



Risk Management in Practice

風險管理實踐

Risks and uncertainties are two unknown outcomes affecting all walks of life from persons to companies on a daily basis. Risks involve situations where outcomes are unknown but their probabilities may be estimated and hopefully managed using data and models. Uncertainties refer to situations or scenarios where both outcomes and probabilities are not predictable nor estimated. So we have risk management but not uncertainty management.

Currently, there are two risk management models that are commonly used by companies to identify, assess, manage and control risks, namely, ISO31000 and COSO ERM (Enterprise Risk Management), with COSO ERM model being more popular for companies listed on Hong Kong Stock Exchange that this model is discussed in this article.

Risk Management in Law

If a company is incorporated in Hong Kong and is subject to the Companies Ordinance, Cap. 622, the directors are required under section 388 to prepare for each financial year an annual report (Directors' Report) complying with the requirements as therein set out including a business review under Schedule 5 to the Companies Ordinance. Under paragraph 1(b) of Schedule 5, the business review must consist of a description of the principal risks and uncertainties facing the company. This constitutes the legal basis for a company incorporated in Hong Kong to prepare a risk management report complying with Schedule 5.

If a company is listed on the Main Board of Hong Kong Stock Exchange and is subject to the Main Board Listing Rules (MBLR), it is required under MBLR13.89 to prepare the Corporate Governance Report disclosing the matters as required under the Corporate Governance Code (CG Code) including compliance with Code Provisions (CP) or their non-compliance with explanations and disclosure of Recommended Best Practices (RBP) on a voluntary basis.

Under the CG Code and as regards risk management and internal control, a listed company is required to review the effectiveness of the risk management and internal control systems of the listed group at least annually on matters as therein set out.

In terms of Principle under the CG Code, the board is responsible for evaluating and determining the nature and extent of the risks it is willing to take in achieving the listed company's strategy – this is the risk appetite of the listed company. The board is also responsible for ensuring that the listed company establishes and maintains appropriate and effective risk management and internal control systems for the purpose of dealing with identified risks, safeguarding the listed company's assets, preventing and detecting fraud, misconduct and loss, ensuring the accuracy of the listed company's financial reports and achieving compliance with applicable laws and regulations. The board should oversee risk management and internal control systems on an ongoing basis. The board is also responsible for ensuring that the effectiveness of the listed group's risk management and internal control systems is reviewed at least annually and management should provide a confirmation to the board on the effectiveness of these systems. The CPs as therein set

風險及不明朗因素兩大未知結果，每日影響著各行各業的人士及企業。風險是指結果未知，但可透過數據與模型估算其發生機率，以期加以管控的情況。不明朗因素則指結果與發生機率皆無法預測或估算的情況或情境。因此，我們能管理風險，但無法管理不明朗因素。

目前企業常用以識別、評估、管理及控制風險的風險管理模型有兩種：ISO31000及COSO企業風險管理，其中COSO企業風險管理模型在香港交易所上市企業中較為普及，本文將重點探討此模型。

風險管理法律

若公司於香港註冊成立並受《公司條例》（第622章）規管，則根據第388條規定，董事須就每個財政年度擬備符合該條例所載要求的年度報告（《董事報告》），其中須包含《公司條例》附表5所訂明的業務審視。根據附表5第1(b)段，業務審視章節須包含對公司面對的主要風險及不明朗因素的描述。此乃在香港註冊成立的公司擬備符合附表5規定的風險管理報告的法律依據。

若公司於香港交易所主板上市並受《主板上市規則》規管，根據《主板上市規則》第13.89條規定，其須擬備《企業管治報告》，披露《企業管治守則》所規定的事宜，包括遵守守則條文或不遵守就解釋，以及自願披露建議最佳常規。

根據《企業管治守則》，在風險管理及內部監控方面，上市公司須至少每年就守則所載事項檢討上市集團的風險管理及內部監控系統的功效。

根據《企業管治守則》的原則，董事會負責評估及釐定上市公司達成策略目標時所願意接納的風險性質及程度——即上市公司的風險承受能力。董事會亦有責任確保上市公司設有並維持適當及有效的風險管理及內部監控系統，以處理所識別的風險、保障上市公司資產、預防及偵測詐騙、不當行為和損失、確保上市公司財務報告準確無誤，以及遵守適用法例及規例。董事會應持續監察風險管理及內部監控系統。董事會亦有責任確保至少每年檢討上市集團風險管理及內部監控系統的有效性，而管理層應向董事會提供有關系統是否有效的確認。守則條文旨在落實前述原則，詳情載於守則條文D2.1條至D2.4條。現時並無針對風險管理及內部監控系統的建議最佳常規。就創業板上市公司而言，《創業板上市規則》亦載有類似條文，規定須遵守創業板《企業管治守則》有關風險管理及內部監控的規定。

