前言

本風險管理準則是由英國主要風險管理機構的精英組成的團隊所研擬出來的成果，這些機構包括風險管理學會(IRM)、保險及風險管理人協會(AIRMIC)及屬政府部門的風險管理國家研討會(ALARM)等。

此外，在長期的諮詢過程中，該團隊也向其他關注風險管理的專業團體極廣泛地徵詢其觀點及意見。

風險管理是一門正在快速發展的學科，對於風險管理的範圍、實施方法以及目的等問題有很多不同的看法及描述，需要以準則來確保下列事項可達一致性：

- *相關的專門術語*
- *實施風險管理的步驟*
- *風險管理的組織架構*
- *風險管理的目的*

重要的是本準則認定風險有好有壞。

風險管理不只是企業或政府機構的事，它也關係到任何短期及長期的活動，我們不能僅從活動的本身來考慮事情，還要兼顧許多可能被活動影響的各種損益關連者(stakeholders)。

達成風險管理的目的有許多種方法，我們無法嘗試在單獨一份文件中盡述，因此我們並不打算以"搬字過紙"的方式來訂定一套僵硬的準則，或建立一套被鑒認的程序。只要能達成本準則的各構成部分的要求，即使方法有別，機構仍可宣稱其符合準則。本準則提供了最佳的實務，機構可以據此作自我評估。

本準則已儘量使用國際標準化組織(ISO)近期文件ISO/IEC風險管理指南73-字彙-準則使用指導方針中的風險專門術語。

由于本領域發展快速，作者歡迎使用此準則的機構能把意見回饋（地址在本準則的封底），本準則將例行作修訂以反映最佳實務。

1. 風險

風險可定義為事件發生的可能性及其結果的組合(ISO/IEC指南73)。

我們進行任何事情，事件及其結果都潛藏獲利 (正面）或威脅成功（負面）的機會。

風險管理逐漸開始重視風險的正面及負面影響；因此，本準則也從這兩方面来考量。

在安全的領域，通常認為只有有負面的結果，因此，安全風險之管理專注於損害的預防及降低。

2. 風險管理

風險管理是機構策略管理的核心部分，它是機構以條理化的方式來處理活動中的風險的步驟，其目的是從每一項活動及全部活動的組合中獲得持續的利益。

好的風險管理專注於風險的界定及處置，目的是為機構的活動帶來最大的持續價值，它整理出所有可能帶給機構正面及負面影響的因素，從而提升達成機構整體目標的可能性，並降低失敗的可能性和不確定性。

