附件 8　資通系統風險評鑑參考指引導引手冊(Quick Guide)

1. 目的

資訊系統風險評鑑參考指引於民國 103 年修訂，配合資通安全管理法及相關子法公布與國際風險管理標準修正，修訂本指引之風險評鑑作法與後續因應作為。

本指引旨在因應資訊系統分類分級與鑑別機制參考手冊已經被資通安全管理法之「資通安全責任等級分級辦法」取代，以協助政府機關內部資安管理相關人員，了解風險評鑑的過程與所採用之技術，用以評鑑機關內資通系統所面臨潛在之風險，以利於採取適當的安全防護控制措施，降低機關資安風險。

各機關應考量施政目標，進行資安風險評估，確定各項資訊作業安全需求水準，採行適當及充足之資安措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全。

本指引係屬建議性質，各機關可參考本指引，針對資通系統與所屬資產進行風險評鑑，但不以此為限，以符合國家/國際資安管理標準之要求。

2. 適用對象

本指引適用於政府機關運用資訊科技從事業務維運之所有人員，為便於閱讀與使用，特將適用對象區分為「一般主管」、「資訊人員」、「資安人員」及「一般使用者」，並針對不同對象建議閱讀之重點。

3. 風險管理架構

3.1.風險的定義

風險的定義，參考 ISO 31000:20018 係指：對於組織目標之不確定影響(effect of uncertainty on objectives)。所謂影響：係指對於預期結果的誤差，包括正向與負向的結果。

所稱組織：適用於各種類型與大小之公務與非公務機關。

組織目標可以包含不同之面向，例如：財務、健康、安全與環保目標等，並且可以應用於不同之階層，上至組織策略、專案工作，下至產品發展與過程，或是資訊安全等均是，風險通常會參考潛在之事件及其可能造成之後果加以描繪與表示，包含事故發生的改變程度與發生的可能性等。

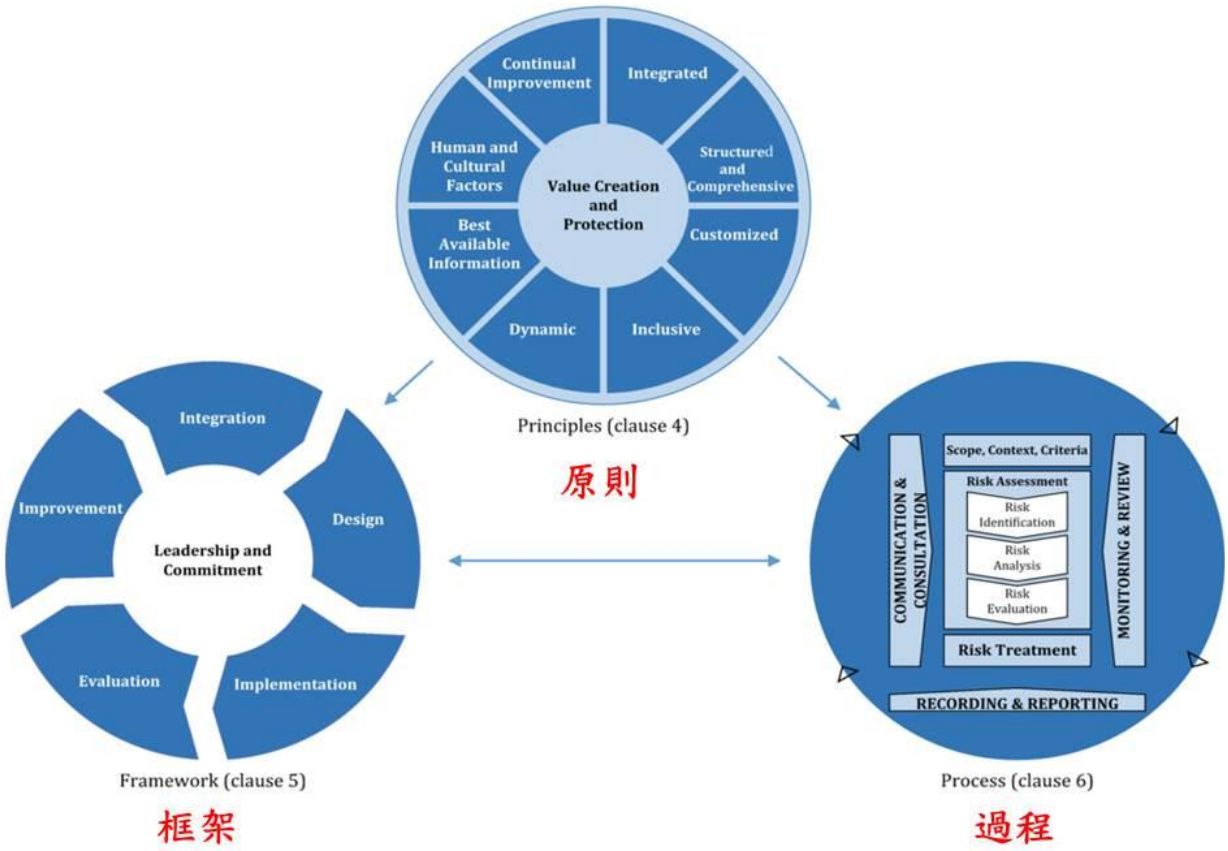
換言之：風險意指任何類型與大小的組織，為達成組織的目標，所面對內部及外部因素影響的不確定性，包含事故發生的改變程度與發生的可能性等。

