"Alert to **Black Swan** and Prevent **Gray Rhino**"

「**警惕**黑天鵝 **防範**灰犀牛」

In addressing the opening ceremony at the Central Party School of the CPC Central Committee presided by Premier Li Keqiang and attended by standing committee members Li Zhanshu, Wang Yang, Wang Huning, Zhao Leji and Han Zheng on 21 January 2019, President Xi Jinping noted that China's national security and stability were under multiple threats from within and without and warned that "we must be alert to Black Swan and prevent Gray Rhino" in managing risks or events that were confronted by China. Since then, the terms "Black Swan" and "Gray Rhino" have been wildly circulated and reported across social media in China. This article will discuss:

- What is "Black Swan";
- What is "Gray Rhino";
- How Black Swan and Gray Rhino events are related to risk management;
- How risks are identified, assessed, responded to and controlled in the context of COSO (Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk Management ("ERM") Framework; and
- The legal and regulatory issues relating to risk management under (a) the Companies Ordinance; (b) the Listing Rules; and (c) the Legal Practitioners (Risk Management Education) Rules, Cap. 159Z ("RME Rules") made under section 73 of the Legal Practitioners Ordinance, Cap. 159.

Black Swan

Prior to the discovery of black swans by the Dutch explorer Willem de Vlamingh in Australia in January 1697, people then believed that all swans were white, and black swans simply didn't exist. In modern times, "Black Swan" was coined by Nassim Nicholas Taleb in his first book "*Fooled by Randomness: the Hidden Role of Chance in Life and in the Markets*" published in 2001, and in his second book published in 2008, titled "*The Black Swan: the Impact of the Highly Improbable*" to denote, in his own words, risk or an event with the following three attributes:

"First, it is an outlier, as it lies outside the realm of regular expectations, and nothing in the past can convincingly point to its possibility. Second, it carries an extreme "impact". Third, in spite of its outlier status, human nature makes us concoct expectations for its occurrence after the fact, making it explainable and predictable."

Under the conventional wisdom, risks are studied quantitatively under the bell shape of the normal distribution curve that black swan risks or events are normally excluded or ignored as being too remote or too uncertain or too unpredictable.

Classic black swan events, to name a few, include the 11 September attacks by terrorists, World War I and II, catastrophic floods, droughts and epidemics. Given that these events or risks are either improbable or unpredictable or both that people develop a psychological bias and "collective blindness" to them, not knowing the fact that such rare, but major, events are by definition outliers makes them dangerous.

習近平主席在2019年1月21日由李克強總理主持、常委栗戰書、汪洋、王滬寧、趙樂際及韓正出席的中共中央委員會中央黨校開班式上致辭時指出：中國的國家安全與穩定面臨著來自內部及外部的多重威脅，並強調在應對中國面臨的風險或事件時，「我們必須警惕黑天鵝，也要防範灰犀牛」。此後，「黑天鵝」及「灰犀牛」二詞在中國社交媒體上廣為流傳並得到廣泛報導。本文將討論：

- 什麼是「黑天鵝」；
- 什麼是「灰犀牛」；
- 黑天鵝及灰犀牛事件與風險管理有何關聯；
- 在COSO（全美反虛假財務報告委員會下屬發起人委員會）企業風險管理框架下如何識別、評估、應對及控制風險；及
- 下列法規下風險管理的相關法律及法規問題：(a)《公司條例》；(b)《上市規則》；及(c)根據《法律執業者條例》（第159章）第73條制定的《法律執業者（風險管理教育）規則》（第159Z章）（「RME規則」）。

黑天鵝

在1697年1月荷蘭探險家威廉．德．弗拉明格（Willem de Vlamingh）於澳洲發現黑天鵝之前，人們認為所有天鵝全是白色，根本就不存在黑天鵝。在現代，納西姆．尼古拉斯．塔勒布（Nassim Nicholas Taleb）於2001年出版的第一本書《隨機騙局：潛藏在生活與市場中的機率陷阱》（Fooled by Randomness: the Hidden Role of Chance in Life and in the Markets）及2008年出版的第二本書《黑天鵝效應》（The Black Swan: the Impact of the Highly Improbable）中提出「黑天鵝」，用他自己的話說，用來表示具有以下三個屬性的風險或事件：