風險管理應該是一項持續發展的步驟，持續運作於機構策略的制定及實施中，它應該條理化地處理機構活動在過去、現在和尤其是未來所面臨的風險。

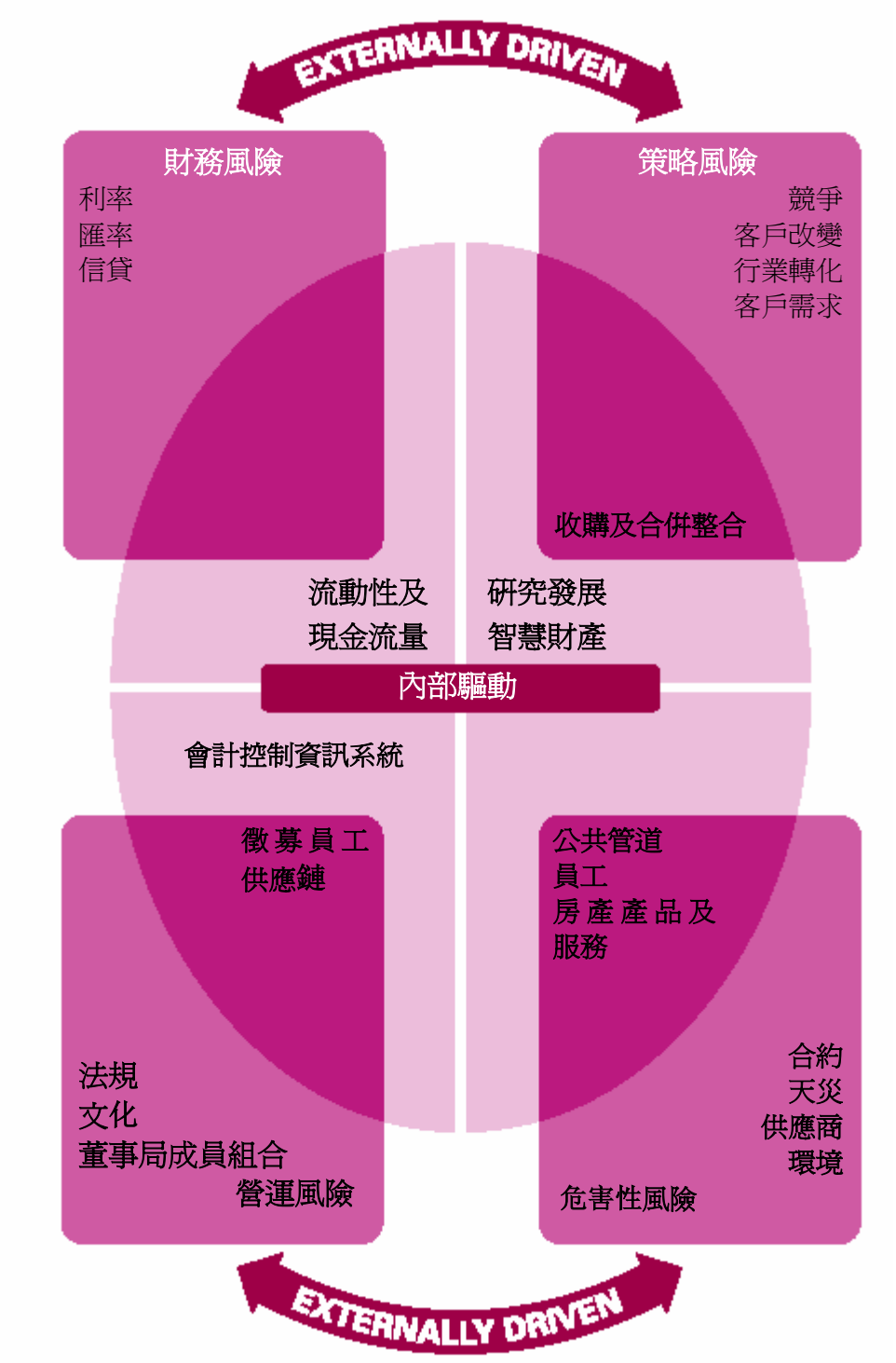
風險管理應該透過最高管理階層把有效的政策及計畫整合於企業文化中，把策略轉換成戰略性及營運性目標、將責任分配到各經理及員工，並視其為職務說明的一部分。風險管理支持問責、績效評估及獎懲，並籍此促進所有階層的營運績效。

2.1 外部及內部因素

機構及其營運所面臨的風險可能是由該機構外部或內部因素所造成，下頁圖表總結了這些領域主要風險的例子，同時也顯示出某些特定的風險可能同時受到外部及內部因素的驅動，而重叠在這兩個領域。它們可再細分為幾種風險型態，例如：策略方面、財務方面、營運方面及突發事件方面等。