3.2.風險管理之原則、框架與過程之關係

風險管理指的是：協同所有之活動以指導並控制組織所關注之風險。

機關所有的活動均涵蓋在風險管理的範圍之內，需對風險進行識別與分析，並評估風險處理方法的影響，滿足機關之風險條件，以達成機關之目標。

以下內容參考 ISO 31000:20018，摘述有關風險管理之原則、框架與過程，詳見圖 1 所示。



資料來源：ISO 31000

圖1　風險管理之原則、框架與過程之關係

3.3.風險管理之框架

風險管理框架的目的是協助將風險管理納入所有活動與功能。風險管理的有效性取決於整合到治理和組織的所有其他活動中，如組織在做決策時即應將風險管理納入考量，詳見圖 2 所示。其內容包含：

●領導與承諾

– 將風險管理與組織的策略、目標及文化相結合。

– 建立風險管理的方法、計劃或行動方案的聲明或政策。

– 為管理風險提供必要的資源。

– 確定可能或不可能採取的風險類型（風險偏好）。

●整合

– 確定管理當責、監管角色及職責。

– 確保風險管理是組織所有功能的一部分，而不是與其分開。

●設計

– 了解組織及其內、外部背景。

– 清楚說明風險管理承諾並分配適當資源。

– 建立溝通與諮詢。

●建置

– 制定適當的實施計劃，包括最後期限。

– 定義由誰於何時、何處以及如何進行不同類型的決策。

– 在必要時修改適用的決策流程。

●評估

– 根據目的、建置及執行情形來衡量框架績效。

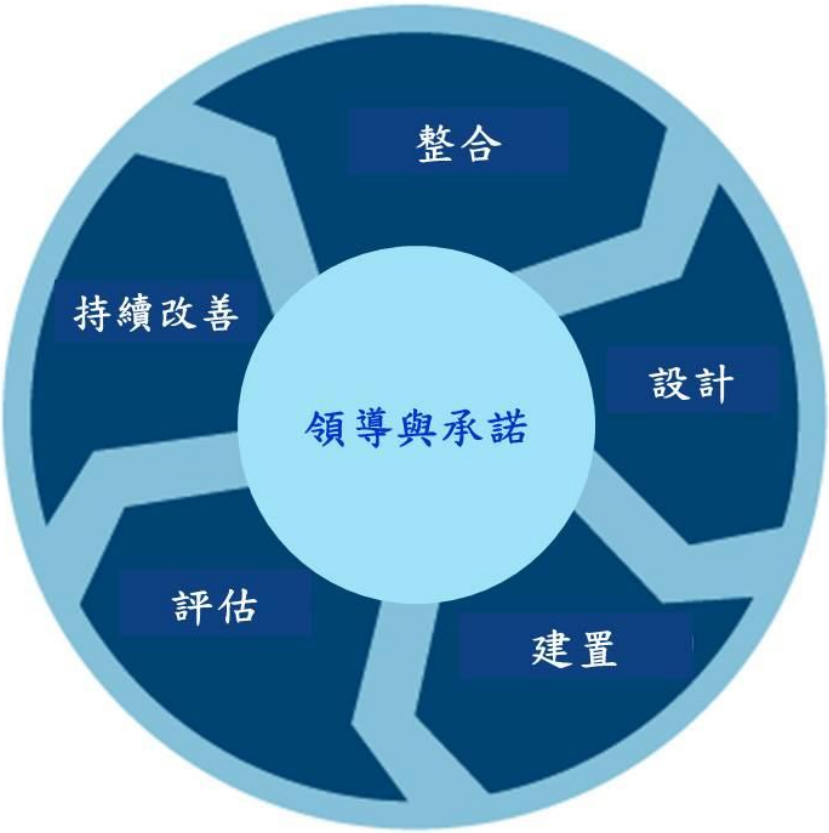
– 確定風險管理框架是否仍適用於實現組織目標。

●持續改善

– 不斷監測與調整框架以解決外部和內部變化。

– 採取措施以提高風險管理的價值。

– 提高風險管理框架的適用性、充分性及有效性。



資料來源：ISO 31000

圖2　風險管理之框架

3.4.風險管理之過程

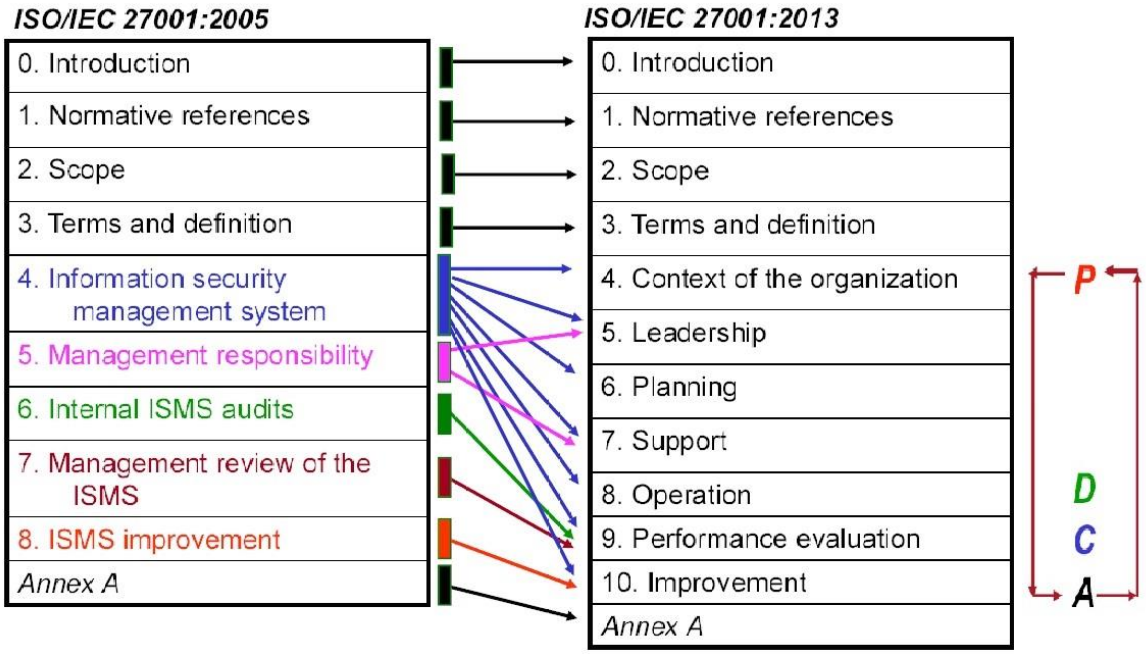
風險管理過程以系統式的將政策、程序及實踐應用於溝通與諮詢、建立全景、風險評估、風險處理、風險監測與審查、風險記錄與報告等風險活動中，其過程詳見圖 3 所示。

資料來源：ISO 31000

圖3　風險管理之過程