「首先，它是一個離群值，處於正常的期望範圍之外，不存在足以證明其可能性的前例。第二，它會帶來極大的「衝擊」。第三，儘管事件處於離群值，人們會出於天性在事後編造出解釋，稱這事件為可解釋或可預測的。」

按照傳統觀點，我們按照正態分佈的鐘形曲線對風險進行定量研究，而黑天鵝風險或事件通常由於可能性太低、太不確定或太不可預測而被排除或忽略。

典型的黑天鵝事件包括911恐怖襲擊、第一次世界大戰和第二次世界大戰、災難性的水災、旱災及流行病。鑑於這些事件或風險發生的可能性低或不可預測，或者兩者兼備，人們對其產生了心理偏見和「集體失明」，無法意識到這些罕見而重大的事件屬於離群值正是它們如此危險的原因。

Gray (or Grey) Rhino

Quite the contrary, rhinos are described as either black or white but in fact most if not all rhinos are gray in colour, neither pure black nor pure white. In risk management sense, the term "Gray Rhino" was first introduced and coined by Michele Wucker at the World Economic Forum Annual Meeting in Davos Switzerland in January 2013 and was further developed in her book in 2016 by the name "The Gray Rhino: How to Recognize and Act on the Oblivious Dangers we Ignore". Like the elephant in the room, a gray rhino is a "highly probable, high impact yet neglected threat…gray rhinos are not random surprises, but occur after a series of warnings and visible evidence". Examples of gray rhino events and the associated risks are the bursting of the housing bubble in the US in 2008, US-China tensions, and the current social unrest in Hong Kong. People are aware of these gray rhino events but take these for granted as something that are outside of their control and do not factor them into their risk assessment.

Black swans and gray rhinos are only particular, and rare, cases under the risk management framework of an enterprise. There are different models or frameworks to address the risk management of an enterprise, the most popular one is the COSO Framework.

Internal Control and Risk Management under COSO Framework

On internal control, an integrated framework has been developed by COSO with five (5) components and seventeen (17) principles. The five components are control environment, risk assessment, control activities, information and communication, and monitoring activities. Under risk assessment component, there are four (4) principles, namely,

- The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to the objectives;
- The organisation identifies risks to the achievement of the objectives across the entity and analyses risks as a basis for determining how the risks should be managed;
- The organisation considers the potential for fraud in assessing risks to the achievement of objectives; and
- The organisation identifies and assesses changes that could significantly impact the system of internal control.

灰犀牛

恰恰相反，犀牛被描述為黑色或白色，而實際上絕大多數犀牛都是灰色，既不是純黑色也不是純白色。從風險管理的角度來看，「灰犀牛」一詞最早是由米歇爾·沃克（Michele Wucker）在2013年1月瑞士達沃斯舉行的世界經濟論壇年會上提出，而後在2016年名為《灰犀牛：危機就在眼前，為何我們選擇視而不見?》（The Gray Rhino: How to Recognize and Act on the Oblivious Dangers we Ignore）的著作中作出進一步闡述。正如「房間裡的大象」，灰犀牛是指「大概率、影響巨大卻被忽視的威脅……灰犀牛不是隨機突發事件，而是在一系列警示信號和跡象之後出現」。灰犀牛事件及其相關風險實例包括2008年美國房地產泡沫破裂、中美緊張局勢以及香港當前的社會動盪。人們已經意識到了這些灰犀牛事件，但將超出他們控制範圍的事情視為理所當然，因此沒有將其納入風險評估。