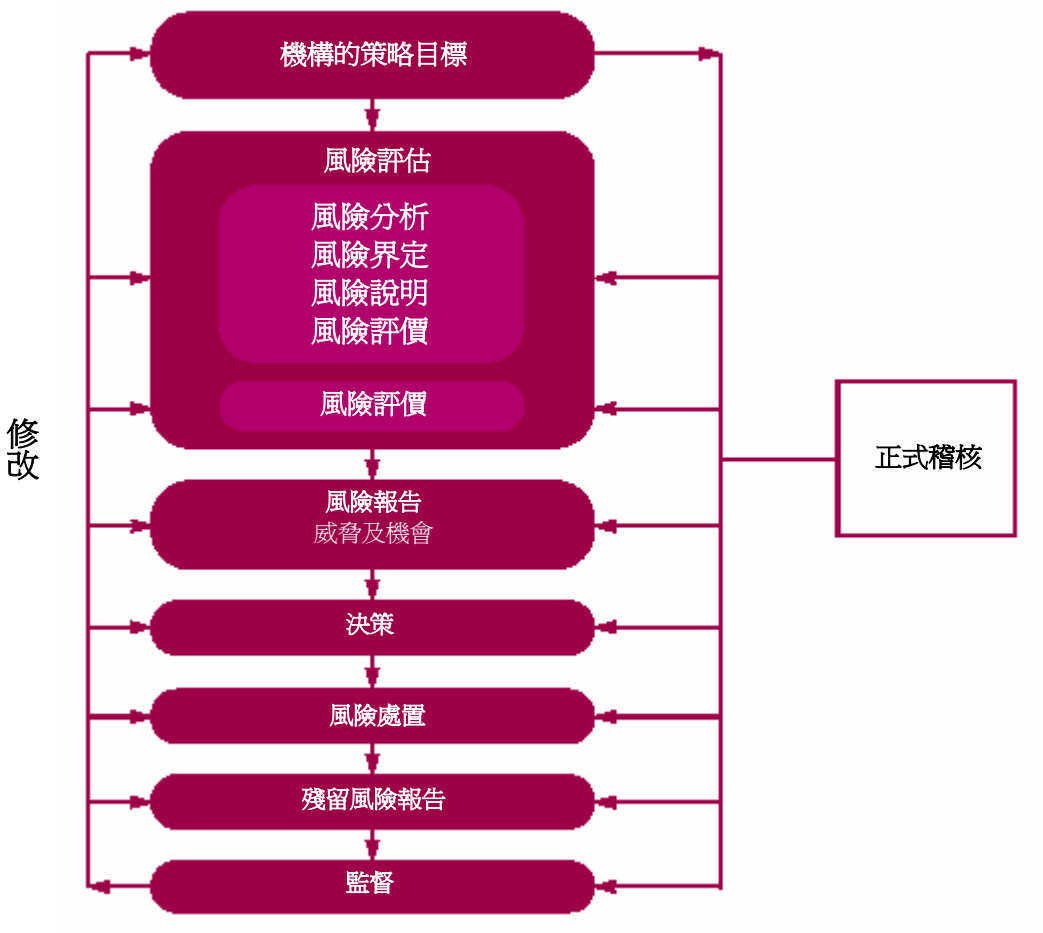
2.1 主要風險驅動因素案例

外部驅動



外部驅動

2.2 風險管理步驟



風險管理透過支持機構策略目標而為機構及其損益關連者提供保障和增加價值，方法如下：

- *為機構提供一個架構,讓未來活動能以一貫且可掌控的方式來進行*
- *透過全面性和系統性了解業務活動、變幻及項目機會/威脅,來改善決策,計畫及優先順序的訂立*
- *更有效地在機構內使用/配置資金及資源*
- *減少企業內非必要領域的開發*
- *保障並強化資產及公司形象*
- *開發並支援人員及機構的知識基礎*
- *提升營運效率*

3. 風險評價

ISO/IEC 指南 73 將風險評價定義為風險分析及風險評估的整體步驟。（請參閱附件）

4. 風險分析

4.1 風險界定

風險界定是界定機構對不確定性情況的暴露程度，必須對機構、其所經營的市場、其所處環境的法律、社會、政治及文化有深入的認識；同時必須徹底了解其策略性及營運性目標，包括成功的關鍵因素以及影响達成這些目標的相關威脅及機會。

界定風險應以有條理的方法來進行，以確保機構內的主要活動及相關風險都經過審視和認定，所有伴隨這些活動的變數都應被界定及分類。

我们可用不同的方法來區分企業的活動及決策，例如：

- *策略性的 – 這些關係到機構的長期策略目標，可能會受到資本可用性、統治權及政治風險、法規變更、名譽及實際環境轉變的影響。*
- *營運性的 – 這些關係到機構為實踐其策略目標所面對的日常事務。*
- *財務性的 – 這些關係到機構財務的有效管理及控制以及外部因素的影響，例如：信貸額、外幣兌換率及利率變動以及其他市場風險。*
- *知識管理 – 這些關係到知識資源的生產、保護及溝通的有效管理及控制，外部因素可能包括未經授權使用或濫用智慧財產、區域性停電以及競爭技術等；內部因素可能是系統故障或重要職員離職等。*
- *守法 – 這些關係到健康與安全、環保、交易描述、消費者保護、資料保護、聘僱方式及法規等*

雖然我们可以聘请顧問來界定風險，但透过內部管道, 利用良好的溝通、一貫且協調的步驟及工具（請參閱附件）,可能會更有效率。由內部”認同”的風險管理流程是必要的。

4.2 風險描述

風險描述的目的是將已界定的風險以結構性的形式呈現出來，例如用表列式。下一頁的風險描述表可用來描述及評估風險。我們必須使用設計良好的架構來全盤進行風險界定、描述及評價. 表中所列各項風險的結果及可能性，經过考虑后, 我們就可以把須要更詳細分析的主要風險之優先順序排列出来。