4. CNS/ISO/IEC 27001 對於風險管理之要求

ISO/IEC 27001 目前版本為 2013/10/1 日公布，CNS 27001 為 2014 年 4 月 24 日修訂公布，其架構區分，詳見圖 4 所示。



資料來源：本計畫整理

圖4　ISO/IEC 27001 內容架構

ISO/IEC 27001:2013 特別強調風險評鑑與處理之過程(Process)，應符合 ISO 31000 風險管理—原則與指引之建議(摘列原文內容如下：The information security risk assessment and treatment process in this International Standard aligns with the principles and generic guidelines provided in ISO 31000)。

5. 風險評鑑技術與方法

CNS 31010:2009 提供系統化的風險評鑑方法選擇及應用的指引文件，摘列適用於各個層級的風險評鑑方法，當然也包含有資訊安全所適用之風險評鑑方法，詳見表 1 所示。

以下所列風險評鑑方法，依據風險評鑑之過程，區分為風險識別、風險分析(含衝擊後果、發生可能性、風險等級)及風險評估等階段，標示所列風險評鑑方法之適用性。

表1　風險評鑑方法

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
腦力激盪	極適用	不適用	不適用	不適用	不適用	
結構或非結構化面談	極適用	不適用	不適用	不適用	不適用	
德爾菲(Delphi)	極適用	不適用	不適用	不適用	不適用	
查檢表	極適用	不適用	不適用	不適用	不適用	
初期危害分析(PHA)	極適用	不適用	不適用	不適用	不適用	
危害與可操作性研究（HAZOP）	極適用	極適用	適用	適用	適用	
危害分析與關鍵管制點（HACCP）	極適用	極適用	不適用	不適用	極適用	
環境風險評鑑	極適用	極適用	極適用	極適用	極適用	
結構化之”如果這樣會怎樣”(SWIFT)	極適用	極適用	極適用	極適用	極適用	
情境分析	極適用	極適用	適用	適用	適用	