持有執業證書的香港律師，須每年完成至少三小時，或過去兩年累計完成六小時風險管理教育課程，並須於申請執業證書續期時向律師會作出確認。風險管理教育包括但不限於參與講座、擔任講師，以及撰寫風險管理及相關活動的文章。

COSO企業風險管理模型下的風險管理實踐

COSO企業風險管理模型源自1985年成立的特雷德韋委員會贊助組織委員會（COSO），旨在應對美國若干財務報告欺詐問題。

out are to implement the Principle as hereinbefore stated, details of which are set out in CP D2.1 to CP D2.4. There is no RBP for risk management and internal control systems. Similar provisions are contained in the GEM Listing Rules for companies listed on GEM as regards risk management and internal control under the CG Code for GEM.

For a solicitor in Hong Kong holding a practising certificate, he is required to attend at least three hours of risk management education (RME) annually or six hours of RME for the past two years and is required to confirm to the Law Society on applying for renewal of his practising certificate. RME includes, amongst others, attending lectures, giving lecturing and writing articles on risk management and related activities.



Risk Management in Practice Under COSO ERM Model

The COSO ERM Model originated from the Committee of Sponsoring Organisation (COSO) of the Treadway Commission formed in 1985 to address certain fraudulent financial reporting in the US.

In a nutshell, the COSO ERM model is based on (a) five (5) risk management components; and (b) twenty (20) principles under the five risk management components.

The five risk management components are (a) governance and culture; (b) strategy and objective-setting; (c) performance; (d) review and revision; and (e) information communication and reporting.

In terms of governance and culture, there are five (5) principles, namely,

- (a) exercising board risk oversight;
- (b) establishing operating structures;
- (c) defining desired culture;
- (d) demonstrating commitment to core values; and
- (e) attracting, developing and retaining capable individuals.

In terms of strategy and objective-setting, there are four (4) principles, namely,

- (a) analysing business context;
- (b) defining risk appetite;
- (c) evaluating alternative strategies; and
- (d) formulating business objectives.

簡言之，COSO 企業風險管理模型基於：(a) 五個風險管理要素，及 (b) 五個風險管理要素下的二十項原則。

五大風險管理要素分別為：(a) 管治及文化；(b) 策略及目標設定；(c) 績效；(d) 審查及修訂；及 (e) 資訊溝通及報告。

管治及文化方面包含五項原則，分別是：

- (a) 行使董事會風險監督權；
- (b) 建立運作架構；
- (c) 界定理想文化；
- (d) 展現對核心價值的承諾；及
- (e) 吸引、培育及留住優秀人才。

策略及目標設定方面包含四項原則，分別是：

- (a) 分析業務環境；
- (b) 界定風險承受能力；
- (c) 評估替代策略；及
- (d) 制定業務目標。

績效方面包含五項原則，分別是：

- (a) 識別風險；
- (b) 評估風險嚴重程度；
- (c) 風險優先排序；
- (d) 實施風險應對措施；及
- (e) 建立組合。

In terms of performance, there are five (5) principles, namely,

- (a) identifying risk;
- (b) assessing severity of risk;
- (c) prioritising risks;
- (d) implementing risk responses; and
- (e) developing portfolio.

In terms of review and revision, there are three (3) principles, namely,

- (a) assessing substantial change;
- (b) reviewing risk and performance; and
- (c) pursuing improvement in enterprise risk management.

In terms of information communication and reporting, there are three (3) principles, namely,

- (a) leveraging information and technology;
- (b) communicating risk information; and
- (c) reporting on risk culture and performance.

Details of the five risk management components and the related twenty principles are contained in the Compliance Risk Management: Applying the COSO ERM Framework dated November 2020 issued by the Committee of Sponsoring Organisation of the Treadway Committee with each chapter describing the details and aspects of each risk management component.

For a company for profits, the following are the basic principles of risk management under the COSO ERM model:

- (a) the risk appetite of the company;
- (b) risk identification;
- (c) risk assessment;
- (d) risk mitigation;
- (e) risk monitor and review; and
- (f) communication and report.

Risk Appetite

Under the COSO ERM model, risk appetite is defined broadly as the overall level of risk that a company pursues to achieve its mission. It refers to the types and amount of risk a company is willing to accept in pursuit of its strategic objective and value creation.