在企業的風險管理框架下，黑天鵝及灰犀牛僅是特殊罕見的案例。有多種處理企業風險管理的模型或框架，最普遍的一種是COSO框架。

COSO框架下的內部控制與風險管理

在內部控制方面，COSO制定了一個包含五(5)大元素及十七(17)項原則的整體框架。五大元素是控制環境、風險評估、控制活動、資訊與溝通及監控活動。在風險評估元素下有以下四(4)項原則：

On risk management, in June 2017, COSO has issued "Enterprise Risk Management – Integrating with Strategy and Performance". The new framework clarifies "the importance of enterprise risk management in strategic planning and embedding it throughout an organisation – because risk influences and aligns strategy and performance across all departments and functions".

The COSO framework on risk managment is a set of twenty (20) principles orgainised into five (5) integrated components. The five components are:

- Governance and Culture with five principles;
- Strategy and Objective Setting with four principles;
- Performance with five principles;
- Review and Revision with three principles; and
- Information, Communication and Reporting with three principles.

Under the component of performance — which is the focus of this article — there are five principles:

- Identifies Risk;
- Assesses Severity of Risk;
- Prioritises Risk;
- Implements Risk Responses; and
- Develops Portfolio View.

In the following sections, focus will be on the identification of risks, assessment of risks, response to risks, and control of risks, and in the context of COSO thought paper entitled "ERM Risk Assessment in Practice" issued in October 2012.

Identification of Risks

Any event is associated with risks. The risk (or event) identification process must be made before any risk assessment. The identification process will produce a comprehensive list of risks — and also the associated opportunities — organised by risk category, financial; operational; strategic; compliance and sub-category (market, credit, liquidity, etc) for business units, corporate functions and capital projects. In the past, black swans would not be identified and would likely be ignored as too remote a risk or too uncertain a risk and in many cases, black swan risks were unaware of. Even if black swan risks are considered, they will be assessed as too remote to be of concern; for example, when a company receives a normal order for goods, it will not consider the risk that such goods will be intercepted by terrorists and so will not assess, nor respond to, nor control such a risk. As regards gray rhinos, they are like the elephant in the room that all is taken for granted and ignored, given that corporations may not have control over such risks. For example, companies in Hong Kong are aware of the Sino-US trade disputes that may have significant impact on all businesses in Hong Kong. The risk associated with such trade disputes is a gray rhino that is known to, but ignored by, all in business. All think that such risks are general risks affecting all, but are not specific risks affecting specific businesses or a specific company.

- 組織設定清晰的目標，以便能夠識別和評估與目標有關的風險；
- 組織識別整個公司層面可能威脅組織實現目標的風險，並分析風險，以此為基礎來確定如何對這些風險進行管理；
- 組織在評估威脅組織實現目標的風險時考慮欺詐的潛在可能；及
- 組織識別並評估可能會嚴重影響內部控制系統的變化事項。

在風險管理方面，COSO於2017年6月發佈《企業風險管理 — 與策略和績效相整合》。新框架闡明了「企業風險管理在策略規劃以及將其融入整個組織中的重要性 — 因為風險影響並協調所有部門和職能部門的策略和績效」。

