與品質管理有關的工具、方法、技術及其應用

ISO 31000

CNS 31000

Risk management – Principles and guidelines

風險管理－原則與指導綱要

目　錄

4.4 實施風險管理

4.5 架構之監測與審查

4.6 架構之持續改進

5. 過程

5.1 一般

5.2 溝通與諮商

5.3 建立前後環節

5.4 風險評鑑

5.5 風險處理

5.6 監測與審查

5.7 記錄風險管理過程

附錄A(參考)強化的風險管理之屬性

參考資料

前言

本標準係依據2009年發行之第一版ISO 31000，不變更技術內容，制定成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

前言

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

簡介

所有類型與規模的組織面臨內部與外部因素及影響，使其不確定是否與何時將達成其目標，此不確定性對組織目標之效應為〝風險〞。

組織的所有活動均涉及風險。組織管理風險時可藉由鑑別、分析，並於其後評估此風險是否須以風險處理修改，以滿足其風險準則。在此過程中，組織與利害相關者溝通與諮商，並監視與審查此風險，且對修改此風險予以控管，以確保無需進一步

簡介

的風險處理。本標準詳細描述此系統化與有條理的過程。當所有組織管理風險至某程度時，本標準制定一些需予以滿足以使風險管理生效之原則。本標準建議組織發展、實施及持續地改進架構，其目的為整合此過程，以將管理風險納入組織的整體治理、策略與規劃、管理、報告過程、政策、價值及文化中。

風險管理在任何時間應用於整體組織的許多領域與階層，同樣地可應用至特定機能、

簡介

專案及活動。雖然風險管理之實務歷經長時間且在許多產業發展，以符合互異的需求，在包羅萬象的架構中採納一致性的過程，可協助確保整個組織的風險可有效果、有效率及協調一致地管理。描述於本標準中的一般方法提供以系統化、透明化及可靠的方式，且在任何範圍與情況下，管理任何形式的風險之原則與指導綱要。風險管理之每一特定產業或應用帶有其各別之需求、對象、感受及準則，因此，本

簡介

標準重要的特色為納入〝建立前後環節〞，作為著手此一般的風險管理過程時之一項活動。建立前後環節將可掌握組織的目標、追求此等目標的環境、其利害相關者及風險準則之多樣性，所有此等將有助於顯現與評估其風險之本質與複雜性。描述於本標準中的管理風險之原則、風險產生的架構及風險管理過程之間的關係示於圖1。

當依據本標準實施與維持時，風險管理可使組織達成，例：

簡介

標準重要的特色為納入〝建立前後環節〞，作為著手此一般的風險管理過程時之一項活動。建立前後環節將可掌握組織的目標、追求此等目標的環境、其利害相關者及風險準則之多樣性，所有此等將有助於顯現與評估其風險之本質與複雜性。描述於本標準中的管理風險之原則、風險產生的架構及風險管理過程之間的關係示於圖1。

當依據本標準實施與維持時，風險管理可使組織達成，例：

簡介

- 增進達成目標之可能性。
- 激勵預先主動的管理。
- 瞭解鑑別與處理整個組織的風險之需求。
- 改進機會與威脅之鑑別。
- 遵守相關法令規章要求及國際常規。
- 改進強制與自願性報告。
- 改進治理。
- 改進利害相關者之信心與信任。
- 建立決策訂定與規劃可信賴的基準。

簡介

— 有效地分配與使用風險處理的資源。
— 改進作業之效果與效率。
— 增進健康與安全績效，以及環境保護。
— 改進損失預防與意外事故管理。
— 降低損失。
— 改進組織之學習，及
— 改進組織的恢復力。

本標準意圖滿足各方面利害相關者之需求，包括：

(a) 在其組織內負責制定風險管理政策的

簡介

人員。

(b)對於確保風險在組織內的整體或特定領域、專案計畫或活動範圍內有效的管理當責之人員。

(c)需要評估組織管理風險的有效性之人員，及

(d)標準、指引、程序及實務規章，在其整體或部分陳述此等文件之特定情況內風險如何予以管理之制定者。

許多組織目前的管理實務與過程包含風險

簡介

管理要項，且許多組織對於特定類型的風險或狀況，業已採納正式的風險管理過程。在此情況，組織可依據本標準施行其現有實務與過程之關鍵性審查。

在本標準中，〝風險管理〞與〝管理風險〞之措辭皆有使用。在一般用語中，〝風險管理〞論及有效地管理風險之結構(原則、架構及過程)，而〝管理風險〞則論及應用此結構於特定風險。