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
企業衝擊分析(BIA)	適用	極適用	適用	適用	適用	●
根本原因分析(RCA)	不適用	極適用	極適用	極適用	極適用	
失效模式與效應分析(FMEA)	極適用	極適用	極適用	極適用	極適用	
失效(故障)樹分析(FTA)	適用	不適用	極適用	適用	適用	
事件樹分析（ETA）	適用	極適用	適用	適用	不適用	
因果分析	適用	極適用	極適用	適用	適用	
原因與效應分析	極適用	極適用	不適用	不適用	不適用	
保護層分析(LOPA)	適用	極適用	適用	適用	不適用	
決策樹	不適用	極適用	極適用	適用	適用	
人因可靠度分析	極適用	極適用	極適用	極適用	適用	
蝴蝶結分析	不適用	適用	極適用	極適用	適用	
可靠度中心維修(RCM)	極適用	極適用	極適用	極適用	極適用	
潛行路徑分析(SCA)	適用	不適用	不適用	不適用	不適用	

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
馬可夫(Markov)分析	適用	極適用	不適用	不適用	不適用	
蒙地卡羅模擬	不適用	不適用	不適用	不適用	極適用	
貝氏統計法(Bayesian statistics)與貝氏網路(Bayes Nets)	不適用	不適用	不適用	不適用	極適用	
FN 曲線	適用	極適用	極適用	適用	極適用	
風險指數	適用	極適用	極適用	適用	極適用	
後果/機率矩陣	極適用	極適用	極適用	極適用	適用	●
成本/效益分析(CBA)	適用	極適用	適用	適用	適用	
多準則決策分析(MDCA)	適用	極適用	適用	極適用	適用	
註記	CNS/ISO/IEC 27005:2011 建議之資訊安全風險評鑑風法： 高階風險評鑑法=企業衝擊分析 詳細風險評鑑法=後果/機率矩陣					