It is trite that risk and return are associated in that higher risk will normally mean higher return but more uncertainties and vice versa. It is also trite that certain industries are riskier than other industries but

審查及修訂方面包含三項原則，分別是：

- (a) 評估重大變動；
- (b) 審查風險及績效；及
- (c) 追求改善企業風險管理。

資訊溝通及報告方面包含三項原則，分別是：

- (a) 運用資訊及技術；
- (b) 傳達風險資訊；及
- (c) 報告風險文化及績效。

五項風險管理要素及相關的二十項原則詳情載於特雷德韋委員會贊助組織委員會於2020年11月發佈的《合規風險管理：應用COSO企業風險管理架構》，其中各章節分別闡述各風險管理要素的詳情及範疇。

對牟利企業而言，COSO企業風險管理模型的基本風險管理原則如下：

- (a) 企業的風險承受能力；
- (b) 風險識別；
- (c) 風險評估；
- (d) 風險緩解；
- (e) 風險監控及審查；及
- (f) 溝通及報告。



with higher returns. Within an industry, certain projects are riskier with higher returns as compared with other projects.

By way of examples, certain industries like cryptocurrencies and block chains, biotechnologies and pharmaceuticals, semiconductors, energies, minings and hedge funds are riskier but with higher returns (if successful) than other industries like real estates for leasing and rental, utilities and manufacturings.

Within an industry say real estate development, certain projects like high end commercial building projects in New Territories are riskier than subsidised housing projects funded by the Government on Hong Kong Island.

The risk appetite of a company is set by the board at the highest level as to which level of risk the company will accept and on that basis to determine which industry and within such industry which project the company will undertake. Once the risk appetite is set, the company will identify the risks that are associated with the industry and the project in the context of the institutional structure of the company.

Risk Identification

There are general risks affecting all industries, for example, regional and international politics, regional and international hot money movement, interest rates, natural disasters, population trends, etc. Within a specific industry, for example real estate which is a core industry in Hong Kong, there are general risks associated with all projects within the real estate industry, notably of which are interest rates, labour supply and demand, and weather conditions.

In addition to general risks, there are specific risks that are associated with the company concerned and need to be identified and addressed. These risks are classified into strategic risk, operational risks, reporting risks and compliance risks.

The above risks are identified in structural or non-structural basis and on an ongoing basis, in the following ways and formats:

- (a) workshops and brainstorming sessions across and with inputs from all levels from directors to department heads to individual officers;
- (b) interviews with executives and staff for qualitative insights based on their operational circumstances;
- (c) process mapping to spot vulnerabilities (risks) and opportunities (returns) in their workflow;
- (d) review of documents, audits indications and historical data for trends;
- (e) scenario analysis, stress testing, and benchmarking against peer companies and where relevant, similar peer industries; and
- (f) data analytics and technology for real time pattern detection.

風險承受能力

根據 COSO 企業風險管理模型，風險承受能力被廣泛定義為企業為實現其使命所願意承擔的整體風險水平，即企業在追求策略目標及創造價值的過程中願意承擔的風險類型及程度。

風險與回報密切相關早已是老生常談 — 風險較高通常意味著回報亦較高，但同時伴隨更多不明朗因素，反之亦然。同樣不言而喻的是，某些行業的風險高於其他產業，但回報亦更高。在同一行業內，某些項目相較於其他項目風險更高，但回報亦更高。

例如，加密貨幣及區塊鏈、生物科技及製藥、半導體、能源、礦業及對沖基金等若干行業，其風險雖高於房地產租賃、公用事業及製造業等，但若然業務成功，這些行業的回報亦更高。

以房地產開發為例，新界一些高級商業大樓項目的風險便高於港島由政府資助的房屋項目。

企業的風險承受能力由最高層的董事會確定，決定企業可承受的風險水平，並據此決定企業將進入那個行業以及在該行業中承接那些項目。確定風險承受能力後，公司將就企業組織架構識別與該行業及項目相關的風險。

風險識別

所有行業均受若干普遍風險影響，例如區域及國際政治、區域及國際熱錢流動、利率、自然災害、人口趨勢等。在特定行業內，例如香港的核心行業 — 房地產，所有房地產項目均承受普遍風險，其中以利率、勞動力供求及天氣狀況尤為顯著。