簡介

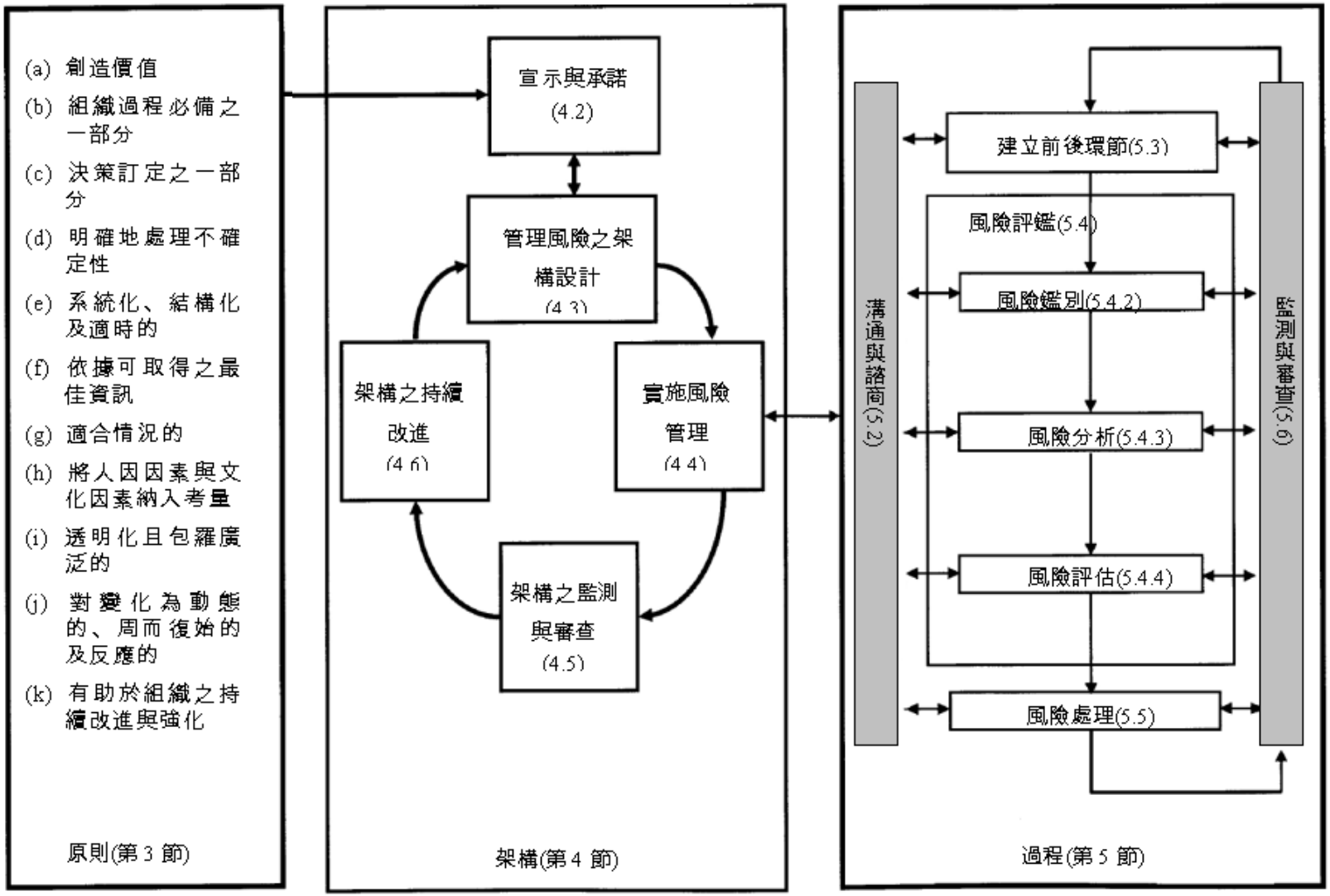

圖1　風險管理原則、架構及過程間之關係

1. 適用範圍

本標準規定風險管理的原則與一般指導綱要。本標準可供任何公共、私有或共有企業、協會、團體或個人使用，因此，本標準並無特定於任何產業或部門。

備考：為方便計，本標準所有不同的使用者均以一般用語〝組織〞稱之。

本標準可適用於組織所有發展階段，且適用於廣範圍的活動，包括策略與決策、作業、過程、功能、專案、產品、服務及資產。

本標準可適用於任何形式的風險，不論其本

質為何，及是否具有正面或負面的結果(後果)。雖本標準提供一般指導綱要，但並無促進組織風險管理統一之意。風險管理計畫與架構的設計與實施，需要考量特定組織不同的需求、其特定目標、情況、結構、作業、過程、功能、專案、產品、服務、或資產與使用的特定實務。

本標準預期可用以調和現有與未來標準中之風險

管理過程。本標準提供一個通用的方法以支援處理特定風險及/或領域的標準，但並

取代該等標準。

本標準並不預期作為驗證之目的。

2. 用語及定義

下列用語及定義適用於本標準。

2.1 風險(risk)

對目標之不確定性的效應。

備考1. 效應係與預期者之偏離，可為正面及/或負面。

備考2. 目標可具有不同考量面(諸如財務、健安全衛生及環境目標)，並可應用於不同層面(諸如策略、整體組織、專案計畫、產品及過程)。

備考3. 風險通常係藉由可能的事件(2.17)與結果(後果)(2.18)，或其組合將其特性化。

備考4. 風險通常以一事件(包括狀況變化)的結果(後果)與相關發生的可能性(2.19)之組合表示。

備考5. 不確定性係有關一事件，其結果(後果)或可能性的瞭解或認知之資訊短缺，甚或部分短缺之狀態。

[CNS 14889，定義2.1]

2.2風險管理(risk management)

指導與管制組織有關風險(2.1)的協調活動。

[CNS 14889，定義3.1]

2.3風險管理架構(risk management framework)

遍及組織的設計、實施、監測(2.28)、審查及持續改進組織的風險管理(2.2)所提供基礎與組織的安排之要件組。

備考1.基礎包括管理風險(2.1)的政策、目標、宣示及承諾。

2.2風險管理(risk management)

指導與管制組織有關風險(2.1)的協調活動。

[CNS 14889，定義3.1]

2.3風險管理架構(risk management framework)

遍及組織的設計、實施、監測(2.28)、審查及持續改進組織的風險管理(2.2)所提供基礎與組織的安排之要件組。

備考1.基礎包括管理風險(2.1)的政策、目標、宣示及承諾。

備考2. 組織的安排包括計畫、關係、
當責、資源、過程及活動。

備考3. 風險管理架構深植於組織的整體
策略與營運政策及實務中。

[CNS 14889，定義3.1.1]

2.4 風險管理政策(risk management policy)

組織有關風險管理(3.1)的整體意圖與方向之聲明。

[CNS 14889，定義3.1.2]

2.5風險對策(risk attitude)

組織評鑑與最後追尋、留置、承受或避開風險(2.1)之途徑。

[CNS 14889，定義4.7.1.1]

2.6風險管理計畫(risk management plan)

在風險管理架構(2.3)內，明訂應用於風險(2.1)管理的途徑、管理要件及資源的方案。

備考1.管理要件基本上包括程序、實務、責任分派、活動之順序與時程安排。

備考2.風險管理計畫可應用於特特定產品、過程與專案計畫，以及組織之部分或整體。

[CNS 14889，定義3.1.3]

2.7風險當責者(risk owner)

具有管理風險(2.1)的當責與職權之人員或實體。

[CNS 14889，定義4.5.1.5]

2.8風險管理過程(risk management process)

系統化地應用管理政策、程序及實務於溝通、諮商、建立前後環節，並鑑別、分析、評估、處理、監測(2.28)及審查風險(2.1)等活動。

[CNS 14889，定義4.1]

2.9 建立前後環節(establishing the context)

當管理風險、設定風險管理政策(2.4)之範圍與風險準則(2.22)時，對界定的外部與內部參數應予考量。

[CNS 14889，定義4.3.1]

2.10 外部前後環節(external context)

組織尋求達成其目標的外部環境。

備考：外部前後環節可包括

— 無論是國際、國家、區域抑或地方的文化、社會、政治、法令、規章、財務、技術、經濟、天然及競爭環境。

— 對組織的目標具有衝擊影響之主要推動者與趨勢，及

— 與外部利害相關者(2.13)的關係，以及外部利害相關者之感知與價值。

[CNS 14889，定義4.3.1.1]

2.11 內部前後環節(internal context)

組織尋求達成其目標的內部環境。

備考：內部前後環節可包括

— 治理、組織的結構、角色及當責。

— 政策、目標，以及能使其達成的策略。

— 從資源與知識(例：資金、時間、人員、過程、系統及技術)為觀點所具有的能力。

— 資訊系統、資訊流及決策過程(正式 與非正式兩者)。
— 與內部利害相關者的關係，以及內部利害相關者之感知與價值。
— 組織的文化。
— 組織所採用的標準、指導綱要及模式，及
— 合約關係之形式與範圍。

[CNS 14889，定義4.3.1.2]

2.12 溝通與諮詢諮商(communication and consultation)