COSO風險管理框架由二十(20)條原則組成，分為五(5)大綜合元素。這五大元素包括：

- 管治和文化，有五項原則；
- 策略及目標設定，有四項原則；
- 績效，有五項原則；
- 審閱及修訂，有三項原則；及
- 資訊、溝通和報告，有三項原則。

在績效元素（本文重點）下的五項原則是：

- 識別風險；
- 評估風險的嚴重程度；
- 風險排序；
- 實施風險響應；及
- 建立投資組合觀。

下文將重點討論風險識別、風險評估、風險響應以及風險控制，並結合2012年10月發佈的COSO思想文件「實踐中的ERM風險評估」。

風險識別

任何事件均存在風險。在作出任何風險評估之前，必須執行風險（或事件）識別過程。在識別過程中，將編寫一份全面的風險及相關機會列表，按風險類別、財務狀況、營運、策略、合規性及子類別（市場、信貸、流動性等）對業務部門、公司職能部門及資本項目進行分類。過去，黑天鵝不會被發現，並且由於風險可能性過低或太過不確定而可能會被忽略，在許多情況下人們無法意識到黑天鵝風險。即使考慮到黑天鵝風險，亦會被評估為可能性過低而不足為慮；例如，當公司收到一份正常的商品訂單時，不會考慮恐怖分子攔截該等商品的風險，因此不會評估有關風險並對此作出響應或控制。至於灰犀牛，它們就像「房間裡的大象」，因習以為常而遭到忽視，因為公司可能沒有控制該等風險的措施。例如，香港公司意識到中美貿易爭端可能會對香港所有企業產生重大影響。與該等貿易糾紛相關的風險即是灰犀牛，眾所周知，卻被所有企業視而不見。所有人都認為該等風險是影響所有人的總體性風險，而不是影響特定企業或特定公司的特定風險。

Assessment of Risks

After the risks are identified, they will be assessed qualitatively (by business judgement) or quantitatively (by risk models, the most popular being the Monte Carlo simulation model). Under COSO, the Likelihood-Impact grid or matric is used with the horizontal line (x-axis) representing the likelihood of the risk occurring and the vertical line (y-axis) representing the impact to the entity if the risk does occur.

The likelihood is categorised into low (chance of risk occurring), medium or high. The impact (based on financial or otherwise) is categorised into low (impact when the risk does occur), medium or high. Based on the Likelihood-Impact analysis, an event may be of low, medium or high risk.

Response to Risks

Once the risks are identified and assessed, management will respond to the risks. Under the COSO framework, a response will include:

- Risk avoidance (or elimination);
- Risk reduction (or mitigation);
- Risk sharing (or transfer); or
- Risk acceptance.

Normally, an enterprise will avoid an event with high risk and accept an event with low risk. For an event with medium risk, an enterprise will (a) reduce the risk by undertaking control measures or activities or (b) transfer the risk by insurance, or (c) share the risk by, for example, taking in a partner who is better equipped to handle such risk.

Control of Risks

Under the COSO framework, risks may be controlled to a certain extent by taking measures to mitigate the inherent risks so that after taking such measures, the residual risks are reduced to a level that is acceptable to the enterprise.

Risk Management under Companies Ordinance

For a company incorporated under the Companies Ordinance, unless exempted, the directors must prepare a directors' report incorporating a business review under section 388. The business review must comply with, and must disclose the information contained in, Schedule 5. Under section 1(b) of Schedule 5, the business review must consist of "a description of the principal risks and uncertainties facing the company".

Risk Management under Listing Rules

For a company listed on Hong Kong Stock Exchange, a listed company is required to incorporate and disclose a business review complying with Schedule 5 of the Companies Ordinance under paragraph 28(2)(d) of Appendix 16 to the Main Board Listing Rules.

Under the Corporate Governance Code of the Listing Rules, by way of principle, the board of a listed company is responsible (a) for evaluating and determining the nature and extent of the risks it is willing to take; and (b) for ensuring and overseeing that the listed company has established and maintained appropriate and effective

風險評估

識別風險後，將對它們進行定性（透過商業判斷）或定量（透過風險模型，最普遍的是蒙特卡洛模擬模型）評估。COSO使用似然影響網格或矩陣，以橫線（x軸）表示發生風險的可能性，豎線（y軸）表示發生風險時對實體的影響。

可能性分為低、中或高三檔（發生風險機率）。（財務或其他方面的）影響分為低、中或高三檔（在發生風險時的影響）。根據可能性影響分析，事件可能具有低、中或高風險。

風險響應

在識別及評估風險後，將針對風險加以管理。在COSO框架下，響應將包括：

- 規避風險（或消除風險）；
- 降低風險（或減緩風險）；
- 風險分擔（或轉移）；或
- 風險承擔。

通常，企業會避免高風險事件，而接受低風險事件。對於具有中等風險的事件，企業將(a)透過採取控制措施或活動來降低風險，或(b)透過保險轉移風險，或(c)透過選擇能夠更好地處理此類風險的合夥人來分擔風險。

