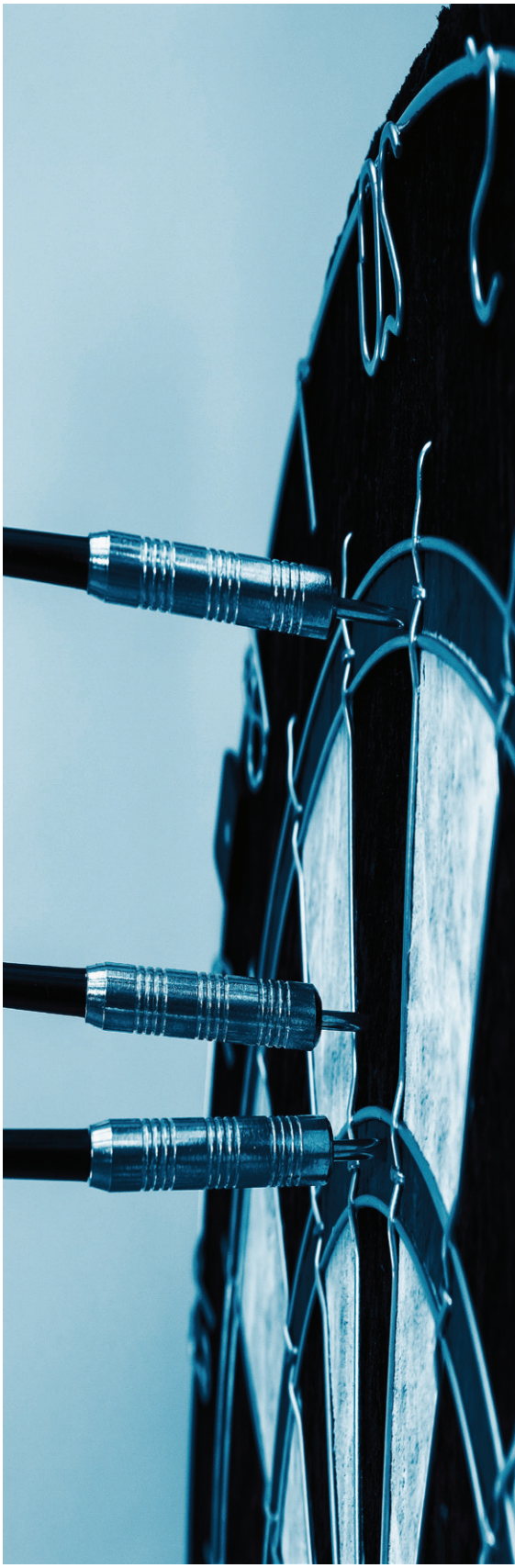
結論

所有公司及公司領導階層人員必須有策略的管理風險。穩健的公司愈來愈明白這樣做的價值，特別是有鑑於十年前發生過全球金融危機、這世代日趨複雜和破壞元素不斷湧現。

制定可鑑識、優先處理及緩減公司面對的風險是高效風險管治的必要目的，這亦有助領導階層人員更清楚了解及有能力應對這些風險。

我希望本文章概述的一些工具和最佳實務措施，可協助領導階層人員管理在VUCA世代面對的風險、簡化複雜的情況及持續監督其如何應對不斷轉變的環境。

Gary Seib FHKIoD is Dispute Resolution Partner of Baker McKenzie.



The 21st Century DIRECTOR 廿一世紀董事

Sponsored by:
贊助機構

CG 企管基金 FOUNDATION

Publisher 出版機構
The Hong Kong Institute of Directors 香港董事學會

Sponsor 贊助機構
Corporate Governance Development Foundation Fund 企業管治發展基金

Project Management 項目統籌
Executive Office, The Hong Kong Institute of Directors
香港董事學會行政處

For enquiries about circulation and advertisement, please contact:
有關發行及廣告查詢，請聯絡：
Chief Business Officer: Ms Miriam Yee
業務總監：余海恩小姐

For editorial enquiries, please contact:
有關編輯上的查詢，請聯絡：
Associate Manager, Communication & Projects: Ms Moni Ching
傳訊及項目副經理：程穎姍小姐

Tel 電話： +852 2889 1414
Fax 傳真： +852 2889 9982
Email 電郵： magazine@hkiod.com

Editor 編輯
Ms Cora Wan 温旭兒小姐

《廿一世紀董事》同時可於網上閱覽
The 21st Century Director is also available at
http://www.hkiod.com/21century.html

ISSN 1996-9619

The Hong Kong Institute of Directors is Hong Kong's premier body representing directors to foster the long-term success of companies through advocacy and standards-setting in corporate governance and professional development for directors.
香港董事學會為香港代表專業董事的首要組織，其宗旨是促進所有公司的持久成就；為達成使命，
學會致力提倡優秀企業管治與釐訂相關標準，以及協助董事的專業發展。

The Hong Kong Institute of Directors Executive Office 香港董事學會行政處
2104 Shanghai Industrial Investment Building, 48 Hennessy Road, Wan Chai, Hong Kong 香港灣仔軒尼詩道48號上海實業大廈2104
Tel 電話 : (852) 2889 9986 Fax 傳真 : (852) 2889 9982 E-mail 電郵 : executive@hkiod.com