組織進行持續與反覆的過程以提供、分擔分享或取得資訊，並著手與事件相關者利害相關者(2.13)進行有關風險(2.1)管理之對話。

備考1. 資訊可能與風險管理的存在、性質、形式、可能性(2.19)、重要性顯著性、評價評估、可接受性及處理有關。

備考2. 諮詢諮商為組織與其事件相關者利害相關者針對一議題在做成作成決策或

決定方向之前，先行告知的雙向溝通過程。
諮詢諮商為係：

－與其使用強力不如透過影響力影響決策之過程。與

－決策達成制定之輸入之一，並非而非參與結合決策制定達成。

[CNS 14889，定義4.2.1]

2.13 事件相關者利害相關者（stakeholder）

可影響、受其所影響、抑或自認會受到決策或活動影響的個人或組織。

備考：決策者可為事件相關者利害相關者。

[CNS 14889，定義4.2.1.1]

2.14 風險評鑑(risk assessment)

風險鑑別(2.15)、風險分析(2.21)及風險評估(2.24)的整個過程。

[CNS 14889，定義4.4.1]

2.15 風險鑑別(risk identification)

尋找發現、認清認知及描述風險(2.1)之過程。

備考1. 風險鑑別包括風險緣由(2.16)、事件(2.17)、其原因及其可能的潛在的結果(後果)(2.18)之鑑別。

備考2. 風險鑑別可包括歷史數據、理論分析、經告知的意見與專家的意見及事件相關者利害相關者(2.13)的需求。

[CNS 14889，定義4.5.1]

2.16 風險緣由(risk source)

單獨或與其他合併而具有本質上可能導致風險(2.1)之要項。

備考：風險緣由可為有形或無形的。

[CNS 14889，定義4.5.1.2]

2.17　事件(event)

所發生或變動的一組特定情況。

備考1. 事件可發生一次或連續發生，且可具有數種原因。

備考2. 事件可含有未發生的事物。

備考3. 事件有時可稱為〝事件(incident)〞或〝事故(accident)〞。

備考4. 未發生結果(後果)(2.18)的事件亦可稱為〝虛驚事件(near miss)〞、〝事件(incident)〞、〝虛驚徵兆

(near hit)”或“驚險(close call)”。[CNS 14889，定義4.5.1.3]

2.18 結果(後果)(consequence)

影響目標事件(2.17)之產出結果(outcome)。

備考1. 一事件可導致一定範圍的結果(後果)。

備考2. 結果(後果)可為確定或不確定，且可對目標物具有正面或負面的影響。

備考3. 結果(後果)可以定性或定量方式表示之。

備考4. 初期結果(後果)可透過推擠(knock-on)效應而升高。

[CNS 14889，定義4.6.1.3]

2.19 可能性(likelihood)

某事發生之機會。

備考1. 在風險管理的術語中，“可能性”一詞用以稱某事發生之機會，不論其是否為界定的、量測的或客觀或主觀決定的、定性或定量的，並使用一般用語或數學方式(諸如在指定期間內發生的機率或頻率)描述。

備考2. 英文〝likelihood〞一詞，在某些語言中並無直接同等字，通常使用同等的〝probability〞替代。然而，在英文中〝probability〞通常以較狹窄的數學方式闡釋，因此在風險管理術語中，使用〝likelihood〞一詞的意義須如同英文以外的許多語言，與〝probability〞一詞具有同樣更廣義的解釋。

[CNS 14889，定義4.6.1.1]

2.20 風險剖繪(risk profile)

任何風險(2.1)集合之描述。

備考：風險集合可包含與整體組織、組織之部分有關者，或依其他之界定。

[CNS 14889，定義4.8.2.5]

2.21 風險分析(risk analysis)

理解風險(2.1)的本質並決定風險等級(2.23)之過程。

備考1. 風險分析提供風險評估(2.24)與有關風險處理(2.25)的決策之基礎。

備考2. 風險分析包括風險預估。

[CNS 14889，定義4.6.1]

2.22 風險準則(risk criteria)

評估風險(2.1)之顯著性時所用的參照用語。

備考1. 風險準則係以組織的目標與外部前後環節(2.10)及內部前後環節(2.11)為基準。

備考2. 風險準則可衍生自標準、法律、政策及其他要求。

[CNS 14889，定義4.3.1.3]

2.23 風險等級(level of risk)

風險(2.1)或多項風險合併之規模，以結果(後果)(2.18)與其可能性(2.19)組合之方式表示之。

[CNS 14889，定義4.6.1.8]

2.24 風險評估(risk evaluation)

將風險分析(2.21)之結果與風險準則(2.22)相比較，以決定風險(2.1)及/或其規模是否可接受或可容忍之過程。

備考：風險評估協助有關風險處理(2.25)之決策。

[CNS 14889，定義4.7.1]

2.25　風險處理(risk treatment)

修改風險(2.1)之過程。

備考1. 風險處理可包括

— 決定不開始或不繼續可能引起風險的活動以避免風險。

— 承受或提高風險以尋求機會。

— 移除風險緣由(2.16)。

— 改變可能性(2.19)。

— 改變結果(後果)(2.18)。

— 與另一團體或多個團體分擔風險[包含合約與風險資金提供]。

— 藉由已被告知的決定留置風險。

備考2. 處理負面結果(後果)的風險處理有時稱為〝風險減輕〞、〝風險排除〞、〝風險預防〞及〝風險降低〞。

備考3. 風險處理可能創造新風險或修改現有的風險。

[CNS 14889，定義4.8.1]

2.26　控管(control)

修改風險(2.1)之措施。

備考1. 控管包括任何可修改風險之過程、政策、設備、實務或其他行動。

備考2. 控管不可能經常能發揮預期或設想的修改效果。

[CNS 14889，定義4.8.1.1]

2.27　殘餘風險(residual risk)

風險處理(2.25)後所殘留的風險(2.1)。

備考1.　殘餘風險可包含未鑑別的風險。

備考2.　殘餘風險亦熟知為〝保留風險(retained risk)〞。
[CNS 14889，定義4.8.1.6]

2.28 監測(monitoring)

持續地查核、監視、重點觀察或測定其狀態，以鑑別出所要求或預期的運行程度之變化。

備考：監測可應用於風險管理架構(2.3)、風險管理過程(2.8)、風險(2.1)或控管(2.26)。
[CNS 14889，定義4.8.2.1]

2.29 審查(review)

對為達成所建立的目標，所進行之主題事決定其適合性、恰當性及有效性之活動。

備考：審查可應用於風險管理架構(2.3)、風險管理過程(2.8)、風險(2.1)或控管(2.26)。

[CNS 14889，定義4.8.2.2]