風險控制

在COSO框架下，可以採取措施減緩固有風險來在一定程度上控制風險，使此後的剩餘風險降至企業可以接受的水平。

《公司條例》下的風險管理

對於根據《公司條例》註冊成立的公司，除非獲得豁免，否則董事必須根據第388條擬備一份納入業務審視的董事報告。業務審視必須符合且必須披露附表5所載資訊。根據附表5第1(b)條，業務審視必須包括「對公司面對的主要風險及不明朗因素的描述」。

《上市規則》下的風險管理

在香港證券交易所上市的公司，必須根據《主板上市規則》附錄16第28(2)(d)段納入及披露符合《公司條例》附表5的業務審視。

根據《上市規則》下的《企業管治守則》，原則上，上市公司董事會負責(a)評估及釐定其願意接納的風險性質及程度；及(b)確保及監督上市公司設立及維持合適及有效的風險管理及內部控制系統。就此而言，守則條文提供了有關如何實施及檢討內部控制及風險管理系統的詳細條文。

RME規則下的風險管理

RME規則規定，任何人若成為律師、實習律師或外地律師，須根據RME規則第5條的規定完成RME一般必修課程。根據第6條的規定，若律師成為合夥人，必須完成主管必修課程。根據第7條的規定，之後所有律師必須每年至少完成3小時，或在連續兩個執業年度內完成

risk management and internal control systems. In relation thereto, the code provisions provide detailed provisions as to how the internal control and risk management systems are implemented and reviewed.

Risk Management under RME Rules

Under the RME Rules, a person is required to attend the general core course on RME on his becoming a solicitor, a trainee solicitor or a foreign lawyer under section 5 of the RME Rules. A solicitor is required to attend the principal's core course on his admission to partnership under section 6. All lawyers are subsequently required to attend at least three hours annually, or six hours in two consecutive practice years, of elective courses on RME under section 7. For the purpose of RME Rules, risk management is defined under section 2 as 'any action or plan of action the objective of which is to minimise the risk of a person's exposure to claims against him in the course of his professional practice and to reduce the extent of loss which may arise from such claims'. In terms of risk management for a law firm, the COSO Framework on risk management is also applicable in the same way as other commercial enterprises. There are also black swans to be alert to and gray rhinos to be avoided for a law firm in its legal practice.

Conclusion

President Xi has made a very correct and timely warning to those compliance professionals who are involved in risk management that they should not only be concerned with normal risks under the normal distribution curve that is likely to occur, but that they should also consider risks or events that rarely occur, but once occurred, the impact will be very significant. To recap President Xi's warning, all compliance professionals should be alert to Black Swans and should prevent Gray Rhinos. M

Vincent P C Kwan
Solicitor and Certified Public Accountant (Fellow) (Non-Practising)
Member (and ex-Chairman), FRA Committee
The Chamber of Hong Kong Listed Companies

6小時的RME選修課程。就RME規則而言，風險管理在第2條中定義為「任何行動或行動方案，其目標是把某人在其專業執業過程中遭申索的風險減至最低，以及減少因該等申索而可能引致的損失的程度」。律師事務所在風險管理方面，也與其他商業企業一樣適用COSO風險管理框架。對於一家律師事務所而言，在法律執業中也要警惕黑天鵝、防範灰犀牛。

結語

習主席對涉及風險管理的合規專業人士發出了非常正確而及時的警告，即他們不僅應關注符合正態分佈曲線的可能發生的常規風險，亦應考慮罕見但是一旦發生將產生巨大影響的風險或事件。重申習主席的警告：所有合規專業人士都應警惕黑天鵝，防範灰犀牛。M

關保銓
律師及資深會計師（非執業）
香港上市公司商會
財經事務及監管政策委員會成員（及前任主席）