資料來源：CNS 31010 附錄 A

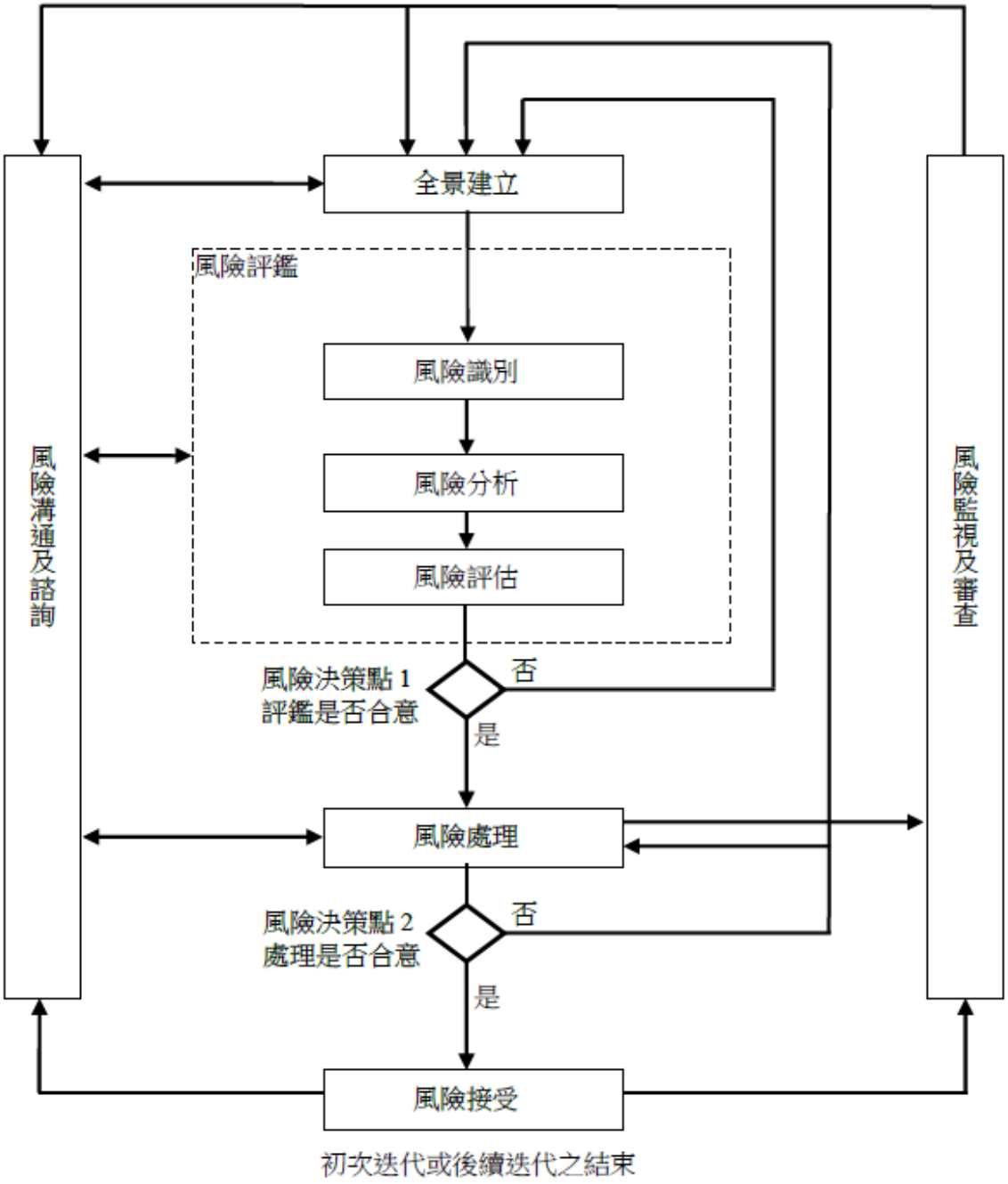
6. CNS/ISO/IEC 27005 資訊系統風險評鑑

ISO/IEC 27005:2011 主要因應：ISO Guide 73:2009 及 ISO/IEC 27000:2009 對於名詞定義的修訂，與 2008 年版本在內容上並無重大差異，相關修訂內容詳見上述標準附錄 G。

本標準提供組織內之資訊安全風險管理的指導綱要，並支援 CNS/ISO/IEC 27001:2013 資訊安全管理系統(Information Security Management System, ISMS)之的特定要求。

本標準並不提供任何資訊安全風險管理之特定方法論。組織可自行依據例如資訊安全管理系統(ISMS)之範圍、風險管理之全景或產業別等，定義其風險管理作法。有數種現存方法論，能在本標準描述之框架下，以實作資訊安全管理系統(ISMS)之要求。

風險管理過程的高階觀點，遵循 ISO 31000 之規定，資訊安全風險管理過程之風險評鑑及/或風險處理活動，以循環作法(亦稱為迭代式)進行風險評鑑能在每一循環中增加評鑑之深度與詳細度。循環作法提供在最小化花費於識別控制措施之時間與耗費間之良好平衡時，以確保高風險被適當評鑑。詳見圖 5 所示。



資料來源：CNS 27005

圖5　資訊安全風險管理過程

首先建立全景，然後進行風險評鑑。若能提供充分資訊以有效地修正風險至可接受等級所需之措施，則評鑑工作完成，隨後並展開風險處理。若資訊不

充分，則需進行再一次的修訂全景（例如：風險評估準則、風險接受準則或衝擊準則）之風險評鑑循環，此循環可能僅及於整體範圍之有限部分(參照圖 5，風險決策點 1)。

風險處理之有效性依風險評鑑之結果而定，可能無法立即將剩餘風險降至可接受等級，若有需要，可變更全景參數（例如：風險評鑑、風險接受或衝擊準則）後進行另一次風險評鑑循環，再執行更進一步之風險處理(參照圖 5，風險決策點 2）

換言之：CNS/ISO/IEC 27005 所描述之資訊安全風險管理過程，係遵照 ISO 31000 之規定，並與行政院風險管理與危機處理作業手冊中所陳述之管理架構一致，均是符合國際風險管理規範之要求。

CNS/ISO/IEC 27005：2011 附錄 E 建議之 2 項資訊安全風險評鑑作法，摘述如後：

6.1.1. 高階風險評鑑作法

「資通安全責任等級分級辦法」所描述之「安全等級設定原則」，其所採用技術類似 ISO 31010 之企業衝擊分析，評鑑對於機關之衝擊程度，並未考量其發生之可能性(亦可視為衝擊發生是必然的)，以評定資通系統之安全等級，亦是 CNS/ISO/IEC 27005:2011 高階風險評鑑的實務作法之一。