3. 原則

為使風險管理有效，組織須在所有階層遵守下述原則。

(a)風險管理創造與保護價值

風險管理有助於達成目標與改進績效，例如人體安全衛生、安全保障、法令與規章符合管理、營運之效率、治理及聲譽。

(b)風險管理為所有組織過程必備之一部分

風險管理並非與組織的主要活動與過程分離之單獨活動，風險管理為管理階層的責任之一部分，並為所有組織的過程，包括策略規劃與所有專案及變動管理過程的整合部分。

(c)風險管理為決策訂定之一部分

風險管理有助於決策者作成充分資訊的選擇、措施的優先排序及區分出行動的替代途徑。

(d)風險管理明確地處理不確定性

風險管理明確地考量不確定性、不確定性之本質，及其可如何予以處理。

(e)風險管理係系統化、結構化及適時的

風險管理系統化、適時及結構化的方式助成效率與一致性、可比較及可靠的結果。

(f) 風險管理依據可取得之最佳資訊

管理風險的過程之輸入係依據如歷史性資料、經驗、利害相關者回饋、觀察、預測與專家的判斷等資訊來源。然而，決策者本身須清楚且須考量使用的資料或模式建立之限制或專家之間意見分歧的可能性。

(g)風險管理為適合情況的

風險管理係與組織的外部與內部前後環節及風險剖繪相結合的。

(h)風險管理將人因因素與文化因素納入考量風險管理認知到外部與內部人員的智能、

感知及意向，可助成或阻礙組織的目標之達成。

(i)風險管理為透明化且包羅廣泛的

利害相關者適當與適時地參與，且特別是組織所有階層的決策者確保風險管理維持相關性與更新。參與亦使利害相關者得以正當地出席，且在決定風險準則時將其意見納入考量。

(j)風險管理對變化為動態的、周而復始的及反應的風險管理持續地察覺與回應變化。

如外部與內部事件產生、前後環節與知識改變、開始風險的監視與審查、新風險出現、某些變化及其他風險消失時。

(k)風險管理有助於組織之持續改進

組織須發展與實施策略，以使組織的風險管理成熟度與其他考量面併行改進。

附錄A對於組織希望更有效地管理風險提供進一步的建議。

如外部與內部事件產生、前後環節與知識改變、開始風險的監視與審查、新風險出現、某些變化及其他風險消失時。

(k)風險管理有助於組織之持續改進

組織須發展與實施策略，以使組織的風險管理成熟度與其他考量面併行改進。

附錄A對於組織希望更有效地管理風險提供進一步的建議。

4. 架構

4.1一般

風險管理的成功將視管理架構的有效性而定，管理架構提供基礎與安排，將深植於整個組織所有階層。架構透過風險管理過程(參照第5節)的實施協助有效地管理風險。此架構確保有關由風險管理過程所產生的風險資訊係充分地報告，並用作為所有相關的組織階層的決策訂定與當責性之基礎。

本節描述管理風險的架構之必要組成，以及其在反覆方式中之相互關聯情況，如圖2所示。

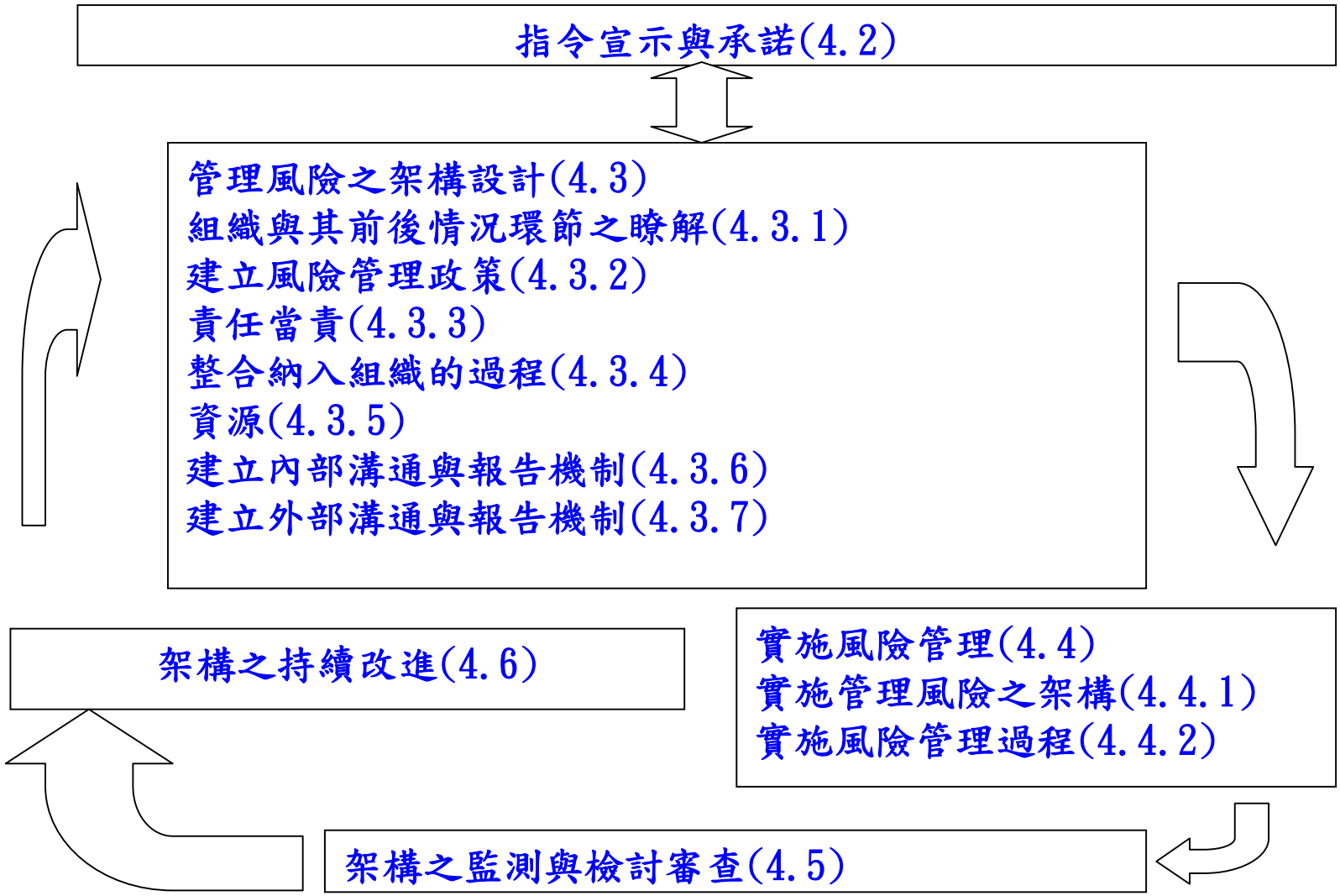

圖2　管理風險的架構組成間之關係

此架構並無意規定一個管理系統，而是要協助組織將風險管理整合於其整體管理系統中，因此，組織須將此架構之組成適應至其特定需求。

若組織現行的管理實務與過程包括風險管理之組成要素，或若組織對於特殊類型的風險或情況業已採納正式的風險管理過程，則此等須依據本標準，包括附錄A所涵蓋的屬性進行關鍵性審查與評鑑，以決定其適切性與有效性。