伴隨企業活動及決策的風險可以分類為策略性、項目性/戰略性及營運性。

特定的項目在規劃階段以及整個生命週期都應該納入風險管理之內。

表 4.2.1 – 風險描述

1. 風險名稱	
2. 風險範圍	對事件之規模、型態、數量及關聯性作本質上的描述。
3. 風險的本質	例如：策略性、营运性、財務性、知識或守法性。
4. 損益關連者	關連人及他們的期望
5. 風險的量化	重要性及可能性
6. 風險容忍度/胃口	風險的潛在損失及財務影響 受風險牽連的價值 潛在損失/獲利的可能性及規模 風險控制的目的及期望的績效水準
7. 風險處置及控制機制	目前管理風險的主要方法 目前控制機制的信心水準 監督及檢討模式的界定
8. 改善的可能行動	降低風險的建議
9. 策略及政策的開發	界定負責開發策略及政策的職能

4.3 風險估計

風險估計是對風險發生的可能性及可能的結果作出量化、半量化或質化的估計。
例如: 結果的威脅性（壞的風險）或機會（好的風險）可能高、中等或低（請參閱表4.3.1），機率可能高、中等或低，但需對威脅及機會作出不同的定義（請參閱表4.3.2及4.3.3）。下頁表中有一些例子，不同的機構會找到不同的對結果及可能性的評估方法來滿足他们的需求。

例如許多機構發現將結果及可能性評估為高、中等或低, 和用3x3的矩陣來表達已足够；但其他機構則可能覺得以5x5的矩陣來評估結果及可能性較為適合。

表 4.3.1 結果 – 威脅及機會

高	對機構的財務影響可能超過£x 對機構的策略或營運活動有嚴重影響 損益關連者嚴重關切
中等	對機構的財務影響可能在£x及£y之間 對機構的策略或營運活動有中等程度的影響 損益關連者的關切程度中等
低	對機構的財務影響可能不超過£y 對機構的策略或營運活動影響程度很低 損益關連者的關切程度低

表 4.3.2 發生的可能性 – 威脅

估計	描述	指標
高 （很有可能）	每年都很有可能發生或發生的機會大於 25%	在一定期間內（例如 10 年）可能發生多次。 最近發生過。
中等 （有可能）	在10年期間內有可能發生或發生的機會小於25%	在一定期間內（例如10年）可能發生一次以上。 由於某些外部影響而難以控制。 曾發生過嗎？
低 （微乎其微）	在 10 年期間內不太可能發生或發生的機會小於 2%	沒發生過。 不太可能發生。

表 4.3.3 發生的可能性 – 機會

估計	描述	指標
高 （很有可能）	一年內很有可能達成所希望的好結果，或發生的機會大於 75%	機會明確,有賴于合理的必然性，根據目前的管理流程在短期內會實現。
中等 （有可能）	可合理期待一年內有好的結果或發生的機會在25%至 75%之間	有實現的可能性，但需要審慎管理。 有超越計畫的機會。
低 （微乎其微）	未來中期有一些機會得到期望的好結果或發生的機會小於 25%	管理階層尚未仔細研究其可能性。 以目前所使用的管理資源要成功的可能性低。

4.4 風險分析方法及技術

分析風險所可使用的技術有很多，有些是針對好的風險、有些是針對壞的風險，而有些則可適用於兩者（請參閱附件第12頁案例）。

4.5 風險素描

風險分析步驟所得結果是產生一個風險的素描，為每一項風險的嚴重性評比，並提供依序處理風險的工具。

評比各項風險可以讓我們看清他们相對的重要性。

這個步驟可以將風險標示於企業受影響的業務、描述已實施的主要控制程序，並指出那些地方的風險控制投資水準應該增加、減少或重新分配。

問責可以幫助確認風險的”擁有權”及適當分配管理資源。

5. 風險評价

完成風險分析步驟後,我们應該將所評估的風險與該機構已建立的風險標準互相對照，風險標準可能包括相關的成本及利益、法律規定、社會經濟及環境因素、損益關連者在意的問題等。因此，風險評價是用來判斷風險對機構的重要性作出決策及決定是否應接受各項特定風險或作出處置。

6. 風險報告及溝通

6.1 內部報告

機構內不同的層級需要從風險管理程序中得到不同的資訊。

董事會應該:

- *知道機構所面臨的最嚴重的風險*
- *知道對股票價值與預期績效範圍差異的影響*
- *讓整個機構保持適當程度的警覺*
- *知道機構管理危機的方法*
- *知道損益關連者對機構保持信心的重要性*
- *知道如何在適當時機與投資大眾溝通*
- *使風險管理步驟能有效運作*
- *發佈明確的風險管理政策，包括風險管理理念及責任。*