高階風險評鑑作業之優點如下：

●一開始採用較簡單之作法，容易獲得風險評鑑參與人員之接受。

●可做為良好之輔助規劃，以建構機關資訊安全之策略藍圖。

●可將資源及預算運用於最有利之處。

惟由於初始採用高階風險評鑑，潛在地存在評鑑結果較不精確，可能未識別某些營運過程或系統，可視需要針對高安全等級之資產，進行詳細風險評鑑作業。

6.1.2. 詳細風險評鑑作法

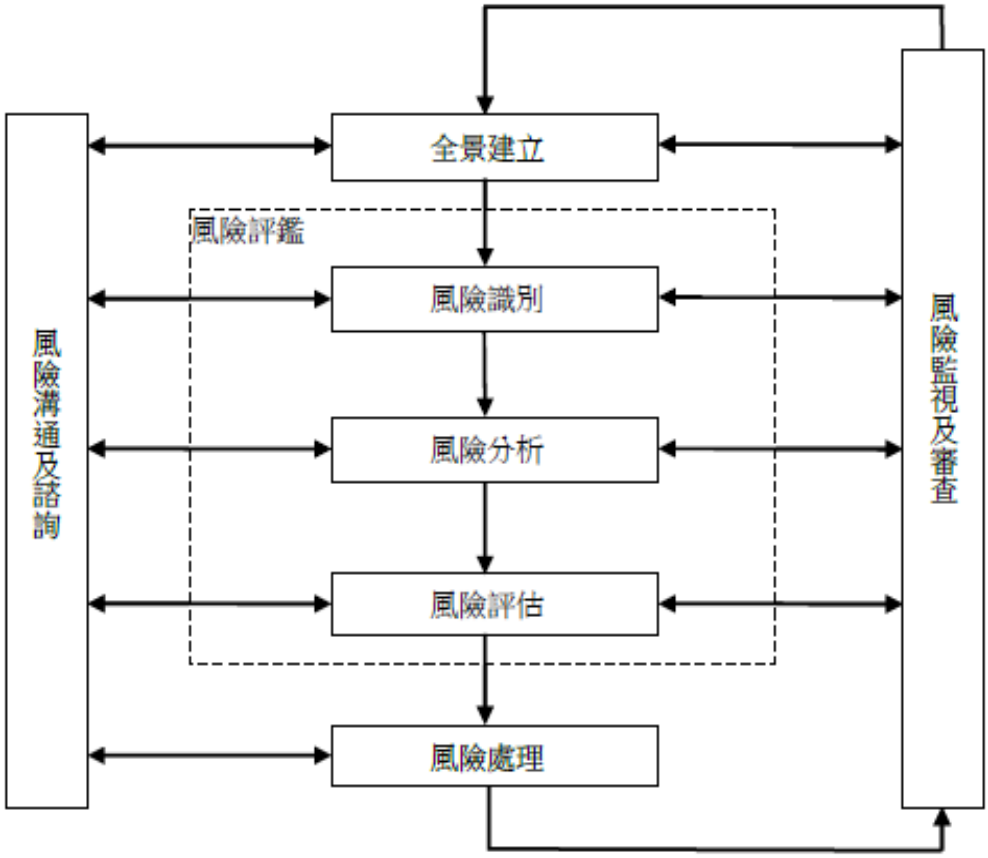
詳細風險評鑑對於資產進行深度之識別與鑑別作業，並針對資產詳細列出其可能面臨之威脅與可能存在之脆弱性，以做為評鑑其風險與風險處理方法之依據。詳細之步驟需考慮時間、耗費程度及專家意見等。

詳細風險評鑑作法可以是定量或是定性的方法，或是二者之結合。宜根據資產之價值，或需被保護之特性，以評鑑威脅發生之可能性。

CNS/ISO/IEC 27005 於附錄 E 中，列舉了符合 ISO 31010 所示之後果/機率矩陣(Consequence/probability matrix)法之實務範例，但不以此為限。

7. 資通系統風險管理過程

本指引主要在協助政府機關內部資訊安全管理人員瞭解風險評鑑的技術，用以評鑑機關內資通系統的風險，以利於採取適當的安全防護控制措施，降低機關資安風險。整體資通系統風險管理過程，包含「風險溝通及諮詢」、「建立全景」、「風險評鑑」、「風險處理」及「風險監視與審查」等 5 階段管理過程，詳見圖 6 所示。



資料來源：本計畫整理

圖6　資通系統風險管理過程

7.1.風險溝通與諮詢階段

在風險管理初期階段，便應發展溝通與諮詢方法，以利風險管理過程中的各階段，向機關外部與內部之利害關係人溝通與諮詢。

風險溝通是決策者與其他利害關係人藉由交換或分享風險資訊，於如何管理風險上達成協議的活動，其所獲得之資訊包含(但不限於)風險之存在、本質、形式、發生可能性、衝擊嚴重程度、處理之方法與風險可接受之程度等。

機關應納編各部門的成員及各領域之專家，組成完整之溝通與諮詢團隊，並提供以下的協助：

●協助建立適當的全景。

●確認利害關係人所關切之議題已經被瞭解並納入考量。

●協助確認風險已經被充分的識別。

●協同不同領域的專家進行風險分析。

●協助從不同的觀點定義風險條件與評估。

●提供保證並支持處理計畫。

●於風險管理過程中，強化適當的變更管理。

●發展適當的外部與內部溝通與諮詢的計畫。

為了讓負責實施風險管理的人員瞭解決策的基礎，以及為何需要執行特定的風險管理活動，雙向溝通是十分重要的。在溝通風險議題時，由於風險管理相關人員與決策者對於假設、觀念、需求及關切議題等的差異，對風險的認知可能不同，因而對風險的可接受性判斷也會有所差異，所以，如何確保風險管理相關人員對風險的認知是特別重要的。

機關應發展正常運作與緊急情況下之風險溝通與諮詢計畫，成立作業小組並與機關內之公關部門或是發言人合作，以協調有關於風險溝通之事務。

執行風險溝通與諮詢，乃期望達到下列目的：

●提供組織風險管理結果提供保證。

●收集風險資訊。

●分享風險評鑑的結果，並提出風險處理計畫。

- 避免或降低因決策者與利害關係人間因缺乏互相瞭解，而導致資訊安全漏洞之發生與後果。
- 支援決策者作決策。
- 取得新的資訊安全知識。
- 與其他機關協調並規劃應變機制，以降低任何事故所造成之後果。
- 賦予決策者及利害關係人對於風險之責任感。
- 強化對於風險之認知。