4.2 宣示與承諾

風險管理的導入與確保其持續之有效性，需要組織的管理階層強烈與持續的承諾，以及在所有階層策略性與嚴格的規劃以達成承諾。管理階層須：

－界定與支持此風險管理政策。

－確保組織的文化與風險管理政策係一致的。

－決定與組織的績效指標一致的風險管理績效指標。

－風險管理目標與組織的目標與策略一致。

－確保對法令規章之符合性。

－指派組織內適宜階層的當責與職責。
－確保必要的資源分配至風險管理。
－向所有利害相關者溝通風險管理之利益，及
－確保管理風險的架構持續維持適宜。

4.3 管理風險之架構設計

4.3.1 組織與其前後環節之瞭解

開始設計與實施管理風險的架構之前，評估與瞭解組織外部與內部兩者之情況係重要的，因其可顯著地影響架構之設計。

評估組織的外部情況可包括

，但不侷限於下列：

(a)無論是國際、國家、區域抑或地方的文化、社會、政治、法令、規章、財務、技術、經濟、天然及競爭環境。

(b)對組織的目標具有衝擊影響之主要推動者與趨勢，及

(c)與外部利害相關者的關係，以及外部利害相關者之感知與價值。

評估組織的內部環節可包括，但不侷限於下列：

- 治理、組織之結構、角色及當責。
- 政策、目標，以及可達成政策與目標的策略。
- 由資源與知識(例：資金、時間、人員、過程、系統及技術)的觀點所瞭解的能力。
- 資訊系統、資訊流及決策過程(正式與非正式兩者)。
- 與內部利害相關者的關係，及其感受與價值觀。
- 組織的文化。

－組織所採用的標準、指導綱要及模式，及

－合約關係之形式與範圍。

4.3.2 建立風險管理政策

風險管理政策須清楚說明組織對於風險管理的目標與承諾，且特別要強調下列事項。

－ 組織對於管理風險之思路。

－ 組織的目標與政策及風險管理政策間之聯結。

－ 管理風險之當責與職責。

－ 處理利益衝突之方式。

－備妥協助管理風險的當責與職責所必要的資源之承諾。

－　風險管理績效將如何予以量測與報告之方式，及

－　定期審查與改進風險管理政策，並回應事件或狀況改變之承諾。

風險管理政策須予以適宜地溝通。

4.3.3 當責

組織須確保管理風險之當責、職權及適當的智能，包括實施與維持風險管理過程並確保任何控管之正確性、有效性及效率。此可藉下列促成。

— 鑑別具有當責與職權的風險當責者來管理風險。

— 鑑別何人當責管理風險的架構之發展、實施及維護。

— 鑑別對於風險管理過程，組織內所有階層的人員之其他職責。

— 建立績效檢測與外部及/或內部報告及通報過程，及

—確保適宜的認可階層。

4.3.4 整合納入組織過程

風險管理須深植於組織所有的實務與過程中，使之相關、有效果及有效率。風險管理過程須成為組織的過程之一部分，但非與之區分。特別是，風險管理須予以深植於政策發展、業務與策略規劃及審查，以及變動管理過程中。