各營運單位應該:

- *了解自己責任領域所面臨的風險、這些風險對其他單位的影響以及其他單位因承受結果而對自己單位帶來的影響。*
- *設立績效指標以便監督核心業務及財務活動、達成目標的進度以及界定介入的狀況 (例如預測及預算）。*
- *有關預算及預測的差異，定期提供適當溝通系統及程序，以便採取行動*
- *系統性地且即時向上級管理階層報告任何新察覺到的風險或現行控制方法失敗之處。*

個人應該:

- *了解對個別風險所負的責任*
- *了解如何持續改善風險管理因應機制*
- *了解風險管理及風險警覺是機構文化的重要部份*
- *系統性地且即時向上級管理階層報告任何新察覺到的風險或現行控制方法失敗之處。*

6.2 外部報告

公司必須定期向損益關連者報告風險管理政策及其對達成目標的有效性。

損益關連者越來越要求机构提供有關非財務績效方面有效管理方面的証據，例如：社區事務、人權、聘僱方法、健康及安全以及環境。

良好的公司管治要求公司採用條理化的風險管理方法：

- *保障損益關連者的利益*
- *確保董事會可執行其職權來主導策略、建立價值並監督機構之績效*
- *確保管理控制程序的建立和適當地實施*

機構應明確陳述對風險管理正式報告的安排並讓損益關連者了解。

正式報告應針對：
- *控制方法 – 尤其是風險管理的管理職責*
- *界定風險所採用的步驟以及風險管理系統執行方式*
- *管理重大風險所採用的主要控制系統*
- *所採用的監督及檢討系統*

系統範圍或系統本身如有重大缺失應與處理步驟一併報告。

7. 風險處置

風險處置是選擇並實施改變風險措施的步驟，風險處置的主要原理是風險控制/減輕，但可進一步衍生為風險迴避、風險轉移、風險融資等。

附註：在本準則中，風險融資係指為風險結果籌措資金的機制（例如購買保險計畫），風險融資通常不是為實施風險處置之成本提供資金（如ISO/IEC指南73所定義者；請參閱附件第17頁）。

任何風險處置系統至少應提供：
- *对機構有良好效率及效果佳的營運*
- *有效的內部控制*
- *遵守法規*

風險分析步驟界定管理階層需關注的風險，從而幫助機構有效營運，但必須根據對機構的潛在利益排定風險控制行動的優先順序。

內部控制的效果要根據預定的控制方法將風險排除或降低的程度而定。

內部控制的成本效益則取決于實施控制的成本與風險降低的預期利益之比對。

我们要衡量建議的控制方法, 必須比較假設不採取行動的潛在經濟影響與採取建議行動的成本，這往往需要比現有的更詳細的資訊及假設。

首先我们必須知道實施的成本，這需要精確計算，因為它立刻就會成為衡量成本效益的基礎；我们也要估算不採取行動的預期損失，透過兩者比較的結果，管理階層便可決定是否須實施風險控制方法。

遵守法規是沒有選擇性的，機構必須了解相關法令並據以實施控制系統，只有當降低風險的成本與風險本身不按比例的情況下才能有一些彈性。

為風險的衝擊取得財務保障的方法之一是透過風險融资，包括購買保險，但是必須了解有些損失或損失元素是無法投保的，例如與工作相關的健康、安全或環境意外的成本並不在保障範圍，這些可能還包括員工士氣及機構聲譽的損失。

8. 風險管理步驟的監督及檢討

有效的風險管理需要有報告及檢討架構，以有效界定與評價風險，及確保控制及回應機制得以建立實施，且應定期稽核政策及標準的遵守情形、檢討標準績效，以便掌握改善的機會。應記住機構是動態的、且在一個動態的環境中營運，我们需掌握機構及環境的變更，並對系統作出適當的修正。

監督步驟應能確定對機構的活動實施了適當的控制，同時了解所有的程序並據以遵守。我们也需要掌握機構及環境的變更並對系統作出適當的修正。

任何監督及檢討步驟應應能判斷：

- *所採用的方法能否得到希望的結果*
- *為執行評價所採用的程序及所蒐集的資訊是否適當*
- *所增加的知識是否有助於作出更好的決策?是否能為未來風險的評價及管理界定應學習的課題*