7.2.建立全景階段

各機關應依有關法令，考量施政目標，進行資訊安全風險評鑑，確定各項資訊作業安全需求水準，採行適當及充足之資訊安全措施，確保各機關資訊蒐集、處理、傳送、儲存及流通之安全。

因此，政府機關應該在其機關資安政策中，明確聲明對該機關施政業務相關資通系統，應執行風險評鑑，並界定出風險評鑑範圍、角色及責任等。

在進行風險評鑑與實作資訊安全各項防護控制措施之前，政府機關應該先行識別該機關內、外各方面的安全需求，包括資訊安全政策以及法令、法規、規章及合約，同時規劃與定義「風險評估準則」、「衝擊準則」及「風險接受準則」等風險管理基本準則。

7.3.風險評鑑階段

本階段主要針對機關在風險評鑑「建立全景階段」所定義的範疇，根據「風險評鑑程序階段」所選擇的風險評鑑迭代作法，進行相對之風險評鑑作法程序的實作，茲根據(A)高階風險評鑑作法、(B)詳細風險評鑑作法等2種風險評鑑作法，以「全球資訊網」做為風險評鑑範例，說明本階段的

執行內容，詳見下列章節之說明。

7.3.1. 高階風險評鑑作法

政府機關自行或委外開發之資通系統「高階風險評鑑作法」，應依據資通安全責任等級分級辦法之規定，做為高階風險評鑑方法，分別就機密性、完整性、可用性、法律遵循性等構面評估資通系統防護需求分級，直接以該規定之分級結果，做為該資通系統的風險評鑑等級，茲以「全球資訊網資訊系統」為例，說明「高階風險評鑑作法」的評鑑過程與結果，詳見圖 7 所示。

- 機密性：屬公開之一般資料。
- 完整性：主要提供資訊公告。
- 可用性： 系統中斷不影響核心業務。
- 法律遵循性：需符合智慧財產權相關法律、兒童及少年福利法、個資法。
- 綜整以上所述評定之結果，機關之「全球資訊網」其安全等級(風險等級)屬「普」級。

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2.完整性	初估	普	本網站主要提供資訊公告
	異動		
3.可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4.法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

資料來源：本計畫整理

圖7　全球資訊網安全等級評估參考範例

7.3.2. 詳細風險評鑑作法

詳細風險評鑑作法乃藉由系統化的方式，找出該資通系統中應該優先處理的資訊及資通系統資產所對應的風險，而施予適切的防護安控措施，以維持組織持續運作無虞。機關應參考 3.2.1 章節中所訂定的「風險評估準則」與「衝擊準則」執行風險分析，得到所有資訊及資通系統資產的風險值；接著執行風險評估，以訂定風險等級，再依據「風險接受準則」，決定「風險可接受等級」，詳見圖 8 所示。

得到需要執行風險處理的資訊及資通系統資產清單之後，接續執行「風險處理」，並確保執行完成「風險處理」之後的風險值是落在「風險可接受

等級」，即進入「風險監視與審查階段」。

茲以「全球資訊網資訊系統」為例，說明詳細風險評鑑的作法，細部活動程序包含「資產識別」、「威脅與脆弱性識別」、「現有控制措施識別」、「後果識別」、「後果鑑別(含資訊及資通系統資產價值鑑別)」、「評鑑事故可能性」、「估計風險等級」、「訂定風險等級」及「決定風險可接受等級」等 9 項作業步驟。

惟實際作業時，「後果識別」與「後果評鑑(含資訊及資通系統資產價值評鑑)」通常同時進行，故將此兩項作業活動結合成一個步驟，後續就 8 個步驟分別說明「全球資訊網資訊系統」詳細風險評鑑的執行範例。