須為全組織的風險管理計畫以確保風險管理政策的實施，且風險管理深植於組織所有的實務與過程中。風險管理計畫可整合納入組織的其他計畫，諸如策略計畫中。

4.3.5 資源

組織須配置風險管理所須適宜的資源。

須考量下列事項。

— 人員、技術、經驗及智能。

— 風險管理過程每一步驟所需的資源。

— 管理風險所使用的組織過程、方法及工具。

— 文件化的過程與程序。

— 資訊與知識管理系統，及

— 訓練方案。

4.3.6 建立內部溝通與報告機制

組織須建立內部溝通與報告機制以支持與鼓勵負起風險當責與當責者責任，此等機制須確保：

— 風險管理架構之關鍵組成要素與任何後續的修改，經適宜地溝通。

— 對於此架構、其有效性及其成果有適切的內部報告。

— 由實施風險管理所產生的相關資訊，於適宜的階層與時間備妥可取得，及

— 具有與內部利害相關者諮商之過程

4.3.6 建立內部溝通與報告機制

此等機制須在適宜時包含由各種來源統合風險資訊之過程，且可能需考量此資訊之敏感性。

4.3.7 建立外部溝通與報告機制

組織須發展與實施如何與外部利害相關者溝通之計畫，此須包括：

— 聯結適宜的外部利害相關者並確保有效的交換資訊。

— 外部報告以符合法令規章及監理要求。

— 提供有關溝通與諮商的回饋與報告。

— 運用溝通以建立組織內之信心，及

— 一旦有危機或突發事件時，與利害相關者溝通。

此等機制須在適當處包含由各種來源統合風險資訊之過程，且可能需考量此資訊之敏感性。

4.4 實施風險管理

4.4.1 實施管理風險之架構

在實施組織管理風險的架構時，組織須：

— 界定實施此架構適宜的時間安排與策略。

— 應用此風險管理政策與過程於組織的過程。

— 符合法令規章要求。

— 確保決策之形成，包括目標的發展與設定，與風險管理過程的成果一致。

— 辦理資訊與訓練課程，及

— 與利害相關者溝通與諮商以確保其風險管理架構維持適宜。

4.4.2 實施風險管理過程

風險管理的實施須確保在組織的所有相關階層與職能中，視同為其實務與過程之一部分，透過風險管理計畫應用第5節所列之風險管理過程。

4.5 架構之監測與審查

為確保風險管理係有效與持續支持組織的績效，組織須：

— 依據指標量測風險管理績效，指標應定期審查其適宜性。

— 定期量測風險管理計畫之進度與其偏離。

— 依組織的外部與內部環節，定期審查風險管理架構、政策及計畫是否仍適宜。

— 報告風險、風險管理計畫之進度，及對風險管理政策遵循狀況如何，及

— 審查風險管理架構之有效性。

4.6 架構之持續改進

須依據監測與審查之結果，形成可如何改進有關風險管理架構、政策及計畫之決策。此等決策須導致組織的風險管理及其風險管理文化之改進。

5. 過程

5.1 一般

風險管理過程須為：

— 管理之必備一部分。

— 深植於文化與實務內，及

— 為組織的業務過程量身打造。

其包含5.2至5.6所述之活動。風險管理過程示於圖3。

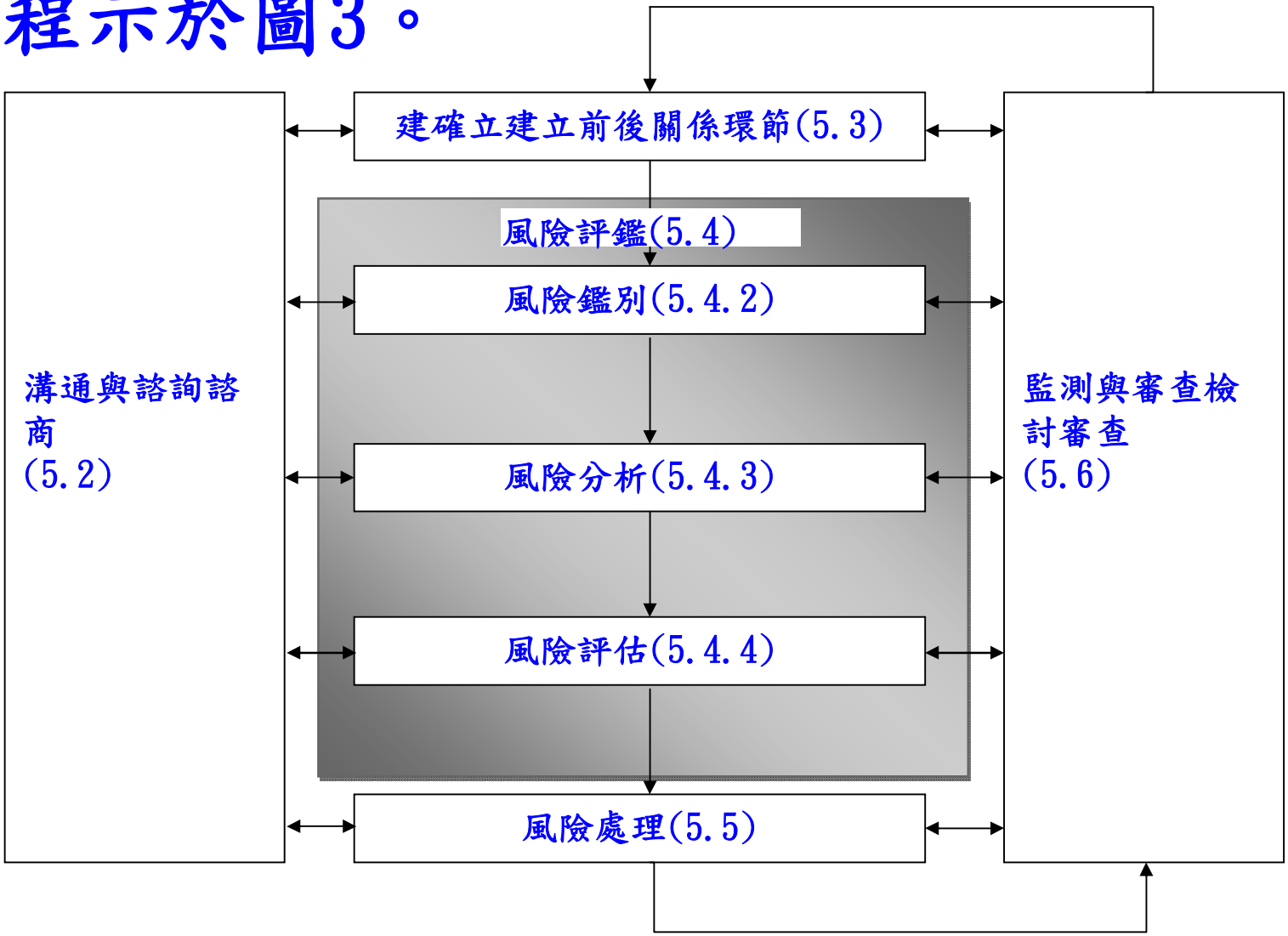

圖3　風險管理過程

5.2 溝通與諮商

在風險管理過程的所有階段中，須進行與外部及內部利害相關者的溝通與諮商。

因此，溝通與諮商計畫須在早期階段發展。此須提出有關風險本身、其緣由，其後果(如已知時)，以及欲採取的處理方法之議題。須進行有效的外部與內部之溝通與諮商，以確保當責實施此風險管理過程者與利害相關者瞭解形成決策的基準，以及為何需採特定措施之理由。

諮商小組方式可

— 適宜地協助建立前後環節。

— 確保利害相關者之利益已被瞭解與考量。

— 協助確保風險經適切地鑑別。

— 帶領不同領域的專家齊聚分析風險。

— 確保當界定風險準則與在評估風險時，不同觀點均予以適宜地考量。

— 保障處理計畫之認同與支持。

— 在風險管理過程中強化適宜的變動管理，及發展適宜的外部與內部之溝通及諮商計畫。

與利害相關者溝通與諮商係重要的，因其依據對風險的感知作出有關風險之判斷。此

等感知可因利害相關者之價值、需求、假設、概念及關切之相異而變化，由於其觀點可對所作決策具有顯著的影響，在決策過程中，利害相關者之感知須予以鑑別、記錄及考量。

溝通與諮商須有助於真實、切題、正確及可理解的資訊之交換，考量機密性與人員誠信考量面。

5.3 建立前後環節

5.3.1 一般

透過建立前後環節，組織清楚的表達其目標，界定當管理風險時需考量的外部與內

部參數，並設定後續過程的範圍與風險準則。當許多此等參數與風險管理架構(參照4.3.1)之設計所考量者類似時，則在建立風險管理過程之前後環節時，須更詳細地考量，尤其是其如何與特定的風險管理過程之範圍關聯。

5.3.2 建立外部前後環節

外部前後環節為組織尋求達成其目標所處的外部環境。

瞭解外部前後環節係重要的，以確保當發展風險準則時，經考量外部利害相關者之目標與關切事項。其係依據全組織之前後環節，但對法令規章要求、利害相關者之

感知，及特定於風險管理過程範圍的風險之其他事項特別詳細。

外部前後環節可包括，但不侷限於下列。

— 無論是國際、國家、區域抑或地方，其社會與文化、政治、法令、規章、財務、技術、經濟、自然及競爭環境。

— 對組織的目標具有衝擊之主要推動者與趨勢，及

— 與外部利害相關者的關係，以及外部利害相關者之感知與價值。

5.3.3 建立內部前後環節

內部前後環節為組織尋求達成其目標所處的內部環境。

風險管理過程須與組織的文化、過程、結構及策略相結合。內部前後環節為組織內可影響組織管理風險方式的任何事務。其須予以建立因。

(a) 風險管理存在於組織目標的前後環節中。

(b) 特定專案、過程或活動的目標與準則須以組織目標之觀點考量為一整體，及

(c) 某些組織無法認清達成其策略性、專案

或商業目標的機會，而此影響到進行中的組織之承諾、可信性、信賴及價值觀。

瞭解內部前後環節係必要的，此可包括，但不侷限於下列：

—治理、組織的結構、角色及責任。

—政策、目標，以及恰當可達成的策略。

—由資源與知識(如資金、時間、人員、過程、系統及技術)的觀點所瞭解的能力。

—與內部利害相關者的關係，以及內部利害相關者之感知與價值。

—組織的文化。

—資訊系統、資訊流及決策過程(正式與非

正式兩者）。

－組織所採納的標準、指導綱要及模式；及

－合約關係之形式與範圍。

5.3.4 建立風險管理過程之前後環節

組織的活動之目標、策略、範圍及參數，或組織將實施風險管理過程的部分，須予以建立。風險管理須從完全考量需求著手，以確證進行風險管理使用的資源。所需的資源、責任與職權及保存的紀錄亦須予以規定。