9 風險管理的架構及行政

9.1 風險管理政策

機構的風險管理政策應揭示公司對風險的態度及所能接受程度及其對風險的管理方法，同時應揭示機構內各部門及人員在風險管理方面的職責。

此外，政策說明應參考法令規定，例如健康及安全方面。

在風險管理步驟中應附有整體性的工具及技術，以便進行業務時在不同階段中使用。為能有效運作，風險管理步驟需要：

- *獲得機構中首席執行長與執行管理階層的承諾*
- *在機構中分派職責*
- *配置適當的資源,為所有損益關連者 提供培訓,強化風險警覺意識。*

9.2 董事會的角色

董事會應負責決定機構的策略方向並營造風險管理有效運作的環境及架構。

這可透過一個執行團隊、非執行委員會、稽核委員會或其他職能部門，只要是適合機構的營運方法且能夠擔任風險管理的推動者即可。

董事會在評估內部控制系統時至少應考慮：

- *公司在其特定業務中所能接受的壞的風險的本質及程度*
- *該風險成為事實的可能性*
- *應如何管理不能接受的風險*
- *公司降低風險可能性及其對業務影響的能力*
- *對風險所採取的控制活動的成本及效益*
- *風險管理步驟的效果*
- *對董事會所作決議的風險含義*

9.3 營運單位的職責

包括：
- *營運單位對風險管理日常事務負主要責任*
- *營運單位管理階層應負責在其營運範圍內推廣風險意識，將風險管理目標納入其業務*
- *風險管理應是管理會議的例行項目，以便討論風險暴露狀況，並根據風險分析重新排定工作優先順序*
- *營運單位管理階層應確保項目從規劃階段到整個實施過程均考慮到風險管理*

9.4 風險管理職能單位的職責

依機構的規模，風險管理單位可能是單獨一個人、一個兼職的風險經理到一個完整的風險管理部門。

風險管理單位的職責應包括：

- *制定風險管理政策及策略*
- *在策略及營運層次擔任風險管理的主要負責人*
- *在機構內建立風險認知的文化，包括提供適當的培訓*
- *為各業務單位建立內部風險政策及架構*
- *設計並檢討風險管理步驟*
- *協調有關職能活動对風險管理事務的咨詢工作*
- *設計風險因應程序，包括突發事故及持續營運計畫*
- *向董事會及損益關連者撰寫風險報告*

9.5 內部稽核的職責

每個機構內部稽核的職責都不相同，實務上，內部稽核的職責包括下列部份或所有的责任：

- *專注於由管理階層所界定的重大風險的內部稽核工作，同時稽核整個機構的風險管理步驟*
- *對風險管理程序提供保證*
- *積極支持並參與風險管理步驟*
- *在風險管理及內部控制方面幫助界定風險/評價及教育員工*
- *協調對董事會及稽核委員會等單位的風險報告*

在為特定機構設定最適當的職責時，內部稽核應確保不違反獨立性及客觀性的專業要求。

9.6 資源及履行

履行機構政策應明確建立各管理階層及各事業單位所需要的資源。

除了原有的營運職責之外，所有單位應明確界定其參與風險管理之協調政策/策略方面的職責。而參與內部稽核及協助風險管理的單位也應同樣闡明其職責。

風險管理應透過策略及預算程序深植於機構內，於引進新員工時,在其他培訓和發展計畫和在營運程序 (例如产品/服務發展項目)中被强调，。

10. 附件

風險界定技術 – 舉例

- *腦力激盪*
- *問卷*
- *營運研究，探討每個營運步驟並描述每個可能影響這些步驟的內部程序及外部因素*
- *產業標竿*
- *情境分析*
- *風險評估研討會*
- *事故調查*
- *稽核及檢查*
- *HAZOP（危害性事件及運作能力研究）*

風險分析方法及技術 – 舉例

好的風險

- *市場調查*
- *探勘*
- *行銷測試*
- *研究及開發*
- *業務衝擊分析*

兩者
- *依賴性模擬*
- *SWOT分析（强项、弱项、機會、威脅）*
- *事件樹狀分析*
- *持续營運計畫*
- *BPEST（業務、政治、經濟、社會、科技）分析*
- *真實選擇模擬*
- *在有風險及不確定情況下作決策*
- *統計推論*
- *中央集中及分散之評估*
- *PESTLE（政治、經濟、社會、技術、法律、環境）*

壞的風險
- *威脅分析*
- *過失樹狀分析*
- *FMEA（缺失型態及效果分析）*