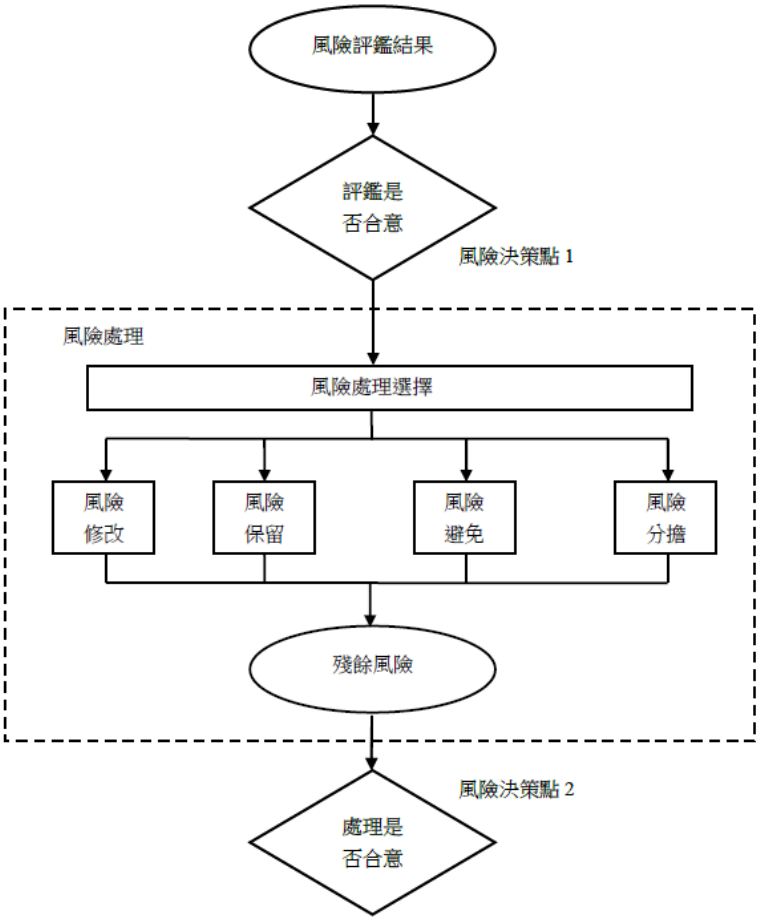
資料來源：CNS/ISO/IEC 27005:2011

圖8　詳細風險評鑑細部活動程序圖

7.4.風險處理階段

風險處理活動應依據風險評鑑之結果及實作風險處理方案之預期成本及預期利益等，以選擇適當之行動方案，一般而言，宜使風險之不利後果，合理的降低。

風險處理活動之選項主要有 4 種，包含風險修改(風險降低)、風險保留(風險接受)、風險避免及風險分擔，詳見圖 9 所示。



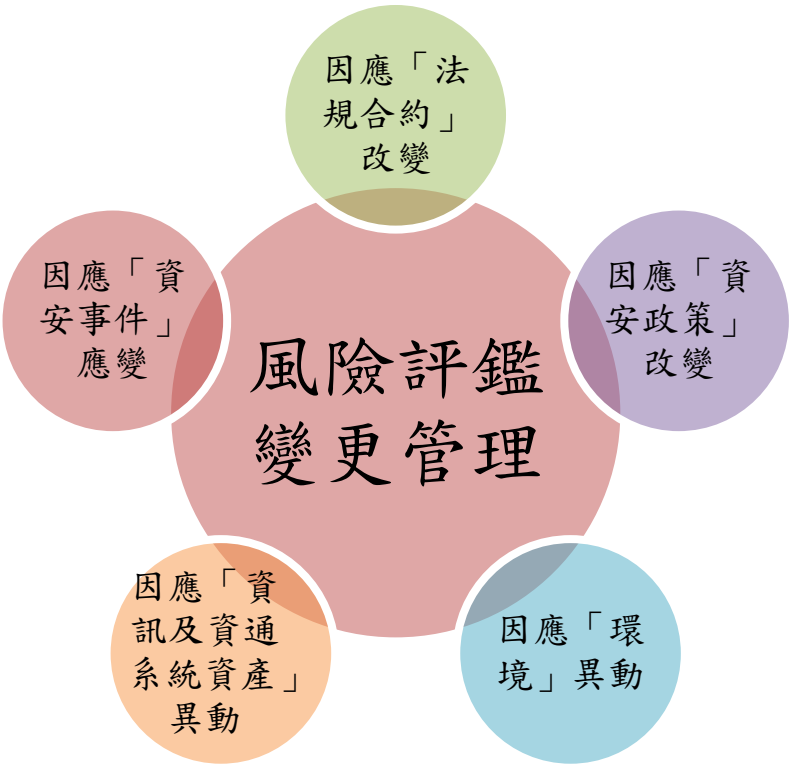
資料來源：CNS 27005

圖9　風險處理活動

7.5.風險監視與審查階段

7.5.1. 風險因素之監視與審查

機關針對所擁有資通系統之風險評鑑報告，應定期審查或因應環境與資通系統發生變更時能及時檢視與更新，以確保風險評鑑報告成為「動態文件」。風險評鑑報告之變更管理是當資通系統發生異動或者當其操作的實體或者網路環境被改變時，用來協助識別該資通系統是否需要新安全需求的過程。這些異動與改變應至少包含「因應法規合約改變」、「因應資安政策改變」、「因應環境異動」、「因應資訊及資通系統資產異動」、「因應資安檢查結果」及「因應資安事件應變」，詳見圖 10 所示。



資料來源：本計畫整理

圖10 風險評鑑審查與變更管理時機圖