風險管理過程之前後環節將依據組織需求而改變。此可包括，但不侷限於下列：

- 界定風險管理活動之目的與目標。
- 界定風險管理過程與範圍內之責任。
- 界定適用範圍，以及風險管理活動進行的深度與幅度，包含特定涵括事項與排除事項。
- 界定以時間與地點為觀點之活動、過程、功能、專案計畫、產品、服務或資產。
- 界定特定專案、過程或活動與組織其他專案、過程或活動間之關係。
- 界定風險評鑑方法論。
- 界定風險管理的績效與有效性評估之方式。

— 鑑別與詳述經作成的決策；及

— 鑑別、限定或設計所需之研究、其範圍與目標，及此類研究所需的資源。

留意這些事項與其他相關因素，須有助於確保所採納的風險管理方法係適宜於狀況、組織及影響其達成目標的風險。

5.3.5 界定風險準則

組織須界定使用的準則以評估風險之重大性。準則須反映組織的價值、目標及資源。某些準則可依法令規章要求及組織簽訂的其他要求衍生規範或導出。風險準則須與組織的風險管理政策(參照4.3.2)一致，在

任何風險管理過程開始時界定，且應持續審查。

當界定風險準則時，須包括下列考量的因素：

－由之本質與型式，及可能產生的結果(後果)，以及如何量測。

－可能性將如何界定。

－可能性及/或結果(後果)之時間組合。

－風險等級如何決定。

－利害相關者之意見。

－風險成為可接受或可忍受之等級，及

－是否須考量合併多個風險，及如是時，如

與何項合併須予以考量。

5.4 風險評鑑

5.4.1 一般

風險評鑑為風險鑑別、風險分析及風險評估之整體過程。

備考：CNS 31010提供有關風險評鑑技術之指導。

5.4.2 風險鑑別

組織須鑑別風險緣由、影響區域、事件(包括狀況改變)與其緣由以及其可能結果(後果)。此步驟之目的為依據可能產生、增強

防止、降低、加速或延遲目標達成的事件，產生一包羅廣泛的風險清單。鑑別出不利用某一機會的相關風險有其重要性，包羅廣泛的鑑別係重要的。因未在此階段鑑別出的風險將不涵蓋在進一步的分析內。

鑑別須包括不論其緣由是否在組織控管下的風險，縱使其緣由或結果(後果)可能不顯著。風險鑑別須包括特定的結果(後果)推擠效應，包含串聯與累積效應之檢查。亦須考量廣範圍的結果(後果)，縱使風險緣由或結果(後果)可能不顯著。以及鑑別可能發生的前後環節，必須考慮到可能的緣由與顯示可能產生何種結果(後果)的情

境，所有重要的緣由與結果(後果)均須予以考量。

組織須應用適合其目標與能力及所面臨的風險之風險鑑別工具與技術。相關與更新的資訊在鑑別風險時係重要的，此須在可能時包括適當的背景資訊。須有具備適宜知識的人員參與風險鑑別。

5.4.3 風險分析

風險分析涉及對瞭解風險之發展。風險分析提供風險評估之輸入並決定風險是否需予以處理，以及決定最適宜的風險處理策略與方法。風險分析亦可提供形成決策之輸

入，該決策必須作出選擇而選項包含不同類型與等級的風險。

風險分析涉及考量風險之原因與緣由、其正面與負面結果(後果)，及該等結果確實發生的可能性。會影響結果的因素及可能性須予以鑑別。風險係藉由決定結果(後果)與其可能性，以及此風險之其他屬性分析之。一事件可具有多重結果(後果)且可影響多個目標，現有控管與其有效性及效率亦須予以考量。

結果(後果)與可能性的表達方式，與兩者綜合以決定風險等級之方式，須反映風險之類型、備妥的資訊以及風險評鑑之輸出

的使用目的，此須與風險準則一致。考量不同風險與其緣由之相互依賴性亦是重要的。

決定風險等級的可信性及其對於先決條件與假設事項的敏感性須在分析中予以考量，同時須與決策者及在適當時與其他事件相關者進行有效的溝通。各項因素諸如專家間的意見分岐、不確定性、可取用性、品質、數量及資訊之進行中的關聯性或模式化之限制等，須予以說明且可予以強調。

風險分析可依不同的詳細程度予以進行，端視此風險、分析之目的以及可取得的

資訊、資料及資源而定。分析可為定性、半定量或定量方式，或為此等之組合，視狀況而定。

結果(後果)與其可能性可透過模式化一事件或一組事件之結果，或由實驗研究或可取得數據外插以決定之。結果(後果)可以有形或無形的影響之方式表示。在某些案例中，需有一個以上的數值或解說符號來詳述不同時間、地點、群體或情況的結果(後果)與其可能性。

5.4.4 風險評估

風險評估之目的係依據風險分析之結果，協助形成有關何項風險需處理，以及處理實施的優先順序之決策。

風險評估涉及將分析過程中所發現的風險等級與考量前後環節時所建立的風險準則相比較。可依據此項比較，考慮風險處理之需求。

決策須考量風險更廣的前後環節，並包括考量由此風險受益的組織除外之團體所承受的風險裕度。須依據法令規章及其他要求作決策。

在某些狀況下，風險評估可導致進行進一步分析之決策。風險評估亦可導致除了維持現有的控管外，不對風險作任何處理之決策。此決策會受到組織面對風險的態度與已制定的風險準則之影響。

5.5 風險處理

5.5.1 一般

風險處理涉及選擇一或多個選項以供改變風險，及實施此等選項。一旦實施，則該等處理提供或修改控管。

風險處理涉及下列之循環過程。

— 評鑑某一風險處理。

－決定殘留風險程度是否可以忍受。

－若無法忍受，產生一個新的風險處理，及

－評鑑此項處理之有效性。

風險處理選項並不必要相互排除或適宜於所有狀況。選項可包括下列：

(a)決定不開始或不繼續會引起風險的活動以避免風險。

(b)承受或增加風險以尋求機會。

(c)移除風險緣由。

(d)改變可能性。

(e)改變結果(後果)。

(f) 與另一團體或多個團體分擔風險(包含合約與風險資金提供)。

(g) 藉由有資訊的決定保留風險。

5.5.2 風險處理選項之選擇

風險處理的選項關係到法令規章及其他如社會責任與天然環境之保護等要求，其最適宜的選擇涉及在實施成本和努力與所產生的利益之間取得平衡。此風險之決策亦須考量到有些風險能夠確保風險處理正當，卻在經濟的基礎上是不正確的，例如嚴重[高負面結果(後果)]但罕見(低可能性)的風險。