除普遍風險外，還存在與特定企業相關的特殊風險，需加以識別及應對。此類風險可分為策略風險、營運風險、報告風險及合規風險。

上述風險透過以下方式及形式以結構化或非結構化基礎持續識別：

- (a) 舉辦跨職級工作坊及集思會，匯集從董事會、部門主管到個人職員所有職級的意見；
- (b) 與高階主管及員工進行訪談，根據其反映的營運情況獲得定性見解；
- (c) 繪製流程圖，以辨識工作流程中的漏洞（風險）及機遇（回報）；
- (d) 審閱文件、審計指標及歷史數據以掌握趨勢；
- (e) 進行情境分析、壓力測試，並參照同業及相關類似行業進行基準比較；及
- (f) 運用數據分析及技術進行即時模式檢測。

Risk Assessment

Once a risk is identified, a company will have to assess this risk based on (a) its likelihood to occur; and (b) if occurred, its impact to the company. This is called the risk likelihood and impact grid with the risk likelihood on the X-axis and the risk impact on the Y-axis. Generally, a risk with a high likelihood and high impact will be high risk. On the contrary, a risk with a low likelihood and low impact will be low risk. Any risk in between is medium risk. Based on the risk grid, a company may assign a percentage to each risk to classify the risks from high risk to medium and to low risks. The likelihood and impact may be assessed qualitatively using professional judgement or quantitatively using risk assessment model, an example of which is the Monte Carlo simulation recommended under the COSO ERM framework.

Once the risks are assessed and depending on the risk appetite of the company, a risk may be avoided or accepted entirely, reduced by way of risk mitigation or shared by bringing in new partners. This is generally called risk management. For most of the risks that cannot be shared, a company will consider ways and means to reduce such risks by risk mitigation.

Risk Mitigation

In order to reduce the risks, certain risk management controls are recommended under the COSO ERM frameworks, namely,

- (a) preventive controls to eliminate and prevent root causes, for example, process redesigns to avoid such risks and access restrictions to minimise cyber threats;
- (b) detective controls to introduce early warning mechanism, for example, key risk indications and audits to identify deviation; and
- (c) corrective controls to reduce post event damages by way of damage control, for example, contingency plans and backup systems.

Risk Monitor and Review

Once all risks are identified, assessed, controlled and mitigated, these risks will be monitored and reviewed on an ongoing basis by all levels of management and staff to ensure that all risk management measures and all controls, preventive, detective and corrective, are implemented properly and effectively. A company is required not only to ensure that these risk management measures and controls are implemented and in place, but also to test them to ensure that they are adequate, proper and effective. At the board level, executive directors (EDs) are responsible for the implementation and operation of these risk management measures and controls and will report the same to the full board. For independent non-executive directors (INEDs), they are responsible for the implementation but may rely on the executive team to ensure that the risk management measures and controls are operated adequately, properly and effectively on an ongoing basis.

風險評估

一旦識別到風險，企業須依據以下兩項原則評估該風險：(a) 發生的可能性，及 (b) 若然發生，對企業的影響。這種評估被稱為風險可能性及影響矩陣，其中X軸代表風險發生的可能性，Y軸代表風險的影響。一般而言，發生可能性高且影響大的風險屬於高風險。反之，發生可能性低且影響小的風險屬於低風險。介於兩者之間的風險皆為中風險。企業可依據風險矩陣，為每項風險分配百分比，從而將風險分為高、中、低不同風險。風險發生的可能性和影響可運用專業判斷進行定性評估，亦可使用風險評估模型進行定量評估，例如COSO企業風險管理架構建議的蒙地卡羅模擬分析。

風險評估完成後，根據企業的風險承受能力，企業可決定完全迴避或接受某項風險、透過風險緩解措施將風險減低，又或引入新合作夥伴攤分風險。此過程通常稱為風險管理。對於無法分攤的風險，企業多會考慮採取風險緩解措施降低此類風險。

風險緩解

為降低風險，COSO企業風險管理架構建議採取特定的風險管理控制措施，包括：

- (a) 預防性控制措施，以消除及防範根本原因，例如重新設計流程以避免此類風險，並實施存取限制，將網絡威脅降至最低；
- (b) 偵測性控制措施，以建立早期預警機制，例如關鍵風險指標及審計以識別偏差；及
- (c) 糾正性控制措施，以透過損害控制降低事後損失，例如應變計劃及備份系統。

風險監控及審查

在識別、評估、控制及緩解所有風險後，各級管理層及員工將持續監控及審查相關風險，確保所有風險管理措施以及所有預防性、偵測性及糾正性控制措施均得到妥善及有效實施。企業不僅須確保風險管理措施及控制措施落實到位，更須進行測試以確保措施充分、妥善且有效。在董事會層面，執行董事負責推動風險管理措施及控制措施的實施及運作，並向全體董事匯報。獨立非執行董事則負責實施，但可依賴管理團隊確保風險管理措施及控制措施持續以充分、妥善且有效的方式運作。

溝通及報告

溝通旨在確保所有風險以及其管理及控制措施從董事會傳達至企業各職級，尤其是總部的高級管理層及駐營業地點的各部門主管。

報告旨在確保各職級（尤其是營運部門）定期審查影響公司風險及其管理和控制措施的所有事項，並將涉及所有或任何預防性控制措施、偵測性控制措施及/或糾正性控制措施的所有觀察結果、漏洞及偏差從基層迅速回報至營運主管、總部，且最終呈報至執行董事會及全體董事。

Communication and Report

Communication is to ensure that all risks and their management and control are communicated from the board to all levels within the company particularly senior management at head office and department heads on sites.

Report is to ensure that all matters affecting the company's risks and their management and control are reviewed regularly by all levels, in particular, the operational departments, with all observations, weaknesses and deviations as regards all or any preventive controls, detective controls and/or corrective controls promptly reported back from ground level, to operational head, to the head office and ultimately to the executive board and full board.



Risk Management Report

For companies listed on Hong Kong Stock Exchange, the above will be contained in the Risk Management Report to be prepared by the executive team or professional risk management advisers (with inputs from the executive team) and will be discussed at the full board meeting together with, and as an integral part of, the Corporate Governance Report as required under MBLR 13.89(1). As a matter of practice, the Risk Management Report will be discussed at board meeting but will not be included nor disclosed in the Corporate Governance Report. For other companies not listed, normally no formal Risk Management Report will be prepared but a general discussion of risk management will be included in the Directors' Report to be prepared by the directors and to be approved by the shareholders at the annual general meeting as required under the Companies Ordinance, Cap. 622.

Conclusion

This article recaps the gist of risk management under COSO ERM framework focusing on the practical aspects as regards risk appetite, risk assessment, risk control and mitigation, risk monitor and review, and risk communication and report, all of which are included in the Risk Management Report which will constitute a part and parcel of (a) the Corporate Governance Report under the Listing Rules for companies listed on Hong Kong Stock Exchange; and (b) the Directors' Report under the Companies Ordinance, Cap. 622 for other companies incorporated in Hong Kong. The Corporate Governance Report and the Directors' Report will be discussed at board level and will be approved by the shareholders in annual general meeting. For companies that are incorporated outside Hong Kong but are listed on Hong Kong Stock Exchange, such companies are required to comply with the Listing Rules and the company laws of places where such companies are incorporated as regards risk management and disclosure. **M**

— Vincent P C Kwan

Solicitor/Certified Public Accountant (Fellow) (Non-Practising)
Member (Formerly Chairman), FRA Committee
The Chamber of Hong Kong Listed Companies

風險管理報告

於香港交易所上市的公司須將上述內容納入由執行團隊或專業風險管理顧問（參考執行團隊意見）編製的風險管理報告，並須根據《主板上市規則》第13.89(1)條規定，與《企業管治報告》於董事會會議上一併討論，並作為《企業管治報告》的一部分。實務上，風險管理報告將於董事會會議上討論，但不會納入或披露於《企業管治報告》內。其他非上市公司通常不會編製正式的風險管理報告，但根據《公司條例》（第622章）規定，董事會將編製並於股東周年大會上提交股東批准的董事會報告中，納入有關風險管理的一般性討論。

結語

本文概述了COSO企業風險管理架構下的風險管理要點，重點探討風險承受能力、風險評估、風險控制及緩解、風險監控及審查、以及風險溝通及報告等實務層面。上述內容均納入風險管理報告，而該報告構成以下文件的組成部分：(a) 於香港交易所上市的公司根據《上市規則》提交的《企業管治報告》；及(b) 其他香港註冊成立公司根據《公司條例》（第622章）規定提交的《董事報告》。《企業管治報告》及《董事報告》須經董事會討論，並於股東周年大會上獲股東批准。在香港境外註冊成立但於香港交易所上市的公司，則須同時遵守《上市規則》以及其註冊地的公司法中有關風險管理及披露的規定。**M**

— 關保銓

律師 / 資深會計師（非執業）
香港上市公司商會
財經事務及監管政策委員會委員（及前任主席）