一些處理選項可予以考量並予以個別或合併應用。組織通常可由採納合併的處理選項而獲益。

當選擇風險處理選項時，組織須考量利害相關者的價值與感知，以及與他們溝通的最適宜方式。如風險處理選項可對組織或利害相關者其他方面的風險產生影響，此須包含於此決策中。雖效果相等，但某些風險處理可能對一些利害相關者較其餘者更能接受。

處理計畫須清楚鑑別須予以實施的個別風險處理之優先順序。

風險處理本身可引進風險。重大的風險可

能是風險處理措施失敗或無效。監測需為風險處理計畫不可或缺之一部分，以對此措施維持有效提供保證。

風險處理亦可引進需予以評鑑、處理、監測及審查的第二次風險。此第二次風險須如同原始風險納入相同的處理計畫，而不以新風險處理。此二風險間之聯結須予以鑑別與維持。

5.5.3 準備與實施風險處理計畫

風險處理計畫的目的係文件化所選定的處理選項將如何實施。提供於處理計畫內的資訊須包括：

— 處理選項選擇的理由，包括預期之獲益
— 認可此計畫的負責人員與負責實施此計畫的人員。
— 建議的行動。
— 所需的資源，包括偶發事件。
— 績效量測與限制。
— 報告與監測之要求事項，及
— 時間安排與時程。

處理計畫須與組織的管理過程整合，並與適宜的利害相關者討論。

決策者與其他利害相關者須注意風險處理

後的剩餘風險之本質與程度。剩餘風險須予以文件化，且施行監測、審查及在適宜時進一步處理。

5.6 監測與審查

監測與審查須同時規劃為風險管理過程之一部分，並納入正常查核或監視。可為定期性或視需要個案處理。

監測與審查的責任須予以清楚界定。

為下列目的，組織的監測與審查過程須涵括風險管理過程之所有考量面。

—確保設計與運作的控管係有效果且有效率的。

－取得進一步資訊以改進風險評鑑。

－由事件(包括虛驚事故)、變化、趨勢、成功及失敗分析並學取教訓。

－偵測外部與內部前後環節之變化，包括風險準則與風險本身的變化，其可能需要修訂風險處理與優先順序，及

－鑑別浮現中的風險。

實施風險處理計畫的進度提供績效檢測。結果可納入組織的整體績效管理、檢測及外部與內部報告活動中。

監測與審查的結果須予以記錄並在適宜時對內與對外報告，且亦須使用為審查風險

管理架構的一項輸入(參照4.5)。

5.7 記錄風險管理過程

風險管理活動須係可追溯者。在風險管理過程中，紀錄提供方法與工具改進的基礎，如其於整體過程中者。

有關紀錄的製作之決定須考量下列事項

- 組織持續學習的需求，
- 為管理目的可再使用的資訊之利益。
- 製作與維護紀錄所涉之成本與辛勞。
- 法令、規章及作業對紀錄的需求。
- 媒體之進入方法、恢復之容易性及貯存

— 保存期間，及

— 資訊之敏感性。

附錄A
（參考）
強化的風險管理之屬性

A.1 一般

所有組織皆須著眼於其風險管理架構適宜的績效水準，而此架構係與所形成決策的關鍵點一致。下列之屬性代表管理風險的高水準之績效，為協助組織依據這些準則量測其本身的績效，對每一屬性提出一些

有形的指標。

A.2　重要成果

A.2.1 組織對其風險具備最新、正確及全面性的瞭解。

A.2.2 組織的風險在其風險準則範圍內。

A.3 屬性

A.3.1　持續改進

重點置於透過組織績效目標的設定、量測、 審查及隨後對過程、系統、資源、能力及技能的修改，持續改進風險管理。

此可由據以量測組織與管理者個人績效之

清楚的績效目標之存在予以顯示。組織的績效可被發布與溝通。通常至少每年審查績效，然後修訂過程，並設定次一階段修訂的績效目標。

此風險管理績效評鑑係整體組織的績效評鑑，以及部門與個人量測系統中不可或缺之部分。

A.3.2 風險之完全當責

強化的風險管理包含全面性、完全界定以及對風險、控管及風險處理任務之當責完全接受。受指派的個人完全接受當責，係適宜地具備技能，並具有適切的資源以查核控管、監測風險、改進控管，及有效

對外部與內部利害相關者溝通有關風險及其管理。

此可由組織的所有人員完全瞭解他們所當責的風險、控管及工作顯示出。通常，此將記錄於職位/職務說明書、資料庫或資訊系統。風險管理角色、當責及職責之界定須為組織所有的職前訓練方案之一部分。

組織藉由提供足以承擔其責任的職權、時間、訓練、資源及技巧，保證當責者準備妥當以完成他們的任務。

A.3.3應用風險管理於所有決策

組織內所有的決策形成，不論其重要與顯著之程度為何，皆涉及明確的風險考量，且涉及應用風險管理至某種適宜的程度。

此可透過會議與決策之紀錄顯示對風險已進行清晰的討論。此外，須可見出風險管理之所有組成均呈現在組織決策形成的重要過程中，例如有關資金分配、有關主要的專案以及有關重組結構與組織的改變之決策。因此等理由，組織內可見到健全的風險管理，它提供有效的治理之基礎。

A.3.4 持續溝通

強化的風險管理包括與外部及內部利害相關者持續溝通，包括全面性與經常的提告風險管理績效，作為良好治理之部分。

此可透過與利害相關者溝通作為風險管理不可或缺與重要的要項予以顯現。溝通確實被瞭解為一雙向過程，這使有關風險等級與風險處理之需要性，可依據適當制定且周全的風險準則作正確獲得資訊決策。

全面性與經常對外與對內報告有關重要的風險與風險管理績效，實質地促成組織內有效的治理。

A.3.5 完全整合於組織的治理架構

風險管理被視為組織各項管理過程之中心，使得風險係以目標的不確定性影響之觀點予以考量。治理架構與過程係以風險之管理為基礎。有效的風險管理被管理者視為達成組織目標之要項。

此可透過管理者在組織內的語言與重要的書面資料中使用〝不確定性〞與風險相結合予以顯現。此屬性通常亦反映於組織的政策說明中，特別是與風險管理有關者。通常此屬性將透過與管理者面談及透過其行動與陳述之證據予以查證。

參考資料

[1] CNS 14889風險管理－詞彙

[2] CNS 31010風險管理－風險評鑑技術

相對應國際標準

ISO 31000:2009, Risk management – Principles and guidelines